Trellix Intrusion Prevention System 11.1.x Product Guide

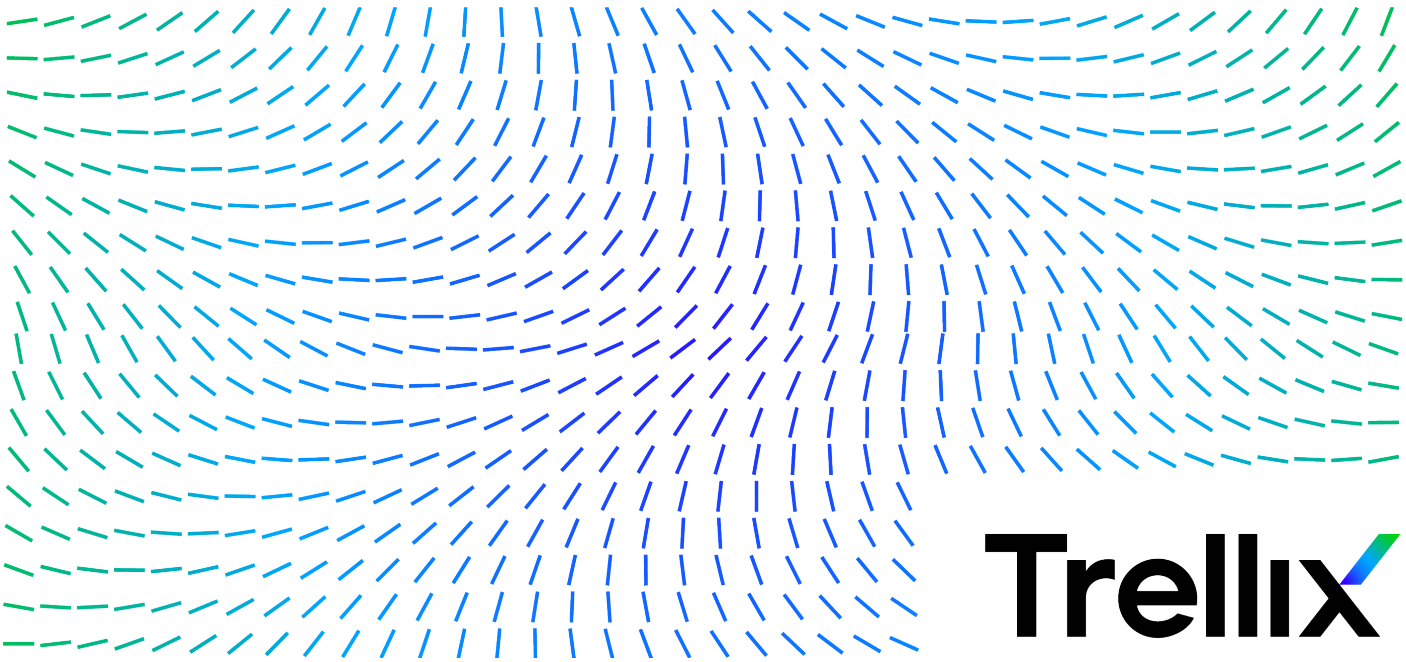
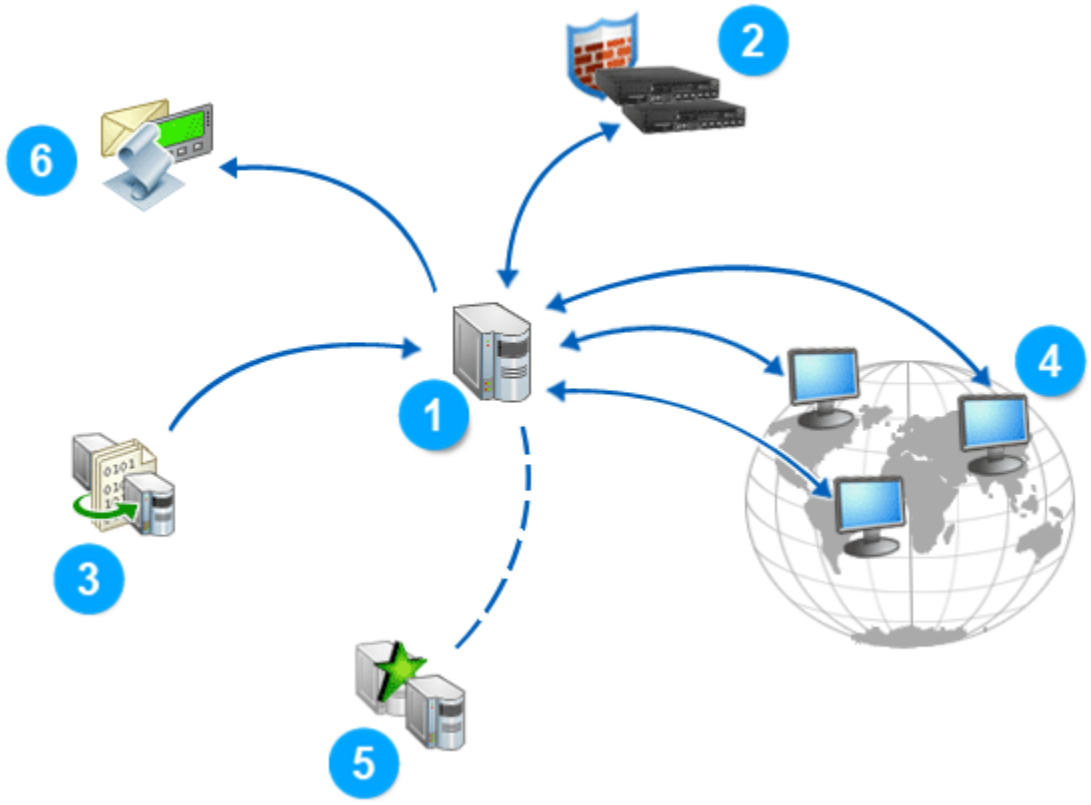


Table of Contents

Quick Tour

Trellix Intrusion Prevention System Overview

Trellix Intrusion Prevention System is a combination of network appliances and software that accurately detects and prevents intrusions, denial of service (DoS) and distributed denial of service (DDoS) attacks, and network misuse. Trellix Intrusion Prevention System combines real-time intrusion detection and prevention for the most comprehensive and effective network security system.



The following table describes the figure in detail.

Item	Description
1	Trellix Intrusion Prevention System Manager
2	Trellix Intrusion Prevention System Sensor
3	Trellix IPS Update Server
4	Web clients accessing the Manager server
5	Manager Disaster Recovery (MDR) server
6	Alert notification - email, pager, and script generation

Ten Steps to using Trellix Intrusion Prevention System

Step 1	**Install the Manager software**. Install the Trellix Intrusion Prevention System Manager software on the server machine and ensure that you are able to log onto the Manager. For details, see [Trellix Intrusion Prevention System Manager Installation Guide].
Step 2	**Set up and configure the Sensor(s)**. Cable and install your Trellix Intrusion Prevention System Sensor(s) using a command line interface (CLI) and the Trellix IPS Manager. For details, see [Trellix Intrusion Prevention System Manager Installation Guide].
Step 3	**Establish trust between the Manager and the Sensor(s)**. The Trellix IPS Sensor initiates all communication with the Manager server until secure communication is established between them. Later, configuration information is pushed from the IPS Manager to the IPS Sensor. • Verify on the appliance CLI that the Sensor has established communication with the Manager. • Verify in the Manager GUI that a node representing the Sensor appears in the Resource Tree under the Device List. For details, see [Trellix Intrusion Prevention System Manager Installation Guide].

Step 4	**Configure policies in the Manager**. Determine the IPS policies applicable to your network. Use the Manager GUI to set up policies. By default, the provided Default policy is applied to all of your Sensor ports. You can choose a specific policy to apply by default to the Root Admin Domain (and thus all monitoring interfaces on the Sensor). For details, see Trellix IPS policies (page 773).
Step 5	**Configure the Update Server and download the latest signature sets**. For your Trellix IPS to properly detect and protect against malicious activity, the Manager and the Sensors must be frequently updated with the latest signatures and software patches available, which is made available to you via the Update Server. Authenticate your credentials with the Update server and download the latest signature set for your Trellix IPS deployment. For details, see Trellix IPS Protection Status (page 64).
Step 6	**View alerts**. The **Attack Log** page displays detected security events that violate your configured security policies. The page also provides powerful drill-down capabilities to enable you to see details on a particular alert like its type, source and destination addresses, and packet logs where applicable. View the alerts periodically and perform forensic analysis on the alert to help you tune Trellix IPS, and provide better responses to attacks. For details, see Attack Log (page 374).
Step 7	**Tune your Trellix IPS deployment**. Once you have configured and started using Trellix IPS, you can further enhance your deployment using the Manager GUI by utilizing some of the more advanced features, such as changing your deployment mode, creating multiple admin domains, defining specific user roles, applying multiple policies to multiple domains, etc. For details, see *Getting familiar with Trellix IPS Manager* (page 42).
Step 8	**Check the system faults status**. The system faults monitor in the Manager details the functional status for all of your installed Trellix IPS system components. Check the faults at regular intervals to view messages that detail system faults experienced by your Manager, appliances, or database. For details, see Monitoring System Faults (page 337).
Step 9	**Block malicious or unwanted traffic**. Analyze the attacks that your network is receiving on a regular basis and take actions, which can range from analyzing the impact and modifying policies, or blocking specific traffic from transmitting through your system. For details, see Trellix IPS policies (page 773).

Step 10	**Generate Reports**. The Report Generator enables a user to generate reports for the security events detected by the system and reports on system configuration. Configure your report settings to generate reports manually or automatically, save them for viewing later, and/or email to specific individuals. For details, see Report Generation (page 239).

Basics of Using Trellix Intrusion Prevention System

This section provides a high-level overview of how to use Trellix IPS.

The process of setting up and running Trellix IPS falls into some basic stages as given below:

Steps:

1. Deciding where to deploy Sensors and in what operating mode
2. Setting up your Sensors
3. Establishing Sensor-to-Manager communication
4. Configuring your deployment using the Manager
5. Updating your signatures and software
6. Viewing and working with data generated by Trellix IPS
7. Tuning your deployment

   Each of these stages consists of a number of tasks; some are simple, some are complex. You will generally perform steps 1 through 3 only once per Sensor.

Setting up your Sensors

The process of setting up a Sensor is described below at a high level.

Steps:

1. Position the Sensor.
   - Unpack the Sensor and place on a sturdy, level counter top.
   - Attach the provided rack mounting ears to the Sensor.
   - Install the Sensor in a rack. Sensors are either 1 or 2 RU, depending on model.

     For detailed instructions on these tasks, see your Sensor model's [Trellix Intrusion Prevention System Product Guide].
2. Install any additional hardware.
   - Install SFP, SFP+, QSFP+, or QSFP28 transceivers (not included) in the Sensor's GE ports.

> **NOTE**
>
> Use only SFP, SFP+, QSFP+, or QSFP28 transceivers purchased either from Trellix or from an approved vendor. For a list of approved vendors, please see our website.

- (Optional) If you have purchased a redundant power supply for your Sensor, install the power supply. Sensors that support a redundant power supply ship with only one power supply; the other must be purchased separately from Trellix. Other Sensor models have an internal power supply.

3. Cable the Sensor for configuration.
   - First, connect the sensor MGMT(management) port to your network for proper communication with the Manager. Then connect the RS232 DB9 Sensor port to a PC(with a provided DB9 cable) or to a Terminal server and configure its IP. Once a trusted communication is established between the Sensor and Manager, the Manager can be utilized for necessary Sensor configurations.

     For detailed information on how to configure the Sensor IP address and establish trust, refer to section [Configure the Sensor] in [Trellix Intrusion Prevention System Installation Guide].

Establishing Sensor-to-Manager communication

The process of setting up a Sensor is described below at a high level.

Steps:

1. Set up the Manager software on the server machine.
   - Install the Manager software on the server machine. This process is described in detail in the [Trellix Intrusion Prevention System Installation Guide.]
   - Start the Manager as described in the [Trellix Intrusion Prevention System Installation Guide]. You can establish communication with a Sensor from the Manager server or from a remote client machine connected to the Manager server via any web browser.
   - You can choose a specific policy to apply by default to the root admin domain (and thus to all monitoring interfaces on the Sensor).

   Whatever policy you have specified will apply until you make specific changes; this policy gets you up and running quickly. Most users tune their policies over time to best suit their environments and reduce the number of irrelevant alerts.

   > **NOTE**
   >
   > By default, the **Default Prevention** policy is applied to all of your Sensor ports. Note that this policy's behavior is to automatically block certain attacks upon detection. For more information on other provided policies, see [Trellix IPS policies] in the [IPS Administration] section.

   Open the **Sensors** tab in **Device Manager** page and add a Sensor, providing the Sensor with a name and a shared secret key value. For instructions on how to open the **Sensors** tab in **Device Manager** page, see the [IPS Administration] section. For instructions on how to add a Sensor to the Manager, see [Trellix Intrusion Prevention System Installation Guide].

2. Configure the Sensor.

   From a console connected physically or logically to the Sensor, configure the Sensor with network identification information (that is, an IP address, the IP address of the Manager server, and so on), and configure it with the same name and shared secret key value you provided in the Manager. For more information on Configuring the Sensor using the Sensor CLI, see the [CLI commands] section.

3. Verify communication between the Sensor and the Manager.

   There are three ways to check that the Sensor is configured and available:

- In the Manager **Dashboard**, check the **System Faults**. (See if the Sensor is active. If the link is yellow, click on the cell to see the System Faults on the Sensor. For more information, see the [Manager Administration] section.
- In the Manager, click Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Physical Ports → **Monitoring Ports**. Look at the color of the button(s) representing the ports on the Sensor, and check the color legend on the screen to see the status of the Sensor's ports. For more information on this process, see the [Manager Administration] section.
- Type **`status`** in the Sensor command line interface (CLI). Check the following line:

  `trust established between sensor and manager = yes`

  If the answer is **no**, recheck that your Sensor name and shared secret are the same on both the Sensor and the Manager.

4. Troubleshoot any problems you run into.

   If you run into any problems, check your configuration settings and ensure that they are correct. For troubleshooting tips, see the [Troubleshooting] section.

5. Verify the monitoring mode of the ports on your Sensor.

   Your IPS Sensor ports are configured by default for monitoring in **Default Prevention** mode; that is, connected in-line on a network segment (for example, between a switch and a router or two switches). If you've cabled the Sensor to monitor in another monitoring mode, check your settings to make sure everything is correct. Some users choose instead to monitor in SPAN mode at first, and move to **tap** and/or **in-line** mode later.

   For more information on verifying port configuration, see [Trellix Intrusion Prevention System Installation Guide].

Configuring your deployment using the Manager

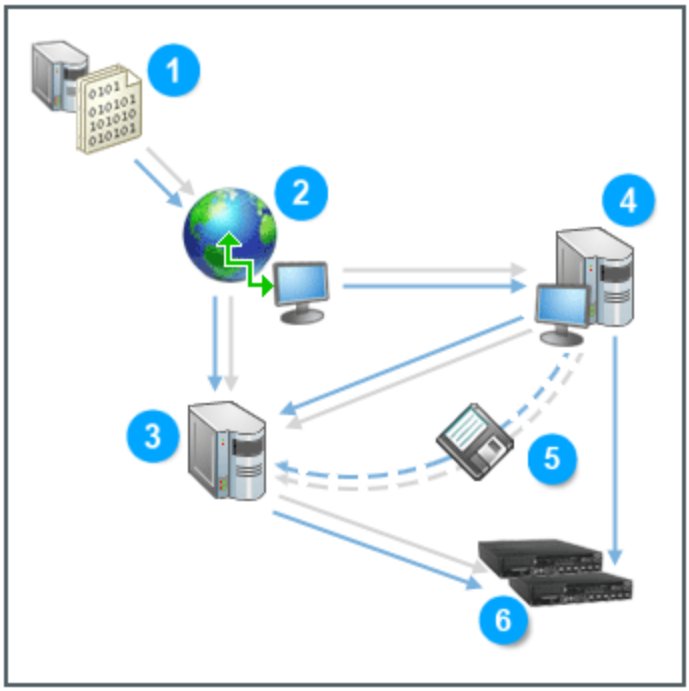
Once you're up and running and reviewing the data generated by the Manager, you can further configure it. For example, you can do the following:

- **Apply security policies to each interface of your multi-port Sensor** (instead of the **Default Inline IPS** policy applied to all interfaces): You can ensure all of your interfaces deploy policies specifically for the areas of your network they are monitoring. For example, you can apply the **Web Server** policy to one interface, the **Mail Server** policy to another, and the **Internal Segment** policy to another, and so on. For more on the policies, see the section Trellix IPS policies (page 773).
- **Configure responses to alerts**: Developing a system of actions, alerts, and logs based on impact severity is recommended for effective network security. For example, you can configure Trellix IPS to send a page or an email notification, execute a script, disconnect a TCP connection, send an *ICMP Host Not Reachable* message to the attack source for ICMP transmissions, or send a block address filter to a host.
  - For information on response actions, see the section Sensor response actions (page 2294).
  - For information on configuring a pager, email, or script notification for alerts, see the section Alert notification options (page 163).
  - For information on configuring a quarantine response, see the section Quarantining hosts (page 1432).
  - You can also send SNMP traps to a third-party management system. For more details, see the sections Forward alerts to an SNMP server (page 890), and Forward faults to an SNMP server (page 191) .
- **Filter alerts**: An ignore rule limits the number of alerts generated by the system by excluding certain source and Destination IP address parameters. If these address parameters are detected in a packet, the packet is not analyzed further (and is automatically forwarded when in Inline Mode). For more information on ignore rules, see [Trellix Intrusion Prevention System Product Guide.]

- **View the system's health**: The **Faults** tab in the **Logs** page details the functional status for all of your installed Trellix IPS system components. Messages are generated to detail system faults experienced by your Manager, Sensors, or database. For more information, see the [Manager Administration] section.
- **View a Sensor's performance**: The Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Summary** action enables you to view performance data for a Sensor. The data collected is a reflection of the traffic that has passed through the Sensor. For more information, see [Manager Administration] section.
- Back up all or part of your Manager configuration information to your server or other location. For more information, see the section Backing up data and settings (page 301).

Updating your signatures and software

An essential element to a reliable IPS is updating the system signature and software images. Trellix periodically releases new Manager software, Sensor signature and software images, and makes these updates available via the Update Server.



Field	Description
1	Trellix IPS Update Server
2	Internet
3	IPS Manager Server
4	PC/TFTP server
5	Import/disk
6	IPS Sensor

There are several options for loading updates to your Manager and Sensors.

1. **Download latest software and signature updates from the Update Server to your Manager**

You can use the Manager interface to download Sensor software and signature updates from the Update Server to the Manager server, and then download the updates to the Sensor.

2. **Import update files from a remote workstation to your Manager**

   If your Manager server is not connected to the Internet, you can download signature and software updates from the Download Server to any host by doing one of the following:

   - Download the update to a host, then log in to the Manager and *import* the update to the Manager server. You can then download the update to the Sensor.
   - Similar to above, download the update from the Download Server to any host, put it on a disk, take the disk to the Manager server, and then *import* the update and download it to the Sensor.

   For more information, see [Trellix Intrusion Prevention System Product Guide].

3. **Download software from the Update Server to a TFTP client and then download to a Sensor**

   You can download software images from the Download Server onto a TFTP server, and then download the software directly to the Sensor using Sensor CLI commands. This is useful if you are unable or prefer not to update Sensor software via the Manager. This method is described in the [Trellix Intrusion Prevention System Installation Guide].

Tuning your deployment

Once you become familiar with the basics of the Manager, you can further enhance your deployment by using some of the more advanced features. Trellix IPS is an extremely complex system and can be tuned on a highly granular level. You might try working with some of the following features as you tune your system:

- Cloning and modifying a provided policy. For more details, see the section Working with IPS policies (page 795).
- Creating Firewall policies to block specific traffic or pass specific traffic without sending it through the intrusion detection engine. For more details, see the section User-based access rules (page 1229).
- If you have started out in SPAN mode, you might try taking advantage of Trellix IPS prevention capabilities by deploying your Sensor to monitor traffic in in-line mode. For more details, see the section Deployment of Sensors in in-line mode (page 587).
- Adding users and assigning management roles. See the section Management of users and user roles (page 94) for more details.
- Adding administrator domains for resource management. See the section Create an admin domain (page 110) for details.
- Changing your interface type to CIDR or VLAN depending on your network configuration. See the section Managing interfaces (page 596) for more details.

Trellix IPS documentation set

The Trellix Intrusion Prevention System product documentation is available on the Trellix Documentation Portal.

The Trellix IPS documentation set is designed to provide you with the information you need during each phase of the product implementation from evaluating a new product to maintaining existing ones. After the product is released, additional information regarding the product is entered into the online Knowledge Base available on Trellix Service Portal.

Refer to the following tables for a list of Trellix IPS software and hardware documentation:

Table 1. Trellix IPS software documentation

Guide	Description
Installation Guide	System requirements, installation of the Manager software, management of IPS Sensor/failover pairs, and upgrade steps
Product Guide	• A high-level view of how to interact with Trellix IPS • Management of devices, such as IPS Sensors and NTBA Appliances • Obtaining updates from the Trellix IPS Update Server • Monitoring alerts and hosts on your network • In-depth details for inline mode configuration • Management of admin domains, users, and roles • Configuration of MDR • Definition of failover pairs • Various IPS features supported up to the latest Trellix IPS release • Achieving virtualization using IPS Sensor • Creation of custom attacks and signatures using the Custom Attack Editor • Generation of reports • Import of Snort signatures • Troubleshooting techniques for Trellix IPS • Recommended practices for using Trellix IPS most effectively • List of all public and debug CLI commands for IPS Sensors • Initialization, upgrade or replacement of a Sensor, troubleshooting an issue, and performance monitoring for the Sensor • Viewing the system health status of your Trellix IPS components • Configuration and management of Trellix Intrusion Prevention System Central Manager • Management of policies and rule sets • Management of ignore rules
Integration Guide	Integration with: • ePolicy Orchestrator • Global Threat Intelligence • Intelligent Virtual Execution Engine • Network Investigator • Trellix Intelligent Sandbox • Threat Intelligence Exchange • Logon Collector • HP Network Automation • Third-party SIEM products

Guide	Description
Manager API Reference Guide	Application Programming Interface (API) framework for external applications to access core IPS functionalities through the REST protocol.

Table 2. Trellix IPS hardware documentation

Guide	Models
Sensor Hardware Guide	NS7600, NS3600
Manager Appliance Product Guide	MLOS
NS-series Sensor Product Guide	NS9500, NS9x00, NS7500, NS7x50, NS7x00, NS5x00, NS3500, and NS3x00
NS-series Reference Guide	1. NS-series Interface Modules 2. NS-series Transceiver Modules 3. NS-series Sensors DC Power Supply Installation
Fail-Open Kit Product Guide	• 100 Gigabit Modular Active Fail-Open Bypass Kit • 10/40 Gigabit Modular Active Fail-Open Bypass Kit • 1/10 Gigabit Modular Active Fail-Open Kit • 1/10 Gigabit Modular Passive Fail-Open Kit • 40 Gigabit Active Fail-Open Bypass Kit

Manager Administration

Trellix Intrusion Prevention System Manager

Trellix Intrusion Prevention System overview

Trellix Intrusion Prevention System is a combination of network appliances and software built for the accurate detection and prevention of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, malware download, and network misuse. Trellix Intrusion Prevention System provides comprehensive network intrusion detection, and can block or prevent attacks in real time, making it truly an intrusion prevention system (IPS).

Trellix IPS components

The following are the major Trellix Intrusion Prevention System components for IDS and IPS:

- Trellix Intrusion Prevention System Sensor
- Trellix Intrusion Prevention System Manager, with its Web-based graphical user interface

Trellix IPS Sensors

Trellix IPS Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of intrusions, misuse, malware, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks. Sensors can be physical or virtual appliances. IPS Sensors are specifically designed to handle traffic at wire-speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment. When deployed at key network access points, a Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

Once deployed and the communication is established, Sensors are configured and managed through the Manager server.

- In this chapter, the term *Sensor* applies to both physical as well as Virtual IPS Sensors unless otherwise specified.
- In this guide, the term *Sensor resources* refers to the monitoring ports, interfaces, and subinterfaces of a physical or a Virtual IPS Sensor.

Sensor functionality

The primary function of a device is to analyze traffic on the selected network segments and to respond when an attack is detected. The device examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The device examines packets and matches the packets against the applied policies. These policies determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a physical or a Virtual IPS Sensor responds according to its configured policy. A Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, “scrubbing” malicious packets, and even blocking attack packets entirely before they reach the intended target.

In addition to its primary function of preventing exploit, recon, and DoS attacks, a Sensor can also do the following:

- **Detect malware**— A Sensor uses various methods to inspect files being downloaded for embedded malware. If a malware is detected, the Sensor blocks the download and takes further response actions.
- **Enforce Firewall access rules**— You can define Firewall access rules (similar to ACLs) in the Manager. Then you can configure a Sensor to enforce these rules on your network.

- **Provide and facilitate Quality of Service (QoS)**— A physical Sensor can facilitate Differentiated Services and IEEE 802.1p by differentiating traffic and tagging them accordingly.
- **Provide connection limiting services**— Based on how you configure, a Sensor can limit the number of connections a host can establish. One of the advantages of connection limiting is that it can minimize connection-based DoS attacks.
- **Export NetFlow data**— If Network Threat Behavior Analysis (NTBA) is deployed, you can configure a Sensor to export NetFlow data to the NTBA Appliance.

NOTE

The Sensor generates an auditlog file that is no more than 128MB. The file is purged from the disk when the audit log is uploaded to the Manager and a new auditlog file is started with a start marker.

All the manager-sensor communications happen over TLS.

Sensor platforms

Trellix IPS offers several types of Sensor platforms providing different bandwidth and deployment strategies.

- NS-series: NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3600, NS3500, NS3200, and NS3100
- Virtual IPS Sensors: IPS-VM600, IPS-VM5000

Trellix IPS Manager components

The Manager is a term that represents the hardware and software resources that are used to configure and manage the Trellix IPS. The IPS Manager consists of the following components:

- Manager server platform
- The Manager software
- A back-end database that is installed along with the Manager
- A connection to Trellix IPS Update Server
- Signature Set

Manager server platform

The Manager server platform hosts the Manager software and the Manager database. It is a server running on an operating system as specified in the [Trellix Intrusion Prevention System Installation Guide.] You can remotely access the Manager user interface from a client machine using a browser. Refer to the [Trellix Intrusion Prevention System Installation Guide] to know the supported browsers and the supported operating systems for the clients.

Sensors use a built-in 10/100 Management port to communicate with the Manager server. You can connect a segment from a Sensor Management port directly to the Manager server; however, this means you can only receive information from one Sensor (typically, your server has only one 10/100 network port). During the Sensor configuration, you will establish communication between your Sensors and your Manager server.

Manager software

The Manager software has a web-based user interface for configuring and managing Trellix IPS. Users connect to the Manager server from a supported client using a supported browser, the details of which are in the [Trellix Intrusion Prevention System In-

stallation Guide.] The Manager functions are configured and managed through a GUI application, which includes complementary interfaces for alerts, system status, system configuration, report generation, and fault management. All interfaces are logically parts of the Manager program.

The Manager user interface has five main tabs:

- **Dashboard** — The **Dashboard** is the first page displayed after the user logs on to the system. Options available within the page are determined by the current user's assigned roles. The Dashboard enables you to view all the critical information regarding Trellix IPS deployment in the same page. The Dashboard is very user configurable. You can configure the information that you want to view, the timeframe for which you want to view the information, the frequency with which the Dashboard must auto-refresh, and so on. All these information can be customized to view for a particular admin domain. You can select the admin domain from the **Domain** drop-down list to display data for the selected admin domain.

  Some of the information displayed on the dashboard includes:

  - Release announcements
  - Information regarding the frequently seen malicious activities on your network. This includes things, such as the most downloaded malware, most callback activity, the most targeted hosts, the most detected attack and so on.
  - System faults of Trellix IPS components which show whether all those are functioning properly, the number of unacknowledged alerts in the system, and the configuration options available to the current user
  - Manager-related details, such as the version, signature set version, users logged on to the Manager, and so on
  - Information like whether the devices are up-to-date
- **Analysis** — This tab presents the options using which you can view the granular details of all the malicious activities on your network. The intention here is to provide you all the critical information needed for further analysis for the selected admin domain.

  One of the key options on the **Analysis** tab is the **Attack Log**, which displays the alerts triggered by the Sensors. The **Attack Log** page displays the hosts detected on your network as well as the detected security events that violate your configured security policies. The Attack Log provides powerful drill-down capabilities to enable you to see all of the details on a particular alert, including its type, source and destination addresses, and packet logs where applicable.
- **Policy** — All the major features in Trellix IPS are policy based. For example, to block exploit and recon attacks, you use the IPS and the recon policies; for Firewall, you use the Firewall policies; for QoS, you use the QoS policies and so on. The **Policy** tab provides the options to manage all these policies and other related functionality.
- **Devices** — You can use the same instance of the Manager to manage both the physical and virtual devices. The **Devices** tab provides all system configuration options, and facilitates adding and configuration of your devices - Sensors, NTBA Appliances, HA pairs of Sensors, etc. This tab provides configuration options on per device basis as well. Access to various activities is based on the current user's role(s) and privileges, administrative domains, attack policies and responses, user-created signatures, and system reports.
- **Manager** — This tab provides the configuration options related to the Manager software. This includes managing administrative domains, users, and roles, downloading signature sets and other software such as Sensor software, integrating the Manager with other Trellix products, maintenance activities such as database backups, and so on.

Other key features of Manager include:

- **Integration with other Trellix products** — You can integrate Trellix IPS with other Trellix products to provide you with a comprehensive network security solution.
  - **Trellix ePolicy Orchestrator - On-prem** — Trellix ePolicy Orchestrator - On-prem is a scalable platform for centralized policy management and enforcement of your system security products, such as anti-virus, desktop firewall, and

anti-spyware applications. You can integrate Trellix IPS with Trellix ePO - On-prem 5.0 and above. The integration enables you to query the Trellix ePO - On-prem server from the Manager for viewing details of a network host.

- **Trellix Global Threat Intelligence** — Trellix Global Threat Intelligence is a global threat correlation engine and intelligence base of global messaging and communication behavior including reputation, volume, trends, email, web traffic and malware. By having Trellix Global Threat Intelligence integration, you can report, filter, and sort hosts involved in attacks based on their network reputation and the country of the attack origin.
- **Trellix Intelligent Sandbox** — Trellix Intelligent Sandbox is an on-premise appliance that facilitates detection and prevention of malware. Trellix Intelligent Sandbox provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.
- **Trellix Intelligent Virtual Execution (IVX)** — Intelligent Virtual Execution (IVX) Engine is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature-based and policy-based defenses. The IVX engine detects zero-day, multiflow, and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyberattack kill chain by identifying never-before-seen exploits and malware.

  Trellix IPS offers integration capability with Intelligent Virtual Execution - Server and Intelligent Virtual Execution - Cloud which utilize IVX engine's technology to perform malware analysis.
- **Trellix Network Investigator** — Network Investigator (NI) is a security analytics solution that allows the analysis of alerts and network metadata gathered from all devices connected to it. Network Investigator can ingest alerts and collect Layer 7 metadata from other Trellix products, including Network Security (NX), Packet Capture (PX), and End-point Security (HX), and provides a high-level view of the network metadata gathered over customizable dashboards supporting multiple configurations. It thus enables users to have a metadata-based view of network activities and search indexed metadata from various network protocols, which allows them to zero down on threat information critical for performing further investigation.

  Trellix IPS offers integration capability with Trellix Network Investigator using which it exports netflows and Layer 7 metadata from IPS Sensors, and alert data from IPS Manager to NI, as per the configuration and filter parameters set by the user. The alert data, L7 metadata information, and net flow records exported by Trellix IPS are displayed on the **Dashboard** of NI's Web UI which users can review and utilize further for the detection and analysis of network threats.

For more information on all the above mentioned integration options, see [Trellix Intrusion Prevention System Integration Guide].

- **Integration with third-party products** — Trellix IPS enables the use of multiple third-party products for analyzing faults, alerts, and generated packet logs.
  - **Fault/Alert forwarding and viewing** — You have the option to forward all fault management events and actions, as well as IPS alerts to a third-party application. This enables you to integrate with third-party products that provide trouble ticketing, messaging, or any other response tools you may want to incorporate. Fault and/or alert forwarding can be sent to the following ways:
    - **Syslog Server** — forward IPS alerts and system faults
    - **SNMP Server (NMS)** — forward IPS alerts and system faults
    - **Java API** — forward IPS alerts
  - **Packet log viewing** — View logged packets/flows using third-party software, such as Wireshark.

Manager database

The Manager server operates with an RDBMS (relational database management system) for storing persistent configuration information and event data. The compatible database is MariaDB. Refer to the [Trellix Intrusion Prevention System Installation Guide] for the current version of MariaDB.

The Manager server includes a database that is installed (embedded) on the target Windows server during Manager software installation.

The database can be tuned on-demand or by a set schedule through the Manager user interface configuration. Tuning promotes optimum performance by defragmenting split tables, re-sorting and updating indexes, computing query optimizer statistics, and checking and repairing tables.

Signature Set

Signature set is a comprehensive set of attack definitions developed and provided by Trellix Advanced Research Center. An attack definition contains one or more signatures, which indicate suspicious or malicious activity. These signatures are then matched against traffic passing through the Sensor monitoring ports.

Each attack definition can be configured to perform response actions like sending an alert to the Manager, dropping traffic, capturing packets, or generating an email. It is used to detect threats and anomalies in the network traffic.

Signature sets are available in Trellix IPS Update Server (Update Server). Trellix regularly updates the signature set with latest attack definitions which you can download from the Update Server.

The threat landscape is constantly evolving, and new attacks are regularly added to the signature set to keep the network protection up-to-date. The attack definitions in the signature set are categorized as high, medium, and low priority attacks. This helps optimize Sensor resources on older Sensor models and Sensors running older software versions, thereby protecting against the most critical and relevant attacks.

Based on the priority attribute configured for the Sensor models, the Manager dynamically compiles the signature set using the current signature set version available in the Manager. The corresponding set of attack definitions are then pushed to the Sensors.

The NS-series and Virtual IPS Sensor models support high, medium, and low priority attack definitions, thereby providing complete attack coverage.

Trellix IPS Update Server

For your Trellix IPS to properly detect and protect against malicious activity, the Manager and Sensors must be frequently updated with the latest signatures and software patches available. Thus, the Trellix IPS team constantly researches and develops performance-enhancing software and attack-detecting signatures that combat the latest in hacking, misuse, and denials of service (DoS). When a severe-impact attack happens that cannot be detected with the current signatures, a new signature update is developed and released. Since new vulnerabilities are discovered regularly, signature updates are released frequently.

New signatures and patches are made available to customers via Trellix IPS Update Server (Update Server). The Update Server is a Trellix IPS owned and operated file server that houses updated signature and software files of Managers and Sensors for customer installations. The Update Server securely provides fully automated, real-time signature updates without requiring any manual intervention.

NOTE

Communication between the Manager and the Update Server is SSL-secured.

Obtaining updates from the Update Server

You have the following options for obtaining updates from the Update Server:

1. Connecting directly from your Manager server (via Manager interface action).
2. Connecting through a proxy server (through Manager interface action). You will then authenticate as in option 1.

Configuring software and attack signature updates

You can configure interaction with the Update Server using the Manager. You can pull updates from the Update Server on demand or you can schedule update downloads. With scheduled downloads, the Manager polls the Update Server (over the Internet) at the desired frequency. If an update has been posted, that update is registered as “Available” in the Manager interface for on-demand downloaded. Once downloaded to the Manager, you can immediately download (via an encrypted connection) the update to deployed Sensors or deploy the update based on a Sensor update schedule you define. Acceptance of a download is at the discretion of the administrator.

- **Automatic update to Manager, manual update from Manager to Sensors** — This option enables Manager server to receive updates automatically, but allows the administrator to selectively apply the updates to the Sensors.
- **Manual update to Manager, automatic update from Manager to Sensors** — This option enables the administrator to select updates manually, but once the update is selected, it is applied to the Sensors automatically without reboot.
- **Fully manual update** — This option allows the security administrator to determine which signature update to apply per update, and when to push the update out to the Sensors. You may want to manually update the system when you make some configuration change, such as updating a policy or response.
- **Fully automatic update** — This option enables every update to pass directly from the Update Server to the Manager, and from the Manager to the Sensors without any intervention by the security administrator. Note that fully automatic updating still happens at the scheduled intervals.
- **Real-time update** — This option is similar to fully automatic updating. However, rather than waiting for a scheduled interval, the update is pushed directly from Update Server to Manager to Sensor. No device needs to be rebooted; the Sensor does not stop monitoring traffic during the update, and the update is active as soon as it is applied to the Sensor.

Getting familiar with Trellix IPS Manager

Trellix IPS Manager is a browser-based graphical user interface used to view, configure, and manage network security appliance deployments.

This section provides a high-level tour of the basic features and interfaces of the Manager and some basic concepts of working with the Manager.

Accessing the Manager from a client machine

To access the Manager from a client machine:

1. Start your browser and then type the URL of the Manager server:

   `https://<hostname or host-IP>`

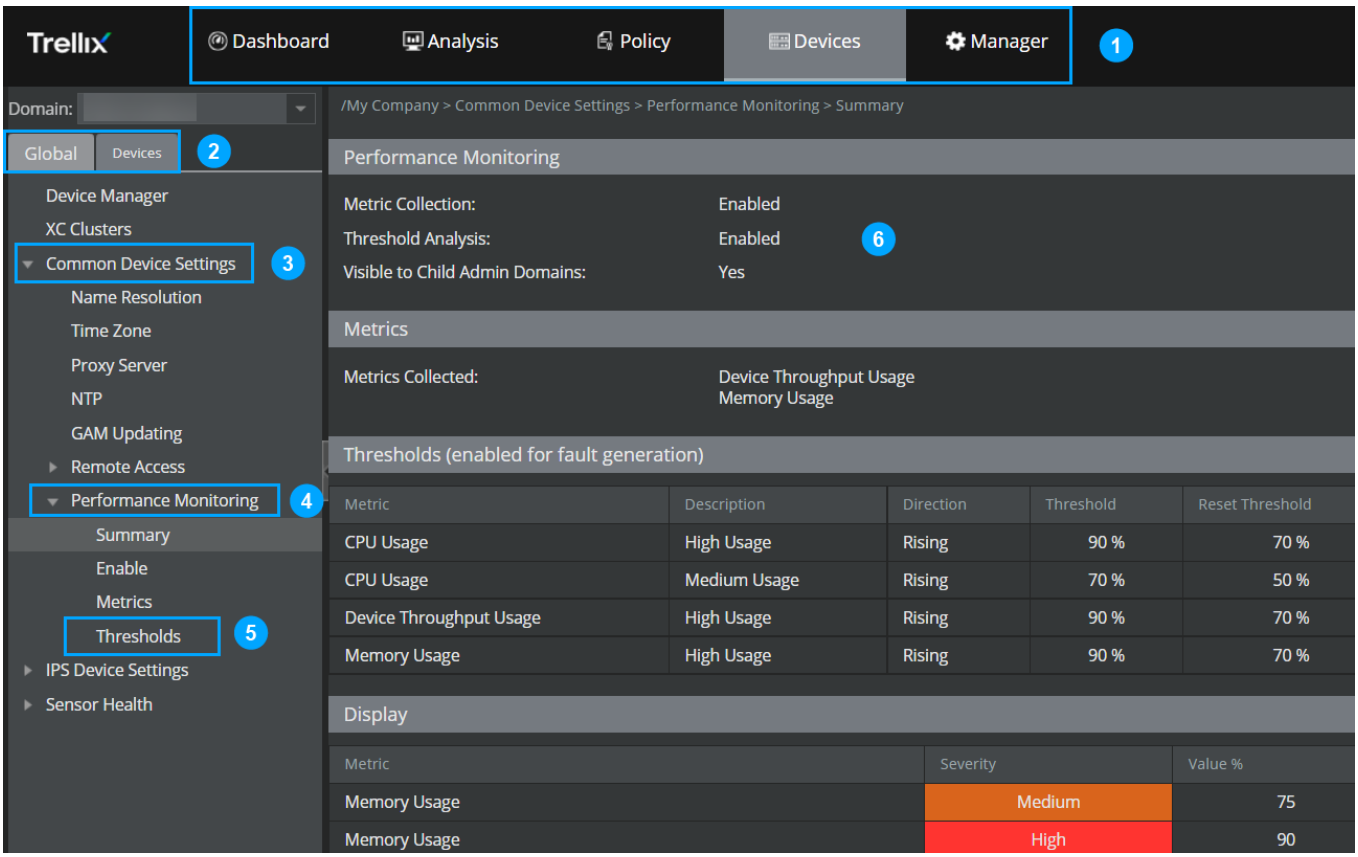
2. Log on to the Manager by entering your **Login ID** and **Password.**

About the Manager user interface design

The Manager user interface is designed with a task-based approach. This gives you the ability to view and drill down into network issues easily throughout the interface.

The Manager user interface is a two-tiered structure to facilitate ease of navigation. You can use the Menu bar to logically navigate around the user interface based on what task you want to perform. The left navigation pane is designed such that you can manage your tasks with more ease in your enterprise level deployments.

Figure 1. Manager user interface



The design provides you with these advantages.

Cal-lout	Description
1	Tab - Tabs are located on the menu bar and display specific set of tabs, menus, and options.
2	Sub-tab - A tab contains sub-tabs, which display a number of menus when clicked.
3	Menu - A menu displays one or more sub-menus when clicked.
4	Sub-menu - A sub-menu displays options or more sub-menus when clicked.
5	Option - An option displays a page in which you can either view or view and modify settings.
6	Display pane - When you click an option to display a page, the area within which the page is displayed is known as the display pane.

- **Information availability** — Network information is available at your finger tips in the **Dashboard** page and helps you to immediately check on any issue.

- **Customized display** — You can drag and drop monitors and set dashboard preferences based on your needs.
- **Operational and Security monitoring** — You can view top threats in your network and check the overall system health on the **Dashboard** page.
- **Dynamic control** — The hyperlinks in the **Dashboard** page enable you to dynamically click and investigate any network or system health issue across the Manager.
- **Context-aware interfaces** — From the Dashboard, you can click and drill down into the Threat Explorer and other relevant pages for further analysis. The details are in sync with what you choose in the **Dashboard** page and help you to investigate further. For example, if you click a hyperlink in the Top Attack Applications monitor, you are directed to the **Threat Explorer** with the core attribute already set in the view. You can then choose to add more filter criteria and drill down to resolve an issue.

Scenario: System Health Check

Assume that you want to view the overall system health and fix an issue with a faulty device.

The **Dashboard** page allows you to view multiple operational monitors namely **Manager Summary, Release Announcements, Running Tasks** and **System Faults**.

1. Select Dashboard → Dashboard Settings → **Monitors** list and select the **Operational** monitor.
2. View the **System Faults** monitor for Manager and device status.
3. For a faulty device, under the **Critical** column, click the hyperlink.
4. The **Faults** tab in the **Logs** page display the fault severity and summary details.
5. View the fault details. For example, a link failure between the port and external device.
6. Fix the issue. In the preceding example, the link needs to re-established between the port and the external device.

Browser requirements

This section contains the client and browser requirements for accessing the Manager.

The following table lists the 11.1 Manager client requirements when using Windows 10.

	Minimum	Recommended
Operating system	Windows 10, English or Japanese **NOTE** The display language of the Manager client must be same as that of the Manager server operating system.	Windows 10, version 1903 English or Japanese
Memory	8 GB	16 GB
CPU	1.5 GHz processor	2.4 GHz or faster
Monitor	32-bit color, 1440 x 900 display setting	1920 x 1080 (or above)

	Minimum	Recommended
Browser	• Microsoft Edge • Mozilla Firefox • Google Chrome **NOTE** To avoid the certificate mismatch error and security warning, add the Manager web certificate to the trusted certificate list.	• Microsoft Edge 111.0 or later • Mozilla Firefox 111.0 or later • Google Chrome 111.0 or later

For the Manager/Central Manager client, in addition to Windows 10, you can also use the operating systems mentioned for the Manager server.

The following table lists the 11.1 Central Manager/Manager client requirements when using Mac:

Mac operating system	Browser
Ventura	Safari 16 or later

Menu bar

The menu bar contains five tabs:

- **Dashboard**
- **Analysis**
- **Policy**
- **Devices**
- **Manager**

A click on each tab opens a tab tree that has sub-tabs, menus, sub-menus, and options.

Figure 2. Menu bar of Manager

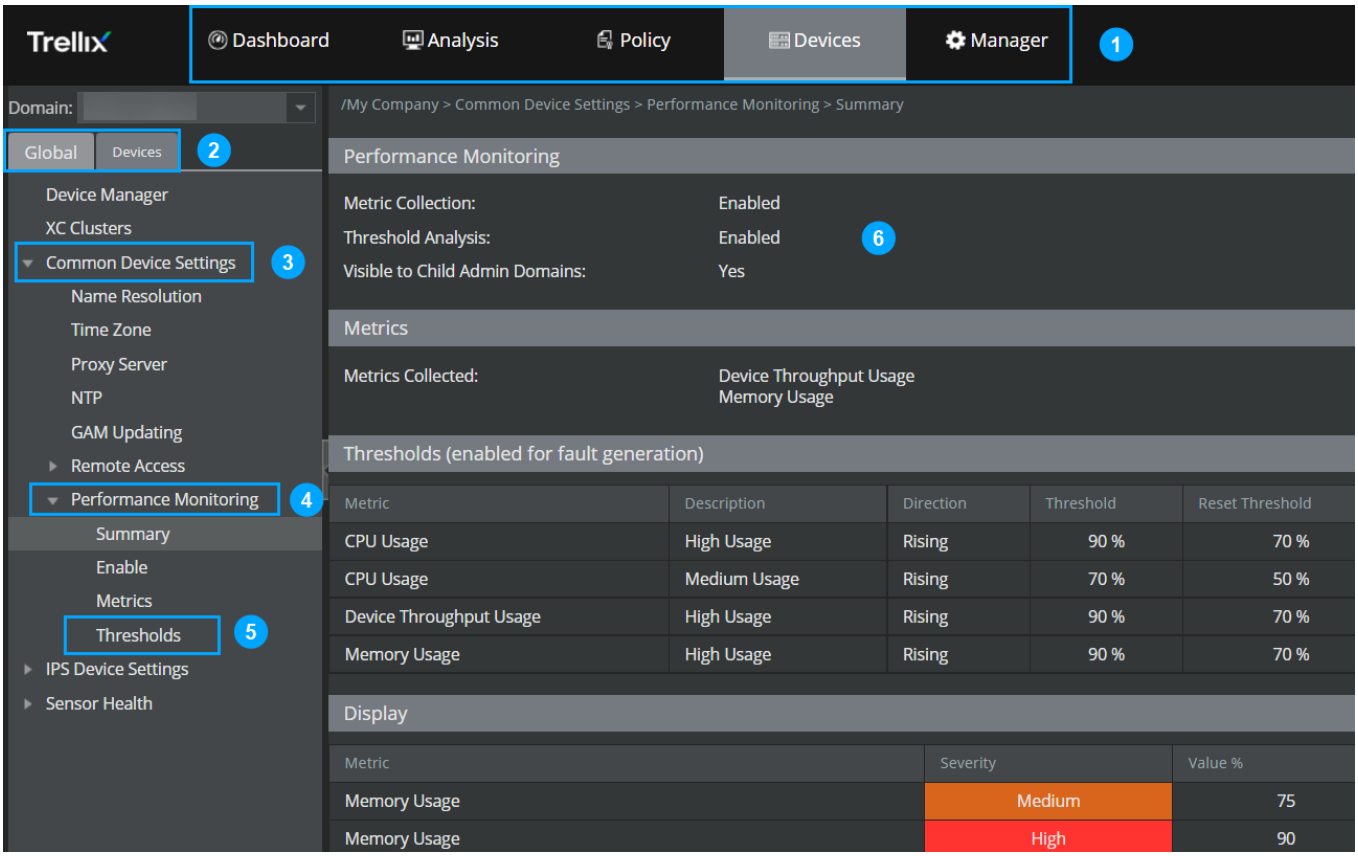
The menu bar also provides you with the following:

- **(Help)**— links to the complete system help.
- **(Log Out)**— logs you out of the Manager and returns to the login screen.

Menus

Each item in the tab tree is a *menu* and represents a set of sub-menus and options. Example: Updating menu.

Figure 3. Manager user interface



The design provides you with these advantages.

Callout	Description
1	Tab – Tabs are located on the menu bar and display specific set of tabs, menus and options.
2	Sub-tab – A tab contains sub-tabs which display a number of menus when clicked.
3	Menu – A menu displays one or more sub-menus when clicked.
4	Sub-menu – A sub-menu displays options or more sub-menus when clicked.
5	Option – An option displays a page in which you can either view or view and modify settings.
6	Display pane – When you click on an option to display a page, the area within which the page is displayed is known as the display pane.

Online Help

- To view online Help, including the table of contents, index, and full-text search, click the question mark (**?**) button on the menu bar.
- To obtain Help on the action displayed in a specific configuration page, click the question mark (**?**) button in the upper-right corner of the right display pane. The corresponding Help page is displayed.

View server/client date and time

A Manager server can be accessed through various clients spread across different geographical locations. When a user accesses a server placed in a different time zone, the server time is converted to the client time zone based on Greenwich Mean Time (GMT), and displayed to the user.

If the clock time between the server and the client has a difference of more than 1 minute, Trellix IPS displays a warning message that prompts the user to reset the client machine clock to match with the server clock. This message is displayed only once per browser session.

If your Trellix IPS deployment is at a geo-location that uses daylight savings, then:

1. On your Windows Operating System, select Start → Settings → Control Panel → **Date and Time**.
2. Select the **Automatically adjust clock for daylight saving changes**.

   This will add an hour to GMT during daylight savings time.

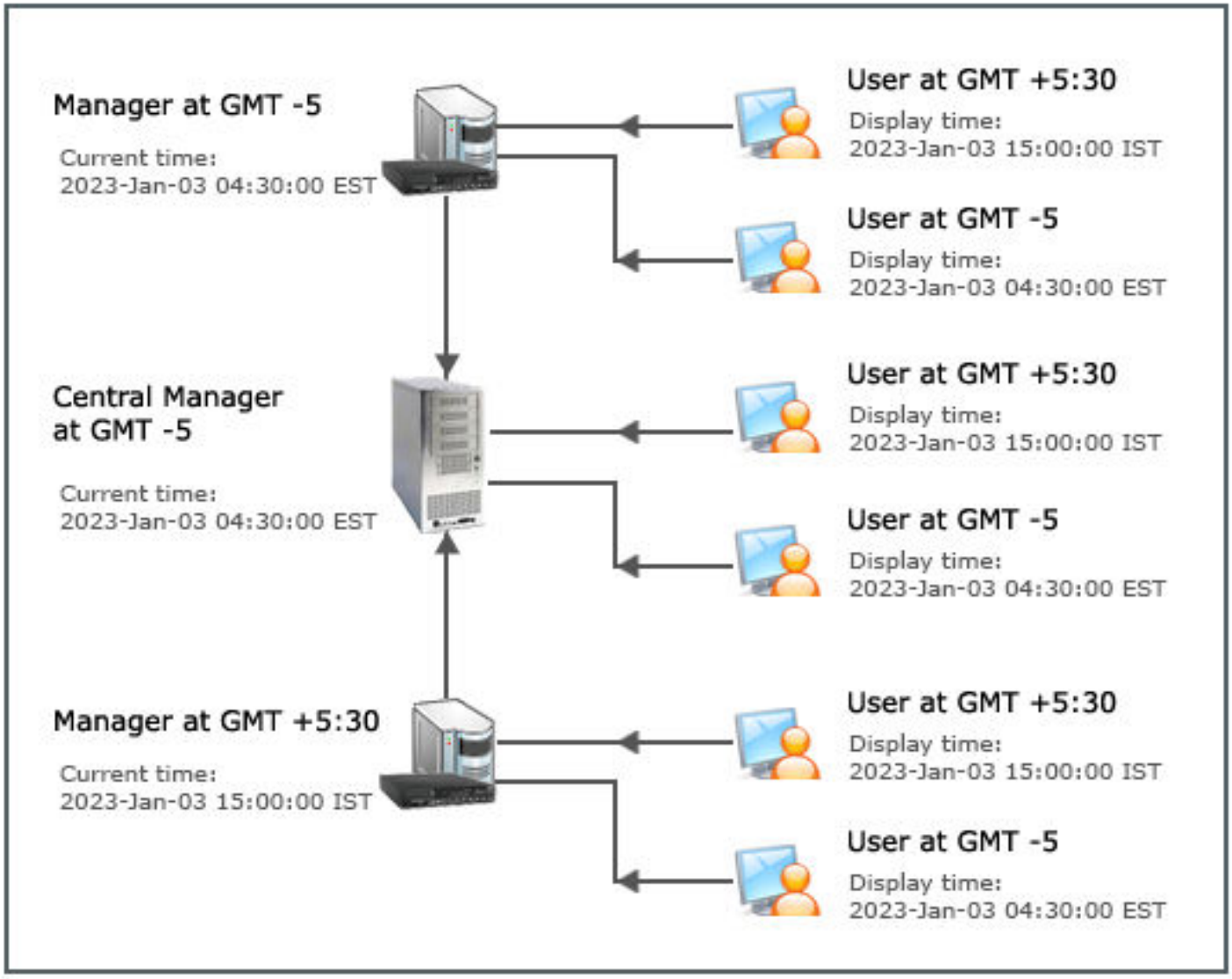
Scenario

Scenario 1: User accessing a server placed in different time zone

Trellix Intrusion Prevention System Central Manager (Central Manager) can access Managers spread across different geographical locations and time zones. If a Manager user is accessing Trellix IPS Central Manager, which is situated in a different zone, the time displayed is the client time zone and vice versa.

For example, Consider a Central Manager running at Eastern Standard Time (EST) that is, GMT-5 hours. There are two users: user1 and user2 accessing the Manager and Central Manager from their respective time zones. User1 is situated at GMT+5:30 hours, and user2 is situated at GMT -5 hours respectively. If the time at Central Manager is 2007-01-03 4.30.00 EST, the time displayed to user1 will be 2007-01-03 15:00:00 IST, while the time displayed to user2 will be 2007-01-03 4.30.00 EST respectively as the last retrieved time in the Home page.

Figure 4. Manager Time Zones



The time stamp format is displayed in yyyy-MMM-dd HH:mm:ss:z or when displayed in a tabular fashion as in reports, it is displayed as yyyy-MM-dd HH:mm:ss:z

For example: 2007-Feb-21 17:52:50 IST or 2007-02-21 17:52:20 IST

Scenario 2: Manager Scheduler actions run at the server time zone

Consider a user who wants to schedule the Trend Analysis Report. The Manager server is placed in Eastern Standard Time (EST) zone, and the user is situated in Indian Standard Time (IST). If the user sets the date and time for the report to generate at 2007-03-03 12:00:00, the report will run at the Manager server date and time that is, 2007-03-03 12:00:00 EST. The scheduled report will have the server time, that is, EST in this example.

In general, scheduling triggered by the server considers the server time. For example, the Trellix IPS Update server messages, values in the Admin Configuration report etc. display the server date and time.

NOTE

If a user triggers a manual report generation, it will run at the client time zone.

Customizable views

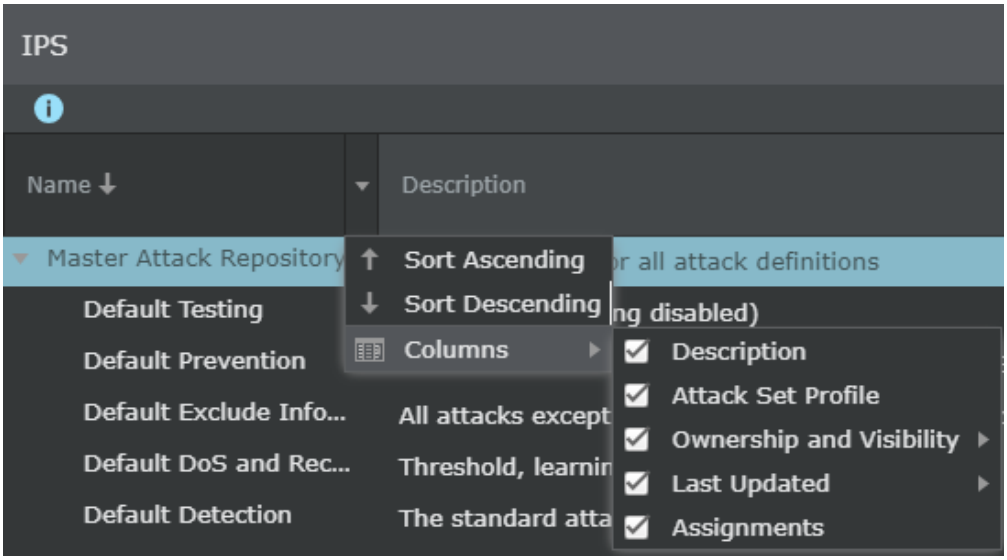
All table views in the Manager UI for alerts, attacks, etc., provide the flexibility of customizing the columns for viewing information.

The Manager supports the following customization to the columns in a table:

- Column visibility (columns shown versus hidden)

  When you hover the mouse over a column, a small drop-down arrow is displayed. This drop-down list contains different columns that display information. You can use the drop-down list to select/hide columns based on the information required for current viewing. The information in the column can be sorted in ascending or descending order.

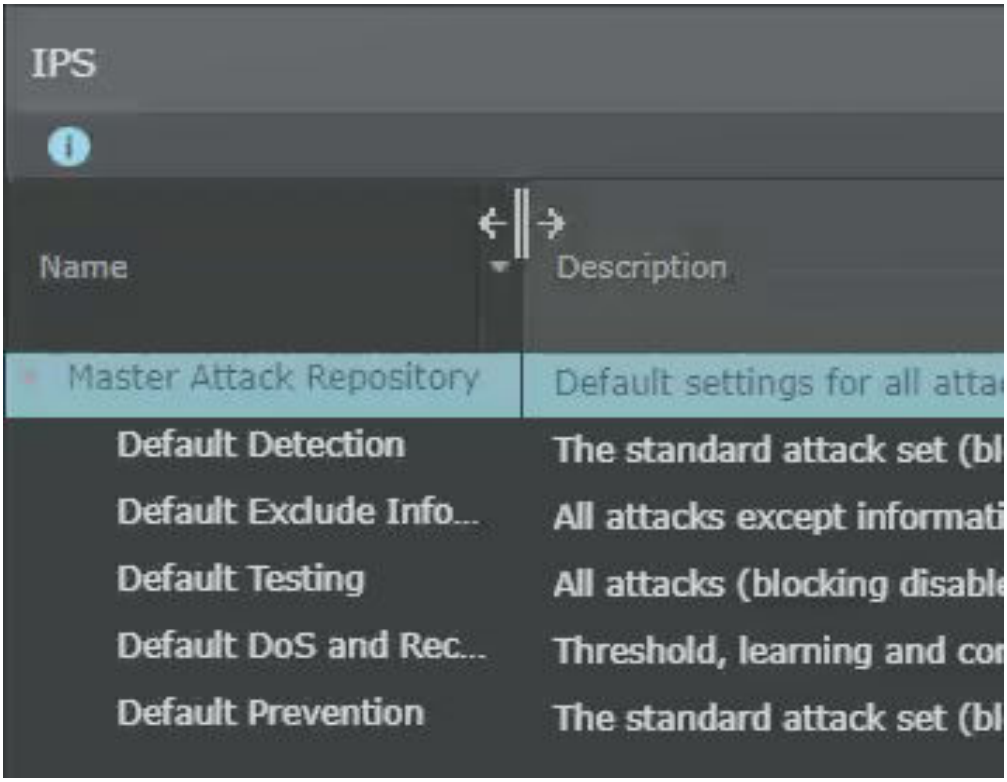
Figure 5. Column visibility



- Column width

  The width of the column can be adjusted (increased/decreased) to view information as required.

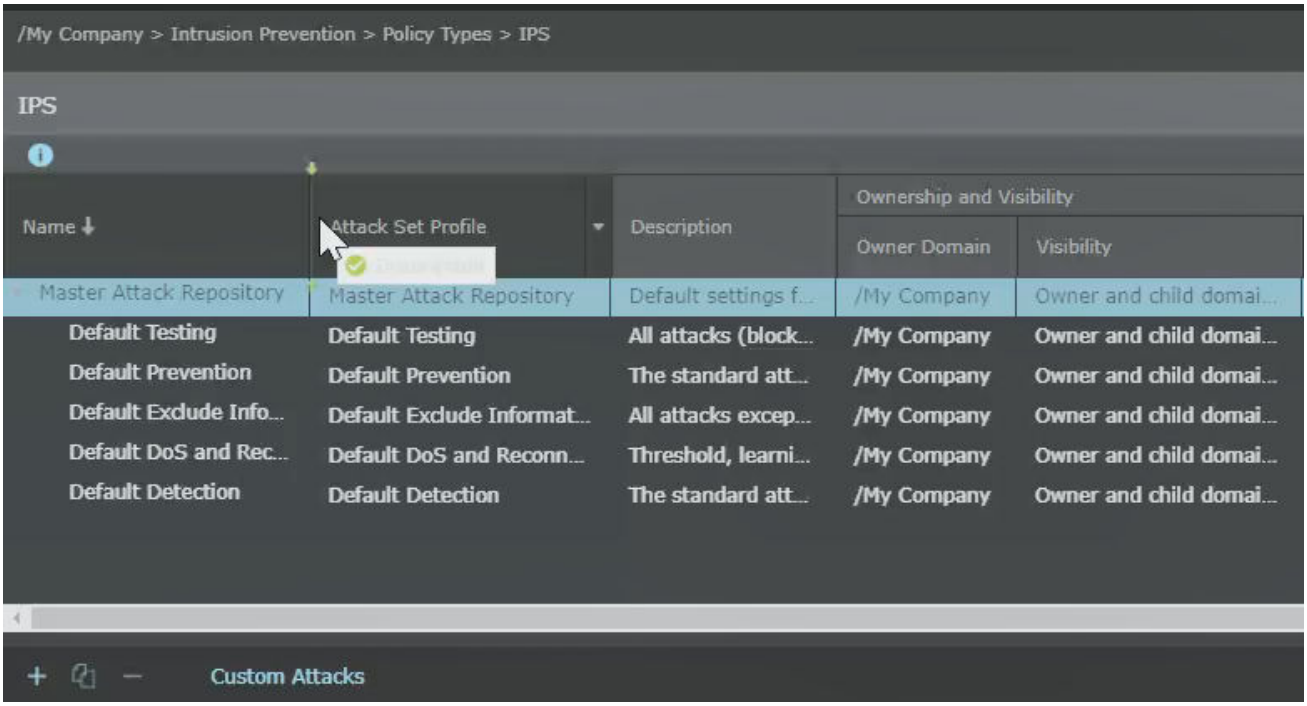
Figure 6. Column width



- Column presentation order (left to right)

  You can rearrange the columns to match the order in which you would like to view the columns.

Figure 7. Column presentation order



- Column sort order (up/down)

  You can modify the panel height in case of vertically stacked panels to suit the screen resolution or viewing priorities.

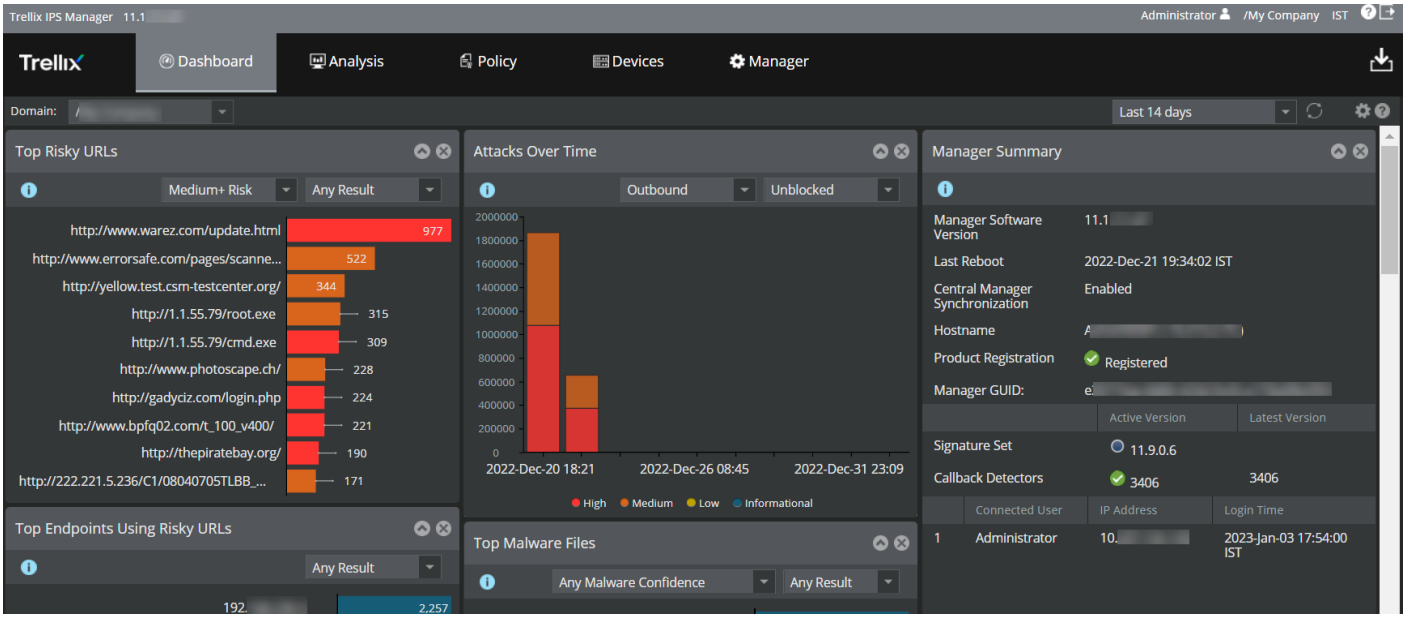
Any change made to the column persists even after you leave the page and/or log out, which means that the columns are displayed with the changes when you log into the account next time. The **Reset GUI Presentation** restores any changes made to the column or panel presentation to its default setting. To access the button, go to Manager → <Admin Domain Name> → Users and Roles → **My Account**. The reset of the settings is applicable for all the tables across the Manager. For the changes of the reset to take effect, you have to either log out and login back to the account or refresh the page.

Dashboard tab

The first page that you view after a successful logon to the Manager is the **Dashboard** page.

The **Dashboard** page is the central interface from which all Manager interface components are available. The **Dashboard** page is logically divided into two sections: the top Menu bar and the lower Monitors section.

Figure 8. Dashboard page



Dashboard Settings

The **Dashboard Settings** dialog enables you to further customize your **Dashboard** page view.

You can perform the following tasks here:

- **Monitors** — Use this option to add the monitors. The default category is **All**. Use the **Operational** or **Security** category to choose the monitors you want to view. You can also customize the data displayed in the monitors based on the admin domain and child domain. Monitors display data based on the admin domain selected from the **Domain** drop-down list.

  The following monitors are displayed under different categories: All, Operational, and Security monitors.

Category	Monitors	Description
All		View both Operational and Security monitors.
Operational		
	CPU Usage	View the high CPU usage of the Sensor.
	Device Summary	View the current versions of the Sensor software and signature set of the logged in domain.
	Manager Summary	View the Manager details such as software version, signature set version, and others.
	Memory Usage	View the high memory usage of the Sensor.
	Release Announcements	View the latest updates and the current version of signature set applied to your Sensor.
	Running Tasks	View the status of all the Sensors configured in the Manager.
	System Faults	View the health of your device and the Manager.

Category	Monitors	Description
	Throughput Usage	View the high throughput usage of the Sensor.
	NOTE Data remains unchanged for the **Manager summary**, **Release Announcements**, and **Running tasks** monitors irrespective of the admin domain selected. The **System Faults** and **Device Summary** monitors display the list of all the child domains linked to the admin domain selected.	
Security		
	Attack Severity Summary	View the unacknowledged alerts in the database, sorted by alert severity
	Attacks Over Time	View the attacks over a period of time in your network.
	Big Movers	View the attacks whose frequency has increased during a selected time period.
	Top Applications (IPS)	View the top applications based on attacks, bytes, or connections.
	Top Applications (NTBA)	View the top applications in the NTBA device based on bytes or connections. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top Attack Subcategories	View the attack subcategories in your network.
	Top Attacker Countries	View the top attacker countries in your network.
	Top Attackers	View the top attackers in your network.
	Top Attacks	View the top attacks in your network.
	Top Callback Activity	View the callback activity.
	Top Destinations (NTBA)	View the top destinations based on bytes or connections. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top Endpoint Executables (NTBA)	View the top executables based on number of endpoints using them or the number of attacks they have initiated. You can filter the executables based on the device, attacks (default) or endpoints, malware confidence, and classification. **NOTE** This monitor is populated only if you have enabled EIA integration.

Cate-gory	Monitors	Description
	Top Endpoints Using Risky URLs	View the top endpoints using risky URLs in your network.
	Top Files (NTBA)	View the top files based on malware confidence level. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top High-Risk Endpoints	View the high-risk endpoints of your network.
	Top Malware Files	View the top malware downloads in your network. You can filter malware based on their confidence and detections (blocked, unblocked, and all).
	Top Risky URLs	View the top risky URLs of your network.
	Top Sources (NTBA)	View the top sources based on bytes or connections. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top Target Countries	View the top target countries in your network.
	Top Targets	View the top targets in your network.
	Top URLs (NTBA)	View the top URLs at risk. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.

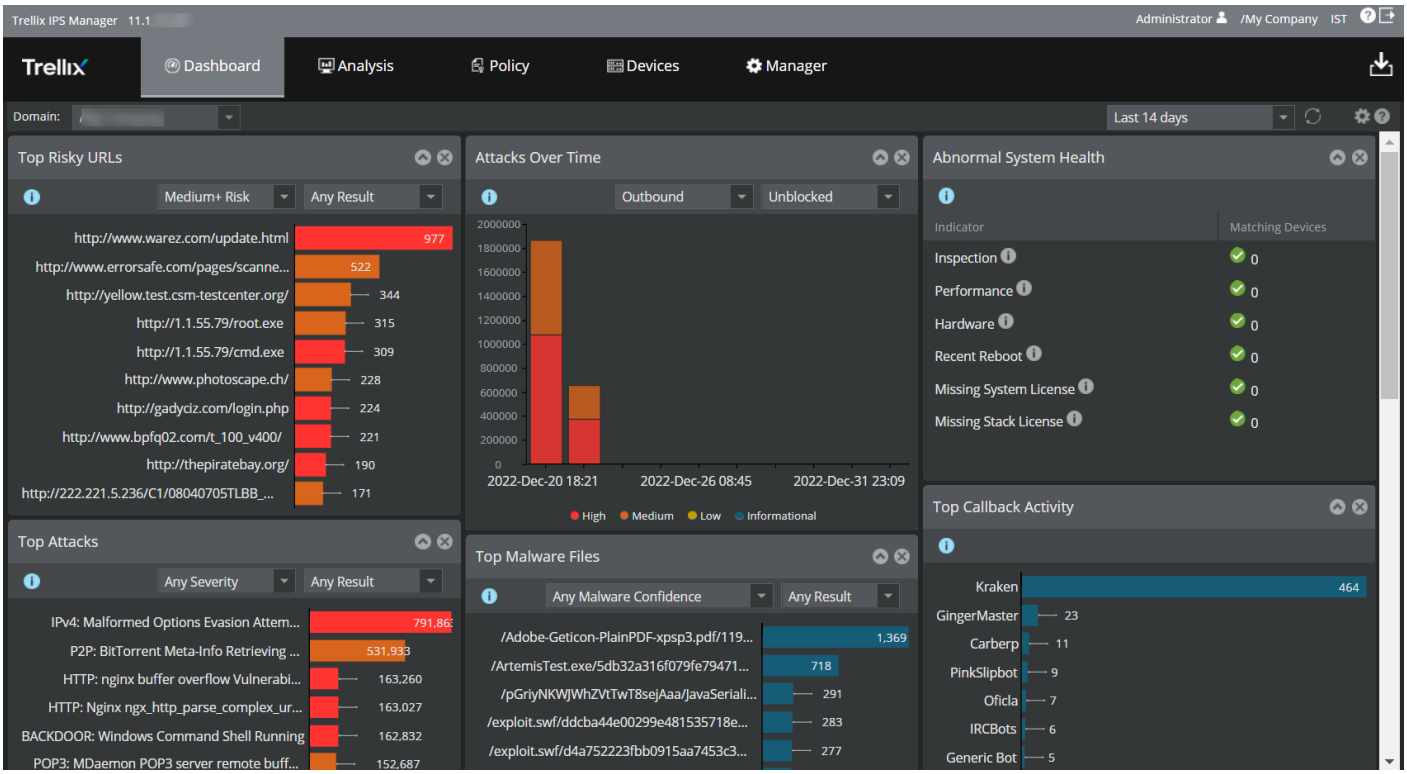
NOTE

The Dashboard displays only the top 10 unacknowledged alerts under each Security Monitor. To view the acknowledged alerts, go to the **Attack Log** page and select **Acknowledged** from the drop-down list. You can also select **Any Alert State** from the drop-down list, and the Manager will display both acknowledged and unacknowledged alerts.

- **Automatic Refresh** — Use this option to set the automatic refresh time. The default time is 10 minutes. The minimum and maximum time for the automatic refresh are 1 minute and 10 minutes, respectively. For a manual refresh, select **Disabled** to disable the automatic refresh.
- **Layout** — Use this option to customize the number of columns to be displayed in the **Dashboard** page. The default layout is 3 columns. The minimum and maximum number of columns that can be displayed are 2 columns and 4 columns, respectively.

The following figure shows the **Dashboard** with a three-column view.

Figure 9. Three-column view



- **Time Range** — Use this option to select the time range to set the time range for viewing data on the selected monitor.

  For example, if you select **Automatic Refresh** time as 10 minutes and the **Time Range** as 1 hour, then the information available for the selected monitor will be for the last 1 hour from the last refresh time. That is, if you select the **Time Range** at 9:30 AM, then you can view the data from 8:30 AM to 9:30 AM. But, as soon as the monitor is refreshed after 10 minutes, the data displayed on the **Dashboard** will be from 8:40 AM to 9:40 AM.

Analysis tab

The **Analysis** tab on the Menu bar enables you to perform network and events analysis.

The following table gives a high-level overview of the tab tree and the available options.

Item	Description
Attack Log	Analyze the alerts detected by your network security appliances.
Threat Explorer	View the top attacks, attackers, targets, and malware within a given period of time and a direction.
Malware Files	Monitor the potential malware downloads on the network and to view or export the related file reports.
Callback Activity	Analyze the callback activities participating in the damage of the endpoints including the background of the bot, the time till it was active, the IP address involved, and similar other useful information such as the host name, the operating system, and the user details.

Item	Description
High-Risk Endpoints	Monitor the suspicious endpoints infected by the malware by providing the name of the endpoint, the user details, and the operating system of the endpoint.
Network Forensics	Capture the network activity information and summarize them for user consumption.
Endpoint Executables	View the entire list of executables that makes network connections to either block or allow them. This item works only if at least one NTBA appliance is connected.
Quarantine	View the list of endpoints quarantined for all the Sensors
MITRE ATTACK View	View and analyze attacks and alerts detected by your network security appliances in the MITRE ATT&CK matrix format. **NOTE** This option is not available in Trellix IPS Central Manager.
Event Reporting	Generate and view the Next Generation and Traditional reports based on the analysis of the events and the network.

Policy tab

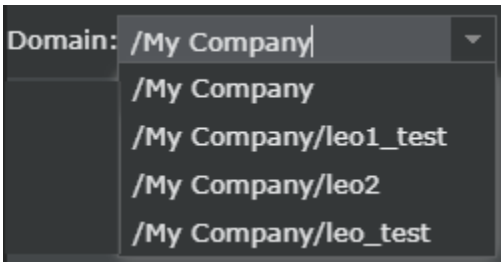
The **Policy** tab enables you to view, edit, and configure different policies when the corresponding options are selected.

The following table gives a high-level overview of the options available in the **Policy** tab tree.

Item	Description
Intrusion Prevention	Configure and manage the IPS policies that govern what traffic is permitted across your network, and how to respond to misuse of the network.
Network Threat Behavior Analysis	Configure and manage the Network Threat Behavior Analysis (NTBA) policies that monitor the network traffic.

You can also configure the policies at various domain levels by selecting your choice from the **Domain** drop-down list.

Figure 10. Domain option



This page enables you to view and manage all policies using a single tab.

Devices tab

The **Devices** tab helps you to manage and configure your devices. The navigation pane has the following sub-tabs:

- **Global** — Manage different functionalities related to the devices like failover pairs, add and remove devices, and others.
- **Devices** — Manage individual device-specific configuration.

  When there are no devices added, a text is displayed as **No Device Managed (Add)**. You can add a device by clicking on the **Add** link.

> **NOTE**
>
> When a new device is added and the trust is established, the device does not get listed in the drop-down list unless you click on the Refresh button on the **Devices** tab.

Global sub-tab

The following table gives a high-level overview of the available options under the **Global** sub-tab:

Item	Description
Device Manager	Information about all the devices configured in the Manager including the health and status of the devices are displayed.
Common Device Settings	Configure the several device settings like **Name Resolution**, **Gateway Anti-Malware Engine updating**, and **Performance Monitoring**.
IPS Device Settings	Apply inheritable global settings to added IPS devices
NTBA Device Settings	Apply inheritable global settings to added NTBA devices

Devices sub-tab

The following table gives the high-level overview of the options displayed in the left navigation pane of the **Devices** sub-tab:

Item	Description
Summary	View the essential details about the device.
Deploy Pending Changes	Deploy the configuration changes to your devices.
Setup	Manage the device by allowing you to configure the physical ports, adjust the time zone, configure the proxy server, NTBA integration, Quarantine, and other similar important functions.
Maintenance	Maintain your device by providing the options to shut down, reboot, import and export configuration.
Troubleshooting	View the device debugging information and logs, current performance monitoring configuration, Denial of Service, and other related essentials to manage your device.
IPS Interfaces	Configure the policies at the interface and sub-interface levels.

Manager tab

The **Manager** tab allows you to set up and maintain activities for your Trellix IPS deployment.

The following table gives a high-level overview of the available options in the tab tree.

Item	Description
Summary	View the summary of the Manager and its status.
Updating	View important information regarding the update and upgrade of the software.
Users and Roles	Add users and assign roles to them thereby granting the users specific privileges to use every security resource deployed in your deployment.
Setup	Create the admin domains and child admin domains, view the alert notifications, configure Manager Disaster Recovery (MDR) pair, etc.
Integration	Manage and configure the integration of Trellix IPS with other products like Trellix ePO - On-prem, Trellix Global Threat Intelligence, and others.
Reporting	Generate configuration reports to view your current software and signature versions, the configuration and status of a Sensor, policy settings, and so forth.
Maintenance	Maintain your device by archiving, pruning, backing up your data, and others.
Troubleshooting	View all the product-specific announcements, the system logs, and system faults. This also gives the details about background processes initiated by administrative users, alert relevance analysis, MDR pair switchover events, Manager policy cache, and helps you to audit the actions of administrative users on the Manager.

View Reports

The **Event Reporting** and **Reporting** menus enable you to produce a range of reports for both the alert information reported to your Manager, as well as information pertaining to your configuration settings. IPS reports are summaries of alert information, such as severity, impact category, source/destination IP, time of alert, and so forth. Configuration reports detail information such as the current Manager and Sensor software versions, proxy server settings, and so forth.

To view the Reports:

Steps:

1. From the **Analysis** tab, click **Event Reporting**. You have the following reports:
    - Next Generation Reports
    - Traditional Reports
2. From the **Manager** tab, click **Reporting**. You have the following options:
    - Configuration Reports
    - Report Automation
    - Preferences

Manager Summary

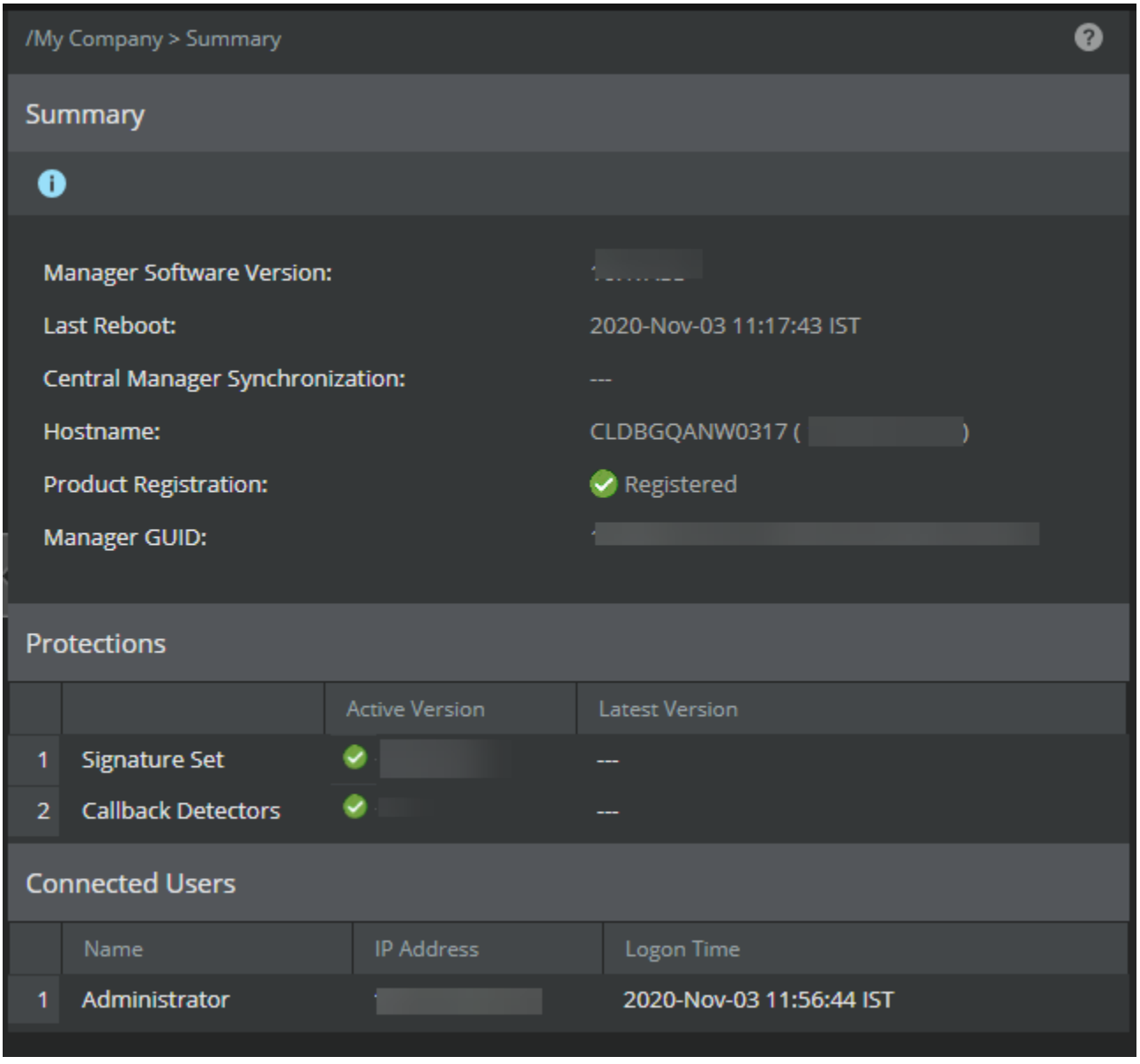
The **Summary** page enables you to view the summary details of the Manager/Central Manager. You can also perform the **Product Registration** here.

View summary details of the Manager

To view summary details of the Manager, do the following:

In the Manager, select Manager → <Root Admin Domain Name> → **Summary**.

The **Summary** page displays.



Status	Description
Manager Software Version	Displays the current Manager software version.
Last Reboot	Specifies the most recent time the Manager service was started

Status	Description
Central Manager Synchronization	Displays the synchronization status of the Central Manager with the Manager.
Host Name	Displays host name and IP address of the Manager server (if host name is not available, only the IP is displayed)
Manager GUID	Displays the unique identifier of the Manager server
Product Registration	Displays if the Manager is registered with Trellix or not.
Protections	Displays the signature set and callback detectors information.
Signature Set	Displays the active **Signature Set** version available in Manager and the latest **Signature Set** version available for download
Callback Detectors	Displays the active **Callback Detectors** version available in Manager and the latest **Callback Detectors** version available for download
Connected Users	Displays the current open Manager user sessions information.
Name	Displays the user of the Manager session.
IP Address	Displays the client machine IP address used to access the Manager.
Logon Time	Displays the start time stamp of the Manager session.
Register Product	Allows you to register the Manager with Trellix. **NOTE** This option is available if your Manager instance unregistered only.

Product Registration

The Manager should be registered with Trellix for receiving automatic updates regarding the signature set, callback detectors, and device software from Trellix in real-time.

At a higher level, the Manager registration with Trellix is a two-step procedure as follows:

1. Obtain the Trellix IPS Registration Key (page 61).
2. Register the Manager instance with Trellix (page 61).

Trellix recommends you register the product immediately after installation when the **Product Registration** window appears after the initial login.

Upon skipping product registration, the following functionalities will be disabled:

- On-demand and scheduled download of Signature Sets in the Manager
- On-demand and scheduled download of Callback Detectors in the Manager
- On-demand download of device software
- Creating vIPS Components and vIPS Protected Groups

On registering the Manager with Trellix, general setup information will be sent to Trellix Research Labs when when **Telemetry** is enabled. The purpose of Telemetry is to facilitate you in providing helpful information to Trellix Trellix about your usage of Trellix vIPS solution so that Trellix in turn optimizes your protection.

NOTE

Telemetry is enabled in the Manager by default. You can change the telemetry configurations from the Manager → <Admin Domain Name> → Setup → **Telemetry** page.

Obtain the Trellix IPS Registration Key

To obtain the Trellix IPS Registration Key, perform the following steps:

Steps:

1. Go to the Trellix Download Server.
2. Login using your **Grant Number** and registered **Email Address**.

   NOTE

   If you do not have a **Grant Number** provided by Trellix, contact Trellix Technical Support and request for a trial **Grant Number**.

   The **My Products** page opens.
3. Make a note of the **Trellix IPS Registration Key**.

   NOTE

   The **Trellix IPS Registration Key** is unique to each customer. For example, if Customer A has two grant numbers, 1234 and 5678, the **Trellix IPS Registration Key** is the same for both of these grant numbers as the registration keys are generated per customer.

Register the IPS Manager with Trellix

To register your Manager with Trellix, do the following:

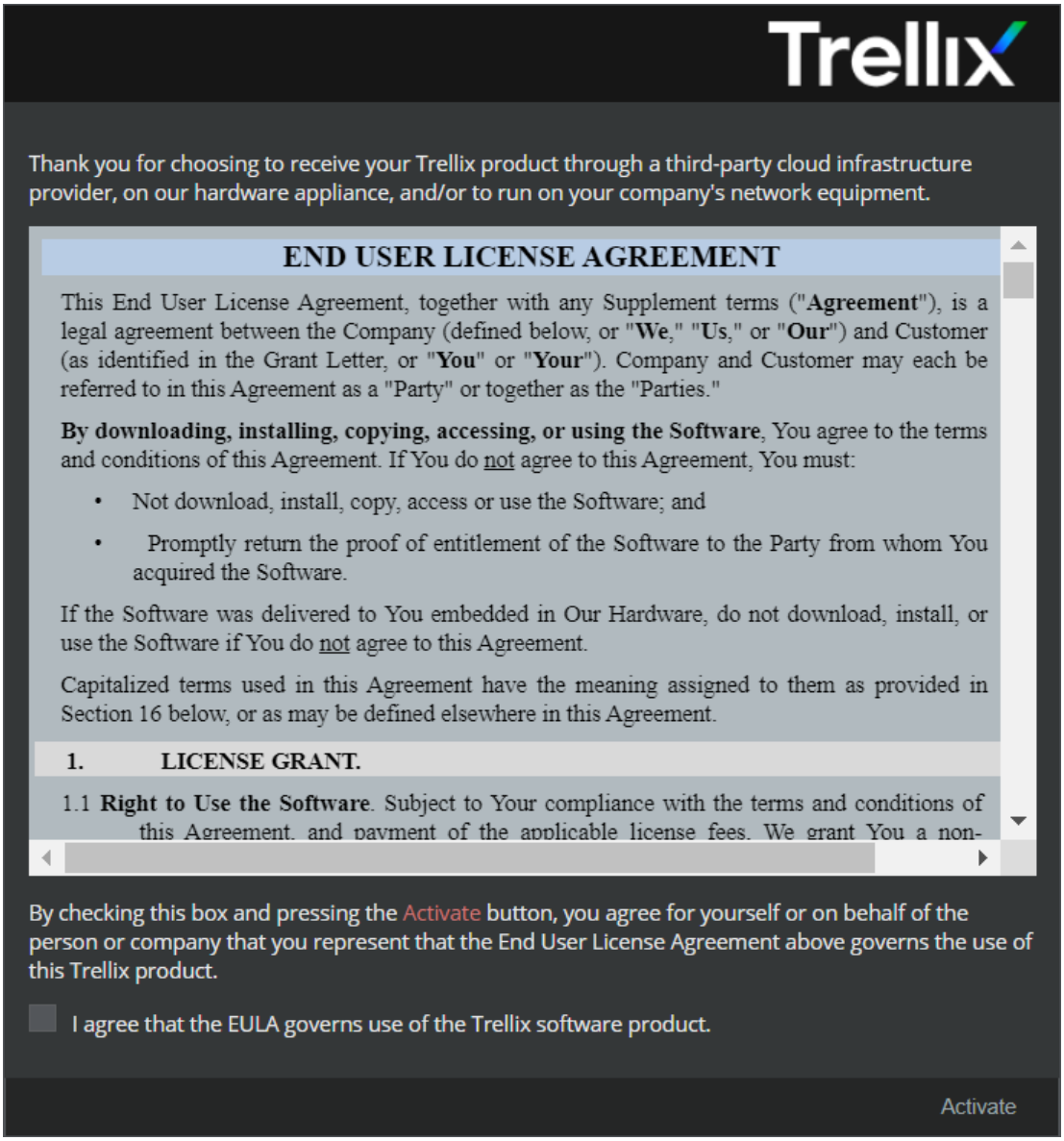
Obtain the Product Registration Key from the Trellix Download Server.

NOTE

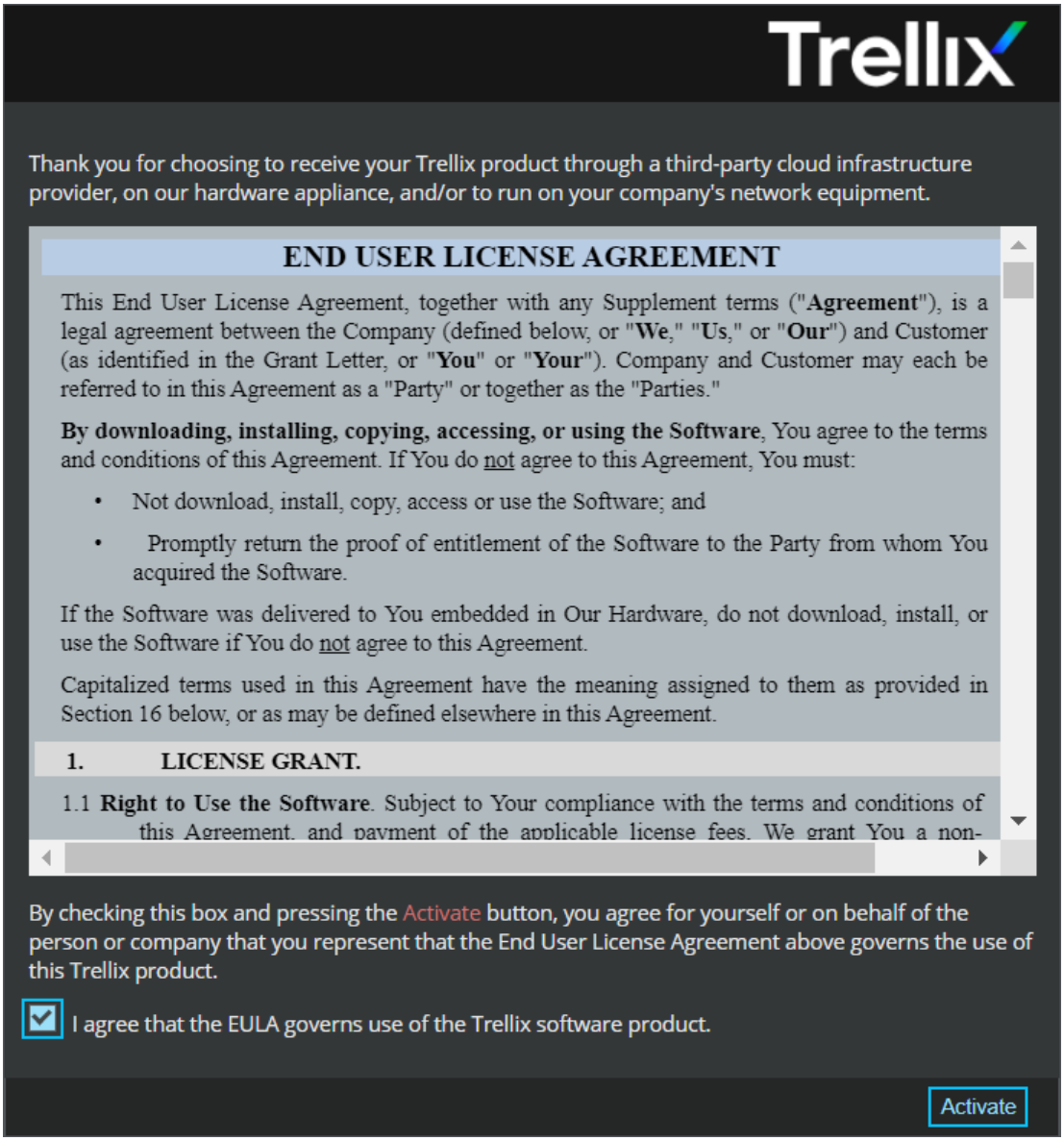
If you have skipped the **Product Registration** during initial login after installation or upgrade, go to Manager → <Admin Domain Name> → **Summary** (Manager → **Summary** in Central Manager), click **Register Product**, and follow the below procedure from step 3 to register the Manager.

1. Log in to the Manager.

   The **End User License Agreement** opens.



2. Select the checkbox and click **Activate**.



NOTE

Trellix recommends you perform **Product Registration** immediately after the initial login. If you do not want to register the Manager, click **Skip**.

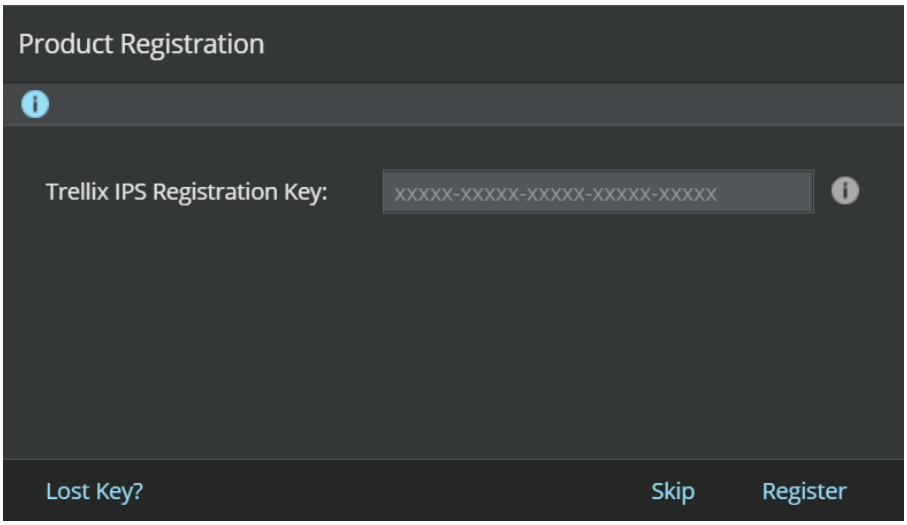
NOTE

When the Manager is not registered with Trellix, the following features are automatically disabled:

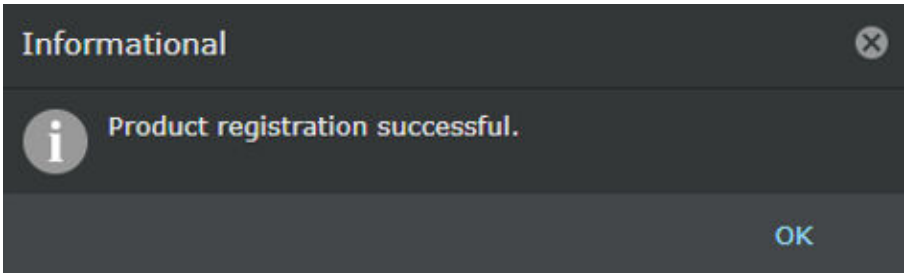
- Download Signature Sets
- Download Callback Detectors
- Download Device Software
- Signature Sets Automatic Updating
- Callback Detectors Automatic Updating

3. The **Product Registration** dialog box appears.

   In case you do not have the registration key readily available, click **Lost Key?** to procure the registration key.



4. Enter the **Trellix IPS Registration Key** and click **Register**.
5. Once the **Product Registration** is complete, an **Informational** dialog box appears with success message.



Trellix IPS Protection Status

The **Trellix IPS Protection Status** page contains the following tabs:

- **Signature Sets** — Download the required signature sets or schedule automatic download from the Update Server to the Manager. You can also schedule automatic deployment from the Manager to devices.

- **Callback Detectors** — Download the required callback detectors or schedule automatic download from the Update Server to the Manager. You can also schedule automatic deployment from the Manager to devices.
- **Device Software** — Download the required Sensor or NTBA Appliance software image file from the Update Server to the Manager.
- **GAM Automatic Deployment** — Schedule and deploy Gateway antimalware engine updates automatically from the Manager to the Sensors under all domains after the manual import of the required .upd file.
- **Manual Import** — Manually import downloaded Sensor or NTBA Appliance software image and signature files to the Manager.

  The Manager allows you to manually import the following device updates from the file system if your Manager deployment has no access to internet.

  - Device software (.jar)
  - Signature set (.ivu or .jar)
  - Callback detectors (.zip)
  - Gateway antimalware updates (.upd)
- **Release Announcements** — View and delete messages related to operating system updates, signature set release, Manager software update, and others.

You can manually download and import the latest software and signatures for the Sensor and the NTBA Appliance. You can also schedule automatic downloads and imports.

IMPORTANT

Make sure you are connected to the internet while downloading and updating antimalware software and signatures. If you are on an air-gap network, refer to the section Offline Signature Set Downloader (page 72).

NOTE

You can perform only one download or upload at a time from any Trellix IPS component, including the Update Server.

Signature set deployment optimization

The Manager/Central Manager is enhanced to reduce the compilation and deployment time of the signature set. The compilation time is the duration required by the Manager to create the signature set file to be deployed to the Sensor. The deployment time is the sum of compilation time - the time required to transfer signature set file from the Manager to the Sensor and the time required to apply the signature set file to the Sensor. The reduction in signature set compile/deploy time reduces the duration of signature set processes in the Manager.

NOTE

To achieve faster signature set compilation/deployment, the Sensor software version must be running on software version 11.1 or above.

The following table provides the test conditions for the Signature set compilation/deployment enhancement:

For example, in a Windows 2022 Manager server with 8 CPU cores, 500 GB HDD, and 32 GB RAM, the time consumed for signature set based processes before and after the signature set deploy and compile enhancement are as follows:

Task Manager server specifications	Policies	Sensor models
VM-based Windows 2022 32GB RAM 8 x 2.6 GHz CPU cores 500GB Hard Disk Drive 16 GB allocated for JVM (by default)	**IPS Policy**: Default Testing with 1000 UDS and Default malware policy **Advanced Malware Policy**: All Malware Engines Enabled	NS-series Sensors Virtual IPS Sensors
Linux based Manager server appliance 64GB RAM 20 CPU cores 1 TB Hard Disk Drive 16 GB allocated for JVM (by default)		

The following table provides the test results for the Signature set compilation/deployment enhancement:

Task	Reduction in time required to complete the task
Manager Installation/Upgrade/Restart	70-80 %
Manual import of a signature set	50-60 %
(Optional) Test compilation of one snort or UDS attacks	70-80 %
(Optional) Saving one thousand snort or UDS attacks	70-80 %
Deploy the signature set to the Sensors	50-60 %
Failover pair Sensor software upgrade using the Manager GUI	25-35 %

For example, consider you are deploying or upgrading the Manager, followed by a manual signature set upgrade, and deployment of Sensor software and signature set to the Sensors. The total downtime required for the completion of these tasks is reduced proportionally according to the percentage in the above table as applicable in your network. If you have any user-defined or snort attacks configured, the time required to Test Compile or Save these attacks is also reduced considerably.

The Sigperf.log file available under the System files tab in the Manager → <Admin Domain Name> → Troubleshooting → **Logs** page provides a detailed log regarding the signature set process in the Manager with the time stamp.

NOTE

The above ranges are obtained from the Trellix test environment and may differ from your network depending on parameters like the internet speed, geo-location, Sensor models, etc.

Automatically updating signature sets and callback detectors

The Manager allows you to schedule the download of the signature set and callback detectors. Once configured, the scheduler downloads the signature set and callback detectors from Trellix IPS Update Server to the Manager. For example, every one hour, the Manager verifies the Trellix IPS Update Server and downloads the new file uploads.

The success/failure of the import process is indicated through fault notifications, emails, and SNMP traps.

Once the new signature set and callback detectors are available on the Manager, they can be scheduled to be deployed on your devices.

A proxy server is provided for all internet communications. You can manage the proxy server and know the proxy details from the scheduler page.

For more information on automatically updating signature sets, refer to Automatic download of signature sets (page 70).

For more information on automatically updating callback detectors, refer to Automatic download of callback detectors (page 76).

Signature sets

The **Signature Sets** option enables you to download available attack signature updates on demand from the Update Server to the Manager server. You can then push the signature download onto your Sensors or NTBA Appliance. You can also download the latest signature sets from an offline utility **`OfflineSigsetDownloader`**. For more information, see Offline Signature Set Downloader (page 72).

TIP

Because incremental emergency signature sets can be downloaded with regular signature sets, you do not need to use the custom attack definitions feature to import late-breaking attacks.

The **Signature Sets** option not only allows you to import regular signature sets, but also incremental emergency signature sets that include attack signatures not yet available in regular signature sets.

Incremental emergency signature sets are meant to address late-breaking attacks that might need to be addressed immediately.

Emergency signature sets are non-cumulative and can only add new signatures, so they do not contain a full set of signatures.

To make sure that you have a complete set of signatures, Trellix IPS verifies to see if a required regular signature set is missing and downloads it before downloading the related emergency signature set.

NOTE

You must use the **Automatic Download** option of **Signature Sets** tab from Manager → <Admin Domain Name> → **Trellix IPS Protection Status** for Trellix IPS to download a required regular signature set automatically, before downloading an emergency signature set. You receive an error if you try to import an emergency signature set through the **Manual Import** tab. For more information about **Automatic Download**, refer to Automatic download of Signature sets (page 70).

When a signature file or version is downloaded, the version is displayed in the **Active Manager Version**. Setting a schedule enables the Manager to verify the Update Server for signature updates on a periodic basis, download the available updates, and push these updates to your Sensors or NTBA Appliances without your intervention.

NOTE

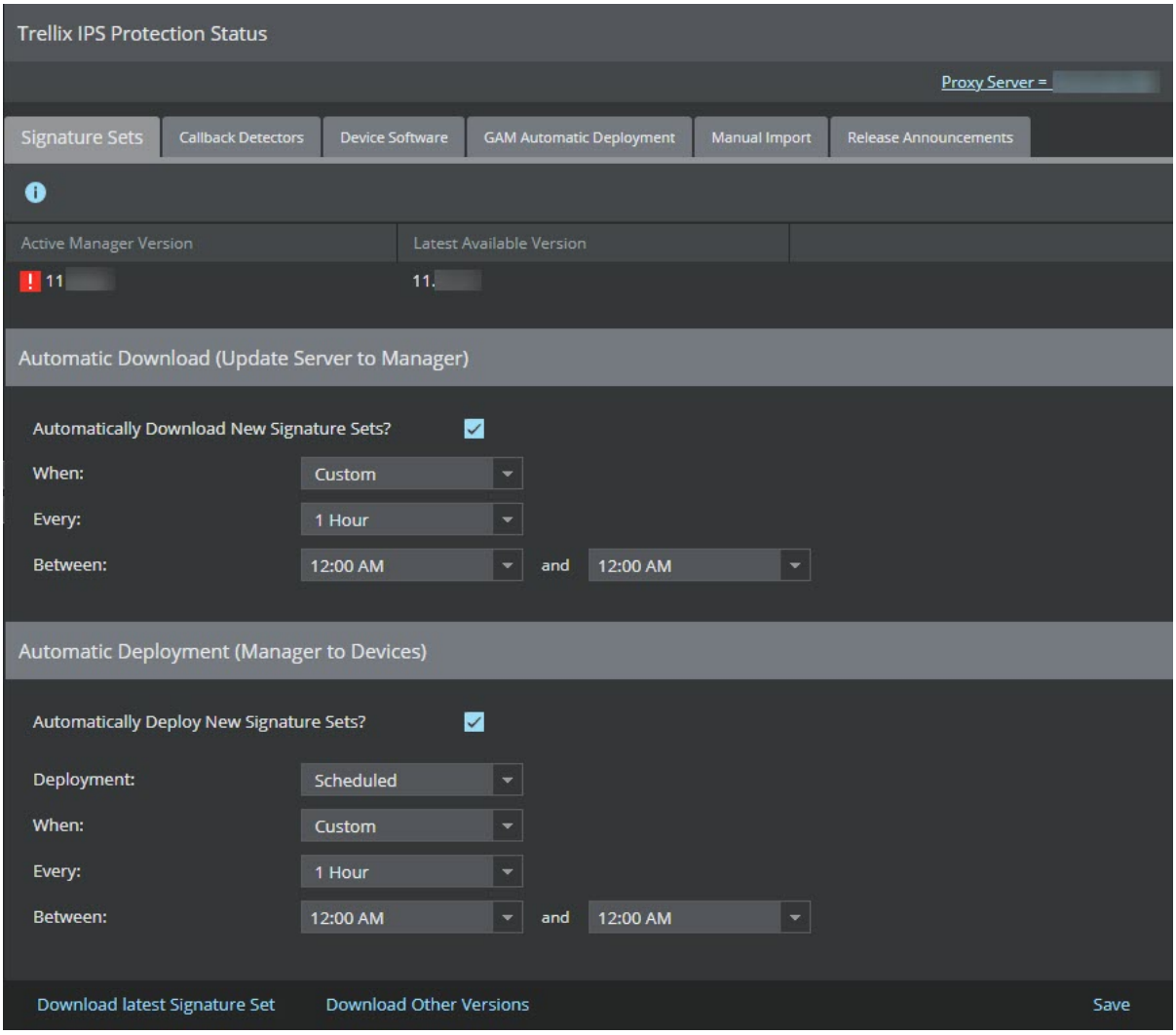
The signature set's major version (i.e, its first two digits) should be equal to or higher than the IPS Manager's major version (i.e, its first two digits) for it to be compatible with the Manager. Starting from 11.1 Update 2 or later, the Manager performs validation based on the signature set file's major version being equal to or higher than its major version and thus prevents the download or manual import of any incompatible signature set version that does not match the validation criteria.

For example, any Manager running on version 11.1 Update 2 supports the download and deployment of signature set version 11.9.x.x, but not signature set version 10.8.x.x or 9.8.x.x. In case of an incompatible signature set file download or its manual import, an error message is displayed on the Manager UI. You can find more details about the error from the ems.log file, or check for the same log entries on the Manager → <Admin Domain Name> → Troubleshooting → Logs → **System Files** tab.

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Signature Sets** tab. The **Signature Sets** tab is displayed.
   - The **Active Manager Version** displays currently available version for your Sensors or NTBA Appliances.
   - The **Latest Available Version** displays the latest available version for your Sensors or NTBA Appliances to download. This signature set is kept in a queue for download to your Sensors or NTBA Appliances. You can only have one version in the queue for download.

   NOTE

   You can also change the display settings to meet your requirements from the filter option.



2. To download the latest signature set, select **Download Latest Signature Set**.

   A **Confirmation** dialog box appears, select **OK**. A status window opens to process the signature download.

3. To download other versions of signature set, select **Download Other Versions**.

   The **Download Specific Signature Set** dialog box appears, it displays the update details such as **Release Date** and **Size (MB)** for that particular **Version**.

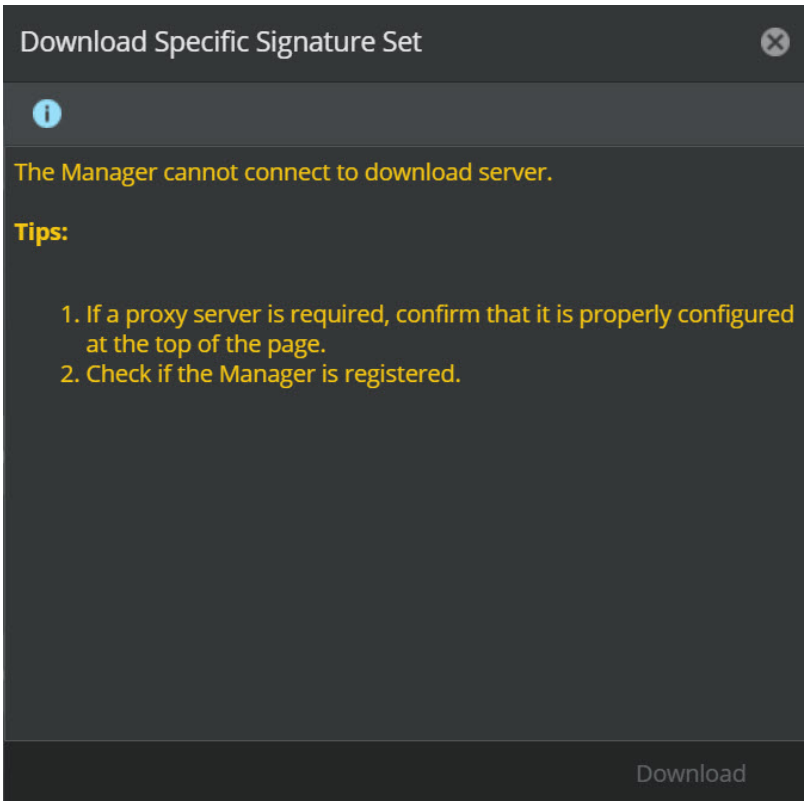
   Select the required version and click **Download**. A status window opens to process the signature download.

   - If the active manager version is the latest available version, **Download Latest Signature Set** is disabled.
   - A icon is displayed beside the **Active Manager Version** if the active signature set version matches the latest signature set version.
   - A icon is displayed beside the **Active Manager Version** if the active signature set version is older than the latest signature set version.

NOTE

In an air-gap network, unregistered, or proxy server disabled Manager:

- The **Latest Available Version** is displayed as **---**.
- A icon is displayed beside the **Active Manager Version**.
- When you select **Download Other Versions**, the **Download Specific Signature Set** does not display the available versions of signature sets.



Automatic download of signature set

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Signature Sets** tab.

   The **Signature Sets** tab is displayed.

2. In the **Automatic Download (Update Server to Manager)**, schedule automatic downloads of signature set by entering the relevant details.

Option	Definition
Automatically Download New Signature Sets?	Enabling it activates the automatic download. By default, it is disabled.

Option	Definition

When	Frequency for the Manager to poll the Update Server. The following options are displayed in the drop-down list:
	• **Daily**: To download new signature sets daily. Set the time at which the download must occur.
	• **Weekly**: To download new signature sets weekly. Set the day of the week and time at which the download must occur.
	• **Custom**: To customize the interval at which the downloads must occur. The following options are displayed:
	  • **Every**: Set the recurrence of time for the Manager to poll the Update Server.
	  • **Between**: Set the time range at which the download must occur.

3. Click **Save**.
4. In the **Automatic Deployment (Manager to Devices)**, schedule automatic deployments of signature sets by entering the relevant details.

Option	Definition
Automatically Deploy New Signature Sets?	Enabling it pushes the updates directly from the Manager to Sensor. By default, it is disabled.

Deployment	The following options are displayed from the drop-down:
	• **Immediate (after download)**: To deploy the signature set immediately after the download.
	• **Scheduled**: To schedule the deployment of signature set. Choosing this provides, **When** option.
	From the **When** option, customize the interval at which the deployment must occur. The following options are displayed in the drop-down list:
	• **Daily**: To deploy new signature sets daily. Set the time at which the deployment must occur.
	• **Weekly**: To deploy new signature sets weekly. Set the day of the week and time at which the deployment must occur.
	• **Custom**: To customize the interval at which the deployments must occur. The following options are displayed:
	  • **Every**: Set the recurrence of time for the devices to poll the Manager.
	  • **Between**: Set the time range at which the deployment must occur.

5. Click **Save**.

To deploy signature set manually to Sensors, see Deploy pending changes to a device (page 88).

NOTE

If the Manager is not registered, **Automatic Download (Update Server to Manager)** prompts **Product registration is required to use this feature**.

Offline Signature Set Downloader

Points for considerations:

Consider the following points before you use this offline utility:

- Download the **offline signature set downloader** from the Trellix Download Server.
- Make sure Java is installed in your machine.
- Internet connection is required to download the latest signature set to the client machine.

`OfflineSigSetDownloader` is an offline utility used to download the latest signature sets from the Trellix IPS Update Server. It displays the 5 latest signature sets available to download. The downloaded file will be available within the **sigsetdownloader** folder. In an air-gap network, the downloaded signature set file can be copied from a remote machine with internet connection to the Manager server.

NOTE

The downloaded signature set file can be uploaded into any Manager version.

To download the latest signature set from Trellix IPS Update Server, perform the following steps:

1. Go to **`<filepath>\OfflineSigSetDownloader`**
2. Run **`OfflineSigSetDownloader.bat`** for a Windows client.

   Run **`OfflineSigSetDownloader.sh`** for a RedHat Linux like CentOS client.
3. Enter "**y**" if you want to configure proxy details and "**n**" if not.

   If yes (**y**), enter the proxy server IP address or hostname, port number, and user credentials (optional) details when prompted.
4. Enter the signature set version that you want to download from the list of latest signature sets available.

NOTE

You can press **Enter** to download the latest version by default.

The signature set file (.ivu) gets downloaded to folder **sigsets**. The **sigsets** folder gets created within the **sigsetdownloader** folder.

Lite Signature Set

The Lite signature set is a lightweight version of the signature set, a version moderated by Trellix IPS researchers. This is to make sure the oldest signatures are excluded without posing an appreciable risk to modern day attacks. Exclusion of older signatures allows you to continue updating your Sensors with the latest attack signatures while keeping the memory use relatively low.

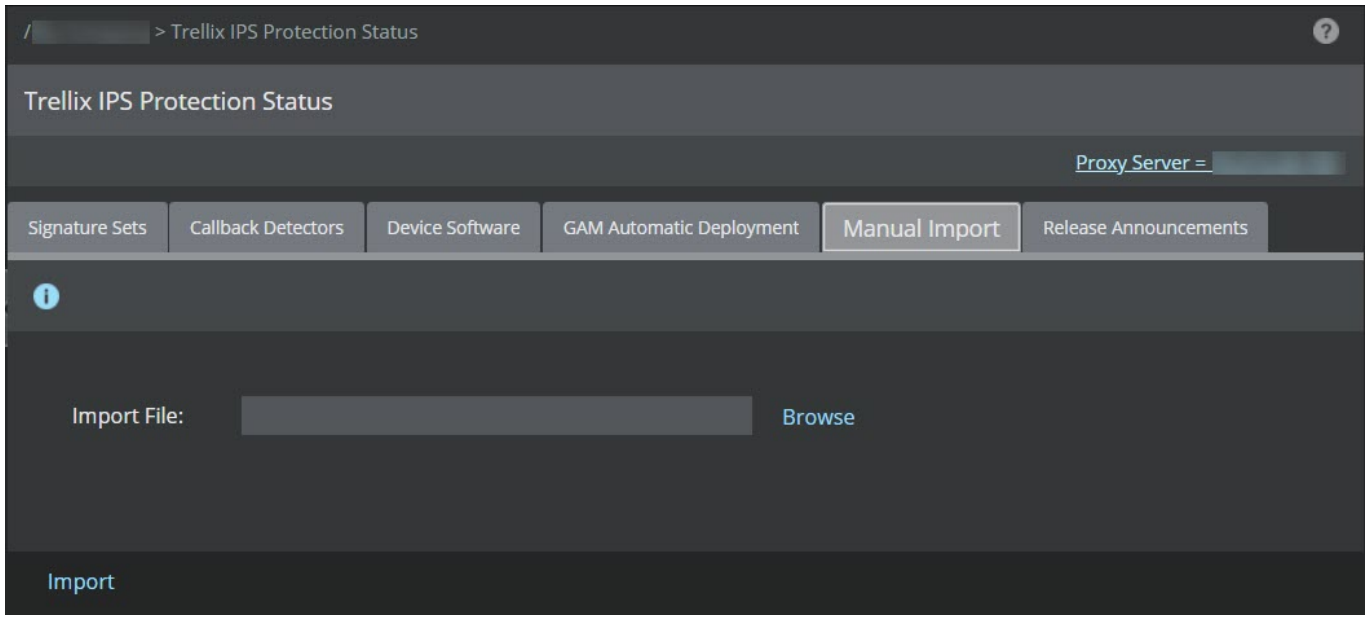
NOTE

The lite signature sets are available only in the Download Server upon entering your Grant number.

Following are the steps to update the signature set with the lightweight version:

1. Download the Lite signature set file (.ivu) from the Trellix Download Server.
2. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Manual Import** tab.

   The **Manual Import** tab is displayed.



3. Click **Browse** and choose the file on your system or a network location and then click **Import**.
4. Download the Sensor software version in the Manager.

   For more information about downloading the Sensor software version, see Device software (page 78).
5. Deploy the pending changes when both the Sensor software upgrade file and the Signature Set Lite is available in the Manager.

   For more information about deploying pending changes, see Deploy pending changes to a device (page 88).

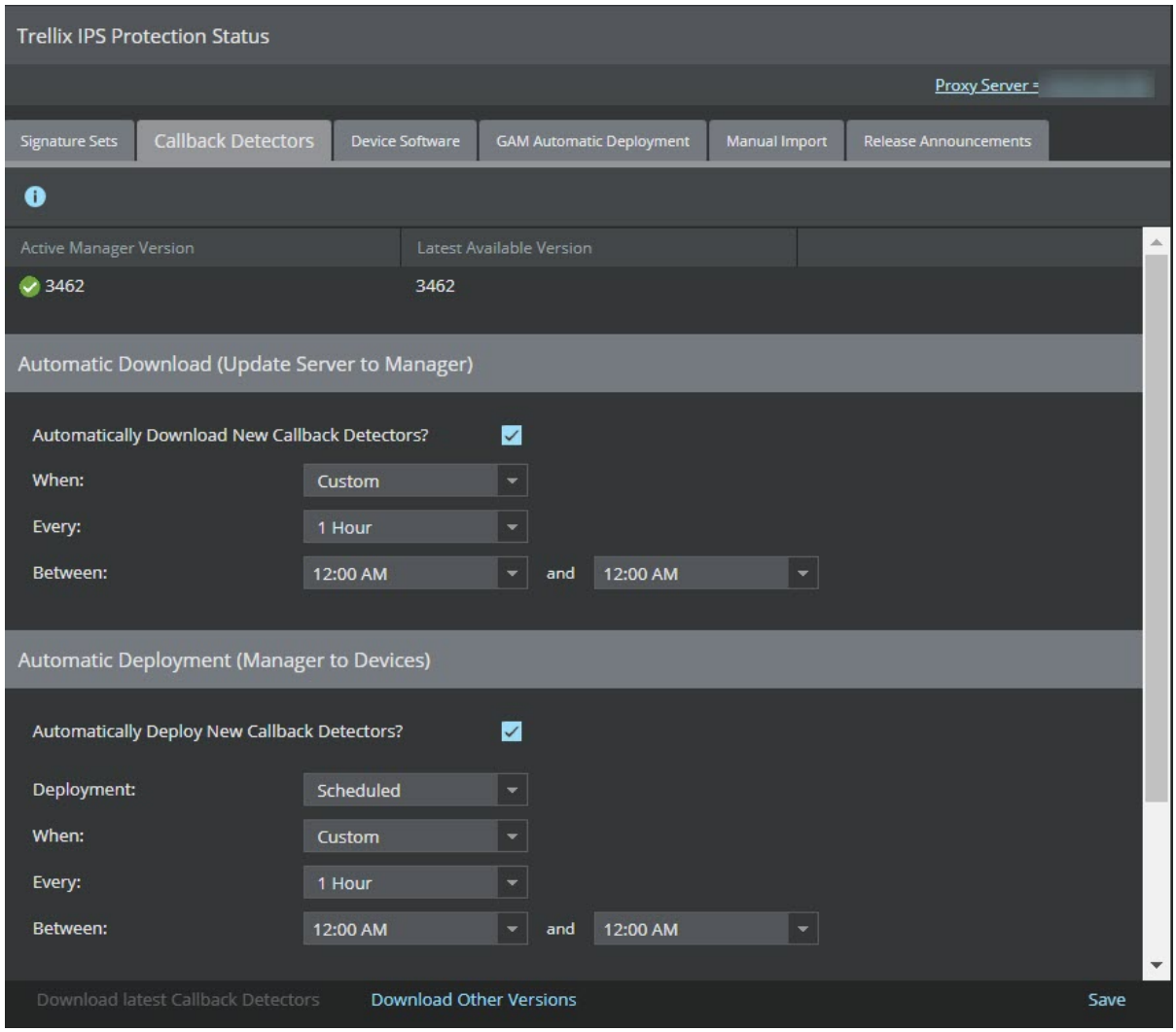
Callback detectors

You can download callback detectors and push it to the Sensor.

Steps:

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Callback Detectors** tab. The **Callback Detectors** tab is displayed.
   - The **Active Manager Version** displays currently available version.
   - The **Latest Available Version** displays the latest available version for you to download.

> **NOTE**
>
> You can also change the display settings to meet your requirements from the filter option.



2. To download the latest callback detectors, select **Download Latest Callback Detectors**.

   A **Confirmation** dialog box appears, select **OK**. A status window opens to process the signature download.

3. To download other versions of callback detectors, select **Download Other Versions**.

   The latest 10 versions are available for you to download. It displays the update details such as the **Release Date** and **Size (MB)** for that particular **Version**.

4. Select the version required and click **Download**.

   The selected callback detectors become the active callback detectors on the Manager.

   To automatically download the callback detectors, refer to Automatic download of callback detectors (page 76).

   You can also view the active and latest callback detectors version in the **Manager Summary** monitor of the Manager Dashboard. In the **Device Summary** monitor, you can view the callback detectors version on specific devices.

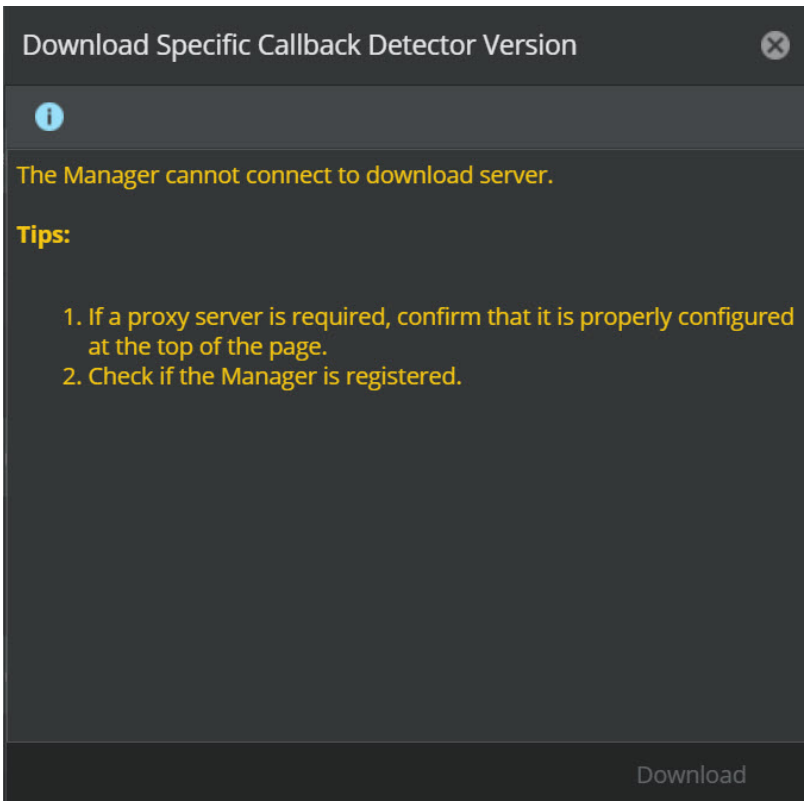
   - If the active manager version is the latest available version, **Download Latest Callback Detectors** is disabled.
   - A icon is displayed beside the **Active Manager Version** if the active callback detector version matches the latest callback detector version.

- A icon is displayed beside the **Active Manager Version** if the active callback detector version is older than the latest callback detector version.

NOTE

In an air-gap network, unregistered, or proxy server disabled Manager:

- The **Latest Available Version** is displayed as **---**.
- A icon is displayed beside the **Active Manager Version**.
- When you select **Download Other Versions**, the **Download Specific Callback Detector Version** does not display available versions of callback detectors.



Automatic download of callback detectors

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Callback Detectors** tab. The **Callback Detectors** tab is displayed.
2. In the **Automatic Download (Update Server to Manager)**, schedule the automatic download of callback detectors by entering the relevant details.

Option	Definition
Automatically Download New Callback Detectors?	Enabling it activates the automatic download. By default, it is disabled.

When	Frequency for the Manager to poll the Update Server. The following options are displayed in the drop-down list:
	• **Daily**: To download new callback detectors daily. Set the time at which the download must occur.
	• **Weekly**: To download new callback detectors weekly. Set the day of the week and time at which the download must occur.
	• **Custom**: To customize the interval at which the downloads must occur. The following options are displayed:
	  • **Every**: Set the recurrence of time for the Manager to poll the Update Server.
	  • **Between**: Set the time range at which the download must occur.

3. Click **Save**. A status window opens to process the download.
4. In the **Automatic Deployment (Manager to Devices)**, schedule the automatic deployment of callback detectors by entering the relevant details.

Option	Definition
Automatically Deploy New Callback Detectors?	Enabling it activates the automatic download. By default, it is disabled.

Deployment	The following options are displayed from the drop-down:
	• **Immediate (after download)**: To deploy the callback detectors immediately after the download.
	• **Scheduled**: To schedule the deployment of callback detectors. Choosing this provides, **When** option.
	From the **When** option, customize the interval at which the deployment must occur. The following options are displayed in the drop-down list:
	• **Daily**: To deploy new callback detectors daily. Set the time at which the deployment must occur.
	• **Weekly**: To deploy new callback detectors weekly. Set the day of the week and time at which the deployment must occur.
	• **Custom**: To customize the interval at which the deployments must occur. The following options are displayed:
	  • **Every**: Set the recurrence of time for the devices to poll the Manager.
	  • **Between**: Set the time range at which the deployment must occur.

5. Click **Save**. A status window opens to process the download.

> **NOTE**
>
> If the Manager is not registered, then, **Automatic Download (Update Server to Manager)** prompts **Product registration is required to use this feature**.

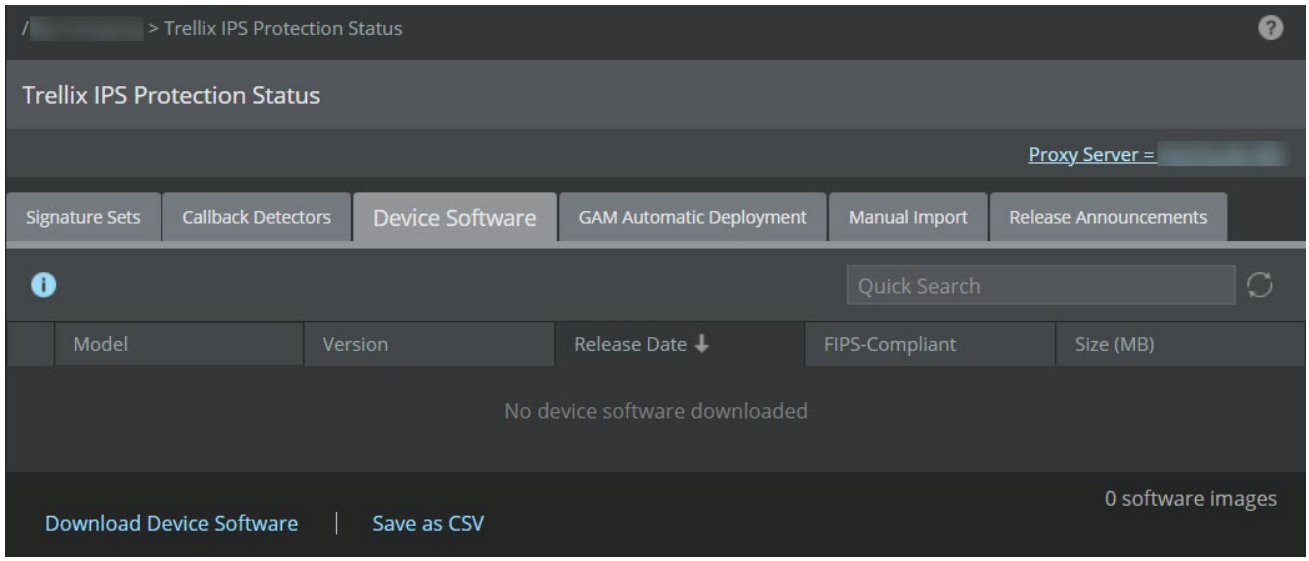
Device software

You can download the available Sensor software and NTBA Appliance updates on demand from the Update Server. If more than one version is available, select the most recent version.

Automation enables the Manager to verify the Update Server for software updates on a periodic basis.

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Device Software** tab.

   The **Device Software** tab is displayed.

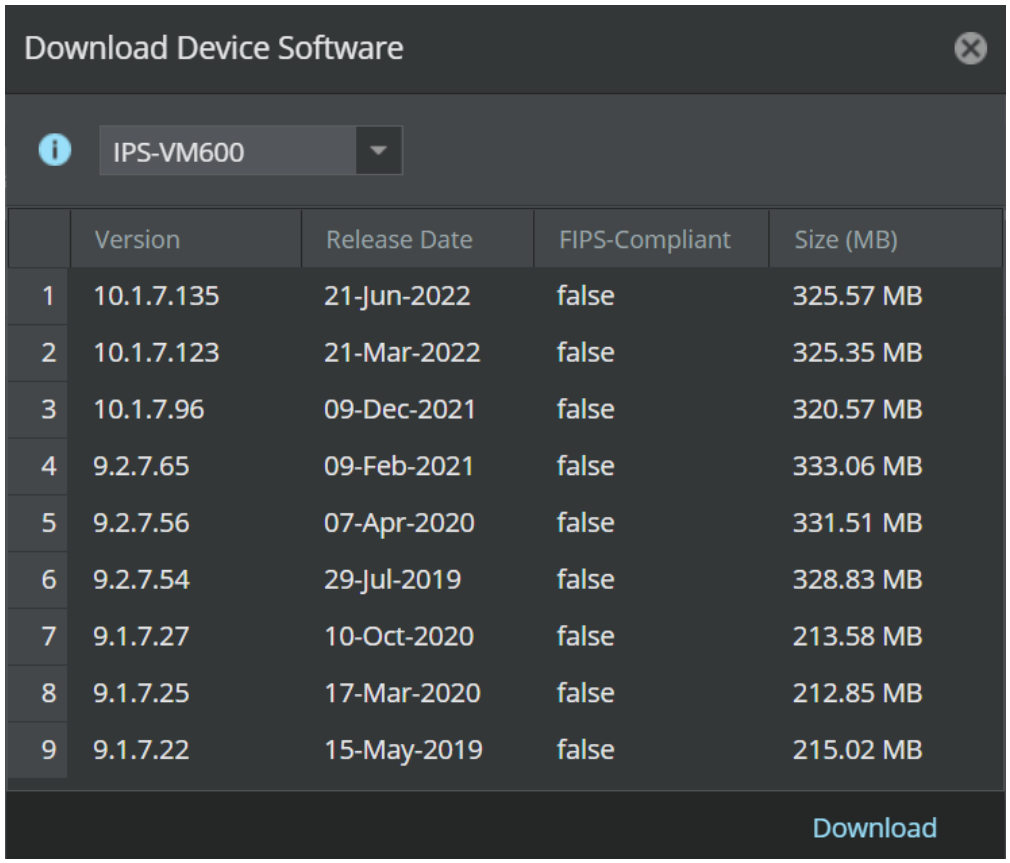


   It displays the details of downloaded device software such as **Model**, **Version**, **Release Date**, **FIPS-Compliant**, and **Size (MB)**.

   To download the details of downloaded device software, select **Save as CSV**. You can also view the total available software images.

2. To download the required device software, select **Download Device Software**.

   The **Download Device Software** dialog-box appears. It displays the details, such as **Version**, **Release Date**, **FIPS-Compliant**, and **Size (MB)**.



NOTE

If you download the **Device Software** directly from the Update Server, the **Release Date** is available in **DD-MMM-YYYY** format. When you manually import the **Device Software**, the date is displayed in **MMM-YYYY** format.

3. Select the Sensor model from drop-down. Then, select the required version of the device software.

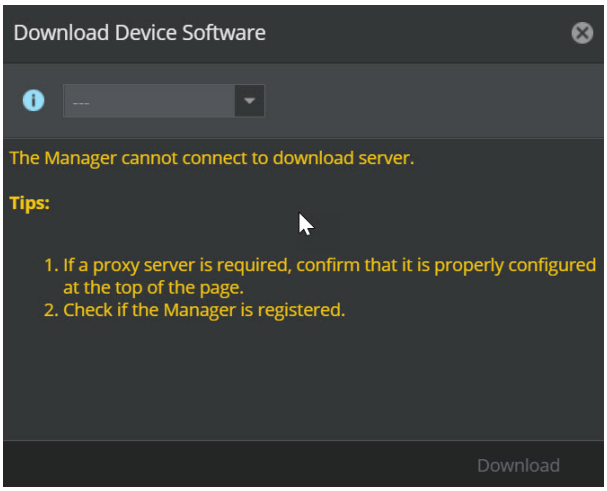
NOTE

Only the latest three Sensor software versions for 10.1 and 11.1 releases will be available for download, provided the releases are supported by the selected Sensor model.

4. Click **Download** to download the software updates.

NOTE

In an air-gap network, unregistered, or proxy server disabled Manager, **Download Device Software** does not display any details of the available software version.



Use the **Deploy Device Software** option to deploy these software updates. For more information, see the [Trellix Intrusion Prevention System Installation Guide].

WARNING

The Sensor functionalities remain unaffected when a new software image is pushed from the Manager to Sensor during an upgrade. However, to upgrade to the new software, a Sensor reboot is required. During the reboot, the Sensor functionalities will be unavailable.

Automatic deployment of GAM updates

The **GAM Automatic Deployment** tab enables you to configure and deploy Gateway antimalware updates to the attached devices across all domains automatically when you upload the required GAM update file to the Manager. You can schedule the automatic deployment of new GAM updates to the Sensors at any time of your preference using this tab. If you are in an air-gap network, the downloaded GAM update file (.upd) can be copied to the Manager server using a remote machine with internet connection.

When GAM update is scheduled for auto-deployment, any new GAM file imported to the Manager using the **Manual Import** tab will be pushed to multiple Sensors at once, which includes Sensors in a fail-open pair, Sensors in a stack, and stacked HA Sensors, as per the configuration made. The automatic deployment of GAM files works even when the Manager is not registered with Trellix, or in a proxy-disabled state. If the Managers are in an MDR pair, the deployment of the GAM file will occur as configured on the Primary Manager.

NOTE

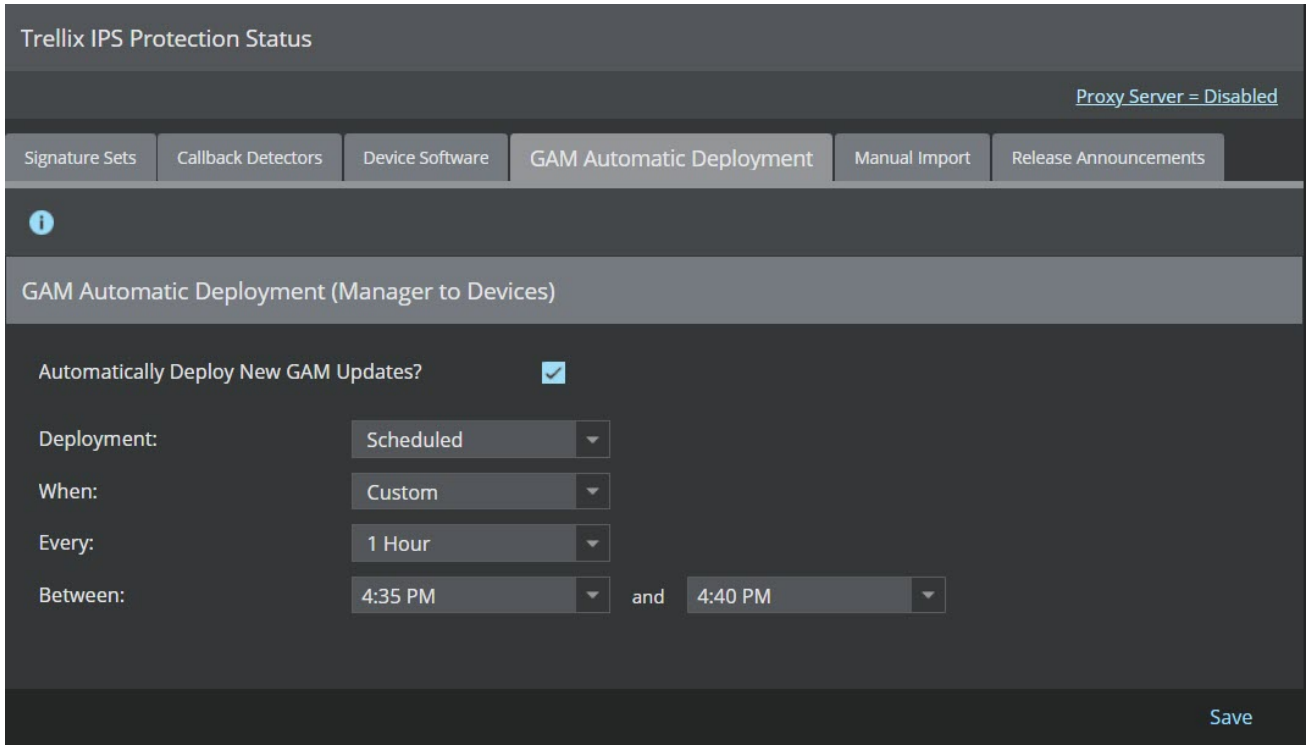
The automatic deployment of GAM updates is not applicable to NTBA or virtual NTBA devices.

Perform the following steps to configure and schedule the automatic deployment of GAM updates:

1. Navigate to Manager → <Admin Domain Name> → Trellix IPS Protection Status → **GAM Automatic Deployment**.

   The **GAM Automatic Deployment** tab is displayed.

Figure 11. GAM Automatic Deployment tab



2. In the **GAM Automatic Deployment (Manager to Devices)** section, configure auto-deployment of the GAM updates by entering the relevant details as given in the table below.

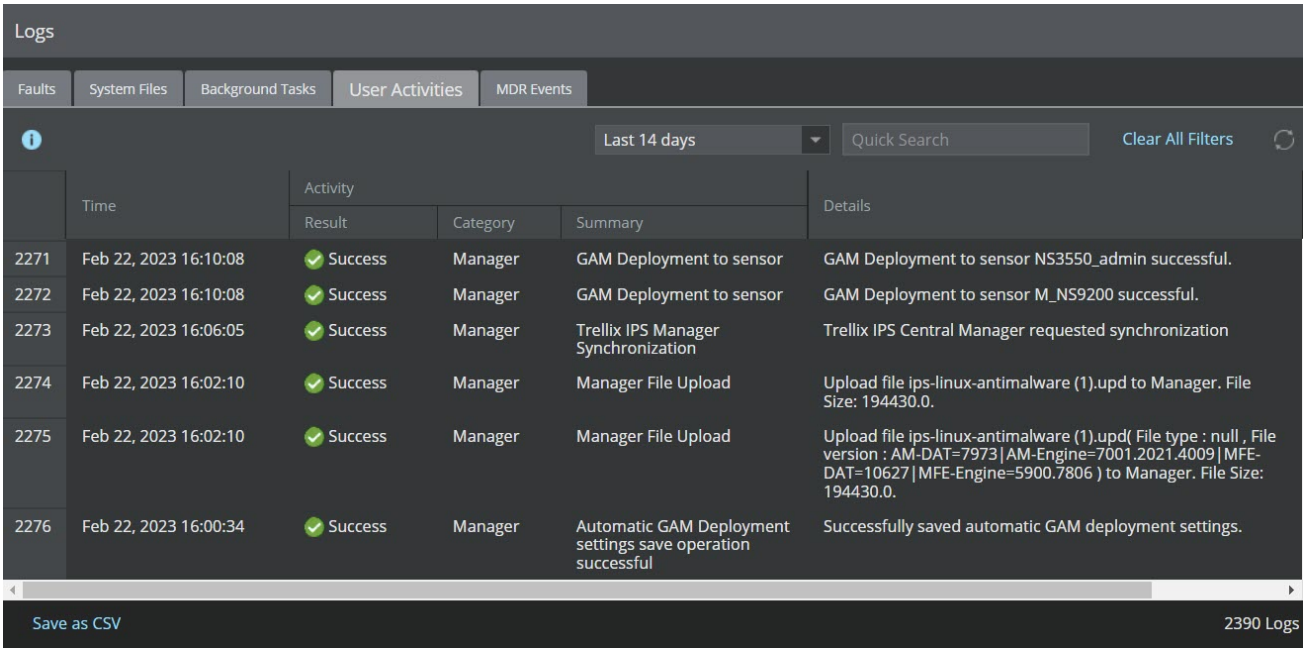
Option	Definition
Automatically Deploy New GAM Updates?	Enabling it activates the automatic deployment option. By default, it is disabled.

Option	Definition
Deployment	The following options are displayed in the drop-down: • **Immediate (after download)**: To deploy the GAM file immediately after it is uploaded on the Manager. **NOTE** When this option is configured, new GAM updates will be auto-deployed to all Sensors that are attached to the Manager at that point of time. If any Sensor is attached to the Manager after the GAM file has already been imported to the Manager, users need to re-import the file for the new GAM updates to be auto-deployed to those Sensors. • **Scheduled**: To schedule the deployment of new GAM file. Choosing this provides the **When** option. From the **When** option, customize the interval at which the deployment must occur. The following options are displayed in the drop-down list: • **Daily**: To deploy new GAM update file daily. Set the time at which the deployment must occur. • **Weekly**: To deploy new GAM update file weekly. Set the day of the week and time at which the deployment must occur. • **Custom**: To customize the interval at which the deployment must occur. The following options are displayed: • **Every**: Set the recurrence of time for the devices to poll the Manager for the deployment. The options available are **1 Hour**, **2 Hours**, **4 Hours**, **8 Hours**, and **12 Hours**. • **Between**: Set the time range at which the deployment must occur.

3. When it is configured, click **Save**.

When GAM updates have been scheduled for automatic deployment, you can check the deployment status on the **User Activities** tab under Manager → <Admin Domain Name> → Troubleshooting → **Logs** after importing the GAM update file (.upd) to the Manager.

Figure 12. User Activities tab showing audit logs related to automatic GAM deployment



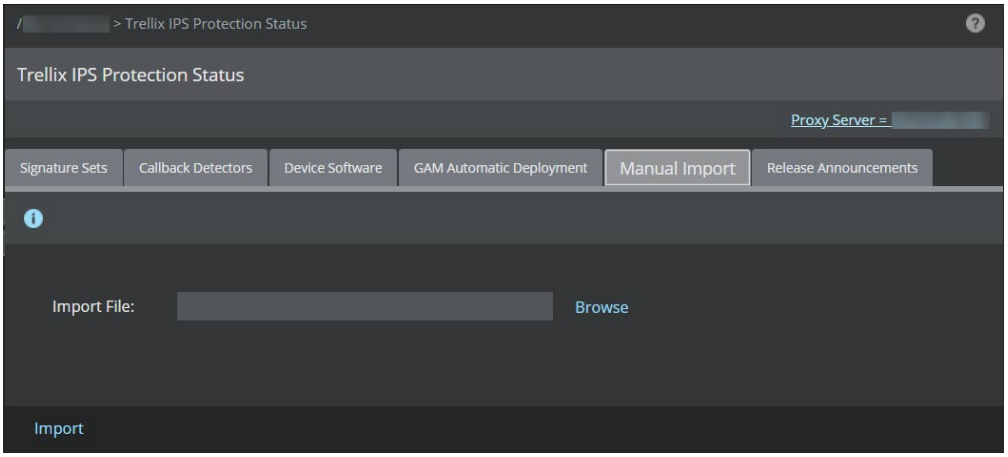
If you wish the deploy the GAM updates on a specific device or selected devices, you can do so from Devices → <Admin Domain Name> → Devices → <Device Name> → **Deploy Pending Changes** page, or from Devices → <Admin Domain Name> → Global → **Device Manager** page. For more information, refer to the section Update Gateway Anti-Malware Engine manually (page 954).

Manually import device updates

The Manager allows you to manually import the following device updates from the file system if your Manager deployment has no access to internet.

- Device software (.jar)
- Signature set (.ivu or .jar)
- Callback detectors (.zip)
- Gateway antimalware updates (.upd)

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Manual Import** tab. The **Manual Import** tab is displayed.



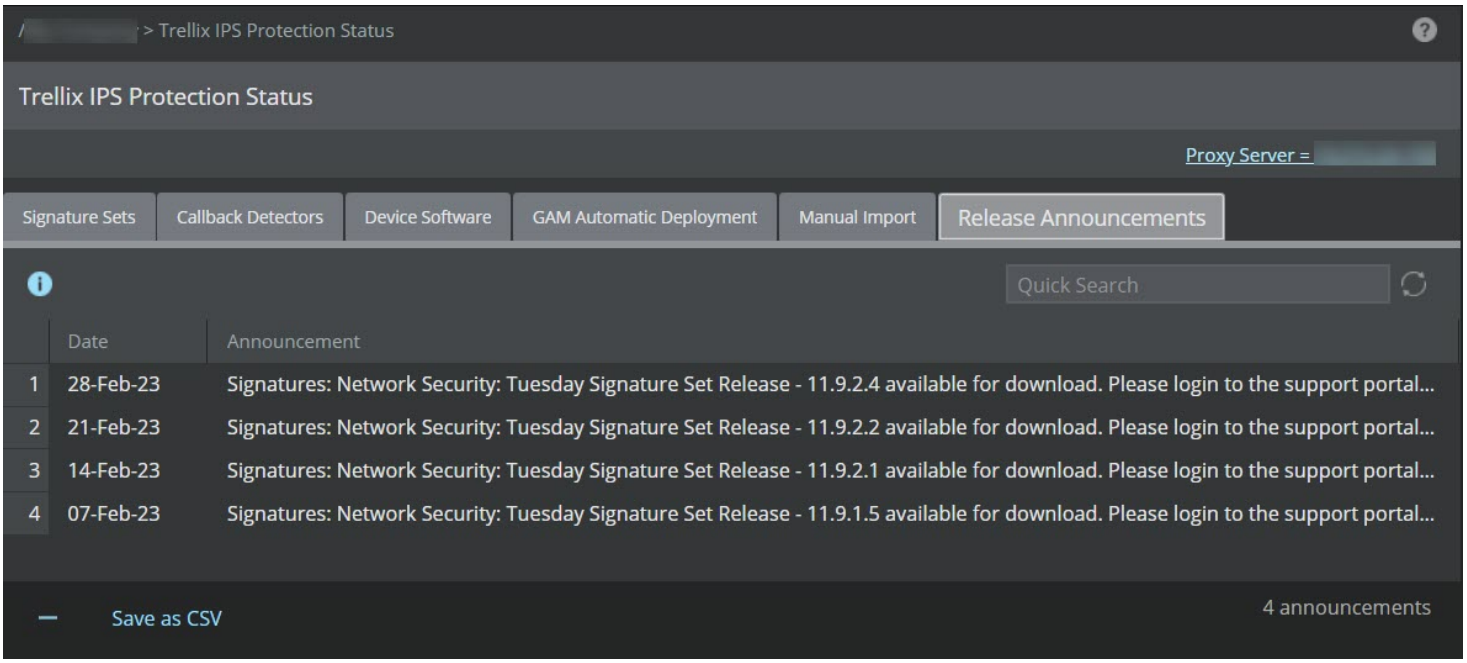
2. Click **Browse** and choose the file on your system or a network location and click **Import**.

   Later, do a configuration update for the corresponding Sensors.

   The Manager audits the import process. The success or failure can be verified in the audit messages.

Release Announcements

The **Release Announcements** tab enables you to view any product or security-related messages. To view the messages, select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Release Announcements** tab. The **Release Announcements** tab is displayed.



The messages can be related to operating system updates, signature set release, Manager software update, and others. The Manager verifies the Trellix IPS Update Server for such messages every 15 minutes and it displays messages that are relevant to the version of Manager and signature set that you are using.

This feature makes sure that all relevant messages from the Trellix IPS support team reach you on time. Because the new messages are displayed on the homepage and **Release Announcements** tab, the chances of you missing any message are remote.

The Manager displays the release date and the message description of the relevant messages on the **Release Announcements** tab. The release date is the date on which the message was posted on the Update Server. You can delete the messages that you have already seen with option and it is not listed again. To download these messages, select **Save as CSV**. You can also view the total available announcements.

The latest four unacknowledged messages are displayed on the Manager **Dashboard** page as well. Click **View All Messages** on the **Dashboard** page to navigate to the **Release Announcements** tab where all messages are displayed that are not deleted.

NOTE

Though all users can view the messages, only users with the role of Super User in the root admin domain can delete messages.

NOTE

In the Manager, child admin domain users can view only the last four messages displayed in the **Dashboard** page.

Update the latest software images on all devices

You can download the available Sensor software updates on demand from Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Select **Device Software** tab. Then, select **Download Device Software**. If more than one version is available for download, select the most recent version. For example, if multiple versions, such as 11.1.1.4, 11.1.1.5, and 11.1.1.6 are available for download, Trellix recommends you download version 11.1.1.6. The latest version of software always contains the changes included in all previous releases. If needed, you can also downgrade your Sensor by choosing from the list of available versions.

The Manager allows you to simultaneously download software images to all your Sensors listed under the **Devices** node. The Manager also provides an option to concurrently perform the Sensor upgrade by selecting the specific Sensor under Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → **Deploy Device Software**. For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Maintenance → **Deploy Device Software**.

NOTE

Once the software is updated in the Sensor, you must reboot all updated Sensors.

To download a software update, do the following:

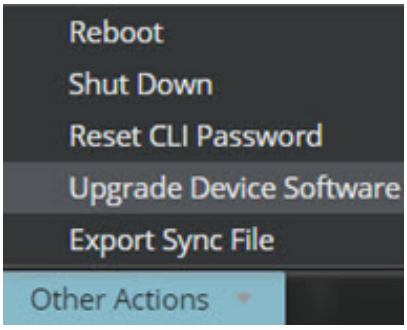
Steps:

1. Go to Devices → <Admin Domain Name> → Global → **Device Manager**.

   The **Device Manager** page is displayed.

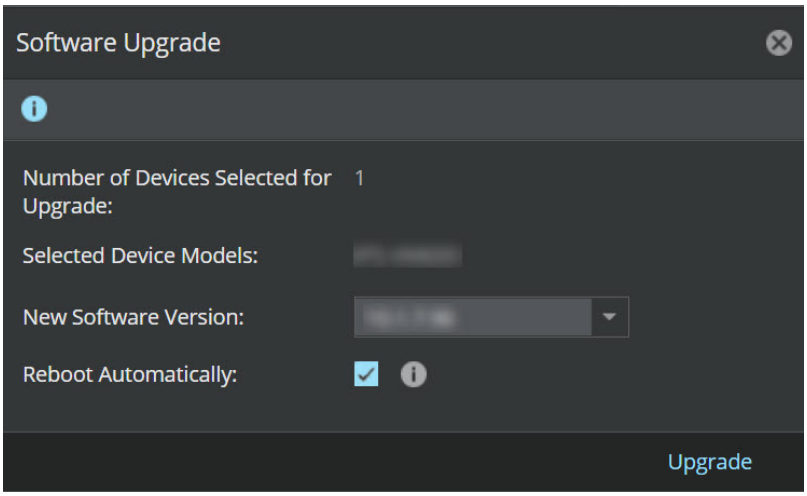
2. Select the **Sensors** tab.
3. From the list, select the required Sensor.

   The Manager also provides an option to concurrently perform the software upgrade for multiple Sensors using same model and software version.
4. Select **Upgrade Device Software** from **Other Actions** drop-down.



The **Software Upgrade** dialog box is displayed.

Figure 13. Software Upgrade dialog box

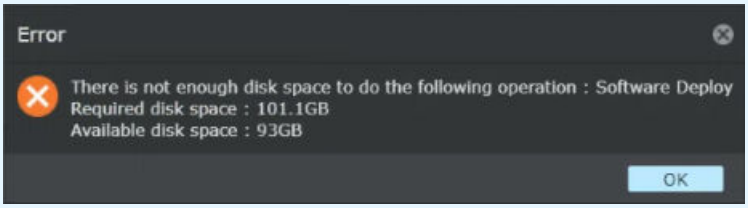


5. Select the **New Software Version** to be downloaded to the Sensor from the drop-down.

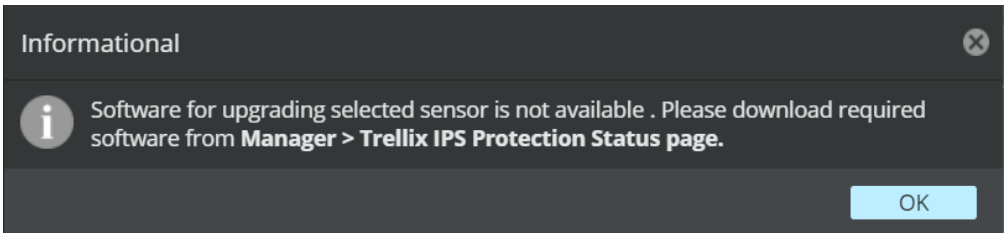
NOTE

- You can only view the downloaded device software versions.
- The Manager reserves 100 GB under required free disk space for Manager operations and considers an additional file size of 1.2 GB to be generated for each software deployment request. Upon receiving the request (single or in bulk), it checks the number of Sensors selected, and calculates the free disk space. If there is insufficient free disk space, an error message is displayed in the UI stating the available disk space and the space required to complete the upgrade task. This enables the Manager to reserve sufficient disk space to keep other processes running and avoid any software upgrade failure scenario.

Figure 14. Error message displayed for device software deployment if there is insufficient disk space



For the Sensor, if required software version is not downloaded in the Manager, an **Informational** dialog box is displayed.



6. To automatically push the Sensor for reboot, enable **Reboot Automatically**.

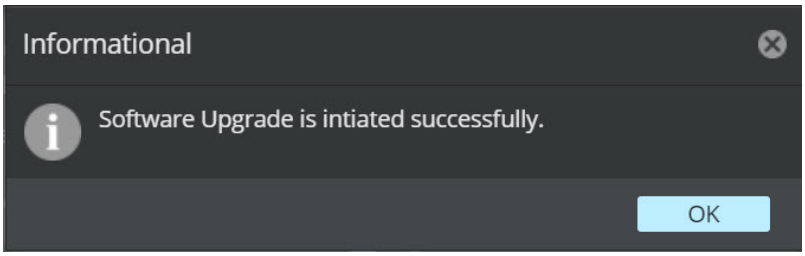
NOTE

By default this option is enabled. If required, it can be disabled.

For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.

7. Click the **Upgrade** to initiate the process.

An **Informational** dialog box is displayed to provide the status update. Click **OK**.



The **Last Upgrade** section of **Device Details** column provides the time stamp of last upgrade performed.

To view the software upgrade status, go to **Upgrade Status** section of **Device Details** column. You can also view the status from **Background Tasks** tab of Manager → <Admin Domain Name> → Troubleshooting → **Logs**.

The following statuses are displayed:

Status	Definition
 **Successful**	When the Sensor upgrade is successful.
 **In-progress**	When the Sensor is upgrading to the latest software version.
 **Failed**	When the Sensor upgrade fails.
---	When no upgrade is performed.

8. The **Export Sync File** from **Other Actions** drop-down is used to update and export files for offline Sensors.

Deploy pending changes to a device

When you make any configuration changes or policy changes on the Manager, or a new/updated signature set is available from Trellix, you must apply these updates to the devices (such as Sensors and NTBA Appliances) in your deployment for the changes to take effect.

Note the following:

- Configuration changes such as port configuration, non-standard ports, and interface traffic types are updated regardless of the changes made to the Sensor, interface/ subinterface.
- NTBA configuration updates refer to the changes done in the several tabs of the **Devices** node.
- Policy changes are updated on the Sensor or NTBA Appliance in case of a newly applied policy, or change made to the current enforced policy.
- Signature updates contain new and/or modified signatures that can be applied to the latest attacks.
- When policy and rule updates are applied to the devices, the current traffic analysis is not impacted until the last phase of configuration updates (i.e the Manager status update is at 95%).

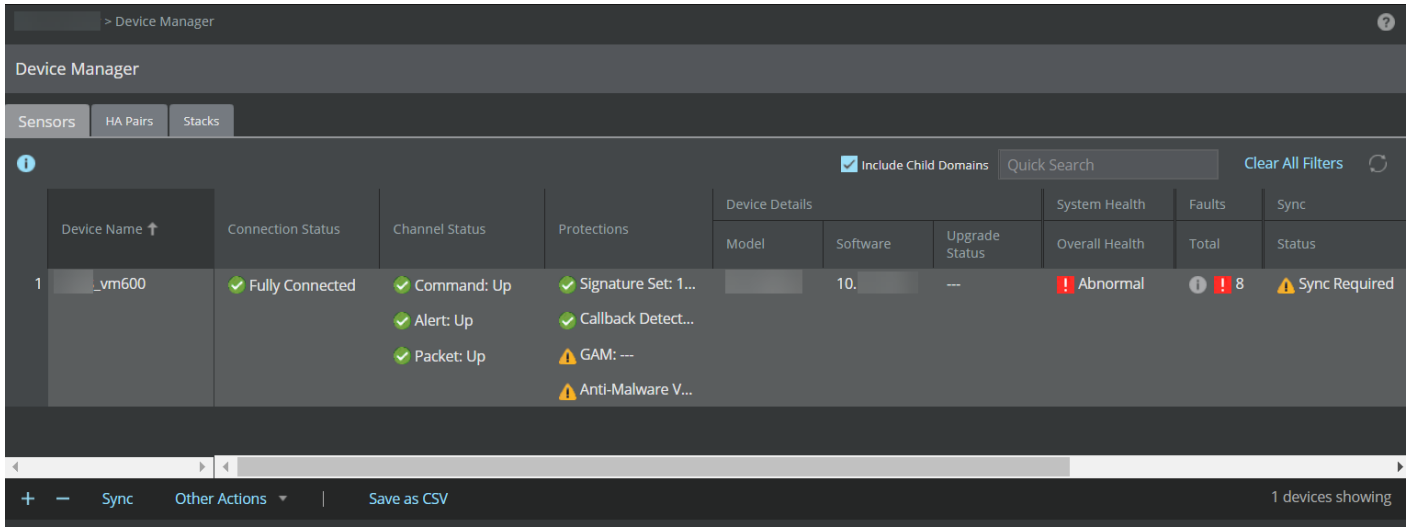
Refer the following steps to deploy the configuration changes to all devices in the admin domain or at a device level.

Steps:

1. Go to Devices → <Admin Domain Name> → Global → **Device Manager**.

   The **Device Manager** page is displayed.

Figure 15. Device Manager

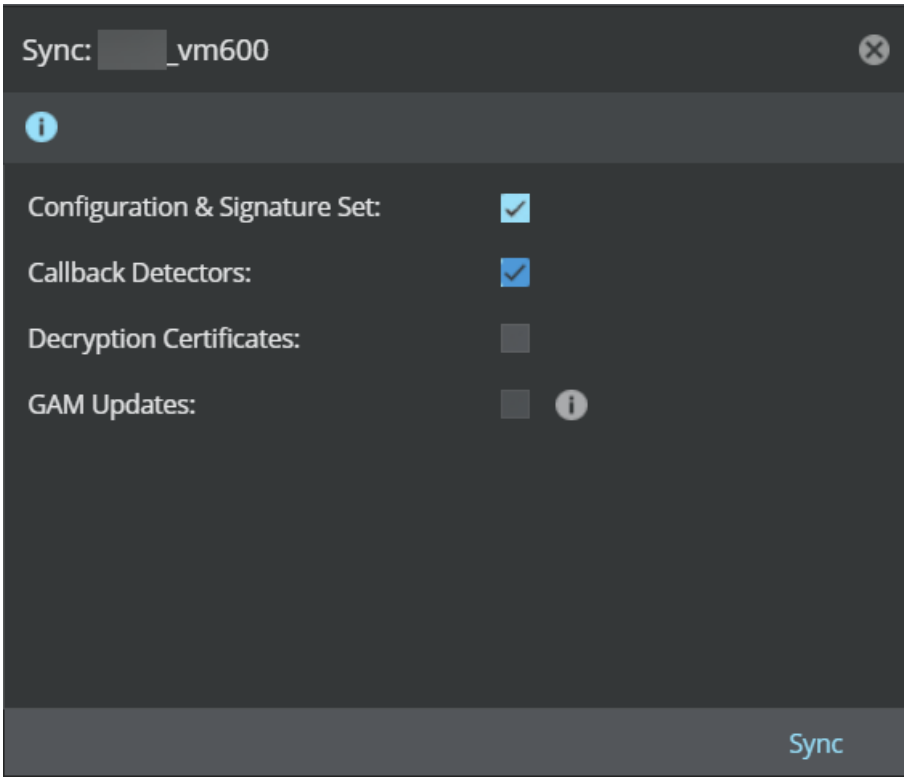


2. Click **Sensors** tab. Select the required Sensor from the list.
3. Select **Sync**.

   The **Sync: <Device Name>** window is displayed.
4. Select the required configurations and click **Sync**.

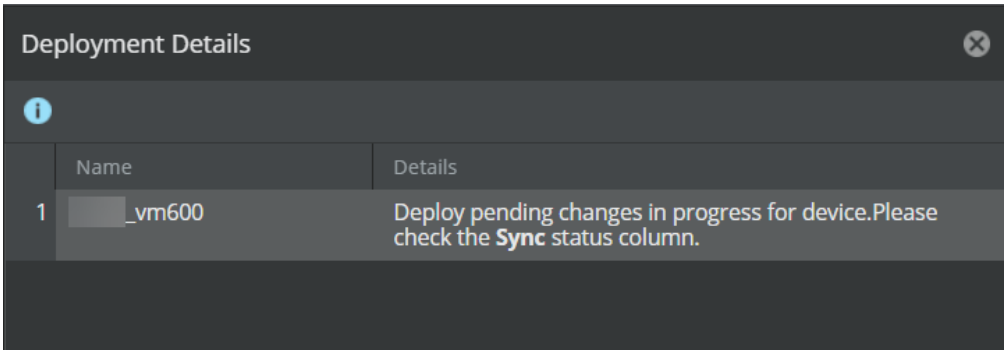
> **NOTE**
>
> The Manager provides an option to concurrently deploy pending changes for multiple Sensors. When you select multiple Sensors for deployment, the **Bulk Sync** window is displayed and enables all check-boxes by default. Select the options you wish to deploy and click **Sync**.

Figure 16. Sync: <Device Name> window



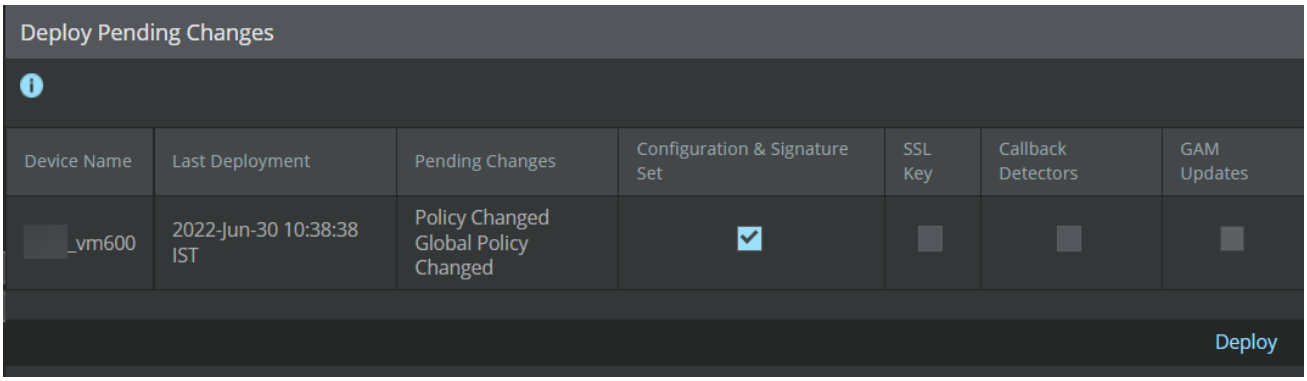
A **Deployment Details** dialog box is displayed. Click .

Figure 17. Deployment Details



You can also deploy the changes to a specific device from **Devices <Admin Domain Name> Devices <Device Name> Deploy Pending Changes**. Select the required configurations and click **Deploy**.

Figure 18. Device-level deploy pending changes



The following status can be viewed from **Sync** section of **Status** column:

Status	Description
Synchronized	Indicates that no pending changes are required.
Sync in progress	Indicates when the deployment is in progress.
Sync required	Indicates if any pending changes are required.
---	Indicates that there is no trust established between the Sensor and the Manager.

5. Click **Export Sync File** under **Other Actions** to view and export the deployment changes file to indirect mode Sensors. The changes can then be deployed to the Sensors manually using the CLI command window.
6. Click to refresh the page and the status of the deployment.

Viewing pending deploy configuration changes

You can view the status and details about the number of devices that are having pending deploy configuration changes. The status of the pending deploy configuration is indicated as an icon in the application menu bar.

The following are the lists of available icons that are displayed, based on the status in the pending deploy configuration.

Icons	Description
	Specifies that there are no pending changes on the devices.
3	Specifies the number of devices where the changes are pending. Clicking on this icon displays the **Deploy Pending Changes** page.

Users and roles

User management in Trellix IPS

Security organizations usually are comprised of multiple individuals, and management of the overall system is generally delegated to different people according to some logical categorization—by department, by geographic location, by system (that is, the email servers, the Web servers), and so on. In Trellix IPS, you delegate the management of system components by organizing the components logically into *admin domains* and then granting various management privileges for the domains to your Trellix IPS users.

The Manager enables the creation of multiple users within the system, and enables Super Users to grant specific privilege rules, called *roles*, to those users to allow them to manage an admin domain and any of its children. Within each admin domain, permission to carry out tasks is limited to only those users with appropriate roles.

For example, recall that a child admin domain can consist of something as granular as an interface on a Trellix IPS Sensor. You use roles to specify who can do what with that interface in that child domain.

What is a role?

A *role* is defined as a group of actions that a user is allowed to perform within a given domain. Roles determine the user's authorized activities, ensuring the users have access to only the functions necessary to complete their particular operational responsibilities.

Trellix IPS implements *role-based authorization*, wherein users can perform only those activities permitted by their role. Roles are always *domain based*, that is, a role governs what activities a user can perform within a particular domain. Users never have roles that are not tied to managing a resource within a specific domain and its children, although users can exist in the database without being assigned a role.

Roles promote the integrity of security configuration by not allowing universal access to every security resource deployed in the system. Thus you can create a user with privileges to manage and configure a single child domain, perform user management tasks within that domain, generate reports, manage Sensors, and so on. You can assign the least privileges necessary for a user to perform his/her specific job function, and no more. The user is limited to the specific role functions within the assigned child domain and its children, and prevents the user from manipulating other domains.

For example, only the Root Admin Domain System Administrator sees the Manager. System Administrators without privileges at the Root Admin Domain level are allowed to configure and maintain their child domains within the system, but do not see the Manager.

NOTE

The Root Admin Domain Super User is able to override the roles of any user.

Creating a user

You create a user from the Manager → <Admin Domain Name> → **Users and Roles** menu, and you can assign the user roles for a particular domain at the time the user is created, or you can assign roles at a later time. Only users who have Super User privileges can assign or modify the assignment of user roles, and then only for the domains permitted by their role(s).

Users are stored in the database with their username, a PBKDF2WithHmacSHA512 hash of their password, their role(s), and their roles in various domains. When the user logs in, the Manager makes available only those activities permitted by the user's role.

As most companies now centralize their user management and authentication, the Manager also supports **RADIUS** and **LDAP** authentication for users. For either authentication method, you configure the authentication server information, and then when creating a user, you can choose whether the user is a RADIUS, LDAP, or Manager Local user.

User accounts for the Sensor can be centrally stored and authenticated with a **TACACS+** (Terminal Access Controller Access Control System plus) server.

Roles within Trellix Intrusion Prevention System

Trellix IPS provides five categories of roles. The section [Role descriptions] lists the five role types with the applicable description and activities available to each.

All role types can view the **Dashboard** page. **No Role** users—as their names imply—have the most limited read-only privileges within the system.

In addition to Trellix IPS-provided roles, custom roles can added in order to assign specific abilities to certain members of an organization.

Role relationships between parent and child domains

Roles apply within the current domain and any of its children. Because child domains are essentially contained within parent domains, if a user is given, for example, Operator role for a parent domain, that role also applies to all children of the parent. Note that additional roles can be granted to the user at the child level, but a role granted at a parent cannot be overridden at a child level. Using the example above of a user granted an Operator role at the Root Admin Domain level, suppose you create a child admin domain. The user with the Operator role inherits that role at the child level; however, if you wanted the user to have Super User status at the child level, you can assign the Super User role within that child domain.

Trellix IPS roles provide a granular level of access within the system. This enables you to provide very limited responsibilities to a number of individuals, or to assign a single user multiple roles so the user can accomplish multiple administrative tasks (for example, grant System Administrator and Security Expert roles) within the system.

Role descriptions

The following section summarizes the Trellix IPS-provided user roles.

Table 3. Roles and Descriptions

Role	Descriptions
ePO Dashboard Data Retriever	The **ePO Dashboard Data Retriever** has rights to retrieve information from Trellix IPS to Trellix ePO - On-prem for displaying Trellix IPS information in Trellix ePO - On-prem.
Policy Administrator	The **Policy Administrator** administers the intrusion prevention environment.
NOC Operator	The **NOC Operator** monitors the security environment.
Report Generator	The **Report Generator** runs reports.
Security Expert	The **Security Expert** role manages intrusion policies. The **Security Expert** administers the IPS and NTBA environments. The **Security Expert** can create, edit, and delete policies, view alerts, manage software and signature update downloads, generate reports, manage system faults, and handle security alerts.

Role	Descriptions
Super User	The **Super User** role (not represented by an icon) enjoys all privileges. Each shipped Manager is configured with one built-in Super User account, including a default password. The **Super User** role provides: • All the privileges possible in the current domain • All the privileges a **Super User** has in all the children of the current domain • The special privilege to assign (or remove) the Super User role for a user in the current domain A **Super User** can be defined at any level, and the role applies to the current domain and all of its children, but not for its parent domain or any other "sibling" domains.
System Administrator	The **System Administrator** role pertains strictly to administration of the system itself. The **System Administrator** administers the Manager and the Device List. The System Administrator manages software and system performance, adds, configures, and deletes Sensors, and handles system faults.

Management of users and user roles

Trellix IPS enables creation of users for various administrative functions. This enables selected entities (users/groups/business units) to manage specific domain resources.

User management in Trellix IPS environment consists of creating users and granting them privileges. Network security requires careful planning when creating users to ensure the integrity of the environment. All users must authenticate at the Manager login prior to performing *any* activities. The username and password is securely stored in the database with matching privilege rules. A class of user privileges, termed *roles*, determines the authorized activities of the various users in the system. Once a user logs in, Manager makes available activities based on the role. Roles promote the integrity of security configuration by not allowing universal access to every security resource deployed in the system.

User management

The **Users** option allows you to add a user, change the default administrator, delete, or edit a user.

The Users list only displays the users created within the current admin domain and any of its children. This list does not display users that were created in a higher admin domain level even if an administrator has a role in that higher admin domain regardless of role. If a user's name is not displayed, the viewing user needs to move to the admin domain level where the user was created in order to administer that user. Admin domain viewing is role dependent.

When you are in Edit mode, you will see the **Reset GUI Presentation** button. This version of the Manager allows you to make changes to a column or panel presentation. For example, you can resize the width of a column in a table or apply a filter by using a small arrow situated next to a column. Once you customize the width of a column or apply a filter, it stays that way even when you log out and log in next time. If you want to reset these changes and revert to the default settings, click **Reset GUI Presentation**.

Add users

To add a new user and optionally assign a domain role, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Users and Roles → **Users**.
2. Click  .

   The **Add a User** page is displayed. Fill in the required fields. The fields marked with an asterisk (*) are required fields.
3. Type the **Login ID**. The Login ID parameters that can be used are as follows:
   - 26 alpha: upper and lower case (a,b,c,...z and A, B, C,...Z)
   - 10 digits: 0 1 2 3 4 5 6 7 8 9
   - 6 symbols: . ' : - _ ( ) space
4. For **Authentication Type** choose one of the following (if available):
   - **Local** — Authenticate locally on Manager.
   - **LDAP** — Authenticate using an LDAP server. If you select this option, also type the **LDAP User DN** (distinguished name).

     Use the following format for the **LDAP User DN**:

     ```
     uid=userName,ou=People,dc=DomainName,dc=com
     ```

     If using Active Directory, use the following format:

     ```
     userloginname@domain.com
     ```

     or

     ```
     cn=userName,ou=People,dc=DomainName,dc=com
     ```

     Use a valid DN, as LDAP authentication may not operate correctly without a valid DN. Consult with your system administrator to obtain the correct DN for your LDAP server.
   - **RADIUS** — Select one of the following RADIUS authentication protocols. If you select this option, also type a valid **RADIUS ID**, which will be used for authenticating your settings against the RADIUS server.
     - **RADIUS** using **PAP** (Password Authentication Protocol)
     - **RADIUS** using the **CHAP** (Challenge Handshake Authentication Protocol)
     - **RADIUS** using the **EAP-MD5** (Extensible Authentication Protocol-MD5)

   If you have selected the **Authentication Type** as **Local**, you will have to fill the **Password** and **Verify Password** field.
5. The **Password** must be a minimum of eight (8) characters and maximum of sixty four (64) characters in length, and must contain a combination of numbers, characters, and special characters. Password parameters that can be used are as follows:
   - 26 alpha: upper and lower case (a,b,c,...z and A, B, C,...Z)
   - 10 digits: 0 1 2 3 4 5 6 7 8 9
   - 32 symbols: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <>? /

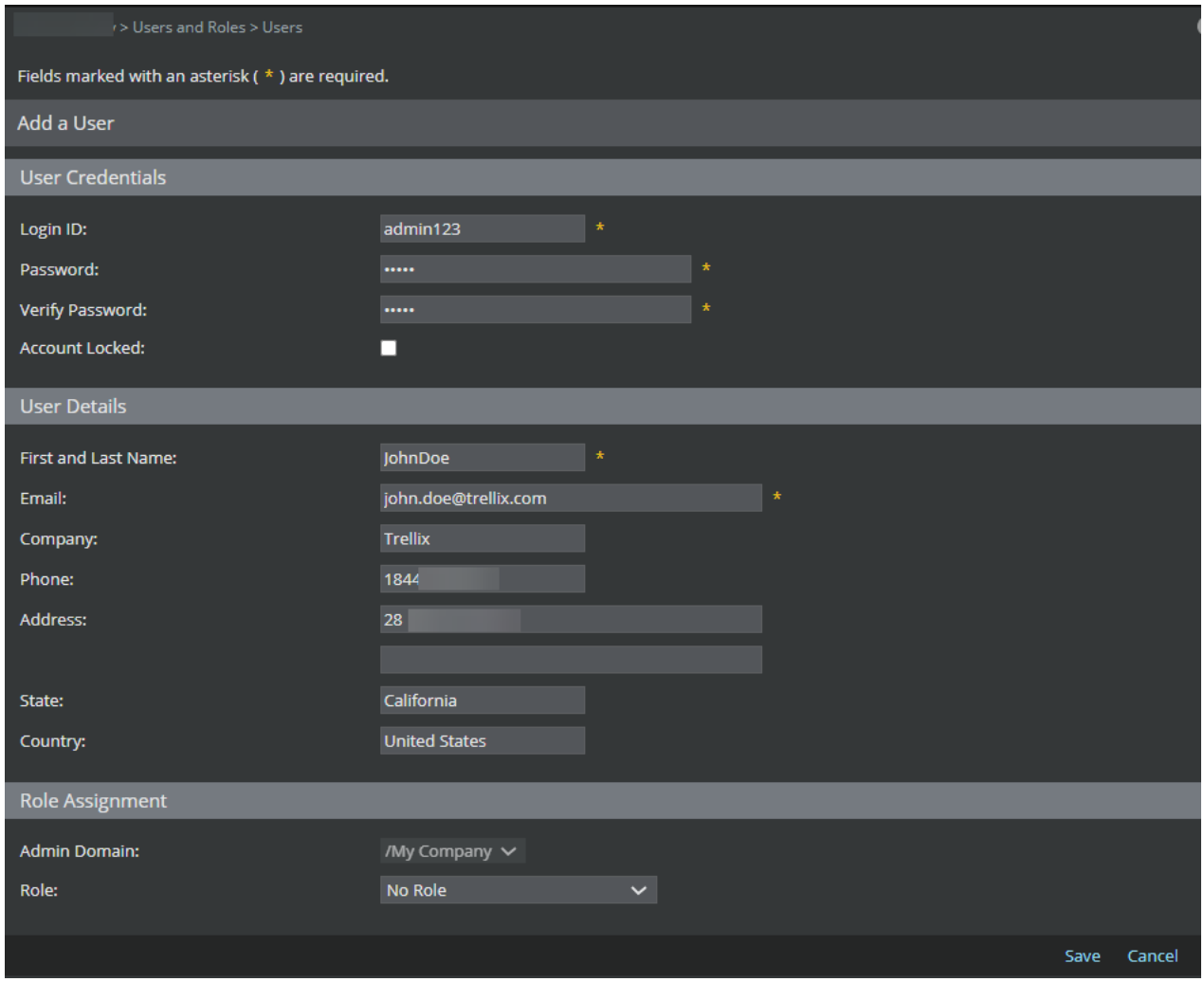
   NOTE

   If RADIUS or LDAP authentication is enabled, you must also select the type of authentication to use for this new user.

> **NOTE**
>
> Trellix **strongly recommends** that you change the default password for security purposes. For more information on the password control, see Configure password complexity settings (page 229).

6. Re-enter the password in **Verify Password**.
7. [Optional] Select the checkbox **Account Locked** to disable the user.
8. The **First and Last Name** must be a minimum of one (1) character and a maximum of thirty two (32) characters in length. The parameters that can be used are as follows:
   - 26 alpha: upper and lower case (a,b,c,...z and A, B, C,...Z)
   - 10 digits: 0 1 2 3 4 5 6 7 8 9
   - 2 symbols: . space
9. Type the **Email** address of the user.
10. Type the relevant details, if required for the following fields: **Company**, **Phone**, **State**, **Address**, and **Country**.
11. In the **Role Assignments** section, select the **Roles** from the drop-down list. **Admin Domain** displays the user domain by default.

Figure 19. Add User page



12. Click **Save**; click **Cancel** to abort.
13. Select Manager → <Admin Domain Name> → Users and Roles → **Users** to view the newly added user.

Edit users

NOTE

Editing a user in Central Manager is similar to that in the Manager, described below.

To edit an existing user, do the following:

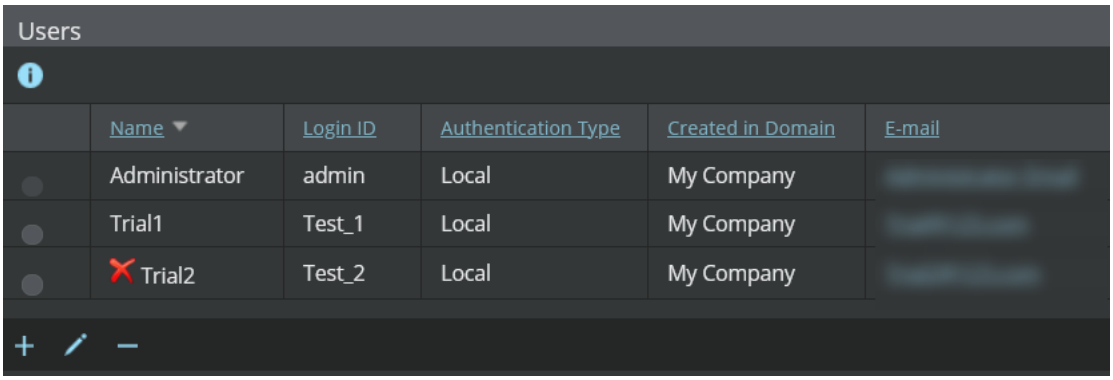
Steps:

1. Select Manager → <Admin Domain Name> → Users and Roles → **Users**.
2. Select a user.

3. Click
4. Type your changes in the appropriate fields.
5. Click **Save**.

View Users

To view the users available in the Manager, select Manager → <Admin Domain Name> → Users and Roles → **Users**.



NOTE

If the account is locked, will be displayed beside the user name in the **Name** column.

Delete users

NOTE

Deleting users in Central Manager is similar to that in Manager, described below.

To delete an existing user account, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Users and Roles → **Users**.
2. Select a user.
3. Click . A pop-up with the following message appears: **You are about to permanently delete this record. Do you wish to continue?**
4. Click **OK** to delete the user record; click **Cancel** to abort.

Assign roles to users

You can assign or remove a role to/from a user at any time.

NOTE

A user granted a role in a parent admin domain inherits the same role in any child domains below the parent, unless the user's role is altered in a child domain.

To assign a role to a user in a domain, do the following:

1. Select Manager → <Admin Domain Name> → Users and Roles → **Role Assignments**.
2. Select a user in the **Role Assignments** table.
3. View the user's role in the field **Roles (Current Domain)**. If no role has been assigned, this field is empty.
4. Click .

   NOTE

   A user can have a different role in any or all admin domains regardless of the admin domain in which the user was created. If the user is to be granted a role in an admin domain higher than the one where it was created, the administrator of that higher domain must assign that role. An administrator can only grant or deny roles in the admin domains where he/she has that privilege. If a user has been allotted a Super user role at the parent and the child domain, the user should select a domain from the home page at the time of login. The home page displays a drop-down above the menu bar in such cases.

   Current Assignments and **New Assignment** sections are displayed. If a role is already assigned to the user, the role in **Assigned Role** column is displayed in **Current Assignments** section.
5. In **New Assignment**, the **Login ID** of the user is displayed by default.
6. Select the **Admin Domain** from the drop-down list.
7. Select the role(s) to be assigned to the user from the drop down list.
8. Click **Save**.

Define Roles

A role is a group of actions that a user is allowed to perform within a given administrative domain. Trellix IPS provides role-based authorization to the users.

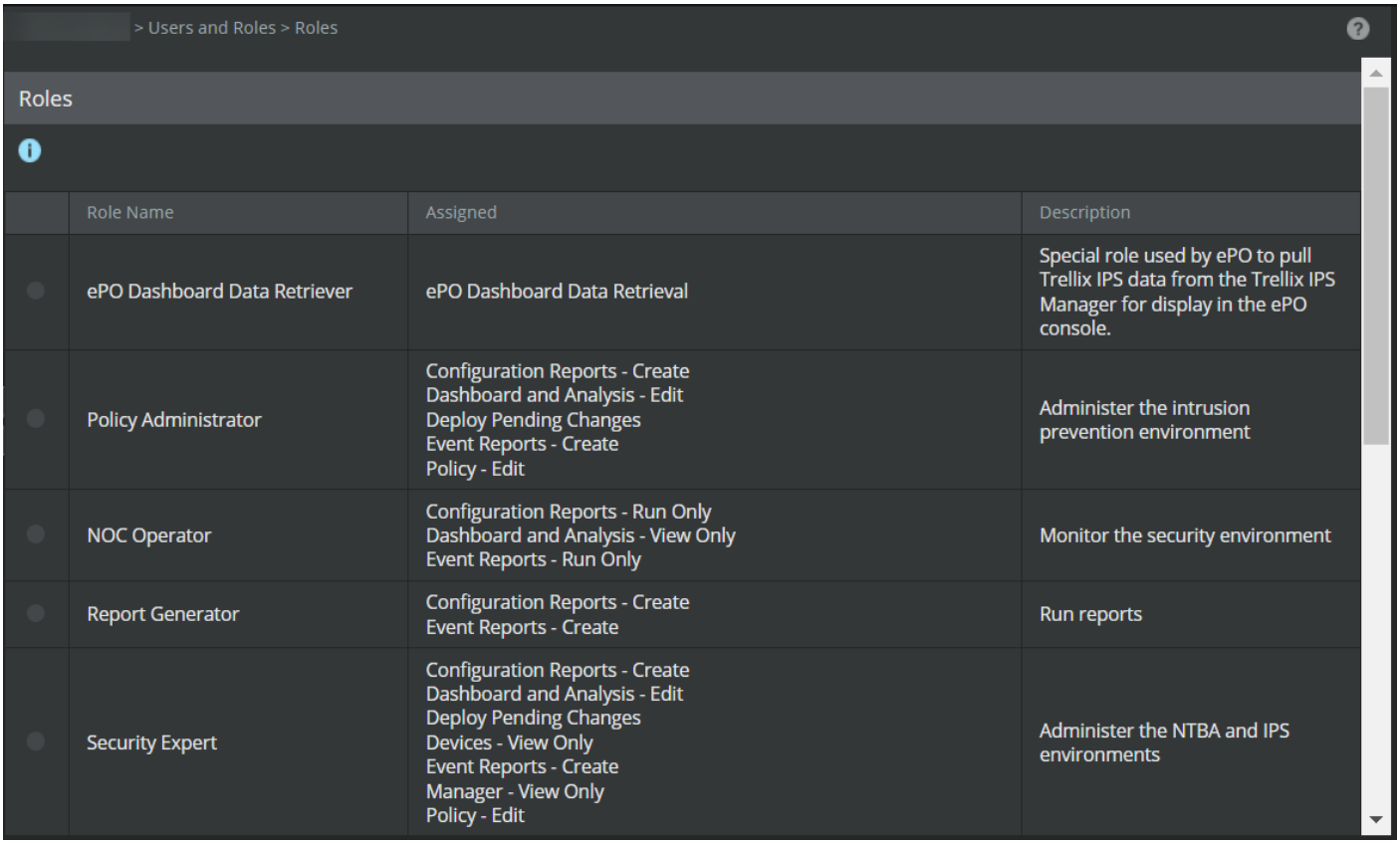
Users authenticate themselves by logging into the Manager. For an admin domain, you can create users and assign roles to the users in the Manager. You can also create users in the child admin domains and assign roles to them.

The role privilege indicates the actions that are allowed for a user with assigned with the particular role. Each role has role privileges with Create, Edit, Run Only, or View Only permissions. For example, Configuration Reports - Create allows the user with that role to have Create permissions for the Reports in the Manager.

Trellix IPS includes default roles, and you can create custom roles. Users created for an admin domain are specific to that domain, but roles can be assigned to the users across domains. That is, you can assign a role to a user in one domain, and another role to the same user in the corresponding child domain.

The **Roles** option (Manager → <Admin Domain Name> → Users and Roles → **Roles**) lists the various default roles and allows you to create custom roles.

Figure 20. Roles page



The following table lists the default role types and their corresponding role descriptions.

NOTE

Options to edit or delete are disabled for the default roles.

Role	Description	Role Privilege
Policy Administrator	Administer the intrusion prevention environment	Configuration Reports - Create Dashboard and Analysis - Edit Deploy Pending Changes Event Reports - Create Policy - Edit Run Vulnerability Scan View Packet Captures

Role	Description	Role Privilege
NOC Operator	Monitor the security environment	Configuration Reports - Run Only Event Reports - Run Only View Packet Captures
Report Generator	Run reports	Configuration Reports - Create Event Reports - Create
Security Expert	Administer the IPS and NTBA environments	Configuration Reports - Create Dashboard and Analysis - Edit Deploy Pending Changes Devices - View Only Event Reports - Create Manager - View Only Policy - Edit Run Vulnerability Scan View Packet Captures
System Administrator	Administer the Manager and the Device List	Configuration Reports - Create Deploy Pending Changes Devices - Edit Event Reports - Run Only Manager - Edit Policy - View Only Synchronize Policy View Packet Captures
ePO Dashboard Data Retriever	Rights to retrieve information from Trellix IPS to ePO, for displaying Trellix IPS information in the ePO.	ePO Dashboard Data Retrieval

Role	Description	Role Privilege
Super User	Full rights. Super Users must manage themselves within the domains they reside.	Configuration Reports - Create Configuration Reports - Run Only Dashboard and Analysis - Edit Dashboard and Analysis - View Only Deploy Pending Changes Devices - Add and Remove Devices - Edit Devices - View Only ePO Dashboard Data Retrieval Event Reports - Create Event Reports - Run Only Guest Portal User Account Manager Manager Central Manager - Edit Manager Central Manager - View Only Manage Managers - View Only Manager - Edit Manager - View Only Policy - Edit Policy - View Only User Auditing - Edit Users and Roles - Edit Users and Roles - View Only View Packet Captures
No Role	The user cannot log on to Manager. This is the state when a user is first created but is yet to be assigned any role.	

Custom roles

Custom roles can be created in the Manager and assigned to users. You can create a new custom role and assign the role by using **Roles** and **Role Assignments** options.

You can edit or delete the custom roles in the **Roles** option. You can also assign roles using the **Role Assignments** option and view the user account information using **My Account** option as before.

Add roles

You can add new roles (custom roles) in the Manager from the Manager → <Admin Domain Name> → Users and Roles → **Roles** option.

> **NOTE**
>
> Only users with 'Users and Roles - Edit' role privilege can create users or roles, assign roles to users, and modify the user account settings.

> **NOTE**
>
> Users with 'Users and Roles - View Only' role privilege can only view the users, roles, or user accounts.

Adding custom roles

Users with 'Users and Roles - Edit' role privilege can add roles. Once added, the roles are listed along with default roles available for the users.

To add a custom role in the Manager, do the following:

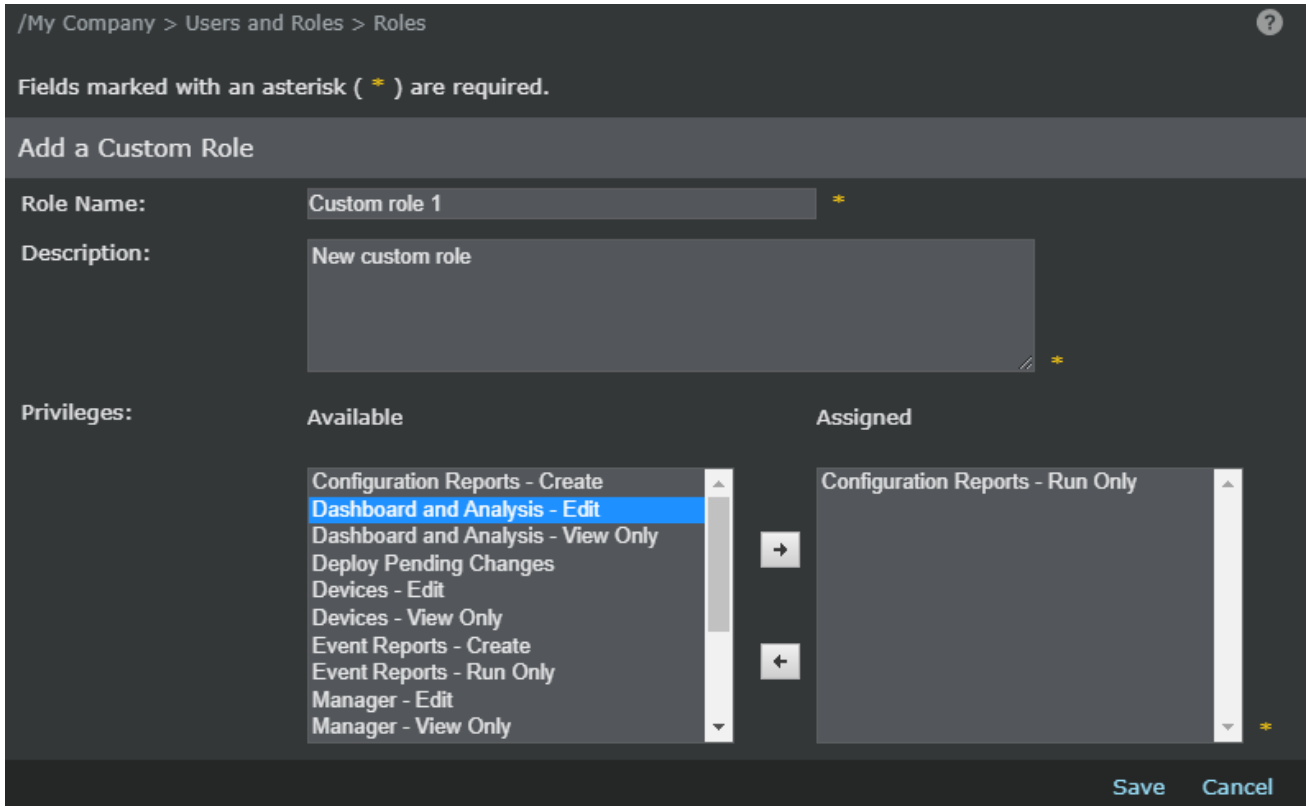
Steps:

1. Select Manager → <Admin Domain Name> → Users and Roles → **Roles**.

   > **NOTE**
   >
   > **Roles** option can be accessed only from the parent administrative domain. Default roles cannot be edited or deleted.

2. Click + to create a new custom role.

Figure 21. Add a Custom Role page



The **Add a Custom Role** window is displayed.

3. Enter a name to identify a role and a description.
4. Select the permissions you want to assign to this role from the **Available** list, and click the arrow to move them to the **Assigned** list. The Read, Write or Operate permissions (RO, RW, etc) for the privileges are in the privilege name.
5. Click **Save**.

Assign custom roles

To assign a custom role to a user, do the following:

Steps:

1. From the **Manager** tab, select <Admin Domain Name> → Users and Roles → **Users**.
2. Click + to add a user.
3. Enter the user information.
4. In the **Role Assignment** section, select the **Role**.
5. Click **Save**. The assigned role is displayed in the **Users** page.

NOTE

A custom role created in the Central Manager can be associated with a Manager user. If this role is deleted or if the Manager is made a standalone, then the role will be deleted in the Manager. Even the role's association with the Manager and user get deleted.

Super User Privileges

Trellix IPS resources are governed by users with Super User access; a Super User is capable of configuring every resource and function in the system. Each shipped Manager is configured with one built-in Super User account, including a default password.

A Super User is only limited by domain boundaries. Only the Super Users created at the root domain have full access; Super Users in a child domain only have Super User privileges in that domain and the subsequently added child domains.

CAUTION

The default Super User account username is **admin** and password is **admin123**. Trellix **strongly recommends** that you change the default Super User password for security purposes. The new password must be at least 8 characters in length and must contain a combination of numbers, characters, and special characters. For more information on the password control, see Configure password complexity settings (page 229).

A Super User can be defined at any level, and the role applies to the current domain and all of its children but not for its parent or sibling domains.

Management of user roles

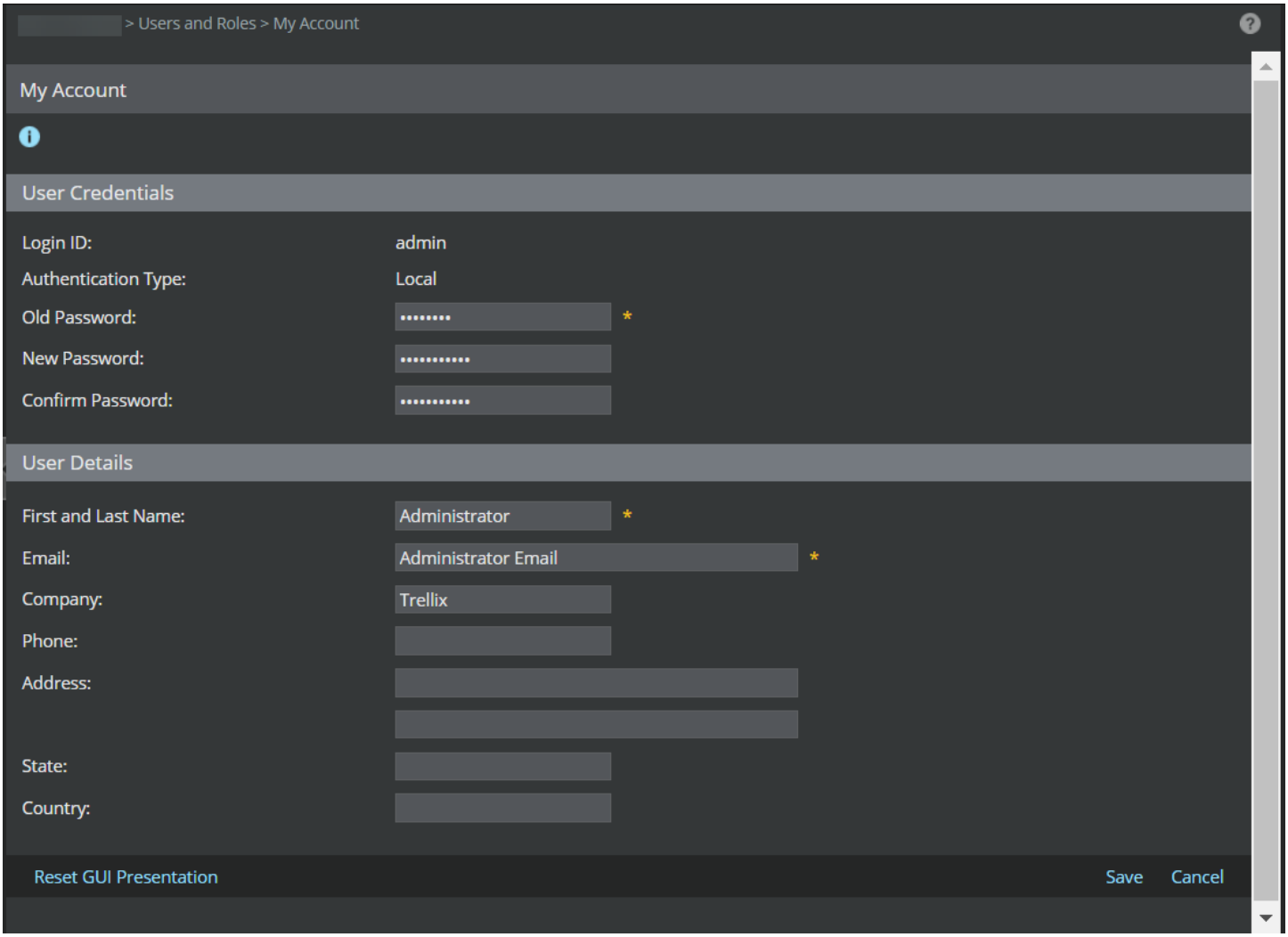
The **Role Assignments** option enables a user administrator to assign roles to users within an existing admin domain. Adding a user to a domain requires the application of a *role*, or privilege, thus limiting a user's configuration abilities.

How to view user account information

The **My Account** option displays the **My Account** page, which lists the account information for the logged-in user. The navigation path for this page is Manager → <Admin Domain Name> → Users and Roles → **My Account**.

If you want to change your information (password, address, and so forth), clear the appropriate field, type the new information, and click **Save**; click **Cancel** to exit without saving changes.

The **Reset GUI Presentation** restores any changes made to the column or panel presentation to its default setting.



Setup

What is an administrative domain?

An administrative domain, or admin domain for short, is an organizational tool used specifically to group Trellix IPS resources so that management of the resources can be delegated to specific Trellix IPS users.

An admin domain can contain other admin domains, Trellix IPS Sensors, Sensor interfaces, and Sensor sub-interfaces. This administrative domain concept enables enterprises to create a central authority that is responsible for the overall Trellix IPS, and to allow this central authority to delegate day-to-day operations of Trellix IPS security resources to appropriate entities—business units, geographic regions, IT departments, individual security personnel, and so on.

Root Admin Domain

The top level admin domain is called the Root Admin Domain. Users with Super User access to the Root Admin Domain have complete control over the entire administrative domain and all resources within it, including any child domains, and thus all security resources in the system.

For example, suppose your company (which we'll call My Company) is headquartered in London, and has satellite offices in New York, Paris, and San Francisco. If your Trellix IPS deployment monitors the entire company, your Root Admin Domain could

encompass all four sites and all of the Trellix IPS components within the environment, and you could manage the entire system from London.

The admin domain is displayed at the top of the tab tree across the Policy, Manager, and Devices tabs. The root admin domain is labeled "My Company".

Parent and child admin domains

Perhaps managing "My Company's" entire Trellix IPS deployment from London is impractical. It might make more sense to delegate management of the Trellix IPS resources protecting various geographical locations to entities in those locations. To delegate management functions to each of the four offices, you would create a subdomain representing each office. These subdomains are called child admin domains or child domains.

Creating child domains enables you to delegate entities more familiar with the subdomain's environment to monitor and/or configure the IPS devices in that subdomain. You are not required to subdivide your admin domains into child domains; however, if you want to delegate responsibilities for managing Trellix IPSTrellix IPS resources among multiple individuals within your organization, you do so by creating child domains.

NOTE

To delegate responsibilities, you create user accounts and give each user a role that defines how the user can interact with the resources in the child admin domain. For more information on roles, see Management of users and user roles (page 94).

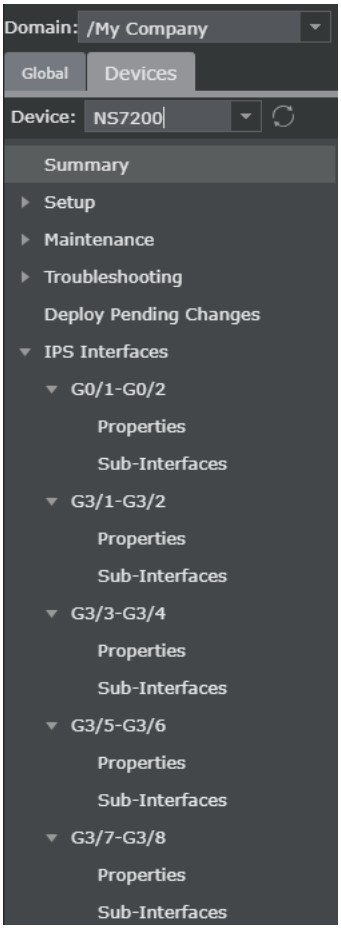
You can further break child domains into smaller subdomains. Any domain with child domains is a parent. A child domain can be parent to other child domains.

You can subdivide your Root Admin Domain into child domains that are large, from a resource perspective, delegating management of all the Trellix IPS resources protecting multiple geographic regions. Or you can create domains that are very small—a few interfaces on a single Sensor, or even a VLAN tag or CIDR address within a segment of traffic transmitting between two hosts in the protected network.

Admin domain hierarchy

Administrative domains are graphically represented in the tab structures as a hierarchical tree structure. In the tab tree, you can drill-down levels using menus, sub-menus, and options. The hierarchy is: Device, interface node, sub-interface node, child admin domain node, and allocated interface node.

Figure 22. Admin domain hierarchy



The Domain field at the top of the tab tree represents the Root Admin Domain.

NOTE

The tab tree structure applies to the way the actions are performed by system users and not necessarily to any networking or physical relationship between the resources.

A user's role determines his/her view of the tab tree. Only resources the user is permitted to view are displayed in the tab tree.

Inheritance

It is important to understand the relationship between parent and child admin domains because (by default) child admin domains inherit policies from parent admin domains, and because users are automatically granted the same privileges in the child domains as those enabled by their roles in the parent domain.

Policy inheritance means that a child takes policies, or inherits them, from the parent. If you do not specify a policy when you create the child, the child automatically inherits the policies of its parent. To override policy inheritance from parent, you assign a policy to the child admin domain that is specific to that child domain.

For more information on policies, see Working with IPS policies (page 795).

User roles work similarly, but with a slight difference. Roles apply within the current domain and any of its children. Because child domains are essentially contained within parent domains, if a user is given, for example, a Super User role for a parent domain, that role also applies to all children of the parent. Thus, to use the domain hierarchy shown in the figure in Admin domain hierarchy as an example, a user assigned a System Administrator role for the Finance department has that role for the Payroll and Accounts Payable domains as well.

Note that additional roles can be granted to the user at the child level, but a role granted at a parent cannot be overridden at a child level.

For more information on roles, see Management of users and user roles (page 94).

Configuration of Administrative Domains

An administrative domain, or admin domain for short, is an organizational tool used specifically to group Trellix IPS resources so you can delegate resource management to specific users. An admin domain can contain other admin domains, Devices, and Device interfaces.

Administrative domains enable enterprises to create a central authority that is responsible for the overall Trellix IPS system, and to allow the central authority to delegate day-to-day security operations to the appropriate entities, such as business units, geographic regions, and individual security personnel.

The top level admin domain is called the *root admin domain*. Users with Super User access to the root admin domain have complete control over the entire administrative domain and all resources within it, including any child domains, and thus all security resources in the system. To delegate management functions to entities within your organization, you would create a sub domain (of the root or other parent domain) representing each entity or department. These sub-domains are called *child admin domains* or *child domains*.

In Trellix IPS Manager, the functions that you can perform at the admin domain level are as follows:

- Configuring and managing admin domains: enables you to view details of admin domains and create child admin domain
- Managing users and user roles: enables the creation of users for various administrative functions
- Viewing system information logs: enables a privileged admin to create audits and logs to view system information
- Setting up fault notifications: allows you to send system fault information to third-party machines such as SNMP servers and Syslog servers.

Child domains

Creating child domains enables you to delegate, monitor, and/or configure Trellix IPS Sensors in that sub-domain to entities more familiar with the sub-domain's environment. You are not required to subdivide your admin domains into child domains; however, if you want to delegate responsibilities for managing Trellix IPS resources among multiple individuals within your organization, you do so by creating child domains. To delegate responsibilities, you create child admin domains and user accounts, giving each user a role that defines how the user can interact with the resources in the child admin domain.

For example, suppose you manage three Trellix IPS Sensors. You can create a child domain and allocate a single port (G0/1) from one of your Sensors to that domain. You can create a user and assign that person a Super User role in only that domain; that user has no role in the root domain, and therefore cannot see or configure root domain resources. The child domain's Super User has been delegated full management responsibilities for the allocated interface.

A user's role determines his/her view of the Resource Tree; only resources the user is permitted to view are displayed in the tree.

Any domain with child domains is a parent; thus, a child domain can be a parent to other child domains. When you create a child domain you can enable or disable it to be a parent for other domains (enabled by default). The root can always have child domains.

It is important to understand the relationship between parent and child admin domains because child admin domains inherit policies from parent admin domains, and users inherit the same privileges in the child domains as enabled by their *roles* in the parent domain.

NOTE

Throughout this guide, named admin domain instances are represented as <Admin Domain Name>. The default root admin domain is **My Company**.

Management of admin domains

Managing an admin domain involves creating an admin domain, changing the root admin domain name, and deleting an admin domain.

Create an admin domain

The procedure to create an admin domain is the same for a domain created under the root or a domain created under a child of the root, and so on. You can create up to four **levels** of child domains under an admin domain. During child domain creation, you have the option of delegating Sensor interfaces from the parent for management by the child.

If you do not want at this time to allocate interfaces or allow Sensor addition, you may enable these options later.

To create an admin domain:

Steps:

1. Click Manager → <Admin Domain Name> → Setup → **Admin Domains**. The **Admin Domains** page is displayed.
2. Select the domain to which you want to add a child domain and then click ➕.
3. Type the required information. The red asterisks (*) denote required fields.

   The tables below describe the fields.

Field	Description
Domain Name	Enter a unique name for identifying the domain. For an enterprise, naming your domain after the specific network segment, department, or building is suggested: HR, Finance, Bldg1, Bldg1-Floor2.
Contact Person	Enter the name of the person responsible for the domain. This person should be someone who can be reached in case of emergency or other domain questions.
E-mail Address	Email address of the Contact Person.
Title	Title of the Contact Person.
Contact Phone Number	Phone number of the Contact Person.

Field	Description
Company Phone Number	Phone number of the Company where the Contact Person works.
Organization	Name of the Contact Person's employer company.
Address	Address of the Organization.
City	Name of the City where the Organization is located.
State	Name of the State where the Organization is located.
Country	Name of the Country where the Organization is located.

You can choose to enter additional details like phone number and address while creating the domain.

The fields mentioned below set restrictions on the child admin domain being created:

Field	Description
Allow Child Admin Domains?	If you select this check box, the administrator of the domain you are currently creating can create child admin domains for the domain. If you create a child admin domain and disallow the creation of further child admin domains, the new child domain cannot have its own children due to rule inheritance.
Allow Devices?	If you select this check box, the administrator of the domain you are currently creating can add, edit, or delete physical Sensors. Otherwise, the domain is only permitted interface or sub-interface resources as allocated in **Step 5**. If you create a child admin domain and disallow the adding of physical Sensors, any children of the new child domain are also disallowed from adding physical Sensors due to rule inheritance.

You can provide the following permissions to an admin domain:

- Create a child admin domain from the existing admin domain by selecting **Allow Child Admin Domains?**
- Add devices in the admin domain by selecting **Allow Devices?**

The permissions can be provided to the admin domain only while creating a new admin domain. Once the admin domain is created, these permissions cannot be edited/modified. To change the permission settings, you have to delete the existing admin domain and create a new admin domain with new permissions.

4. For IPS devices, select the IPS policy from **Default IPS Policy** drop-down list. For the NTBA Policy and Worm Policy, the fields mentioned below are displayed:

Field	Description
Default NTBA Policy	Sets the default NTBA Policy to be inherited by child admin domain resources. Several pre-configured policies are provided that encompass different network environments.
Default Worm Policy	Sets the default Worm policy to be inherited by child admin domains.

5. Click **Save**.

   The **Allocated Interfaces** page appears.

6. Click **Allocate**.

7. Select a Sensor from **Select an IPS sensor** drop-down list to allocate interfaces/sub-interfaces to the child domain. You can allocate interfaces/sub-interfaces from one or more Sensors.
8. Click **Allocate**. You may only select one interface from one Sensor at a time.
9. Repeat until you have allocated all the interfaces you require.
10. Click **Finish**.

    The child admin domain you created appears at the bottom of the resource list of the domain in which it was created.

Modify the admin domain name

You can customize some of the settings of your root domain, including the name that appears across all the tree-tab structures and subsequent system configuration navigation. Customizing the admin domain name helps to properly maintain the environment that is being protected.

Steps:

1. Click Manager → <Admin Domain Name> → Setup → **Admin Domains**. The **Admin Domains** page is displayed.
2. Select the root admin domain (**My Company**) from the **Admin Domains** page in the Manager. For Central Manager, there is only one admin domain, whose details are displayed.
3. Click  .
4. Clear the **Domain Name** and type your new domain name.
5. Clear the **Contact Person** and type a name. This typically would be the Super User.
6. Clear the **E-mail Address** and type a new email address.
7. Optionally, change the other fields if required.
8. Click **Save**. In all the tree-tab structures, the root domain name changes from **My Company** to the modified name.

Details of an admin domain

Navigate to Manager → <Admin Domain Name> → Setup → **Admin Domains** and click **View** to see the currently configured information for the selected admin domain.

NOTE

The **View** option is available for the users with **Manager View Only** permission.

NOTE

At the fourth level of admin domain hierarchy, **Summary** of the current admin domain is displayed by default.

NOTE

The information displayed for the selected admin domain varies according to the features available. For instance, if the NTBA license is enabled, information on **Default Anomaly Policy** and **Default Worm Policy** is displayed on this page.

Delete an admin domain

To delete an existing admin domain, do the following:

1. Click Manager → <Admin Domain Name> → Setup → **Admin Domains**. The **Admin Domains** page is displayed.
2. Select an admin domain from the **Admin Domains** List page.
3. Click and then click **OK** to confirm.

> **NOTE**
>
> An admin domain with resources such as Sensors and interfaces cannot be deleted until all resources have been removed.

Modification of child domain configurations

You can use the **Admin Domains** action to do the following:

- Edit the details of a selected domain.

> **NOTE**
>
> The root is the only domain that can be edited from its own node. All child nodes under the root must be edited directly from the parent domain where the child was created.

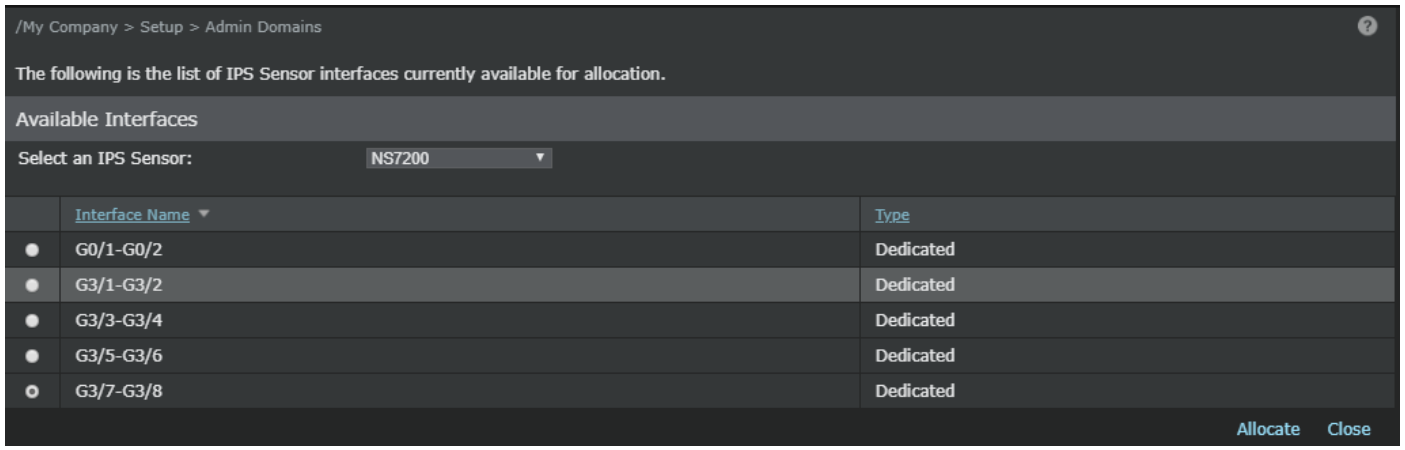
- Allocate or remove interfaces to/from an existing child domain:
  - You can allocate additional Sensor interfaces from the parent to the child. You have an opportunity to allocate interfaces to a child domain during the child domain creation. However, if you decide to allocate more interfaces to a child after creating the child domain, you must perform that task from the parent admin domain where the child was created.
  - You can revoke (that is, remove) interfaces from the child admin domain. This must be performed from the parent domain where the child was created. Revoking an interface brings the interface back under full control of the parent domain; the child domain can then no longer configure the revoked interface.

Edit domain details or the number of interfaces in a child admin domain

Steps:

1. Select the appropriate (named) parent domain by navigating to Manager → <Admin Domain Name> → Setup → **Admin Domains**.
2. Select the child domain to be edited from the parent's Admin Domains list.
3. Click .
4. Change any of the general information fields that require updating/editing in the **Edit the Admin Domain** page.
5. Click **Next**.

Figure 23. Allocated Interface page



6. Do one of the following:
   - Select an already allocated interface and click **Revoke** to remove the interface(s) from the child domain.
   - Select a Sensor and an interface and then click **Allocate** to allocate more interfaces to the child domain.
7. Click **Finish**.

Telemetry

The purpose of telemetry is to facilitate you in providing helpful information to Trellix about your usage of Trellix IPS solution so that Trellix in turn optimizes your protection. Telemetry data analysis empowers Trellix with essential monitoring and reporting capabilities, and assists the company in gaining valuable business intelligence insights and enhancing threat intelligence capabilities.

Currently, the IPS Manager collects two types of telemetry data with user's content and sends to Trellix telemetry servers at different intervals:

- **Threat telemetry data**: Threat telemetry comprises data related to alerts that enables Trellix to proactively identify and mitigate security risks.
- **Device telemetry data**: Device telemetry comprises a comprehensive set of information, including general setup, Virtual IPS cluster usage details, fault summary, and license information.

> **NOTE**
>
> Virtual IPS cluster usage details and license information are necessary for Trellix business intelligence and sent automatically to Trellix telemetry servers on a daily basis.

When the Manager is registered with Trellix using the Trellix IPS Registration Key, the **Telemetry** pop-up window appears in which you can configure the threat and device-specific data you want to send to Trellix and save the changes. If you wish to change the telemetry configurations later, you can do so from Manager → <Admin Domain Name → Setup → **Telemetry** page.

You can find details about the IPS telemetry data being uploaded to Trellix telemetry servers at different intervals from the ems.log file, or check for the same log entries in the Manager → <Admin Domain Name → Troubleshooting → Logs → **System**

Files page. You can also track the status of telemetry data uploading and saving on the **User Activities** tab, and look for errors related to the same on the **Faults** tab in the Manager → <Admin Domain Name → Troubleshooting → **Logs** page.

NOTE

- IPS telemetry data is stored in the telemetry servers for an indefinite period.
- For more information on the usage of telemetry data by Trellix GTI and Trellix Insights, see the chapters *Integration with Trellix Global Threat Intelligence* and *Integration with Trellix Insights* in *Trellix Intrusion Prevention System Integration Guide*.

Configure Telemetry

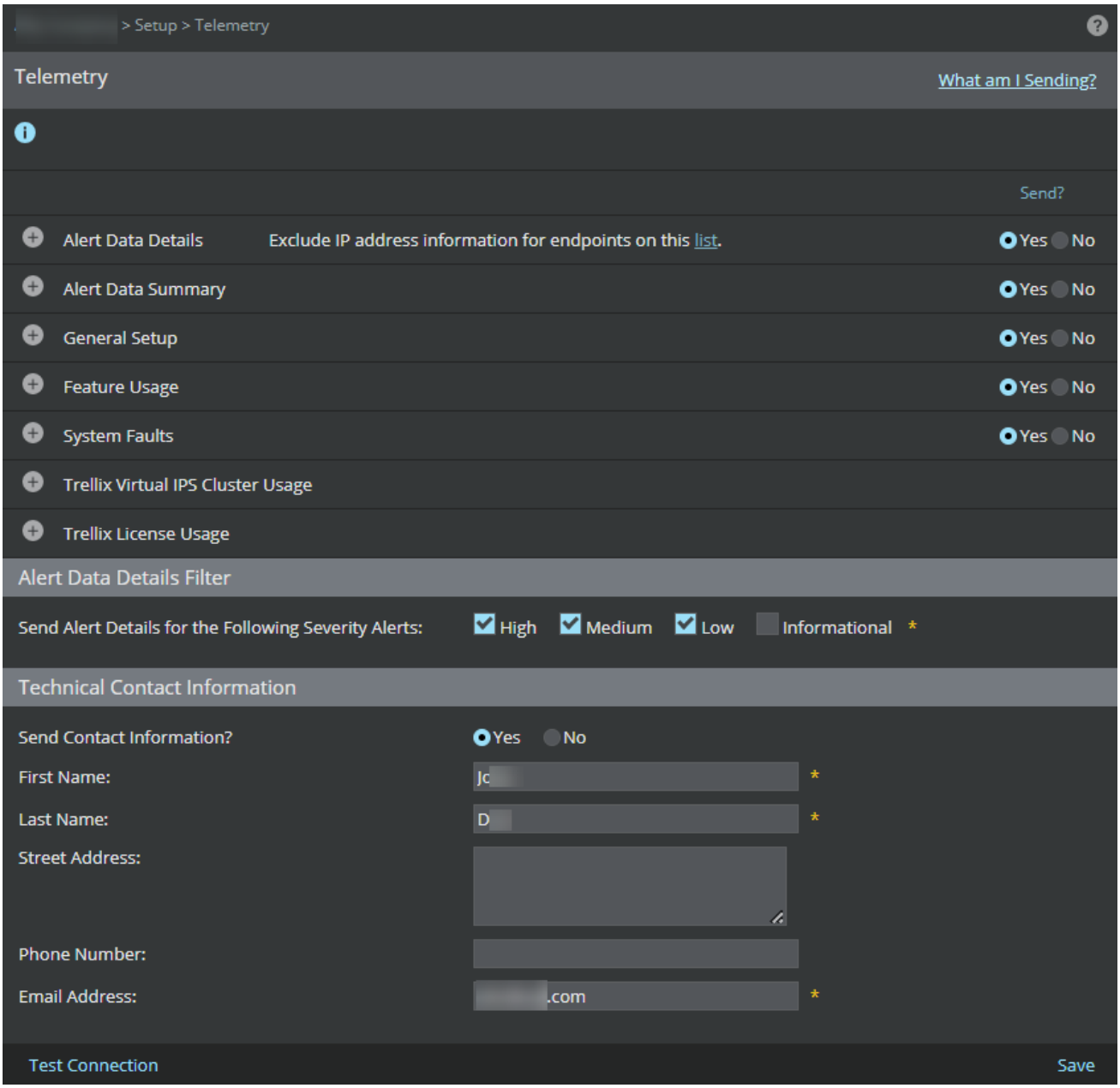
You can configure telemetry information in the **Telemetry** pop-up window that is displayed when you open the Manager for the first time, or by using the **Telemetry** page.

Perform the following steps to configure telemetry in the Manager:

1. Navigate to Manager → <Admin Domain Name> → Setup → **Telemetry**.

   The **Telemetry** page is displayed.

Figure 24. Telemetry page



2. Configure the following information categories (all of them are enabled in the **Telemetry** page by default). Select **Yes** to provide consent on the relevant information categories for which you prefer to send details to Trellix:

   - **Alert Data Details** - Select **Alert Data Details** for complete integration with Trellix endpoint reputation (that is, Trellix GTI endpoint reputation) services. This permits you to report, monitor, and take actions on endpoints/hosts involved in attacks based on their network reputation and/or country of origin. When the **Alert Data Details** option is selected, the following attributes are sent in real time for each alert seen and in batches every 3 hours to Trellix telemetry servers:

     - Application Name
     - Attack Name

- Attack Time
- Attacker DNS Name
- Attacker IP Address
- Attacker Country
- Attacker OS
- Attacker Port
- Attacker Risk
- Callback alert information
- Category
- Count
- Detection Mechanism
- Direction of Attack
- For correlated alerts: Triggered component attacks and their connection logs
- For heuristic attacks against web application servers: Threshold, confidence, weight, and the matched blocked strings
- For Trellix Intelligent Sandbox attacks: File name, size, type, MD5 hash, UUID, and malware confidence
- Malware Engine Results
- Malware URL
- Trellix IPS Attack ID
- Protocol
- Relevance (and method used to determine it)
- Result
- Signature ID
- Sub-Category
- Target DNS Name
- Target IP Address
- Target OS
- Target Port
- Target Risk
- Type
- URI

The following alert summary information is sent hourly to Trellix telemetry servers:

- A count of each attack seen
- The list of Trellix IPS attack IDs seen.

The following general setup information is sent daily to Trellix telemetry servers for the correct interpretation of the alert data:

- Manager software version and active signature set version

You can also exclude data from specific endpoint IP addresses by using the **Exclude IP address information for endpoints on this list** option in the header. For more information, see Exclude IP address information for specific endpoints (page 121).

> **NOTE**
>
> No participation is required to enable Trellix File Reputation (that is, Trellix GTI File Reputation) service.

- **Alert Data Summary** — Select **Alert Data Summary** for partial integration with Trellix endpoint reputation (that is, Trellix GTI endpoint reputation) services. This enables you to look up GTI for endpoints/hosts involved in attacks based on their network reputation and/or country details from the **Attack Log**. When the **Alert Data Summary** information category is selected, The following alert summary information is sent hourly to Trellix telemetry servers:
  - A count of each attack seen
  - The list of Trellix IPS attack IDs seen
  - The number of alerts whose relevance was determined by each available method
  - Top 10 (as per executable confidence) EIA attacks

  The following general setup information is sent daily to Trellix telemetry servers for the correct interpretation of the alert data:
  - Manager software version and active signature set version

  > **NOTE**
  >
  > No participation is required to enable Trellix File Reputation (that is, Trellix GTI File Reputation) service.

- **General Setup** — When this information category is selected, the following general setup information is sent daily to Trellix telemetry servers:
  - Manager install type, software version, and active signature set version
  - Manager OS type, OS version, and VM type (if applicable)
  - Manager GUID, MDR GUID (as applicable), and Telemetry GUID
  - Is Central Manager in use
  - Is Manager Disaster Recovery (MDR) in use
  - OS type, OS version, and VM type (if applicable) of each device
  - Serial number, model, software, and hardware version of each device
  - Is each device part of an HA pair and/or stack
  - The number of monitor ports operating in inline, SPAN, and tap modes
  - The number of dedicated, CIDR, and VLAN interfaces defined
  - The number of administrative users, the custom roles in use, and the permissions in those roles
  - Callback Detector and GAM version for each active device
  - Interface name, protection category and assigned IPS, Malware and Inspection Options policy IDs

- **Feature Usage** — When this information category is selected, the following feature usage information is sent daily to Trellix telemetry servers:
  - Are inbound MSRPC/SMB fragments being reassembled
  - Are outbound MSRPC/SMB fragments being reassembled
  - Callback Detectors status and version
  - Gateway Anti-Malware engine and DAT versions
  - Is ePO integration enabled
  - Is IPS alert notification enabled (SNMP, syslog, email, pager, script)
  - Is inbound GTI IP reputation lookup enabled
  - Is outbound GTI IP reputation lookup enabled
  - Is GTI IP reputation lookup used to enhance SmartBlocking decisions
  - Is inbound heuristic Web application server protection enabled
  - Is outbound heuristic Web application server protection enabled
  - Is inbound XFF header parsing enabled
  - Is outbound XFF header parsing enabled
  - Is advanced callback detection enabled, and are events sent to NTBA for further analysis
  - Is inbound chunked HTTP response traffic being decoded
  - Is outbound chunked HTTP response traffic being decoded
  - Is inbound HTML-encoded HTTP response traffic being decoded
  - Is outbound HTML-encoded HTTP response traffic being decoded
  - Is inbound base64-encoded SMTP traffic being decoded
  - Is outbound base64-encoded SMTP traffic being decoded
  - Is inbound GTI URL Reputation enabled
  - Is outbound GTI URL Reputation enabled
  - Is inbound Microsoft Office File Deep Inspection enabled
  - Is outbound Microsoft Office File Deep Inspection enabled
  - The L7 data collected (protocols and their fields)
  - The advanced malware policy definitions
  - The list of methods enabled for determining alert relevance
  - The number of default IPS policies in use
  - The number of custom IPS policies in use
  - The number of custom Trellix IPS-format attacks in use
  - The number of Snort rules in use
  - The number of ignore rules defined
  - The number of NS-series devices with IPS licenses assigned
  - The number of sub-interfaces in use

- The number of device-pre firewall policies assigned
- The number of port firewall policies assigned
- The number of interface firewall policies assigned
- The number of device-post firewall policies assigned
- The number of IPS attack definitions whose default settings have been customized
- The number of custom NextGen reports and their SQL queries
- The number of interfaces with application identification enabled
- The number of IPS devices with Trellix Intelligent Sandbox integration enabled and malware policies with Intelligent Sandbox analysis enabled
- The number of NTBA devices with EIA integration enabled
- The number of Virtual IPS sensors and Virtual IPS sensor licenses
- The number of Interfaces using policy group
- The number of custom policy group assigned
- The number of default policy group assigned
- The number of devices enabled inbound SSL decryption
- The number of devices enabled inbound SSL decryption with Diffie-Hellman
- Total number of devices with outbound SSL decryption enabled
- Name, grant ID, license key, Sensor model, and allowance count associated with each proxy SSL decryption license
- Total number of devices assigned a system license
- The number of system licenses available and in use
- Name, grant ID, license key, expiration, model and device associated with each system license
- Block and alert only based CVE coverage for each of the IPS policies in use
- Engine status and file types enabled for each of the Malware policies in use
- Option status for each of the Inspection options policies in use

- **System Faults** — With this information category selected, the following system fault information is sent hourly to Trellix telemetry servers:
  - Device Faults
  - Manager Faults

  NOTE

  Though these two events are represented separately, they are sent to Trellix GTI as a single event.

- **Trellix Virtual IPS Cluster Usage** — The following data specific to vIPS clusters is sent daily to Trellix telemetry servers:
  - Name and grant ID associated with each Virtual IPS Sensor license
  - Virtual Sensor license compliance status

- Total number of allowed virtual Sensors
- Total number of Virtual Sensors currently in use with vIPS Clusters
- Total number of virtual probes currently in use with vIPS Clusters
- Maximum number of virtual probes used
- Manager version

> **NOTE**
>
> The above information is necessary for Trellix business intelligence and sent automatically whenever at least one Virtual IPS cluster is defined.

- **Trellix License Usage** — The following data specific to licenses and devices is sent daily to Trellix telemetry servers:
  - System License Details (License ID, Grant ID, Customer Name, expiry time)
  - SSL License Details (License ID, Grant ID, Customer Name, expiry time)
  - Virtual Sensor license details (License ID, Grant ID, Customer Name, expiry time)
  - Virtual Sensor license details (License ID, Grant ID, Customer Name, expiry time)

> **NOTE**
>
> The above information is necessary for Trellix business intelligence and is sent automatically.

3. In **Alert Data Details Filter** field, select the alert severity level(s) for which you want to send the alert details. Available severity levels are **High**, **Medium**, **Low**, and **Informational**.

> **NOTE**
>
> The **Alert Data Details Filter** is displayed only when you select **Alert Data Details** category.

4. In **Technical Contact Information** field, update the following fields to provide your contact information. The Manager collects the contact information only when you provide consent to send them via **Send Contact Information?** option.
   - **First Name**
   - **Last Name**
   - **Street Address**
   - **Phone Number**
   - **Email Address**
5. [Optional] To check whether communication to the GTI server is established, click **Test Connection**.
6. Click **Save** to finish the telemetry configuration task.

Exclude IP address information for specific endpoints

You can define blocks of addresses to be grouped together. By defining these blocks, the information on any alert that contains any IP address matching these blocks will not be sent to Trellix telemetry servers.

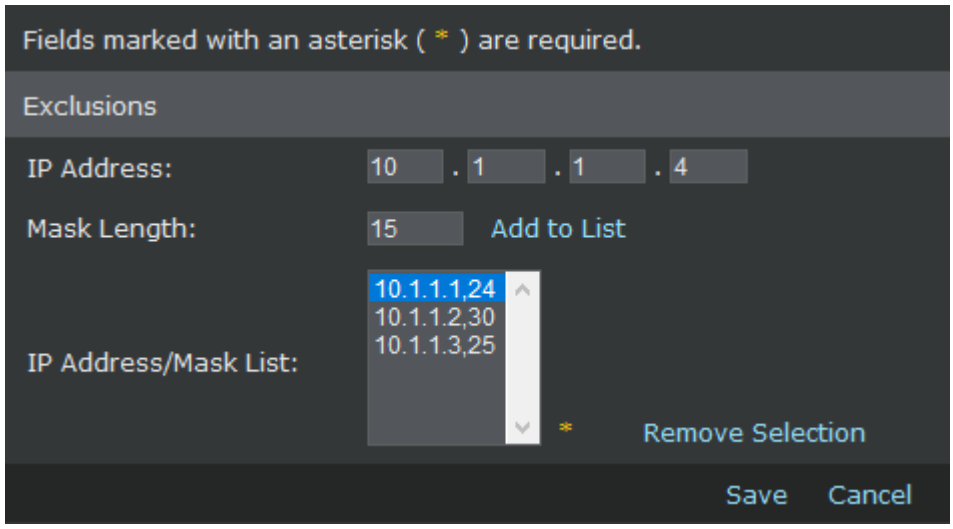
To exclude IP address information for hosts:

1. Go to Manager → <Admin Domain Name> → Setup → **Telemetry**.

   The **Telemetry** page is displayed.

2. Click the **list** hyperlink within **Exclude IP address information for endpoints on this list.** displayed in the **Alert Data Details** section header.

   The **Exclusions** dialog is displayed.



3. Enter the IP address for exclusion in the **IP Address** field.
4. Enter the CIDR value for the mask in the **Mask Length** field.

   NOTE

   The CIDR value should be between 0 to 32.

5. Click **Add to List**.

   The IP address, mask length gets added and is displayed in the **IP Address/Mask List** field.

   NOTE

   You can remove an item in the **IP Address/Mask List** by clicking **Remove Selection**.

6. Click **Save**.

Using Default - Telemetry Next Generation reports

Default - Telemetry Next Generation reports display a complete list of the threat and device telemetry data sent to Trellix. If, at any point, you want to review the data you are sending to Trellix telemetry servers, you can do so by running the required Default - Telemetry Next Generation report(s) from the Analysis → <Admin Domain Name> → Even Reporting → **Next Generation Reports** page.

Following is the list of telemetry reports available in the **Next Generation Reports** page.

Table 4. Telemetry reports

Report Name	Description
Default - Telemetry (Insights Security Posture)	The telemetry information sent by the Manager to the Trellix Insights when Insights integration is enabled. **NOTE** This information is used to derive the security posture score on Trellix Insights.
Default - Telemetry (IPS/Insights)	The information sent by the Manager to the Trellix IPS product team and Trellix Insights team when telemetry is enabled
Default - Telemetry (Trellix)	The information sent by the Manager to the Trellix corporate team when telemetry is enabled
Default - Telemetry (Trellix - Titan F Telemetry Server)	The information sent by the Manager to the Titan F telemetry server when telemetry is enabled

To run and view any Default - Telemetry Next Generation report, follow the steps described in Run Next Generation default report (page 495).

Manager Disaster Recovery (MDR)

Sometimes the worst happens. In this age, where outages to IT systems can cost millions of dollars in lost revenue, lost productivity, and legal issues, every organization must face the near certainty of a system failure occurring at a future date. Anticipating these events and planning corrective courses of action is a prerequisite to business success. Most organizations now employ some manner of business continuity planning (BCP), a subset of which is disaster recovery planning (DRP). To this end, Trellix IPS has long provided a Sensor high-availability configuration; but what if the worst should happen to your Manager server? Most companies are not willing to rely on the manual method of Manager data archival, restoration of backups, and importing of exported policies to recover their Manager as part of their IPS DRP.

Here enters the MDR feature. With MDR, two Manager servers are deployed as part of Trellix IPS. One host is configured as the Primary system; the other as the Secondary. Each uses the same major release Manager software with mirrored databases; however, the two hosts' hardware configuration does not need to be identical. The Secondary Manager can be deployed anywhere, for example, at a disaster recovery site, far from the Primary Manager.

The Primary Manager is the active Manager by default. This Manager communicates with the Update Server, pushes configuration data to the Sensors, and receives alerts from the Sensors.

The Secondary Manager remains in a standby state by default. While in standby mode it monitors the health status of the Primary Manager and retrieves Sensor configuration information from the Primary Manager at configured intervals of time.

NOTE

The Secondary Manager is a warm standby system; it will not guarantee state synchronization with the Primary Manager. It does update configuration information at regular intervals (every 15 minutes), but it does not maintain state. (You can also manually update Secondary Manager configuration rather than waiting for the automatic update.)

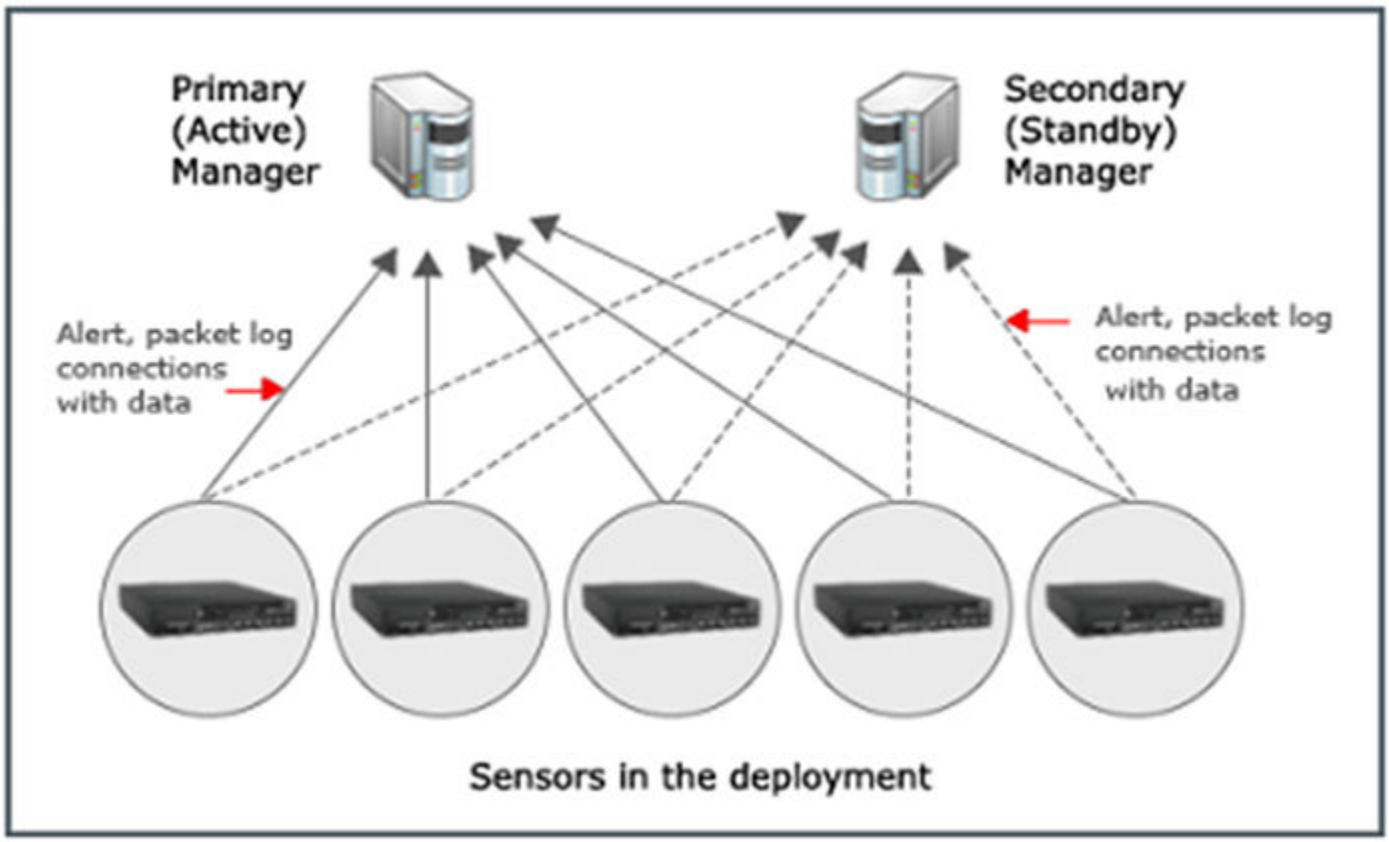
An MDR pair can manage both hardware Sensors as well as Virtual Sensors deployed in an AWS environment.

A Sensor connected to an MDR pair maintains communication with both Managers at all times. The Sensor sends alerts, packet logs to both the Managers. Real-time synchronization between the MDR pair ensures that the data present in the active mode is exactly mirrored in the standby.

In case one of the Managers goes down, after it comes up, it will be updated with the missed alerts and packet log data during the next synchronization from the peer Manager. This synchronization restores the missed alerts and packet log data only from previous 24 hours. The maximum number of alerts and packet logs restored with synchronization is 10,000.

Sensors can only be added to an active Manager. (A new Sensor added to the active Manager in an MDR pair establishes trust first with the Primary Sensor, and then attempts on its own to establish trust with the Secondary.)

Figure 25. Communication of an MDR pair with Sensors



Switchover

Switchover, or failover from the Primary to the Secondary, can be manual/voluntary or involuntary.

NOTE

In a situation where you have planned manual downtime and the downtime is expected to be brief, Trellix recommends that you manually suspend MDR, preventing the Secondary Manager from taking over and becoming active. You can then resume MDR when the downtime period is over.

The Secondary Manager performs regular “health checks” on the Primary Manager. If the Primary Manager is found to be unavailable during a health check by the Secondary Manager, the Secondary Manager waits for a configurable time interval. If the Primary Manager is still unavailable after that time period elapses, control then switches over to the Secondary Manager.

NOTE

You can switch over to the Secondary manually, as well.

Once the Secondary Manager is active, the Primary moves to standby. The Sensors are made aware of the switchover, communicate with the Secondary Manager, and the system continues to function without interruption.

All “in-flight transactions” are lost upon failover from Primary to Secondary Manager. For instance, if the Primary Manager failed while a user was in the middle of a policy edit, the Secondary Manager will not be able to resume the policy edit.

NOTE

The MDR feature, in fact, assumes that the Secondary Manager is a standby system, and that it will NOT assume control indefinitely. The Primary Manager should be diagnosed and repaired, and be brought back online.

While the Secondary Manager is active, Trellix recommends against making any configuration modifications on the Secondary Manager, as these modifications could cause potential data synchronization problems when the Primary Manager is resurrected.

Once the Primary Manager has recovered, you can switch control back to the Primary system. During this switch back, if you have made configuration changes on the Secondary, you have a choice whether to retain the configuration on the Primary or overwrite with changes made on the Secondary. After switch-back, alert and packet log data is copied from Secondary to Primary Manager, and can be viewed in the **Attack Log** page. Data is re-synchronized, the Sensors return to communicating with the Primary, and the system is restored with the Primary Manager active and the Secondary Manager in standby mode.

NOTE

You can easily dissolve the MDR relationship between the two Managers and return either Manager to stand-alone mode.

Preparations for Manager Disaster Recovery (MDR)

The Setup → **MDR** option enables you to have a standby Manager available in cases where the Primary Manager fails.

Manager Disaster Recovery (MDR) feature is available for deployments where the following conditions are met:

- Two Managers (called Primary and Secondary) are available. The Primary is in active mode and the secondary in standby mode.
- The Primary and Secondary use the same Manager software release version. Manager version of both Primary and Secondary Manager needs to be similar for the creation of MDR pair.
- The Primary and Secondary Managers share the same database structure.

The Primary and Secondary Managers can be located in the same Network Operations Center (NOC) or in geographically diverse locations, as long as they can communicate via SSL through TCP port 443. Managers can also be on different hardware.

If the Primary and Secondary Managers are located in different geographical regions, then there needs to be time synchronization between the two Managers keeping the Coordinated Universal Time (UTC) as the standard time.

Let's say, one Manager is in California (UTC - 8 hours), and the other Manager is in New York (UTC - 5 hours). The MDR setup will work in this scenario as long as the time set in both the Managers are in sync with each other. That is, at 09:00 UTC hours, if the Manager in California shows 01:00 hours local time, and the Manager in New York shows 04:00 hours local time, MDR will work.

Note that the Sensor does not have a built-in clock. It gets UTC time from the Manager.

NOTE

When upgrading the Primary and Secondary Managers, first suspend MDR. Otherwise, MDR may malfunction. Once MDR is suspended, upgrade the Primany Manager, and then upgrade the Secondary Manager. Once both Managers are upgraded, resume MDR.

Sensors communicate to the Primary and Secondary Managers independently. The Secondary Manager receives configuration information from the Primary on a regular basis. If the Managers are unable to communicate with each other, the Secondary Manager queries each Sensor and becomes active only when a majority of Sensors fail to reach the Primary. The Secondary Manager can also become active by performing manual switchover.

NOTE

Custom roles created on the Primary Manager are automatically copied onto the Secondary Manager.

When the Secondary Manager becomes active, all the alerts present in Primary manager also appears in the **Attack Log** page of the Secondary Manager. The switch-back from the active Secondary Manager to the Primary Manager does not occur automatically. There is a manual switch-back action that is required to be performed from the Primary Manager.

After switch-back, alert and packet log data is copied from the Secondary Manager to the Primary Manager. This data can be viewed in the **Attack Log** page.

MDR communication

The MDR architecture incorporates Sensor to Manager communication and Manager to Manager communication.

A Sensor connected to an MDR pair maintains communication with both Managers at all times. The Primary Manager synchronizes data with the Secondary Manager every 15 minutes. However, the Primary and Secondary Managers receive system events from a Sensor independently, and store the events also independently. If the Sensor has trouble communicating with the Primary Manager, it will send a system event to the Secondary Manager about the communication error between it and the Primary Manager.

Sensor to Manager communication

Sensors in Trellix IPS are MDR-aware. When Sensors first establish trust with the Manager, they query the Manager to find out if the Manager is part of an MDR pair. The Manager responds and, if it is part of an MDR pair, includes its current status (active or standby) and the IP of its peer Manager. The Sensor then establishes trust with the peer as well.

The Sensor sends alerts and packet logs to both the Managers. Real-time synchronization between the MDR pair ensures that the data present in the active mode is exactly mirrored in the standby. This ensures minimal loss of data if the active Manager goes down. Alerts and packet logs sent by the Sensor to the Manager can be viewed in the **Attack Log** page.

In addition to alerts, faults are also synchronized between the Managers. You can view all hosts, alerts, and packet log data in the **Attack Log** page.

If one of the Managers goes down, after it comes up, the other Manager will update the missed alerts and packet log data to the first Manager during synchronization.

Manager to Manager communication

The Primary and Secondary Managers exchange a "heartbeat" communication once each minute, . This communication includes a byte of data specific to the health of the Manager in question. Manager receiving the heartbeat concludes that its peer has failed under two scenarios:

- One of the Trellix IPS subsystems reports a failure.
- A heartbeat has not been received within the **Downtime Before Switchover** interval (configured using the **Pair Creation** action). For example, if the default interval is 5 minutes and the heartbeat is sent once a minute, the Secondary Manager takes control after five minutes of missed heartbeats.

If the Secondary Manager becomes unavailable, the Primary remains active and logs the failure. If the Primary Manager becomes unavailable, the Secondary logs the event and becomes active.

If both Managers are online but are unable to communicate with each other, the Secondary Manager queries each Sensor and becomes active only if more than half the Sensors cannot communicate with the Primary Manager.

Data synchronization between the Primary and Secondary Manager occurs every 15 minutes.

Alert Synchronization between an MDR Pair

When the alert is sent to the Manager, it is acknowledged for storage or marked for deletion.

If one Manager goes down, after it comes up, the other Manager will update the missed alerts and packet log data to the first Manager during synchronization.

> **NOTE**
>
> Alert synchronization between peer Managers restores missed alerts and packet logs from previous 24 hours. The maximum number of alerts and packet logs restored with synchronization is 10,000.

MDR alert synchronization model

There are 2 types of alert actions that can be performed in the Attack Log:

- Acknowledge/Unacknowledge
- Delete

The active Manager identifies these alert actions that are performed in the Attack Log and forwards these alert actions to the standby Manager. The standby Manager accepts these alert actions and updates in the Attack Log.

Alert action synchronization between Managers

The actions that are triggered on these generated alerts from the active Manager are synchronized with the standby Manager in real time.

The following table explains the possible scenarios that can be observed during MDR alert action synchronization.

Scenario	MDR alert action synchronization
No Communication between MDR Managers.	Alert actions from active manager fails to synchronize to the standby Manager in real time. These actions are saved in the database and cache, and will be synchronized to the standby Manager as soon as the connection is back.
Standby Manager is down.	Alert actions from active Manager fails to synchronize to the standby Manager in real time. These actions are saved in the database and cache, and will be synchronized to the standby Manager as soon as the connection is back.
Active Manager goes down comes back as standby.	Any alert actions done in the new active manager will be synchronized to the new standby Manager.
MDR is suspended.	Alert actions are not synchronized when the MDR is in suspended mode. These actions are saved in the database and cache, and synced when MDR is resumed.

NOTE

Alert synchronization between the peer Managers restores the missed alerts and packet logs from previous 24 hours. The maximum number of events restored with synchronization is 10,000.

Configure MDR

Prerequisite:

You must have a freshly installed Manager to be configured as the Secondary Manager.

The **Pair Creation** action enables you to configure both the Primary and Secondary Managers used for MDR.

Initial MDR Configuration

First, you must configure MDR separately on both the Primary and Secondary Managers.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → **MDR**.

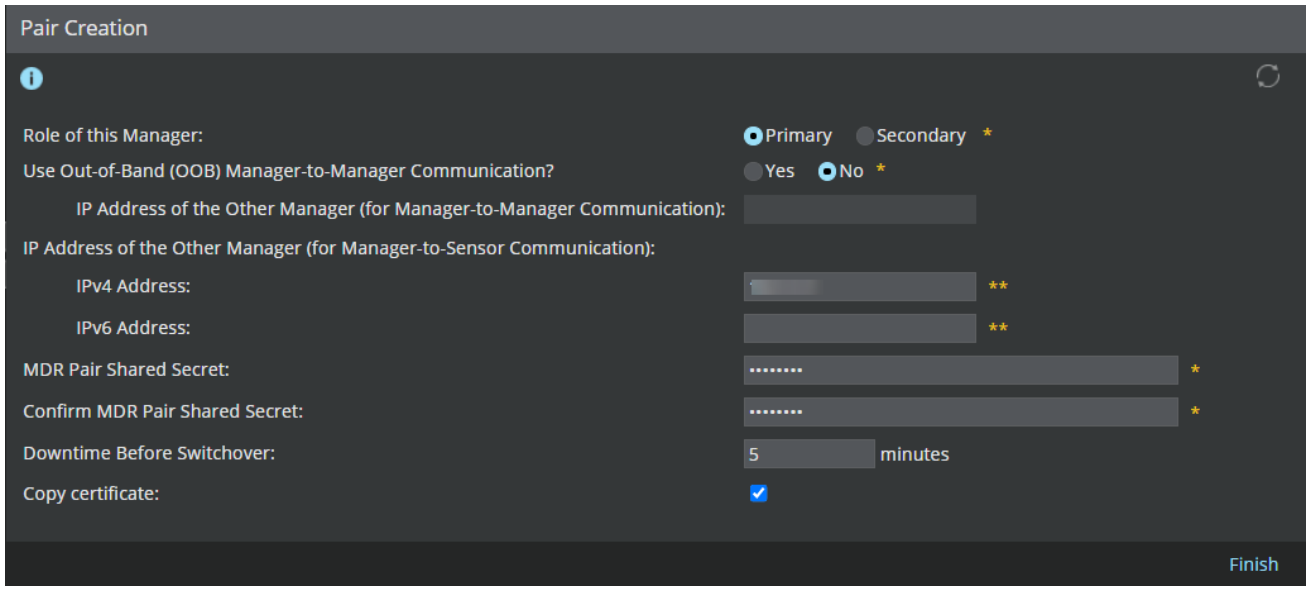
NOTE

The Manager supports a maximum of three IP addresses during MDR configuration. The Manager assumes that all the IP addresses are bound to the same host name.

NOTE

The Manager supports one public IPv6 address per NIC. This means that there should be only one IPv6 address for the IPv6 stack supported by your operating system.

Figure 26. MDR Pair Creation page



2. Fill in the following fields:

Table 5. Option definitions

Option	Definition
Role of this Manager	Select **Primary** to use this Manager as the active Manager, or **Secondary** to use this Manager as the standby.
Use Out-of-Band (OOB) Manager-to-Manager Communication?	• Yes to use separate interfaces for Manager-Manager and Manager-Sensor communication. • No to use the same interface for Manager-Manager and Manager-Sensor communication.
IP Address of the Other Manager (for Manager-to-Manager Communication)	This option appears if you selected the option **Yes** in **Use Out-of-Band (OOB) Manager-to-Manager Communication?**. Enter the IP address of the other Manager that you want to use for Manager-Manager communication. **NOTE** If you set **Use Out-of-Band (OOB) Manager-to-Manager Communication?** to **Yes** in the Primary Manager, then set this option as **Yes** in your Secondary Manager as well. A mismatch in this option setting between the Primary and Secondary Manager pair will result in an MDR configuration failure.

Option	Definition
IP Address of the Other Manager (for Manager-to-Sensor Communication)	Enter the IP address of the other Manager that is used for communication with the Sensor.
MDR Pair Shared Secret	The same shared secret key must be entered on both Managers for MDR creation to be successful. Enter a minimum of eight characters and use no special characters.
Confirm MDR Pair Shared Secret	Re-enter the same shared secret key.
Downtime Before Switchover	Enter the downtime in minutes before the switch to the Secondary Manager occurs. Downtime before switchover should be between 1-10 minutes. This field is disabled if the **Role of this Manager** of Manager is set to Secondary.
Copy certificate	Select this option to Copy the SSL certificate for web server authentication from Primary Manager to Secondary Manager in the MDR pair. **NOTE** The **Copy certificate** option is available only in the Primary Manager. **NOTE** The **Copy certificate** option does not impact working of the Manager MDR.

3. Click **Finish** to confirm your changes.

NOTE

When you click **Finish** and your peer Manager's MDR settings are not yet configured, then Trellix IPS displays a warning to remind you to configure the peer Manager MDR settings.

You can configure either **IPv4 address** or **IPv6 address** or both for Manager-Sensor communication as given in the following scenarios:

- If a Sensor is connected to Manager over an IPv4 network, or you want to add a Sensor from the IPv4 network to the Manager, you need to enter the **IPv4 address** of the peer Manager.
- If a Sensor is connected to Manager over an IPv6 network, or you want to add a Sensor in the IPv6 network to the Manager, you need to enter the **IPv6 address** of the peer Manager.
- If there are Sensors configured in Manager over both IPv4 and IPv6 networks, you need to configure both **IPv4 address** and **IPv6 address** of the peer Manager.

NOTE

While configuring the **IP Address of the Other Manager (for Manager-to-Sensor Communication)**, make sure that the operating system support both IPv4 and IPv6 stacks.

- When **Use Out-of-Band (OOB) Manager-to-Manager Communication** is set to No, **IP Address of the Other Manager (for Manager-to-Sensor Communication)** is used for both Manager-Manager and Manager-Sensor communication.
- When **Use Out-of-Band (OOB) Manager-to-Manager Communication** is set to Yes, **IP Address of the Other Manager (for Manager-to-Sensor Communication)** is used only for Manager-Sensor communication.

IMPORTANT

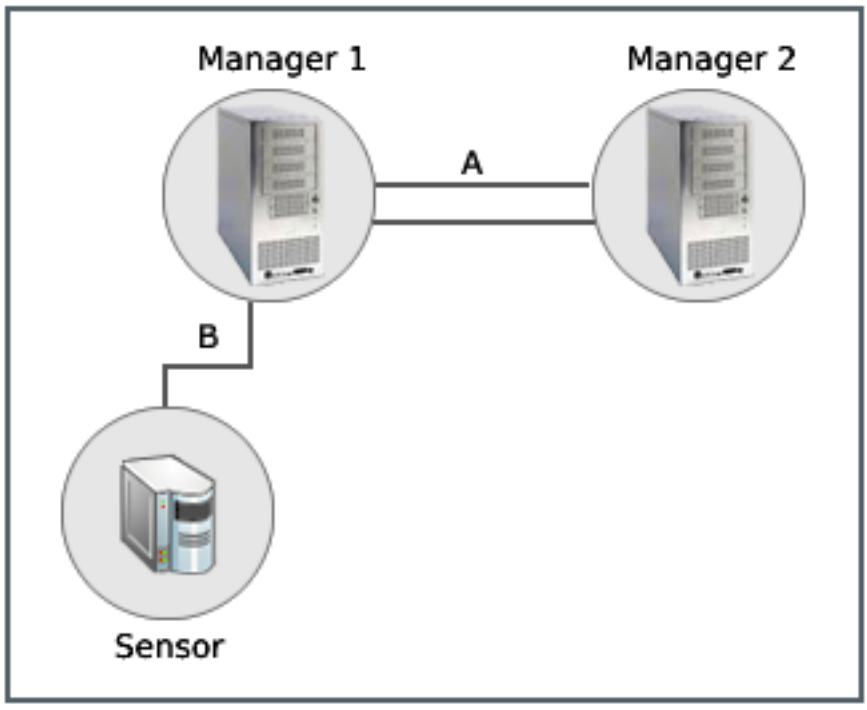
You need to use the **IP Address of the Other Manager (for Manager-to-Sensor Communication)** while establishing trust between the Sensor and Manager. Ensure that your peer Manager is configured to use the same IP address as selected from the **Dedicated Interface** list during the Peer Manager installation. If misconfigured, Trellix IPS generates an error message to prompt you to enter the correct IP address. For more information on Sensor communication Interface, see [Trellix Intrusion Prevention System Installation Guide].

Scenarios for MDR configuration

Scenario 1

Two Managers are in an MDR pair, and you are adding the Sensor configuration information in Manager 1.

Figure 27. MDR Scenario 1



If connection A between Manager 1 and Manager 2 is over IPv4 network, and you are adding Sensor configuration in Manager 1, the communication between Manager 1 and Sensor (that is, connection B) should also be over IPv4 network.

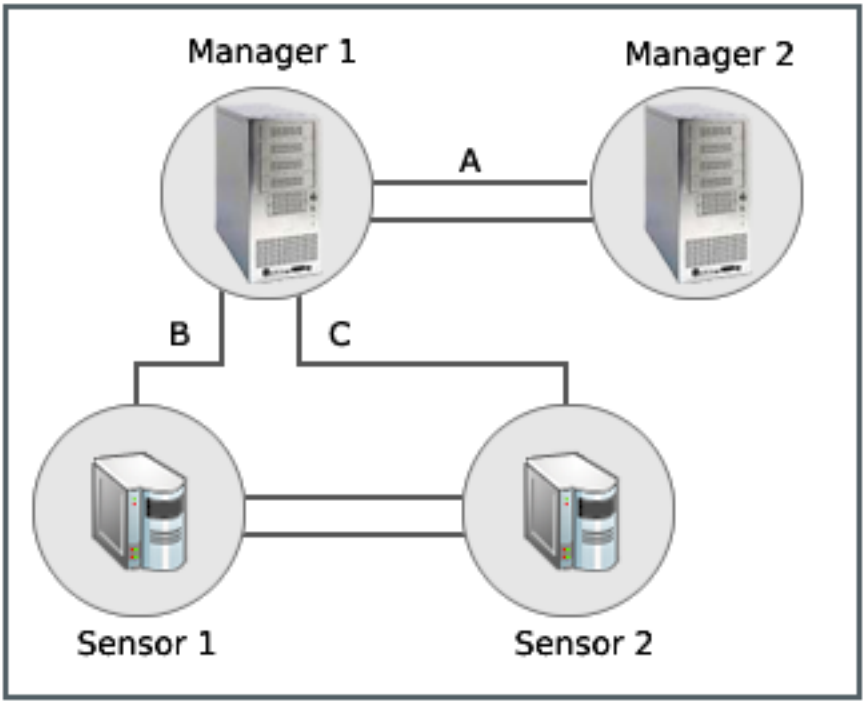
Similarly, if connection A between Manager 1 and Manager 2 is over IPv6 network, and you are adding Sensor configuration in Manager 1, the communication between Manager 1 and Sensor (that is, connection B) should also be over IPv6 network.

If connection A between Manager 1 and Manager 2 is over both IPv4 and IPv6 networks, and you are adding Sensor configuration in Manager 1, the communication between Manager 1 and Sensor (that is, connection B) can be configured over either IPv4 or IPv6 network.

Scenario 2

Suppose Manager 1 is standalone (not part of an MDR pair), and you want to add a peer Manager (that is, Manager 2) with Manager 1 to form an MDR pair.

Figure 28. MDR Scenario 2



If the communication between Sensors and Manager 1 (that is, connection B and C) is over IPv4 network, the communication between Manager 1 and Manager 2 (that is, connection A) should also be configured for IPv4 network.

Similarly, if the communication between Sensors and Manager 1 (that is, connection B and C) is over IPv6 network, the communication between Manager 1 and Manager 2 (that is, connection A) should also be configured for IPv6 network.

If B and C support both IPv4 and IPv6 networks, A can be configured to support either IPv4 or IPv6 network.

Using NAT (Network Address Translation)

Network Address Translation (NAT) is a technique in which the source and/or destination addresses of IP packets are rewritten as they pass through a router or firewall. It is commonly used to enable multiple hosts on a private network to access the Internet using a single public IP address.

Only static NAT entries are supported in Manager. Consider the following scenarios to explain the use of NAT in Manager:

Scenario 1: Manager using a private IP address

To establish the Manager-Sensor communication, configure the Manager's public IP address (external reachable) on the Sensor by using the following CLI command:

```
set manager IP
```

> **NOTE**
>
> To support multiple NIC cards, you need to select the respective local IP address in **Sensor Communication Interface** during Manager installation.

> **NOTE**
>
> For more information on **Sensor Communication Interface**, see [Trellix Intrusion Prevention System Installation Guide].

Scenario 2: Sensor using a private IP address

The Manager-Sensor communication works as usual. You need not make any changes to the setup to achieve this.

Configuring MDR with NAT

To set up MDR with NAT, consider the following scenarios:

Scenario 1: Manager-Sensor communication with NAT and Manager-Manager communication without NAT

Configure the public IP address (external reachable) in the **Peer Host IP address** field to establish Manager-Sensor communication.

> **NOTE**
>
> To support multiple NIC cards, select the respective IP address in the **Sensor communication Interface** field during installation. For more information, refer to [Trellix Intrusion Prevention System Installation Guide].

Configure the **OOB Peer Manager IP** field with the local IP address of the peer Manager to reach the Manager without using NAT.

If Manager is in a private network, enter the public IP address in the **Peer Host IP address** field of the Secondary Manager.

Scenario 2: Manager-Sensor Communication with NAT and Manager-Manager communication with NAT

Configure the public IP address (external reachable) in the **Peer Host IP address** field to establish Manager-Sensor communication.

You need not configure **OOB Peer Manager IP** field as communication takes place using the **Peer Host IP Address** field.

NOTE

In case the peer Manager uses different translated IP addresses, you can configure the public (external reachable) IP address in the **OOB Peer Manager IP** field.

How to view the current details of MDR

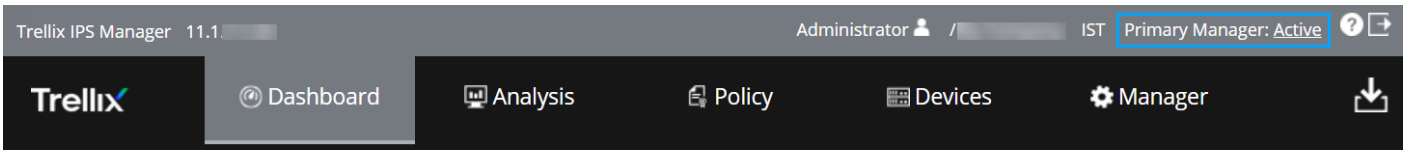
The **Pair Creation** action enables you to view the current state of MDR functions including Primary Manager status, Secondary Manager status, and a summary of current MDR settings. To view the MDR status and the details, click Manager → <Admin Domain Name> → Setup → **MDR**. You will be able to see the status and the details only if you have configured a peer manager already as part of MDR.

NOTE

The **Pair Creation** action assigns a GUID to the MDR pair. The GUID of the primary Manager in an MDR pair is assigned as the **MDR Pair GUID**. That is, if the GUID of the primary Manager is 8a4534bd-9c6b-4a40-aa2d-383611358801 and GUID of the secondary Manager is 8a4594bd-8c6b-4a90-cd2d-431211358832, the Manager Pair GUID is 8a4534bd-9c6b-4a40-aa2d-383611358801.

You can also view the MDR status in the application header.

Figure 29. MDR status



MDR status displays the role of the Manager, whether it is Primary or Secondary. It also displays the status link of the Manager, whether it is in Active or Standby mode. Clicking on the **Active** status link navigates to the **MDR** page on the **Manager** tab.

MDR Actions

After configuring MDR, the following actions are available:

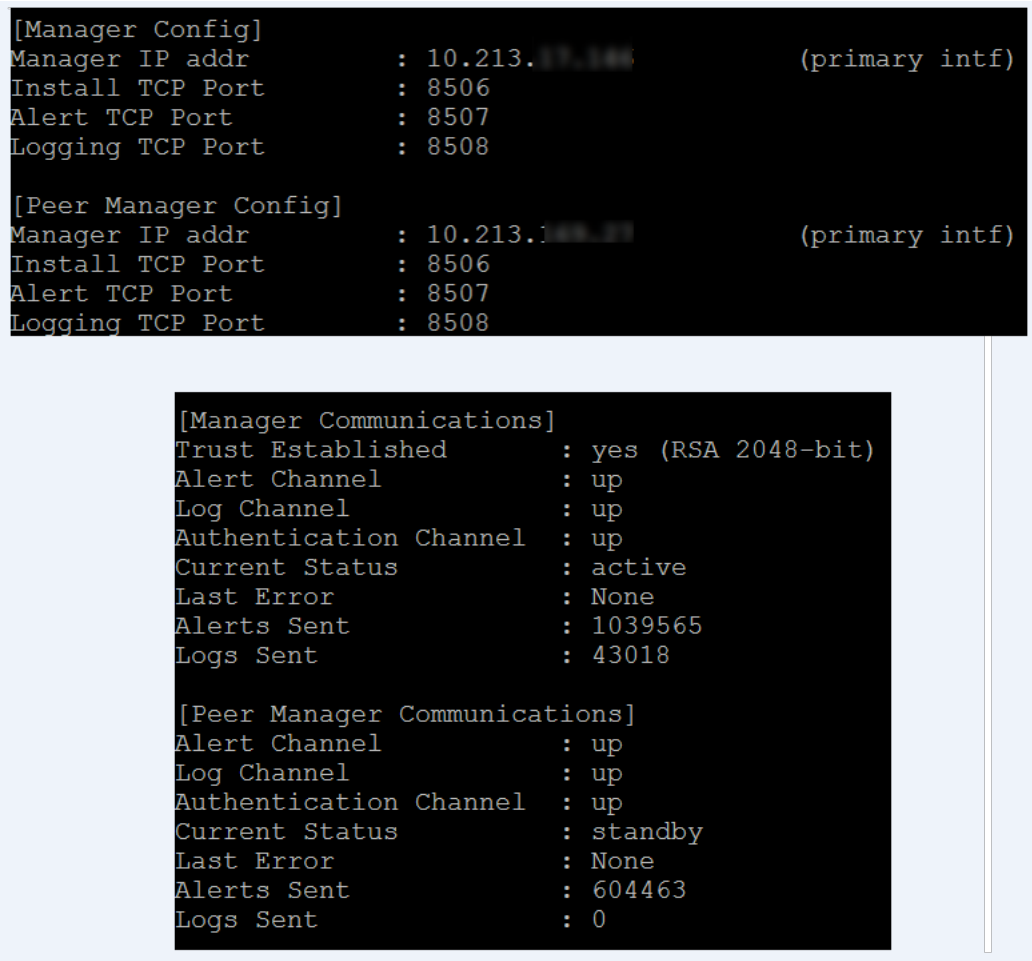
Action	Description	Availability
Reset to Standalone	End MDR and have sole control of Sensors using one of the Managers.	Available on both the Primary and Secondary Managers.
Switch Over	Request that the Secondary Manager be active.	Available only when the Primary Manager is active.
Switchback	Switch back from the Secondary Manager and make the Primary Manager active.	Available when the Primary Manager status is in standby mode.

Action	Description	Availability
Suspend MDR	Instruct the Secondary Manager not to monitor via MDR Status check and to resume MDR only when indicated.	Available only on the Primary Manager when in the active state.
Resume MDR	Resume MDR mode when the MDR is suspended.	Available only when the Primary Manager is in the suspended state.
Force Switch	Force the Secondary Manager to become active.	Available only when the Secondary Manager is in standby mode.
Retrieve Configuration	Transfer configuration data from the Primary Manager to the Secondary Manager. This is provided to allow manual synchronization between Managers in addition to the automatic transfer of configuration data at regular time intervals.	Available in the Secondary Manager only when it is in standby mode.

MDR verification via CLI

The **show** and **status** commands include information specific to MDR. For more information on using CLI commands, see the [CLI commands] section.

Figure 30. MDR verification via CLI



Manager Disaster Recovery (MDR) best practices

A newly created MDR pair does not synchronize for the first 15 minutes after creation. This is by design because, depending on the quantity of the Sensors, it takes approximately 5 to 10 minutes for the newly formed pair to finish MDR-related tasks and become stable.

If you have only one or two Sensors, you can press the **Retrieve Configuration** button in the **MDR** page of the secondary Manager soon after MDR creation to force the Managers to synchronize. In most cases, however, we recommend you wait for 15 minutes and allow the new MDR pair to synchronize automatically.

If you return to the user interface of the primary Manager, the details on the Manage MDR page validate the information seen on the secondary.

Manage Central Manager details

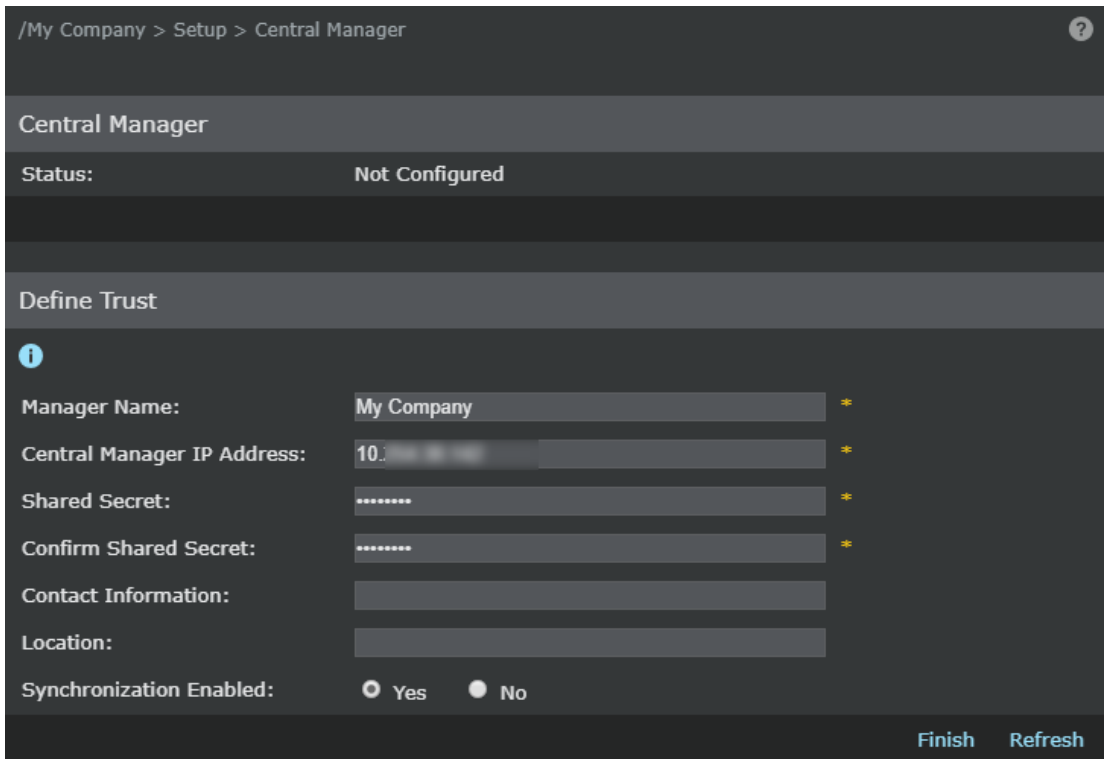
To enable trusted communication between your Manager and Central Manager, you need to specify the details of Central Manager in Manager. Once communication has been established, Central Manager can synchronize with Manager and can access its configuration.

To add a Manager to Central Manager, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → **Central Manager**.

Figure 31. Central Manager Trust Establishment page



2. Type the **Manager Name**.

   The **Name** must begin with a letter. The maximum length of the Name is 40 characters.

> **NOTE**
>
> Special characters except hyphens and underscores are not allowed.

3. Enter **Central Manager IP Address**. This can be either IPv4 or IPv6 address.
4. The **Shared Secret** must be a minimum of 8 characters and maximum of 64 characters in length. The **Shared Secret** cannot start with an exclamation mark nor have any spaces. **Secret** parameters that can be used in Manager are:
   - 26 alpha: upper and lower case (a,b,c,...z and A, B, C,...Z)
   - 10 digits: 0 1 2 3 4 5 6 7 8 9
   - 32 symbols: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <? /

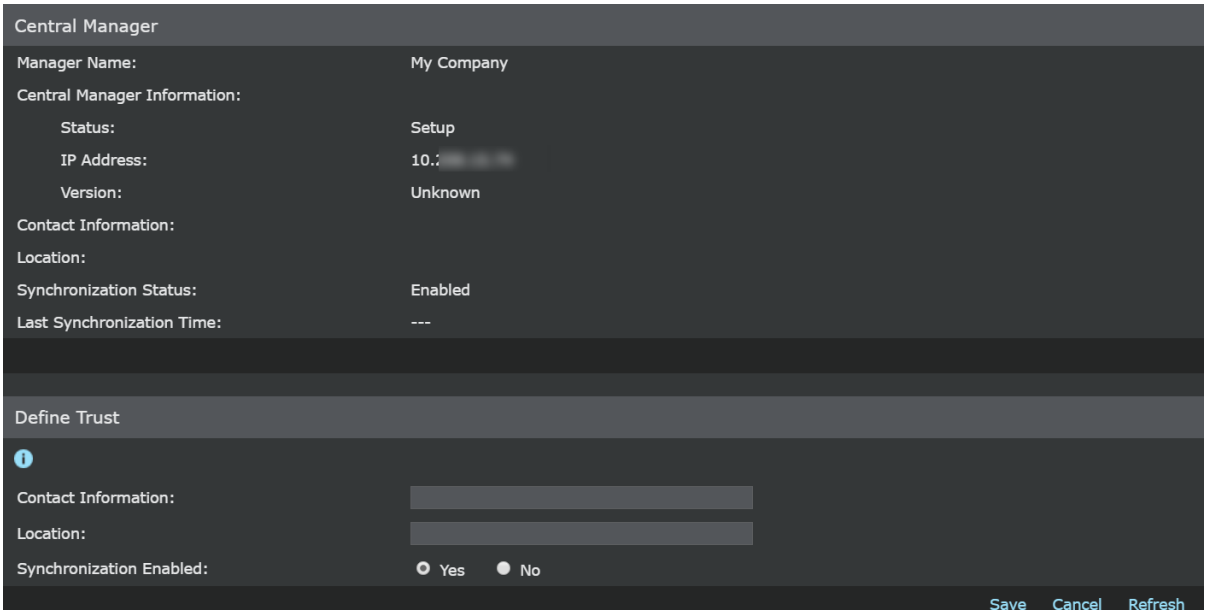
> **CAUTION**
>
> The exact, case-sensitive **Manager Name** and **Shared Secret** must also be entered into the Central Manager setup. If not, the Manager will not be able to register itself with the Central Manager.

Retype the **Shared Secret** to confirm.

5. Type the **Contact Information** and **Location** (Optional).
6. **Synchronization Enabled** is enabled by default. Select **No** to disable synchronization with Central Manager.
7. Click **Finish** to begin the Central Manager-Manager trust establishment process.

> **NOTE**
>
> Trust establishment to Central Manager may take a while. You will need to Refresh the page to see the latest settings.

Figure 32. Central Manager Details



Establishing communication with Central Manager

Trellix IPS provides a centralized, "manager of managers" capability named Trellix Intrusion Prevention System Central Manager.

Trellix IPS Central Manager allows users to create a management hierarchy that centralizes policy creation, management, and distribution across multiple Trellix IPS Managers. For example, a policy can be created in the Central Manager and synchronized across all Managers added to that Central Manager. This avoids manual customization of policy at every Manager.

The Central Manager provides you with a single sign-on mechanism to manage the authentication of global users across all Managers. Sensor configuration and threat analysis tasks are performed at the Manager level.

A Manager can be added to Central Manager using a method similar to that of adding a Sensor to a Manager, or configure Managers to work in MDR mode by establishing trust between a Secondary and Primary pair.

NOTE

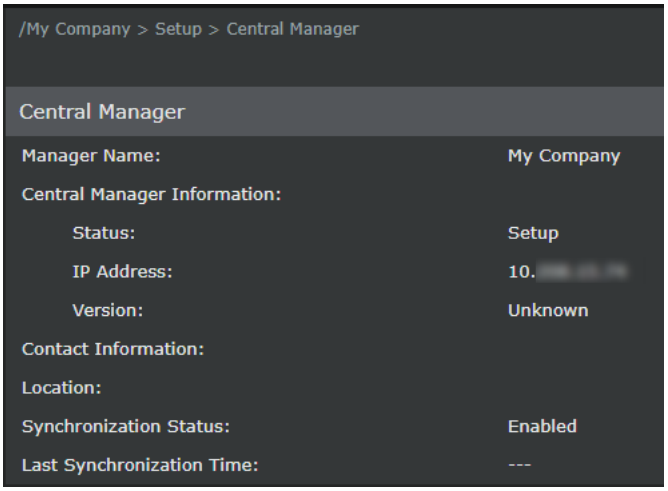
When trust establishment is initiated from Manager to Central Manager, the system may take approximately two minutes to display the configured Manager on the Central Manager Resource Tree.

The Manager → <Admin Domain Name> → Setup → **Central Manager** option enables the viewing and managing details for synchronizing with Central Manager.

Viewing Central Manager details

The Central Manager page shows Central Manager configuration details such as Manager Name, Central Manager IP Address, contact information, location, and Synchronization Enabled (Y/N). If Central Manager is configured in an MDR pair, then details of the MDR pair are available in Manager.

Figure 33. Central Manager Details Page



Field	Description
Manager Name	Logical name given to Manager to connect to the Central Manager
Status	Status of trust establishment between the Manager and Central Manager
IP Address	Central Manager server's IP address
Version	Central Manager's version number
Contact Information	Name of contact person
Location	Geographical location (area, city)
Synchronization Status	Enable synchronization between the Central Manager and Manager (It is Enabled by default)
Last Synchronization Time	The last synchronized time between the Central Manager and Manager

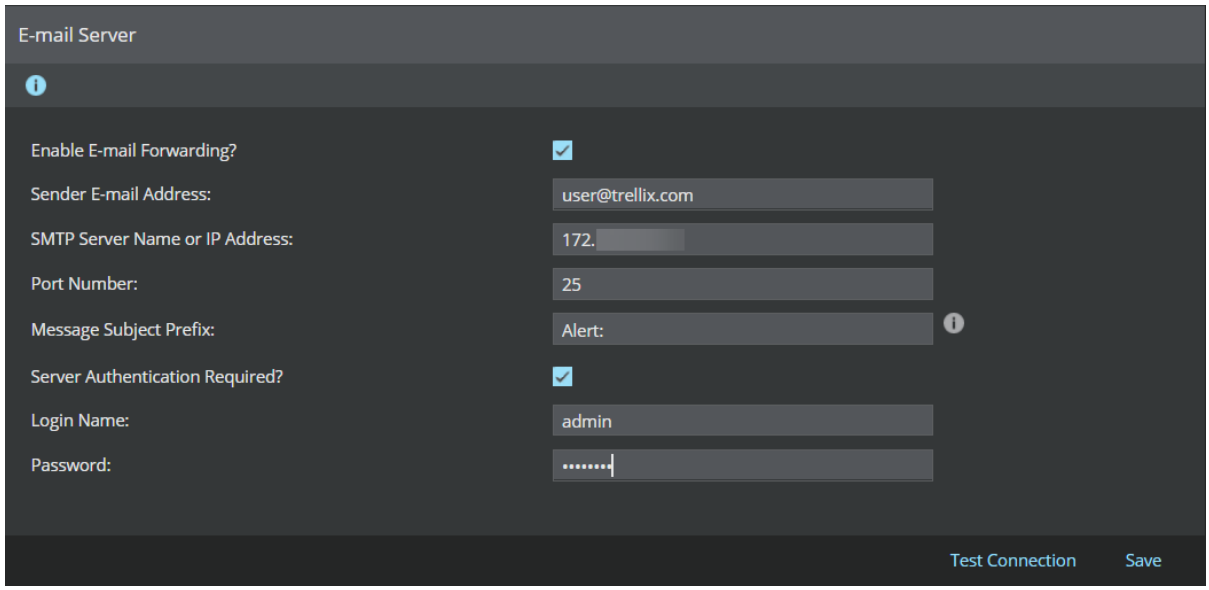
Specify an email server for notifications

Using the **E-mail Server** option, you can configure Manager (or Central Manager) to point to an email server for sending out system emails. For example, these emails can be security notifications that have been prioritized by selecting **E-mail** or **Pager**. Using this action, you can also specify the **From** address for the system emails.

To configure a mail server for notifications, do the following:

1. Select Manager → <Admin Domain Name> → Setup → **E-mail Server**.

Figure 34. E-mail Server Configuration



2. Provide the following information:
   - **Enable E-mail Forwarding?** — Select the check box to allow notifications to be sent to an email server, or deselect the check box to disable notifications to the email server.
   - **Sender E-mail Address** — Email address from where messages are sent.
   - **SMTP Server Name or IP Address** — IP address or name of the email server.
   - **Port Number** — Port number on which SMTP Server is listening.

     NOTE

     By default, port **25** (default SMTP port) is set in the **Port Number** field. You can change it depending on the SMTP port you set while configuring the email server.

   - **Message Subject Prefix** — This is an optional field where the text entered in it is prefixed to the message subject for all emails sent by the Manager.
   - **Server Authentication Required?** — Select the check box if Server Authentication is required, or leave it unchecked if Server Authentication is not required.
   - **Login Name** — of the sender's email account.
   - **Password** — of the sender's email account.

3. Click **Save** to apply all the changes.

> **NOTE**
>
> Upon saving the changes, you can click **Test Connection** to test if the SMTP server connection is successful or not.

Specify a proxy server for Internet connectivity

If you employ a proxy server for Internet connectivity, you can configure the Manager or your devices to connect to that server for proxy service. This is necessary if you want to download updates directly to Manager from the Update Server or if you want to download host reputation and country of origin information during integration with TrustedSource.

The Manager supports application-level HTTP/HTTPS proxies, such as Squid, iPlanet, Microsoft Proxy Server, and Microsoft ISA.

> **NOTE**
>
> To use Microsoft ISA, you must configure this proxy server with basic authentication. Trellix IPS does not support Microsoft ISA during NTLM (Microsoft LAN Manager) authentication.

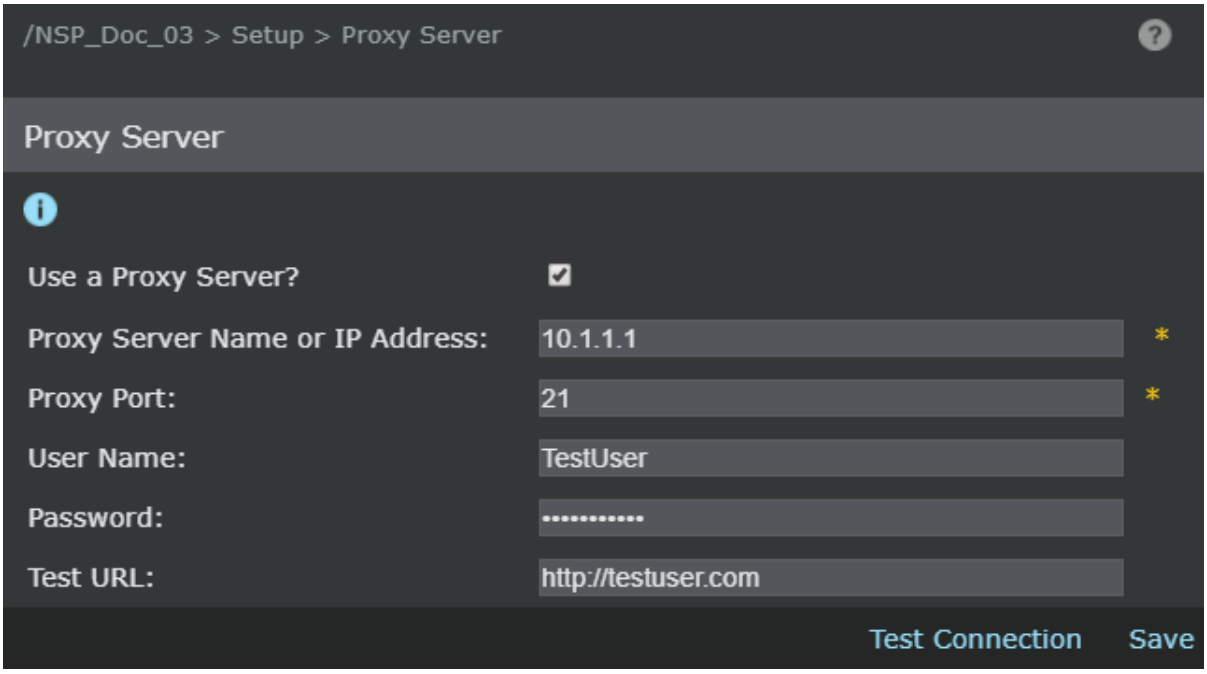
> **NOTE**
>
> SOCKS, a network-level proxy, is not currently supported by Trellix IPS.

To specify your proxy server, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → **Proxy Server**. The **Proxy Server** page is displayed.

Figure 35. Proxy Server Settings



2. Type the **Proxy Server Name or IP Address**. This can be either IPv4 or IPv6 address.
3. Type the **Proxy Port** of your proxy server.
4. Type **User Name** and **Password**.
5. Provide the appropriate URL. You may test to ensure that the connection works by entering a **Test URL** and clicking **Test Connection**.
6. Click **Save** to save your settings.

   When the Manager or the device makes a successful connection, it displays a message indicating that the proxy server settings are valid.

Managing Licenses

Licenses are required by the Manager to access certain Sensor functionalities. You can use the **Licenses** page to manage the following licenses:

- System
- Proxy Decryption
- Virtual Sensors

System

The NS9500, NS7600, NS7500, NS3600, and NS3500 Sensors require a license to activate the baseline throughput of 10 Gbps on NS9500 Sensors, 5 Gbps on NS7600, 3 Gbps on NS7500, 1 Gbps on NS3600, and 750 Mbps on NS3500 Sensors. The license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the details of the throughput for the Sensors.

In the case of the NS9500 standalone and stack, and NS7500 Sensors, a new license with higher throughput, or upgrade license is required to increase the throughput of the Sensor. Various throughputs available for NS9500, NS7600, NS7500, and NS3600 Sensors are as follows:

Sensor	Existing license	*Upgrade license
NS9500 standalone **NOTE** You must have a stack Sensors setup to upgrade licenses from Standalone to Stack.	10 Gbps	• 10 to 20 Gbps • 10 to 30 Gbps Standalone to stack: • 10 to 40 Gbps • 10 to 60 Gbps • 10 to 100 Gbps
	20 Gbps	• 20 to 30 Gbps Standalone to stack: • 20 to 40 Gbps • 20 to 60 Gbps • 20 to 100 Gbps
	30 Gbps	Standalone to stack: • 30 to 40 Gbps • 30 to 60 Gbps • 30 to 100 Gbps
NS9500 stack	40 Gbps	• 40 to 60 Gbps • 40 to 100 Gbps
	60 Gbps	60 to 100 Gbps
	100 Gbps	NA
NS7600	5 Gbps or, 10 Gbps or, 15 Gbps	NA
NS7500	3 Gbps	• 3 to 5 Gbps • 3 to 7.5 Gbps
	5 Gbps	5 to 7.5 Gbps
	7.5 Gbps	NA

Sensor	Existing license	*Upgrade license
NS3600	1 Gbps or, 3 Gbps or, 5 Gbps	NA
*Upgrade capacity licenses are available for perpetual licenses only. Those are not applicable for demo or subscription licenses.		

For more information, see the [Trellix Intrusion Prevention System Installation Guide].

NOTE

Upgrade capacity licenses are not available for individual NS7600 and NS3600 sensors or NS7600 and NS3600 Sensors in failover pairs.

Proxy Decryption

The proxy SSL decryption feature requires a license to access a few Sensor functionalities. The proxy license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the number of Sensors on which the proxy SSL feature can be enabled.

A valid outbound and inbound proxy based SSL decryption license can be obtained for the following Sensor models:

Sensor Model	Outbound proxy based SSL decryption	Inbound proxy based SSL decryption
NS9500 (Standalone) with 30 Gbps	Yes	Yes
NS9500 (Standalone) with 20 Gbps	Yes	Yes
NS9500 (Standalone) with 10 Gbps	Yes	Yes
NS9200	Yes	NA
NS9100	Yes	NA
NS7500 with 7.5 Gbps	Yes	Yes
NS7500 with 5 Gbps	Yes	Yes
NS7500 with 3 Gbps	Yes	Yes
NS7300	Yes	NA
NS7200	Yes	NA

For more information, see Managing licenses for proxy based SSL decryption (page 1144).

NOTE

Proxy based SSL decryption (both inbound and outbound) is not supported in NS7600 and NS3600 Sensors.

Virtual Sensors

Virtual Sensors require a software license to activate the baseline throughput of 5 Gbps and 1 Gbps on VM5000 and VM600 Sensors respectively. These licenses can either be individual .jar files, or they can be bundled together and provided to you in the form of a .zip file. Each license supports a pre-defined number of Virtual IPS Sensors, and this number is specific to the license file you have procured. The Manager supports both formats. The license procured contains the details of the Sensor's throughput. The Manager checks the compliance periodically to check the number of licenses against the Sensor's throughput.

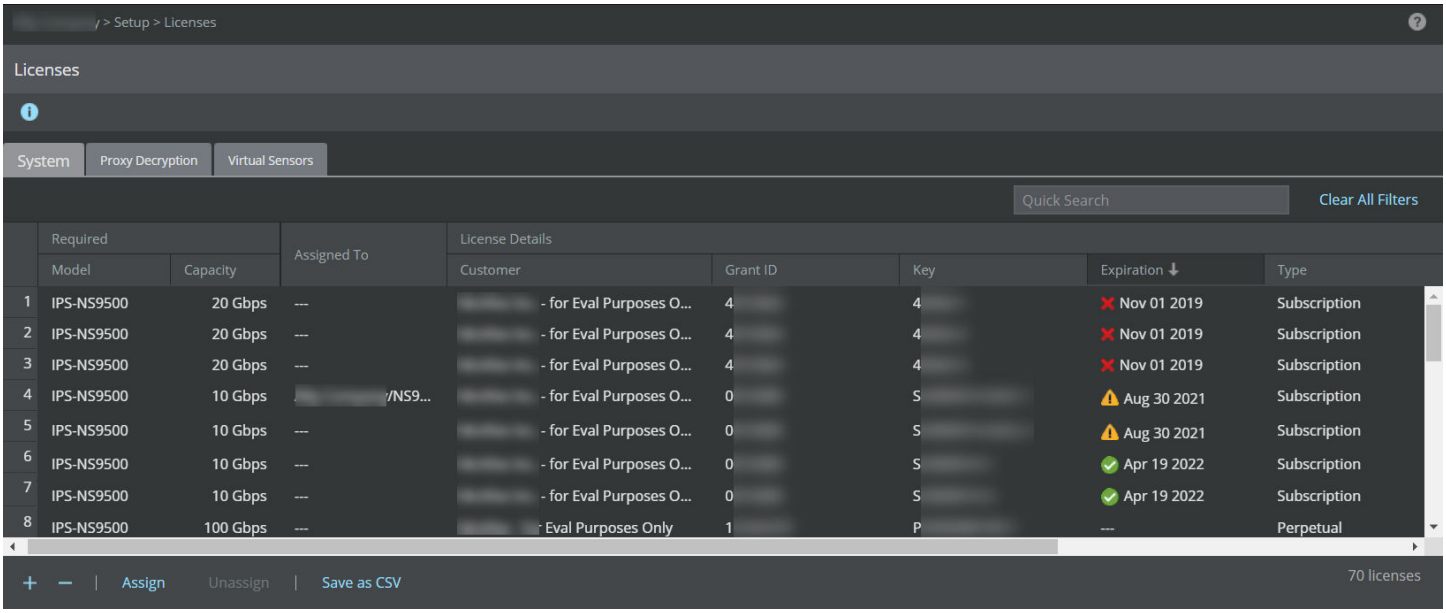
In the case of the VM5000 Sensor, 5 active licenses each of 1 Gbps are required to achieve the throughput of the Sensor. For the VM600 Sensor, only 1 active 1 Gbps license is required.

For more information, see Managing licenses for Virtual Sensors in [Trellix Virtual Intrusion Prevention System Product Guide].

System and Proxy Decryption tab

The **System** and the **Proxy Decryption** tabs in the **Licenses** page displays information regarding the number of licenses available, their capacity, and all the details required for a license. This page also allows you to add, remove, upgrade, assign, and unassign licenses.

To view the **System** tab, go to Manager → <Admin Domain Name> → Setup → Licenses → **System**.



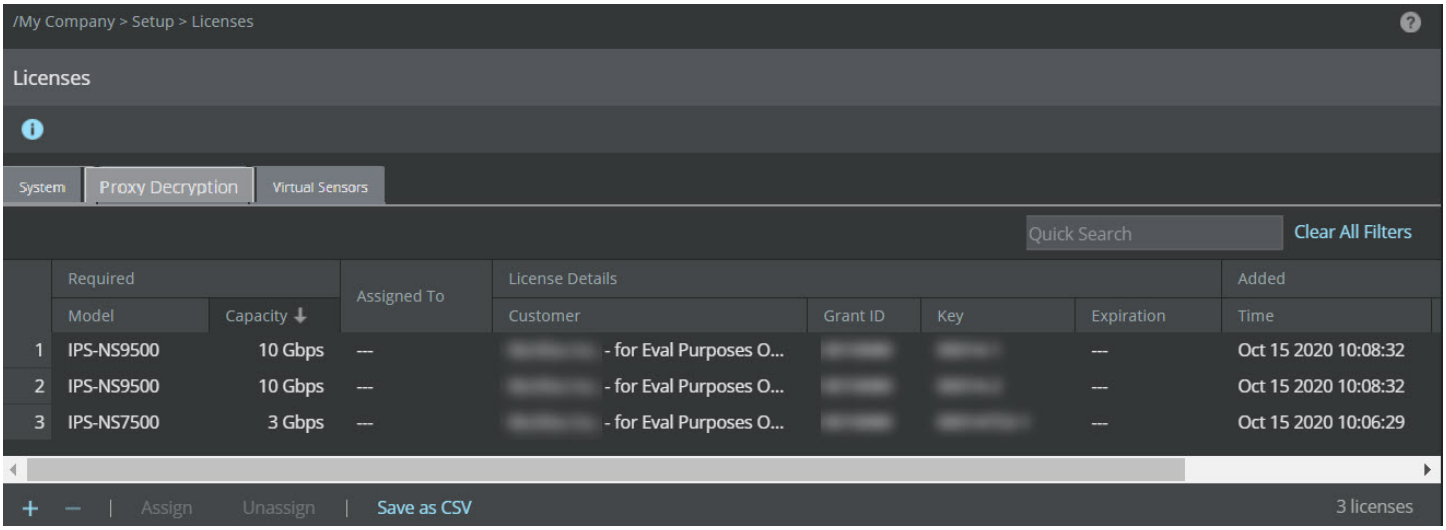
The following details are displayed on the **System** tab:

Option	Definition
Required	**Model** – Sensor model compatible with the license **Capacity** – Throughput limit for the license
Assigned To	Name of the Sensor assigned to the license

Option	Definition
License Details	**Customer** – Customer for whom the license file was generated **Grant ID** – Trellix Grant ID of the corresponding customer **Key** – License key number of the customer **Expiration** – Expiration date of the license **NOTE** The expiration is applicable only for demo and subscription licenses. • : Valid license • : Expired license • : Expired license running on grace period **NOTE** A grace period of **30 days** is provided to subscription-based **System** licenses after they expire. **Type** – Displays if the license is **Perpetual**, **Subscription**, or **Evaluation (Demo)** type. **NOTE** It is recommended to install subscription license from Manager version 10.1.7.44 and later.
Added	**Time** – Date in <mm-dd-yy> format, and time when the license was added **By** – Name of the user who added the license
Comments	Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and your comment is automatically saved.
+	Add a license
−	Delete a license
Assign	Assign a license to the Sensor
Unassign	Unassign a license from the Sensor
Save as CSV	Export the license usage details as a **.csv** file

For more information, see [Trellix Intrusion Prevention System Installation Guide].

To view the **Proxy Decryption** tab, go to Manager → <Admin Domain Name> → Setup → Licenses → **Proxy Decryption**.



The following details are displayed on the **Proxy Decryption** tab:

Option	Definition
Required	**Model** – Sensor model compatible with the license **Capacity** – Throughput limit for the license
Assigned To	Name of the Sensor assigned to the license
License Details	**Customer** – Customer for whom the license file was generated **Grant ID** – Trellix Grant ID of the corresponding customer **Key** – License key number of the customer **Expiration** – Expiration date of the license
Added	**Time** – Date in <mm-dd-yy> format, and time when the license was added **By** – Name of the user who added the license
Comments	Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and your comment is automatically saved.
+	Add a license
−	Delete a license
Assign	Assign a license to the Sensor
Unassign	Unassign a license from the Sensor
Save as CSV	Export the license usage details as a **.csv** file

Virtual Sensors tab

The **Virtual Sensors** tab in the **Licenses** page displays your compliance, and maintains the count for Virtual IPS Sensors. This page also displays and allows you to add and remove individual licenses.

To view the **System** tab, go to Manager → <Admin Domain Name> → Setup → Licenses → **Virtual Sensors**.

The following details are displayed in the **Virtual Sensors** tab:

Option	Definition
Status	Overall compliance which can either be **Compliant** or **Non-compliant**. If the vIPS Sensor count is within the maximum limit defined in the license, the overall state is displayed as **Compliant** with a green icon preceding it. If the vIPS Sensor count exceeds the maximum limit, the overall state is displayed as **Non-Compliant** with a red icon preceding it.
Additional Licenses Required	Additional number of licenses required for compliance
Trellix Virtual IPS Sensors	Number of Virtual IPS Sensors in use along with the maximum number
Virtual Probes	Number of Virtual Probes in use
Allowed Virtual Sensors	Displays the allowed number of virtual sensors as per the license imported
License	**Customer** – Customer for whom the license file was generated **Grant ID** – Trellix Grant ID of the corresponding customer **Key** – License key number of the customer
Added	**Time** – Date in <mmm-yy> format, and time when the license was added **By** – Name of the user who added the license
Comments	Enables you to add your comment per license file that is imported. Double-click in the **Comment** field and enter your comment. Click outside this field and your comment is automatically saved
+	Add a license
−	Delete a license
Save as CSV	Export the license usage details as a **.csv** file

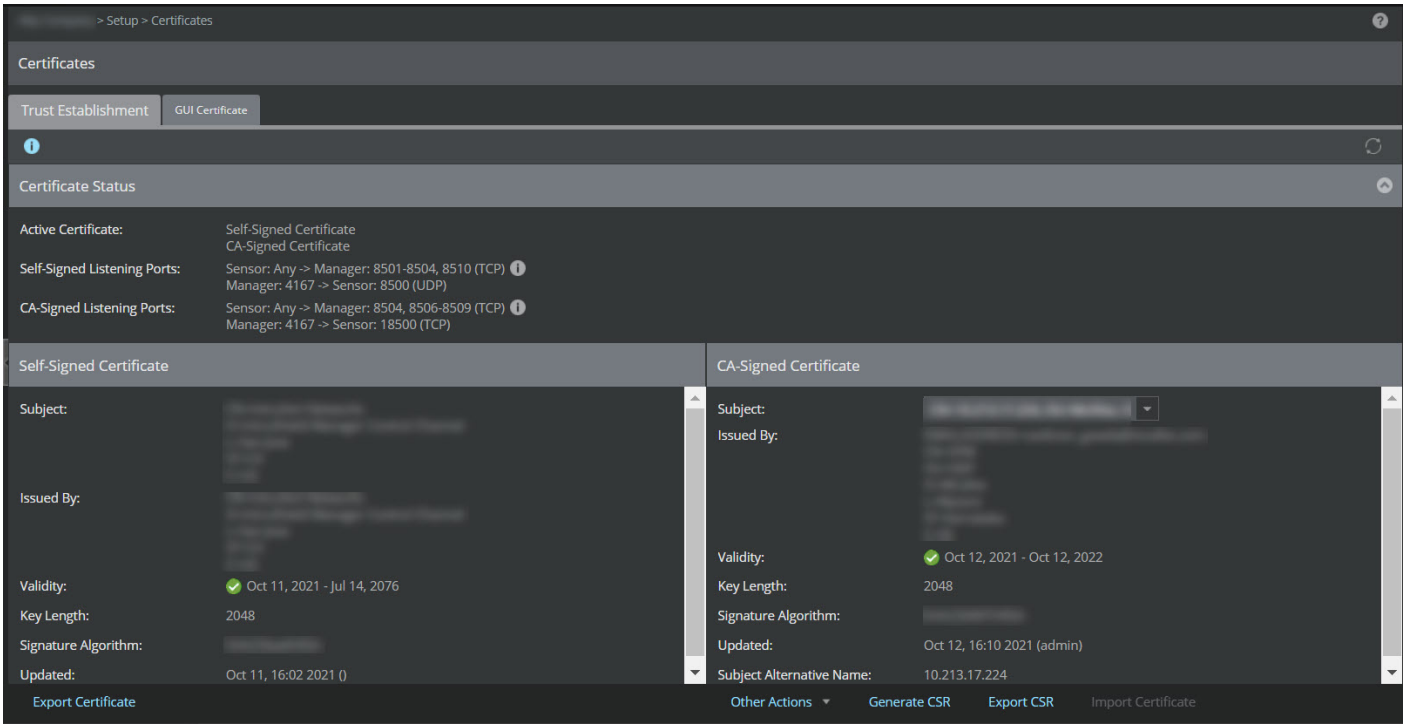
Managing Certificates for Manager and Sensor

The Manager and Sensor can also use a CA-signed certificate to establish trusted connection. By default, the Manager and Sensor use a self-signed certificate to establish trust. You can also use a CA-signed certificate chain issued by trusted CAs, such as Verisign, GeoTrust, and others, to establish trust between the Manager and the Sensor.

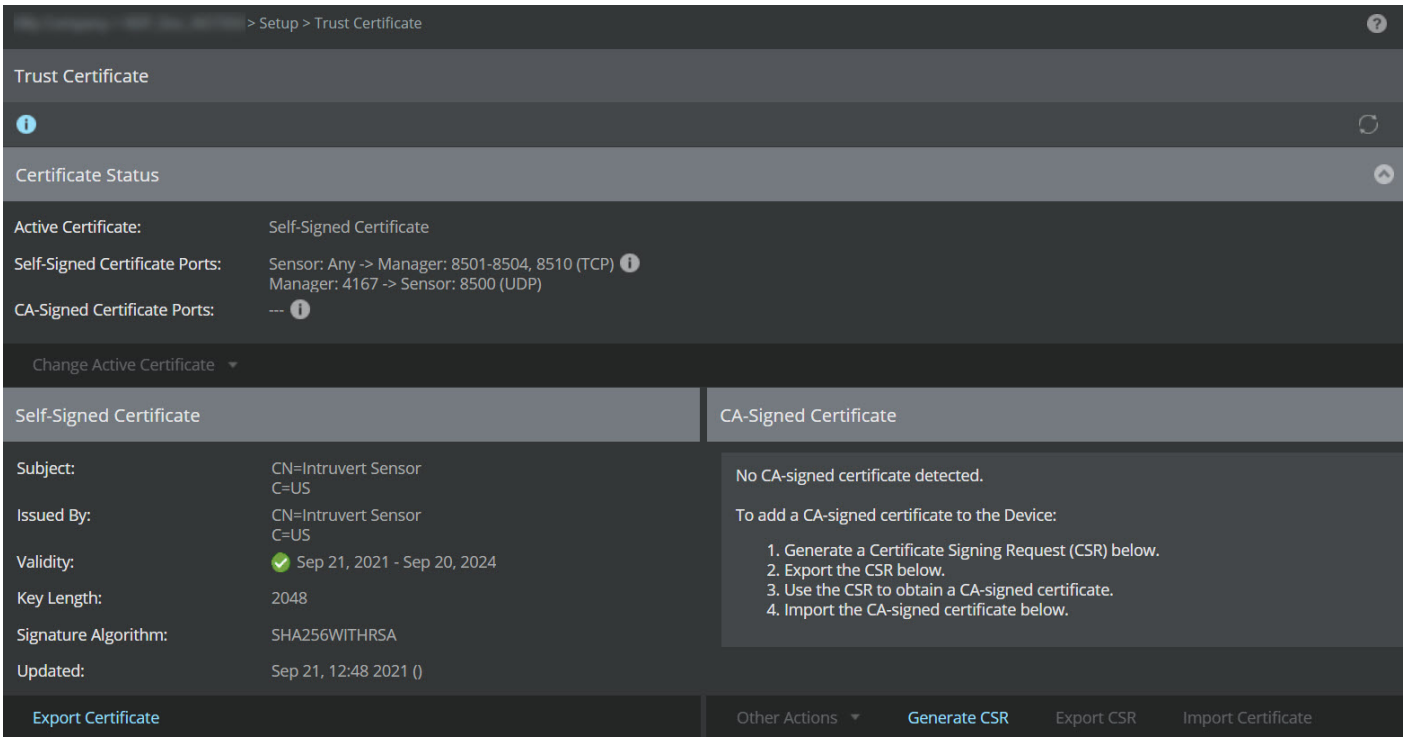
To manage the certificates for the Manager, go to Manager → <Root Admin Domain> → Setup → **Certificates**.

The **Certificates** page opens. It consists of following tabs:

- **Trust Establishment**
- **GUI Certificate**



To manage the certificates for the Sensor, go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Trust Certificate**.



The **Trust Certificate** page contains the following details:

Certificate Status

This section displays the following information:

Option	Definition
Active Certificate	Displays the type of the active certificate as either self-signed or CA-signed
Self-Signed Listening Ports	Ports used by the Manager to establish trust with Sensor when both use self-signed certificates
CA-Signed Listening Ports	Ports used by the Manager to establish trust with Sensor when both use CA-signed certificates

The action supported for **Sensor** in this section is:

Option	Definition
Change Active Certificate	Changes the active certificate of the Sensor from self-signed to CA-signed or CA-signed to self-signed

Self-Signed Certificate

This section displays the following information regarding the self-signed certificate issued by Trellix:

Option	Definition
Subject	Displays the following information about the certificate: • **Common Name** • **Organization** • **Department** • **City** • **State/Province** • **Country**
Issued By	Name of the signing authority for the certificate
Validity	Duration for which the certificate is valid
Key Length	Number of bits used in the cryptographic algorithm
Signature Algorithm	Signature Algorithm used for the certificate
Updated	Date when the certificate was last updated

The action supported for Manager and Sensor in this section is:

Option	Definition
Export Certificate	Exports the self-signed certificate to the remote machine accessing the Manager

CA-Signed Certificate

This section displays the following information regarding the CA-signed certificate:

Option	Definition
Subject	Displays the following information about the certificate: • **Common Name** • **Organization** • **Department** • **City** • **State/Province** • **Country** The drop-down list displays all certificates in the certificate chain.
Issued By	Name of the signing authority for the certificate
Validity	Duration for which the certificate is valid
Key Length	Number of bits used in the cryptographic algorithm
Signature Algorithm	Signature Algorithm used for the certificate
Updated	Date when the certificate was last updated

The actions supported for Manager and Sensor in this section are:

Option	Definition
Generate CSR	Generates the Certificate Signing Request (CSR). **NOTE** The CSR for both the Manager and the Sensor are generated in the Manager and is stored in the Manager database.
Export CSR	Exports the Certificate Signing Request (CSR) to the remote machine accessing the Manager
Import Certificate	Imports the CA-signed certificate from the remote machine accessing the Manager
Other Actions	
Remove Certificate	Removes the CA-signed certificate
Export Certificate	Exports the CA-signed certificate

For more information about **GUI Certificate**, refer to CA-signed certificate for the Web Server Authentication (page 160).

Considerations for CA-signed certificate chain

The CA-signed certificate chain for the Manager and the Sensor is considered valid if the following conditions are met:

- The CSR should not be modified after exporting from the Manager. This will cause the certificate validation in the Manager to fail.
- The certificate must be X.509v3 version.
- The CA-signed certificate chain should comply with the following requirements:
  - Should be issued from a trusted Certificate Authority
  - Should be in .pem format
  - Must contain valid serial numbers and valid issuer domain name
  - Must include minimum SHA256 with RSA 2048 bit encryption
- The number of intermediate CA-certificates in the certificate chain should be between 0 and 4.
- The certificate chain should be in correct order. The chain should begin with the identity certificate (also known as leaf certificate) followed by intermediate CA-certificate 1, intermediate CA-certificate 2, ... intermediate CA-certificate N and end with the root CA-certificate.
- The identity certificate must be signed by the intermediate CA. The intermediate certificate must be signed by the root CA.
- The Basic Constraint **CA** flag must be set to **True** in case of root and intermediate certificates. For identity certificate, the flag must be set to **False**.
- The certificate must comply with the following parameters:
  - **ExtendedKeyUsage**: *TLS WebServerAuthentication* and *TLS WebClientAuthentication*
  - **KeyUSage**: Must not be set to *Critical*.
- Ensure that the validity period for the certificate specifies a valid date range.
- OCSP requests and responses use **`CertID.issuerNameHash`** and **`CertID.issuerKeyHash`** parameters to validate the revocation status of CA certificates.

NOTE

In a Common Criteria (CC) evaluated configuration, revocation using OCSP is not claimed for Sensor - Manager channel.

Currently, the Manager supports SHA-1 hashing algorithm for the two parameters which needs to be managed in OCSP server configuration.

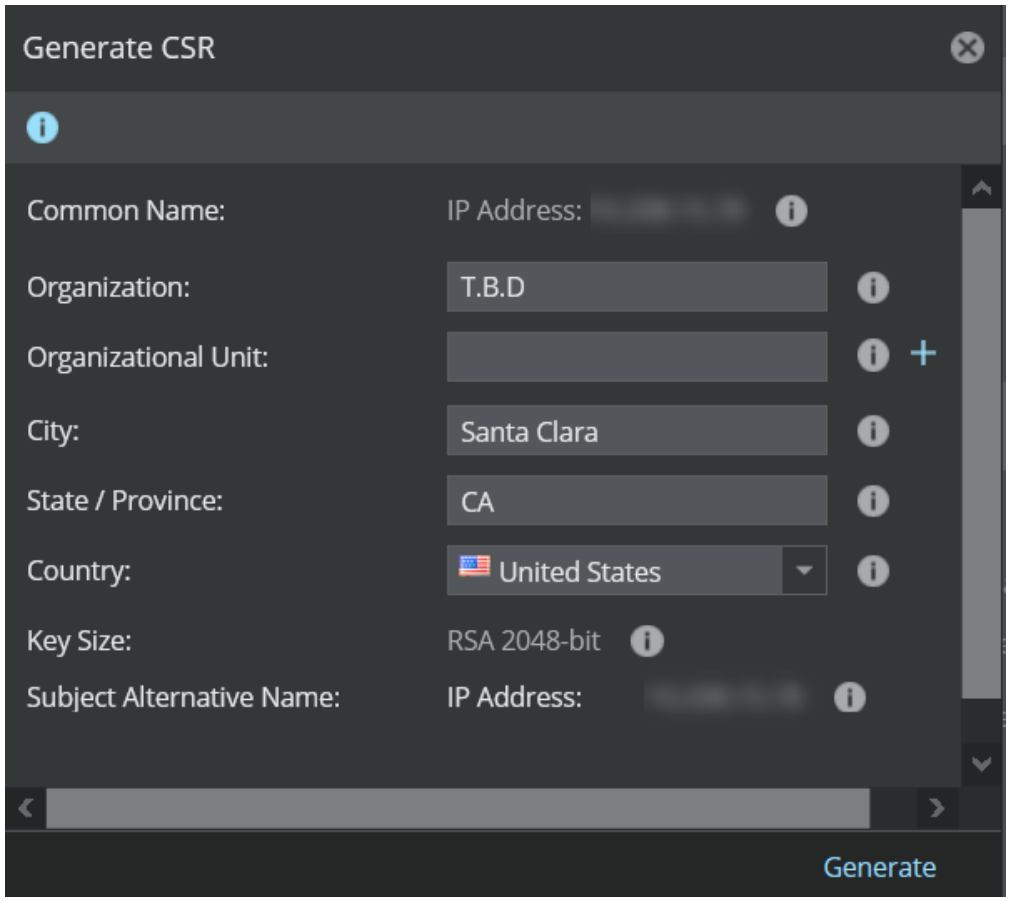
Generate Certificate Signing Request (CSR)

Certificate Signing Request is used to apply for a CA-signed certificate. To generate a CSR from the Manager, perform the following steps:

1. To generate a CSR for the Manager, go to Manager → <Root Admin Domain> → Setup → **Certificates**.

   To generate a CSR for the Sensor, go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Trust Certificates**.

2. In the **CA-Signed Certificate** section, click **Generate CSR**. The **Generate CSR** window opens.



3. Enter the following details in the **Generate CSR** window:

Option	Definition
Common Name	Displays the IP Address of the device.

Option	Definition
Organization	Legal name of your organization. This field should not contain any wildcard characters (such as * or ?).
Organizational Unit	[Optional] Name of the organizational unit. **NOTE** Additional organizational units can be added based on your requirement. A maximum of 10 organizational units can be added.
City	[Optional] City where the organization is located. This field should not contain any abbreviations.
State/Province	[Optional] State or province where the organization is located. This field should not contain any abbreviations.
Country	Country where the organization is located.
Key Size	Only 2048-bit RSA keys are supported which is displayed by default.
Subject Alternative Name	Displays the IP address of your server by default. This field is non-editable.

NOTE

The maximum length for **Organization**, and **Organizational Unit** fields are 64 characters. The maximum length for **City** and **State/Province** fields are 128 characters.

4. Click **Generate**.

Apply for CA-signed certificates

You can apply for CA-signed certificates based on the CSR generated. To apply for the certificate, perform the following steps:

1. To apply for a CA-certificate, you must first export the CSR for the Manager and Sensor.

   To export CSR for the Manager, go to Manager → <Root Admin Domain> → Setup → **Certificates**.

   To export CSR for the Sensor, go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Trust Certificates**.

2. In the **CA-Signed Certificate** section, click **Export CSR**. The CSR is exported to the `Downloads` folder of the remote machine accessing the Manager.

NOTE

The **Export CSR** button becomes active only after you generate the CSR.

3. Once the CSRs are exported, send both the Manager and Sensor generated CSRs to a Certified Authority of your choice.
4. The CA processes the CSR and returns the CA-signed certificate.

Import the CA-signed certificate

To import the CA-signed certificate chain, perform the following steps:

1. To import the CA-signed certificate chain for the Manager, go to Manager → <Root Admin Domain> → Setup → **Certificates**.

   To import the CA-signed certificate chain for the Sensor, go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Trust Certificates**.
2. In the **CA-Signed Certificate** section, click **Import Certificate**.

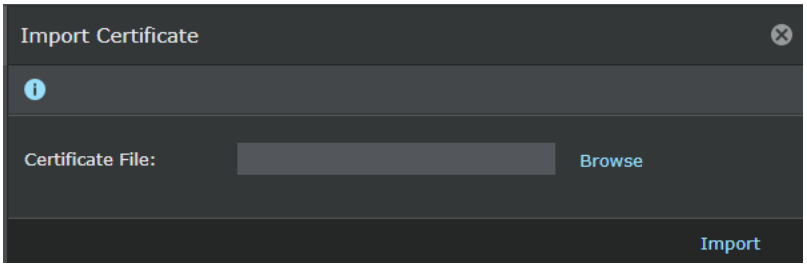
NOTE

If the Manager or Sensor already contains CA-signed certificate, the **Import Certificate** option will be disabled.

NOTE

The **Import Certificate** button becomes active only after you generate and export the CSR.

3. In the **Import Certificate** dialog box, click **Browse**.



4. Browse to the directory that contains the certificate chain, click **Open**.

NOTE

The CA-signed certificate chain should be in .pem format.

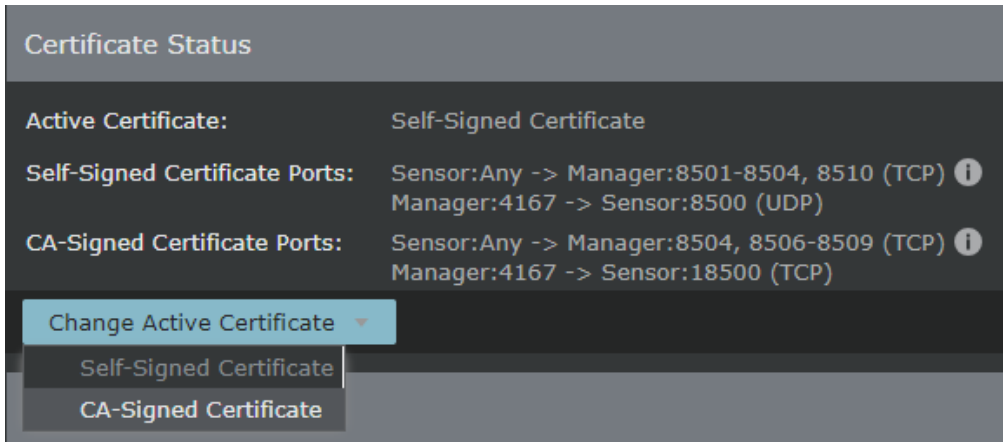
5. Click **Import** for the manager and each sensor connected to the manager.

   The Manager validates the CA-signed certificate chain with the CSR. If the validation is successful, the certificate chain details are displayed in the **CA-Signed Certificate** section.

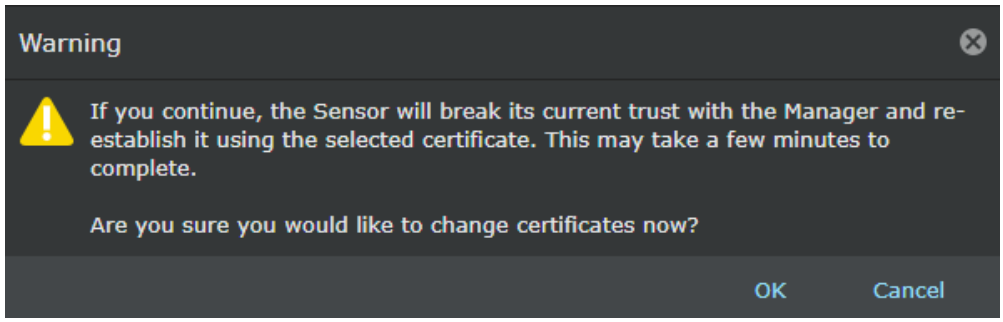
Change the active certificate for the Sensor

To change the active certificate for a Sensor, perform the following steps:

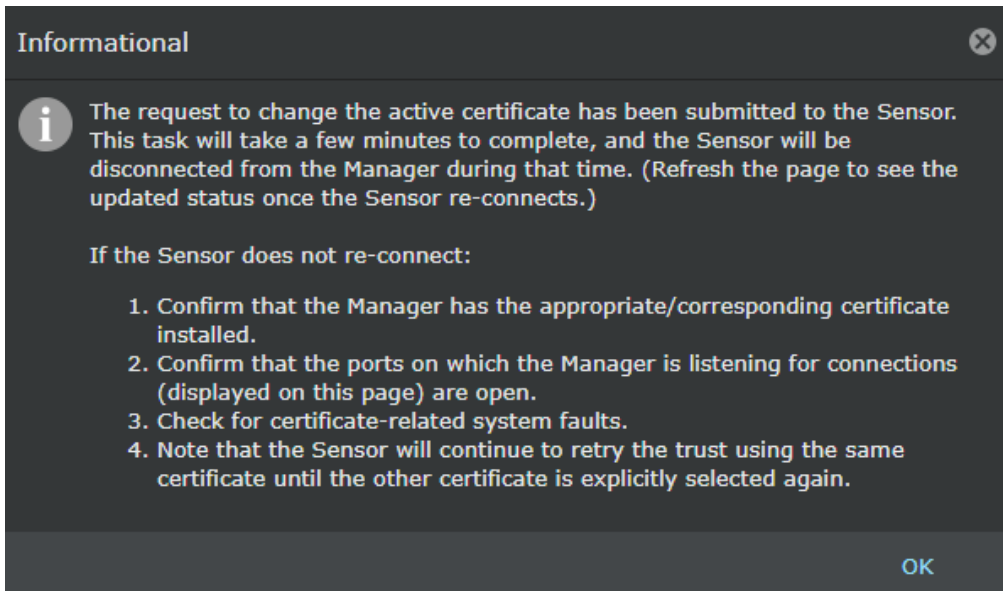
1. Go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Certificates**.
2. In the **Certificate Status** section, click **Change Active Certificate** drop down.



3. Select the certificate (self-signed or CA-signed) based on your requirement.
4. Click **OK** to confirm.



5. Click **OK** to change the active certificate.



NOTE

If your Manager is part of an MDR pair, you can change the certificate from self-signed to CA-signed or vice versa only for the primary (active) Manager.

Migrating the Manager-Sensor trust from self-signed to CA-signed certificate chain

The high-level steps to establish trust between the Manager and the Sensor using CA-signed certificate chain are given below. Perform these steps to:

- Provision the Manager with its CA-signed certificate
- Use the Manager to provision the Sensor with its CA-signed certificate
- Migrate the trust based on the existing self-signed certificates to the provisioned CA-signed certificates between the Manager and the Sensor

NOTE

For CA migration in an MDR setup, you must first create an MDR pair, then create Certificate Signing Request (CSR) and migrate to CA.

1. Generate CSR for the Manager and Sensors.
2. Export the CSR for both the Manager and Sensors and send it to a CA of your choice.
3. The CA processes the CSR and sends a CA-signed certificate.

NOTE

For validations for CA-signed certificate, see Considerations for CA-signed certificate chain (page 152).

4. After receiving the CA-signed certificate chain, import the certificate chain to the Manager. You need to migrate the Manager to CA-signed certificate chain before migrating the Sensors.

NOTE

Migrating the Manager to CA-signed certificate chain is a one time activity. Once the Manager is migrated to the CA-signed certificate chain, you must migrate the Sensors that are attached to the Manager.

5. The Manager validates its CA-signed certificate chain against its generated CSR.
6. From the Manager, import the CA-signed certificate chain to the Sensors managed by the Manager.
7. The Manager validates the Sensor's CA-signed certificate chain against its generated CSR.
8. If the validation is successful, from the Manager change the active certificate to use the CA-signed certificate chain to establish trust between Manager and Sensor. The switch is completed one Sensor at a time.

This migration is applicable to the Manager and all Sensors managed by the Manager. The Manager can establish trust with Sensors using either self-signed certificate or CA-signed certificate chain.

NOTE

The trust establishment works when both the Manager and Sensors are using the CA-signed certificate chain or when both are using self-signed certificate.

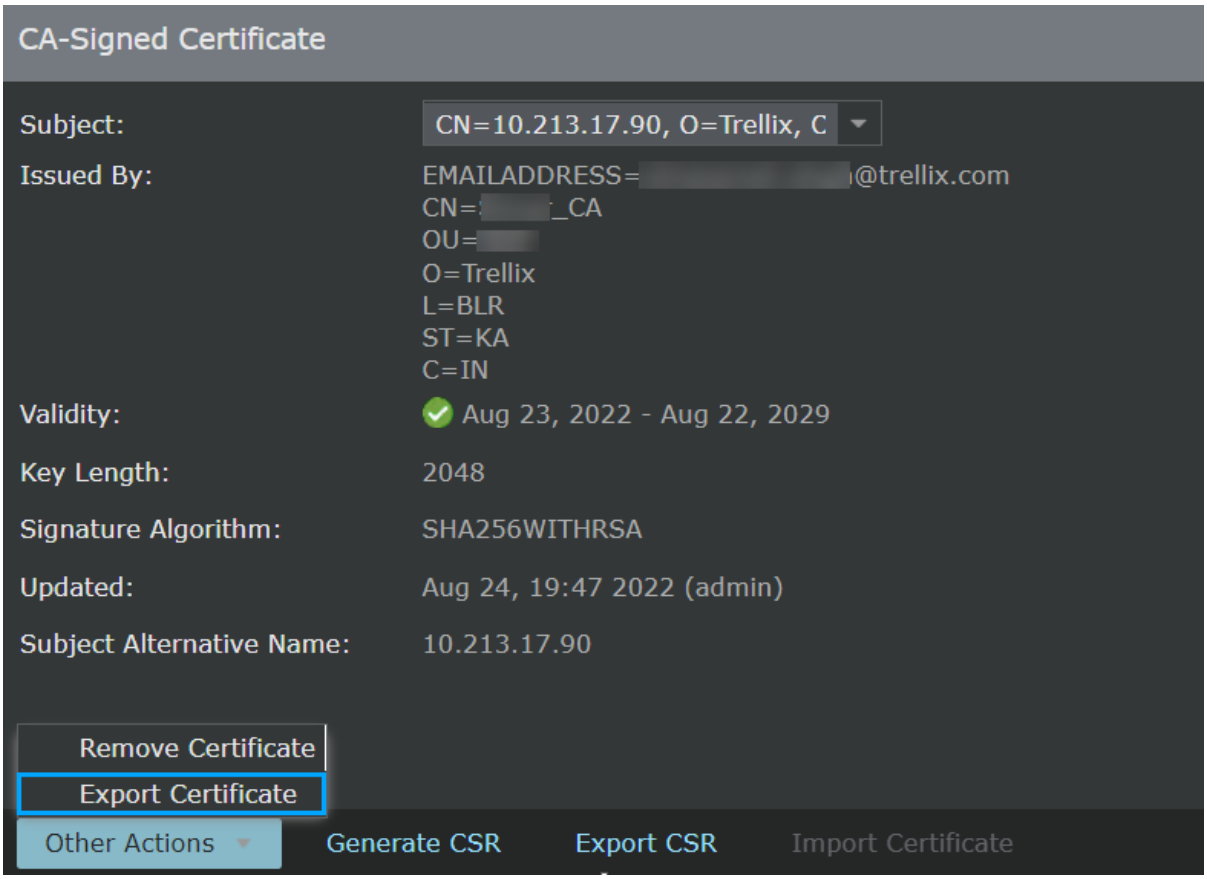
Export the CA-signed certificate chain

To export the CA-signed certificate chain, perform the following steps:

1. To export the certificate chain for the Manager, go to Manager → <Root Admin Domain> → Setup → **Certificates**.

   To export the certificate chain for the Sensor, go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Trust Certificates**.

2. In the **CA-Signed Certificate** section, click Other Actions → **Export Certificate**.



The CA-signed certificate chain will be exported to the remote machine accessing the Manager.

Remove the CA-signed certificate chain

Prerequisites:

You can remove the CA-signed certificate chain only if the following conditions are met:

- You can remove the certificate chain for the Manager only if all the Sensors managed by the Manager is using self-signed certificate.

- The active certificate should be changed to self-signed before removing the CA certificate from the Manager.

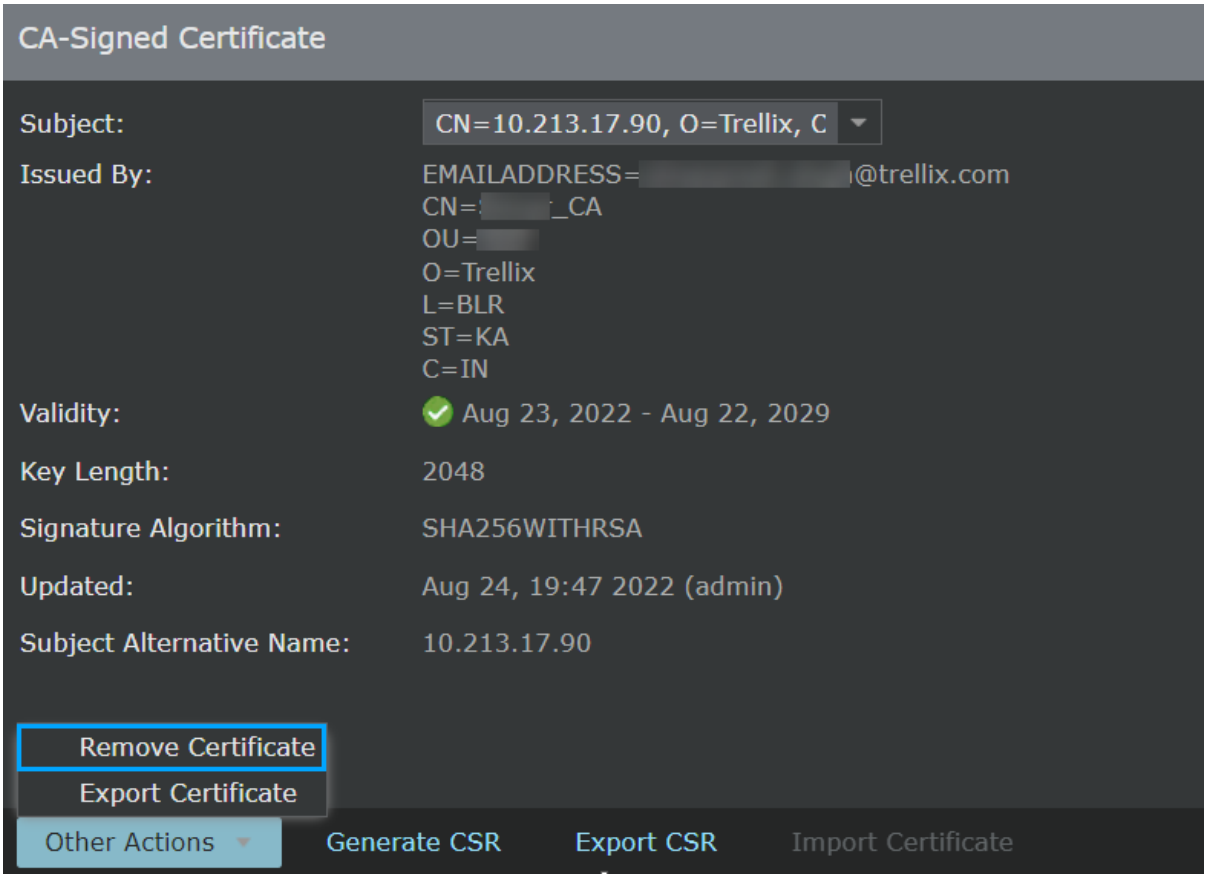
To remove the certificate chain, perform the following steps:

Steps:

1. To remove the certificate chain for the Manager, go to Manager → <Root Admin Domain> → Setup → **Certificates**.

   To remove the certificate chain for the Sensor, go to Devices → <Root Admin Domain> → Devices → <Device Name> → Setup → **Trust Certificates**.

2. In the **CA-Signed Certificate** section, click Other Actions → **Remove Certificate**.



The CA-signed certificate chain will be removed from the Manager.

NOTE

You must remove the CA-signed certificate chain separately for every Sensor and then have the trust reestablished with the Manager.

CA-signed certificate for the Web Server Authentication

The Manager/Central Manager use self-signed certificate to establish a trusted connection with the client systems. You can also use a CA-signed certificate issued by trusted CAs, such as Verisign, GeoTrust, and others, to establish trust between the Manager server and the client systems.

Considerations for CA-signed certificate for the Web Server Authentication

The CA-signed certificate for the Manager is considered valid if the following conditions are met:

- The certificate must be X.509v3 version.
- The CA-signed certificate chain should comply with the following requirements:
  - Should be issued from a trusted Certificate Authority
  - Should be in P12 format
  - Must contain valid serial numbers and valid issuer domain name
  - Must include minimum SHA256 with RSA 2048 bit encryption
- Ensure that the validity period for the certificate specifies a valid date range.

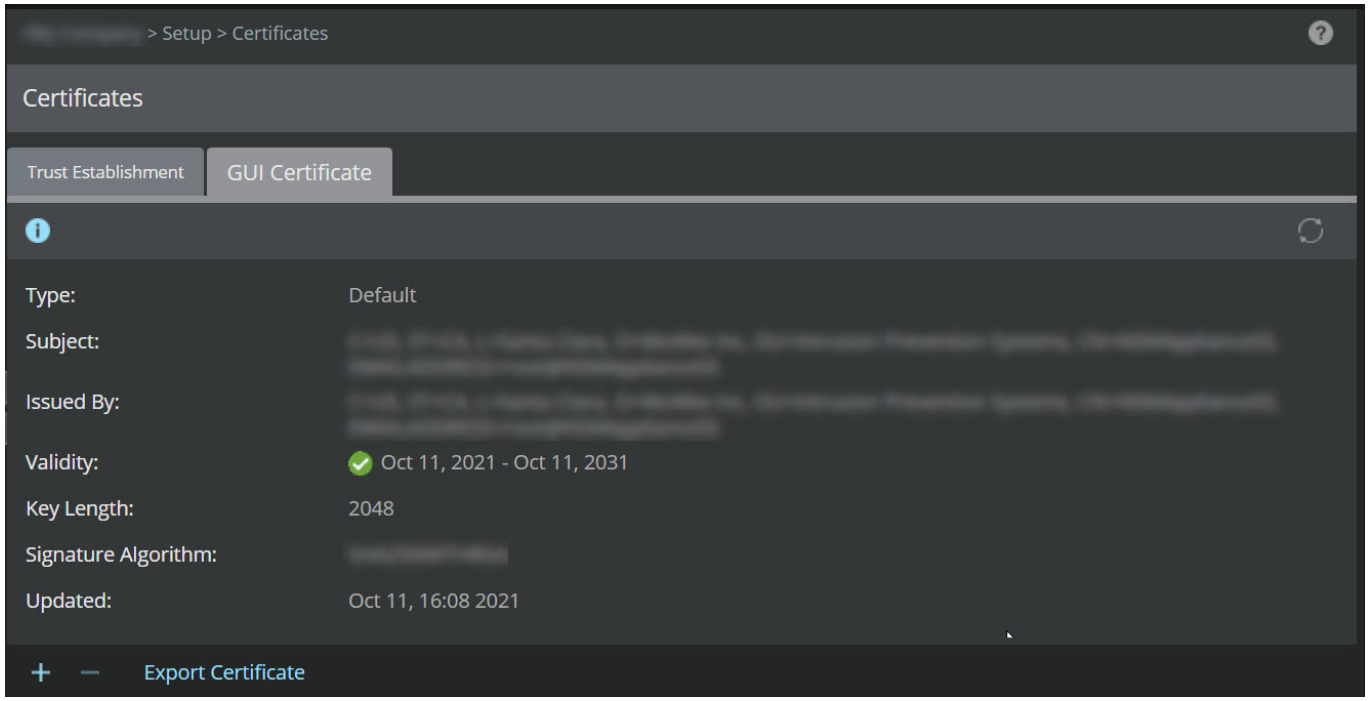
Import the CA-signed certificate for Web Server Authentication

To import the CA-signed certificate to the Manager, perform the following steps:

Steps:

1. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Certificates**. Select **GUI Certificate** tab.

   The **GUI Certificate** tab is displayed.



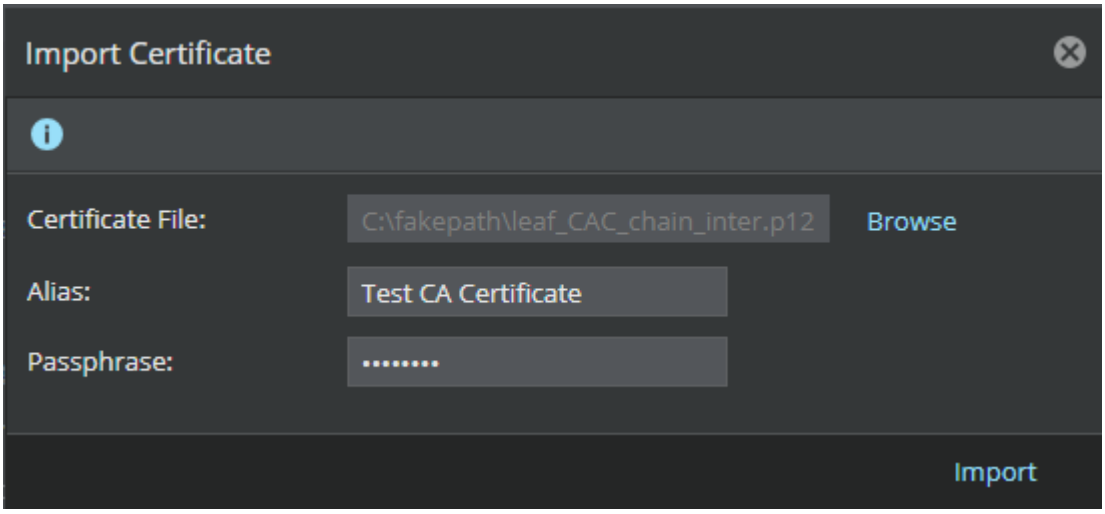
2. Click +.

   The **Import Certificate** dialog box opens.

> **NOTE**
>
> The + option is available only when the Manager uses a self-signed certificate. You cannot add a new CA-signed certificate to the Manager that is already using a CA-signed certificate for establishing trust with the client systems.

3. In the **Import Certificate** dialog box, click **Browse**.
4. Browse to the directory that contains the CA-signed certificate, click **Open**.

> **NOTE**
>
> The CA certificate should be in P12 format.



5. Provide an **Alias** and the **Passphrase** of the certificate.
6. Click **Import** to upload the certificate to the Manager.
7. Restart the Manager server.

The Manager server starts to use the CA signed certificate to establish trust with the client systems.

Export the CA-signed certificate for Web Server Authentication

To export the CA-signed certificate from the Manager, perform the following steps:

Steps:

1. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Certificates**. Select **GUI Certificate** tab.

   The **GUI Certificate** tab is displayed.

2. Click **Export Certificate** and save the file to a location of your choice.

Delete the CA-signed certificate for Web Server Authentication

To delete the CA-signed certificate from the Manager, perform the following steps:

Steps:

1. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Certificates**. Select **GUI Certificate** tab.

   The **GUI Certificate** tab is displayed.

2. Click −.

   The **Confirmation** dialog box opens.

   > **NOTE**
   >
   > The − option is available only when there is a CA-signed certificate in the Manager. You cannot delete the self-signed certificate in the Manager.

3. Click **OK** to confirm deletion.

   > **NOTE**
   >
   > When the CA-signed certificate in the Manager is deleted, automatically a self-signed certificate is used for the web server authentication.

4. Restart the Manager server.

   The Manager server automatically starts using self-signed certificate to establish trust with the client systems.

Alert notification options

The Manager can send alert information to third-party repositories, such as SNMP servers and syslog servers. Further, you can configure your Sensor to forward syslog notifications directly to a syslog server, thereby ensuring that the Sensor forwards alerts to a server other than that assigned to the Manager.

In addition to SNMP and syslog notifications, the Manager can also be configured to notify you through email, pager, or script of detected attacks.

For the alert notifications for the Sensor and the NTBA Appliance, select Manager → <Admin Domain Name> → Setup → Notification → **(IPS/NTBA) Events**.

Alert notifications are forwarded to syslog servers based on the configuration. Within the configuration, settings notification destination form only one aspect. The Manager and Sensor send notifications depending on the attack, the attack severity, or both.

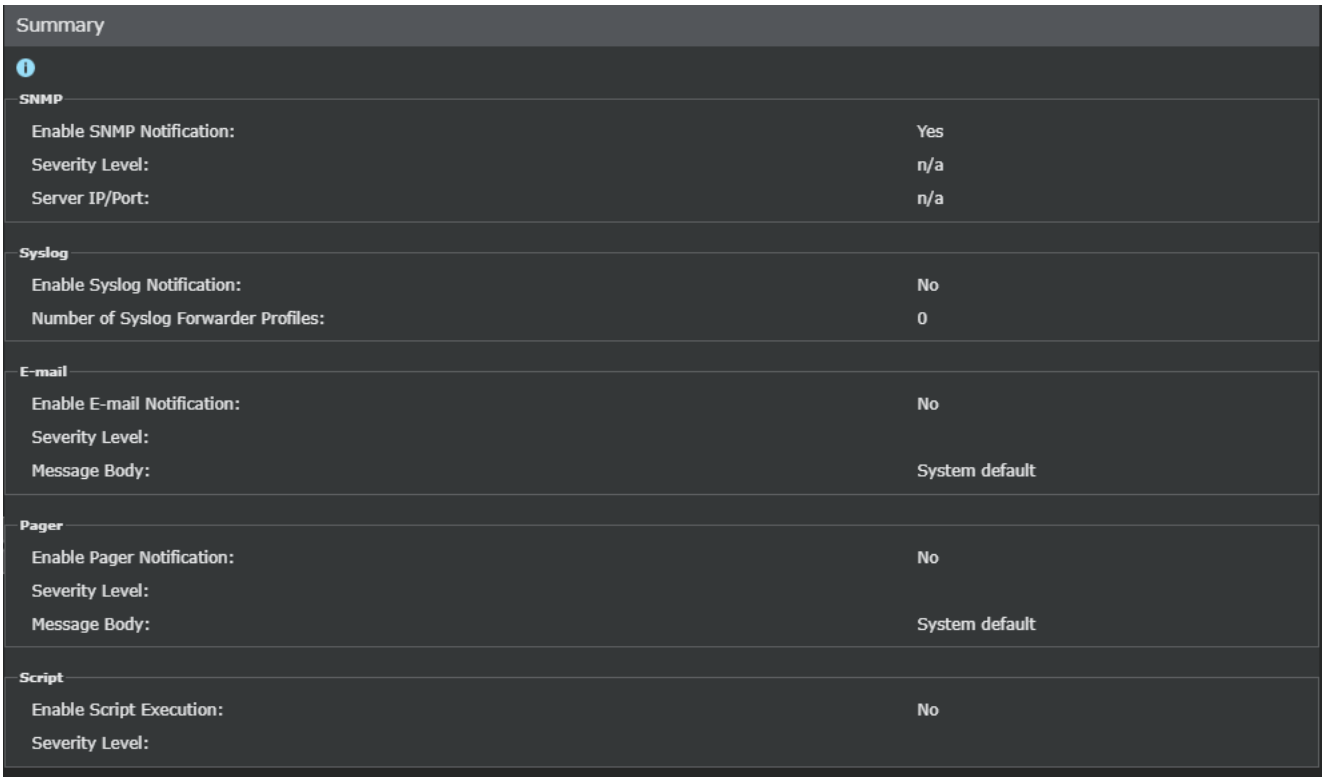
TIP

The Manager forwards all the audit records to a syslog server over a TLS secured connection in real-time.

How to view alert notification details

The **Summary** page for alert notification (Manager → <Admin Domain Name> → Setup → Notification → (IPS/NTBA) Events → **Summary**) displays a summary of configured alert notification settings. The summary displays your configuration settings made for each individual notification option.

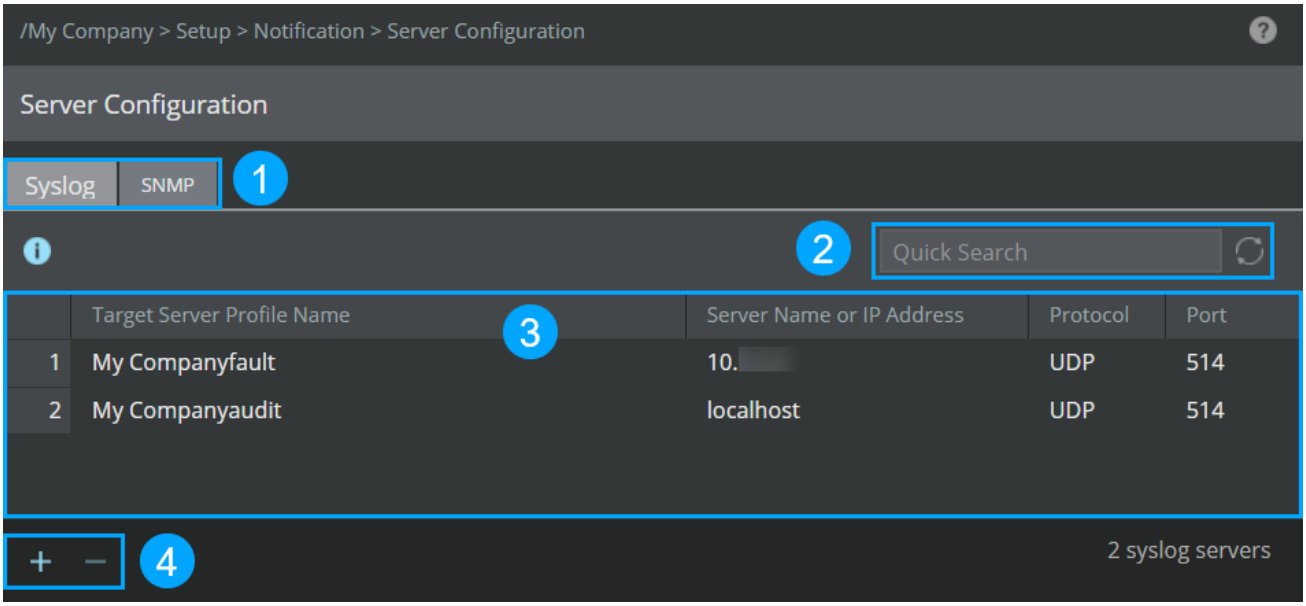
Figure 36. Summary page



Configure SNMP and Syslog servers

The Manager → <Admin Domain Name> → Setup → Notification → **Server Configuration** page in the Manager and Central Manager allows you to configure the Syslog and SNMP servers. These servers are then used in configuring Syslog and SNMP notifications in **IPS Events**, **Faults**, and **User Activity**.

Figure 37. Sever Configuration



Callout	Description
1	Tabs namely, **Syslog** and **SNMP**
2	Top-right menu
3	Grid view
4	Bottom-left menu

The following options are available in the tabs of the **Server Configuration** page:

Options	Description
Top-right menu	
Quick Search	Enter the keyword in the *Quick Search* field and the results are automatically displayed.
	Refreshes the tab.
Bottom-left menu	
	Add new servers.
	Delete existing servers. You can delete only one server at a time. A **Deleted** notification appears in case of successful deletion. Else, an **Error** dialog-box appears stating the reason for unsuccessful deletion.

NOTE

If you are upgrading the Manager to 11.1 Update 2 or later software versions, the Manager automatically lists any existing SNMP and Syslog servers under the respective tabs in this page. The server profile name is automatically assigned by the Manger in this format **<Domain Name><event/fault/audit><profile number>**. For example, you are upgrading the Manager from 11.1.7.3 to 11.1.7.41. The SNMP servers are configured for the admin domain named **IPS-Denver** and two child domains named **IPS-Welton** and **IPS-Larimer**. **IPS-Denver** has 3 existing profiles while **IPS-Welton** and **IPS-Larimer** have 2 existing profiles.

When you upgrade the Manager to 11.1.7.41 or later versions, this configuration is automatically mapped under the SNMP tab under each domain. User accessing the admin domain named **IPS-Denver** will be viewing the server profile names as **IPS-Denverfault1**, **IPS-Denverfault2**, and **IPS-Denverfault3**. User accessing the child domain **IPS-Welton** will be viewing 2 server profiles **IPS-Weltonfault1** and **IPS-Weltonfault2**. Similarly, user accessing the child domain **IPS-Larimer** will be viewing 2 server profiles **IPS-Larimerfault1** and **IPS-Larimerfault2**.

User accessing one domain will not be able to view the servers created in other domains.

In case user has used the same Syslog or SNMP server for IPS Events, Faults, and User Activity, three server profiles will created under the SNMP and Syslog tabs. Users can opt to delete the duplicate entries and have only one entry assigned to all the profiles. Before deleting the duplicate entries, ensure that the associated servers are not attached to any of the Syslog or SNMP notification profiles.

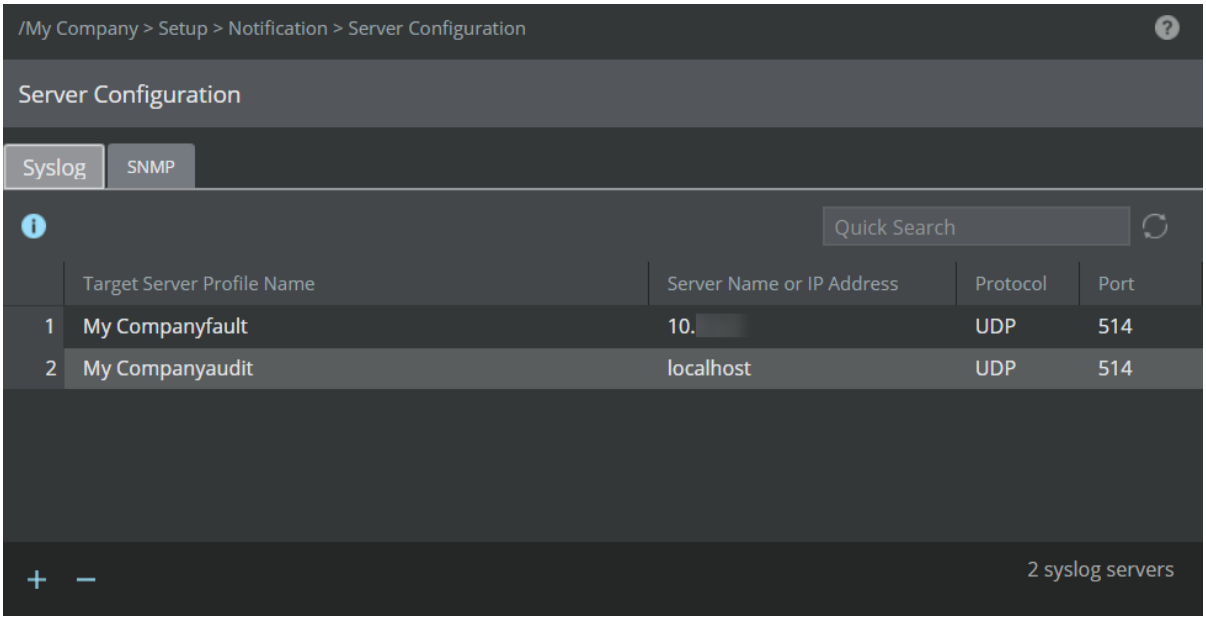
NOTE

Before upgrading the Manager to 11.1 Update 2 or later software versions, if user has created a Syslog server (under **IPS Events** page) at admin domain level and same server is used in child domains, post upgrade, the user sees profiles with the same name at both admin and child domain levels. In this case, if the user plans to remove one of the profiles from any of the domains and tries creating or updating a profile with the old name in the same domain or any other domain, an error is displayed stating the name is already in use.

Syslog tab

Grid view

Figure 38. Syslog tab

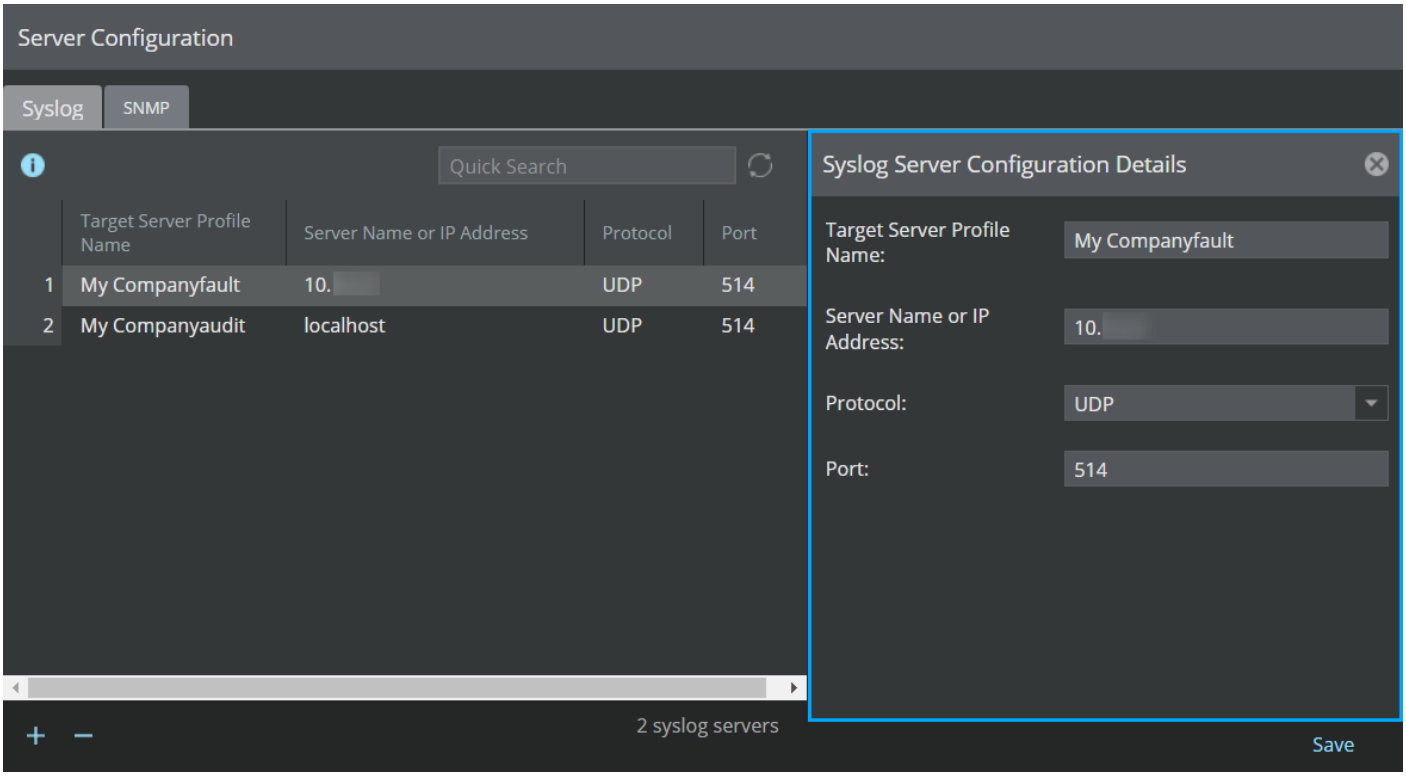


The following columns are available in the grid view of the **Syslog** tab:

Option	Definition
Target Server Profile Name	The name of the target server for identification purpose
Server Name or IP Address	The Name or IP Address associated with the server
Protocol	The protocol used - **TCP**/**UDP**
Port	The listening port of the target server

You can also view the server details in the **Syslog Server Configuration Details** panel to the right of the page by double-clicking anywhere on a Syslog entry.

Figure 39. Syslog Server Configuration Details



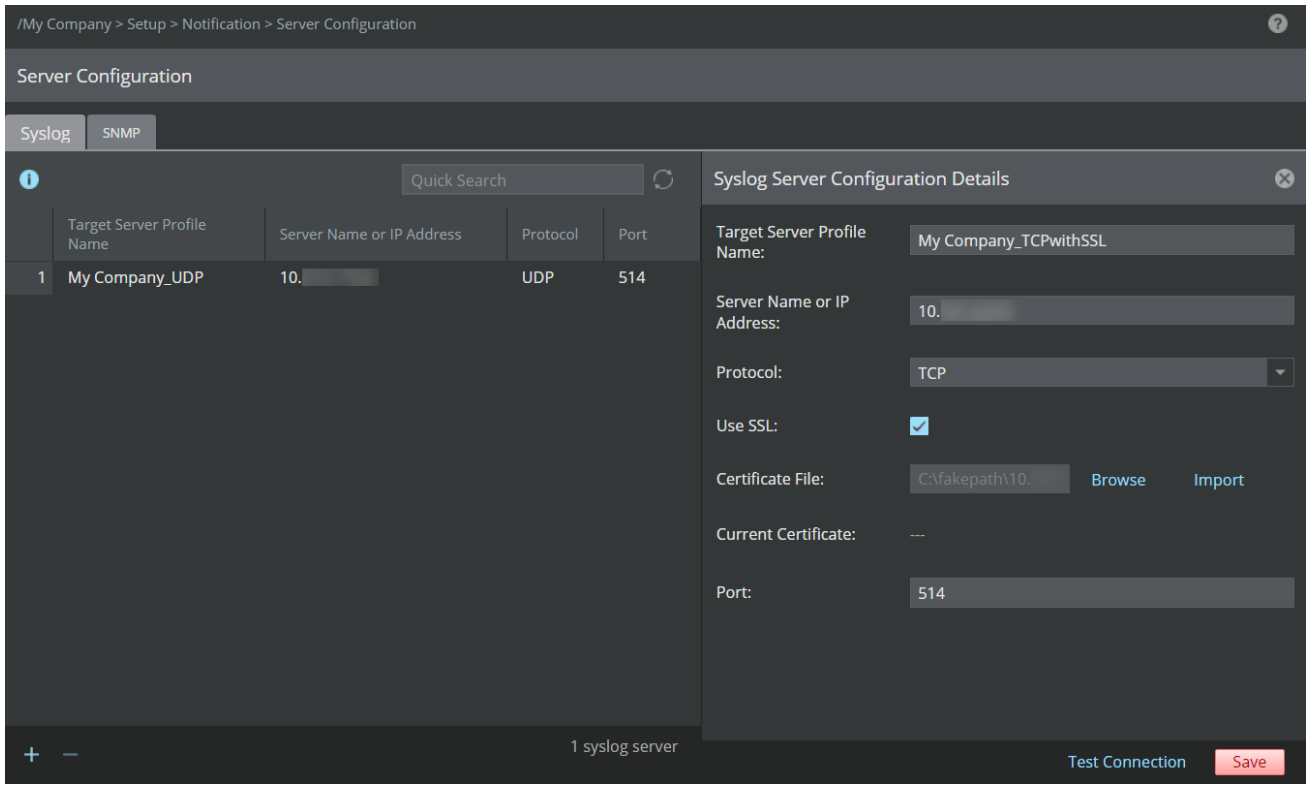
Configure a Syslog server

You can add, edit, or delete a Syslog server from the Syslog tab.

Steps:

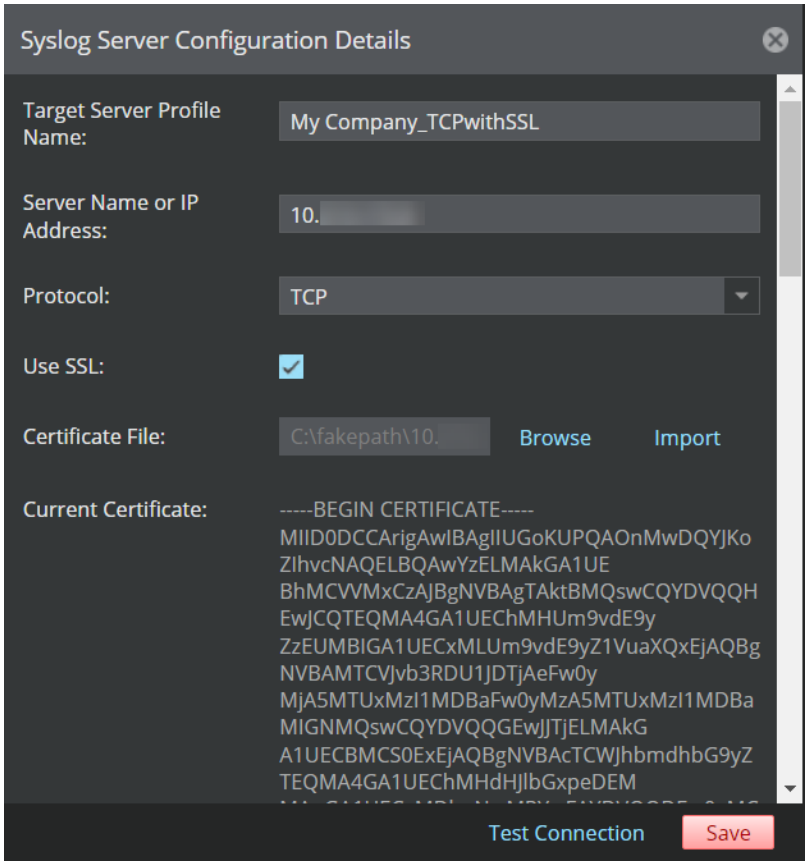
1. To add a Syslog server, go to the **Syslog** tab and click the + icon at the bottom-left corner of the page.

   The **Syslog Server Configuration Details** panel opens to the right of the page.



2. Specify your options in the appropriate fields.

Field	Description
Target Server Profile Name	Specify a profile name for the server addition. This name will be used while configuring the Syslog notification profile. **NOTE** It is recommended to specify the Server Profile Name as **<DomainName>_<ServerProfileName>** to avoid confusing with child domains names.
Server Name or IP Address	The server name or IP address of the target Syslog server. The IP address should be IPv4.
Protocol	The protocol used. This can be **TCP**/**UDP**.
Port	The listening port of the target server
The following options appear only when **TCP** Protocol is selected.	
Use SSL	If you are selecting this check-box, you need to provide a certificate for SSL communication.

Field	Description
Certificate File	Click **Browse** to select the certificate. Upon selecting the certificate, click **Import**. The supported certificate file format is **.pem**. 
Current Certificate	Displays the imported/existing certificate content.
Test Connection	Click **Test Connection** to check if the connection is successful. If a TCP server is down, at least five attempts will be made to ping the server before a fault is raised.

3. Click **Save**.

   The Syslog server is added under the **Syslog** tab.

4. If you want to modify an existing entry, double-click the specific Syslog entry. The **Syslog Server Configuration Details** panel opens where you can update the required fields and save the changes.

5. In case you want to delete an existing server, select the specific entry and click −. You can delete only one server entry at a time.

OCSP guidelines

Validity check of syslog server certificates is performed on the TOE during upload as well as during session establishment with the syslog server.

1. OCSP responders must be setup for the leaf as well as intermediate CA certificates so that the TOE can process the certificates with OCSP URLs in them.

2. If the connection cannot be established for the validity check, the administrator should check that:
   - The OCSP responders are setup for all leaf and intermediate CA certificates during loading as well as connection establishment.
   - OCSP responders are set up as per the information in the OCSP URL of the certificates such as IP address and port number
   - Index file being passed to the OCSP responders include correct details of all certificates being verified.
   - Appropriate OCSP signer and CA certificates and private keys are passed to the responders.

OCSP requests and responses use **`CertID.issuerNameHash`** and **`CertID.issuerKeyHash`** parameters to validate the revocation status of CA certificates.

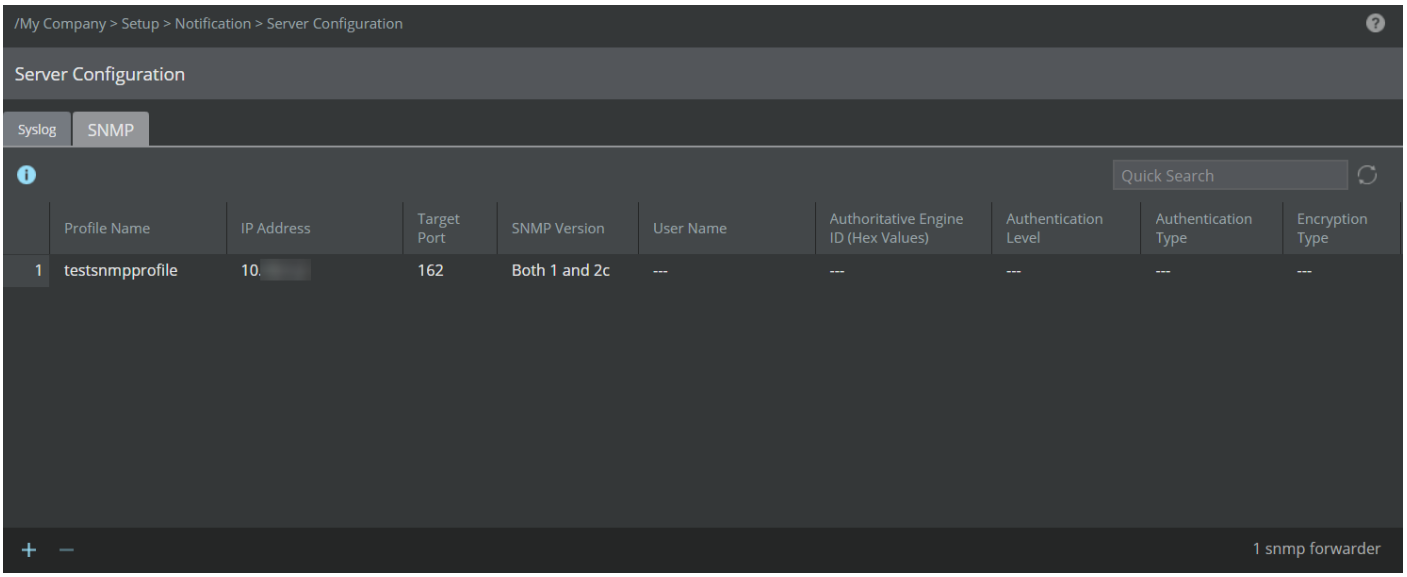
NOTE

In a Common Criteria (CC) evaluated configuration, revocation using OCSP is not claimed for Sensor - Manager channel.

SNMP Tab

Grid view

Figure 40. SNMP tab



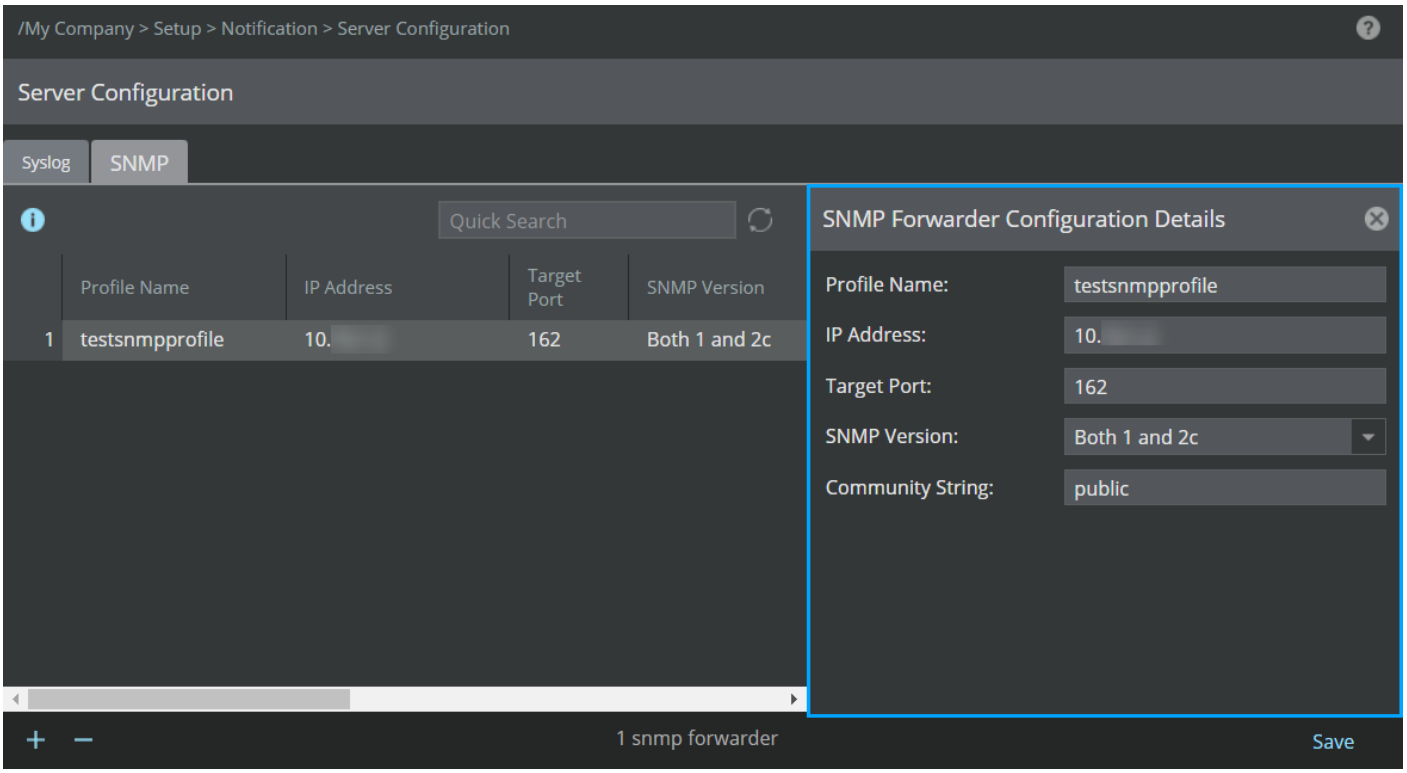
The following columns are available in the grid view of the **Syslog** tab:

Option	Definition
Profile Name	The name of the target server for identification purpose
IP Address	The IP Address associated with the server
Target Port	The listening port of the target server
SNMP Version	The version of SNMP running on the target SNMP server

Option	Definition
User Name	The username for authentication
Authoritative Engine ID (Hex Values)	The authoritative (security) engine ID used for SNMP version 3 REQUEST messages by primary Manager.
Authentication Level	The authentication level
Authentication Type	The authentication protocol (MD5, SHA, or SHA256) used for authenticating SNMP version 3 messages
Encyption Type	The privacy protocol (DES, AES, or AES256) used for encrypting SNMP version 3 messages

You can also view the server details in the **SNMP Forwarder Configuration Details** panel to the right of the page by double-clicking anywhere on an SNMP entry.

Figure 41. SNMP Forwarder Configuration Details

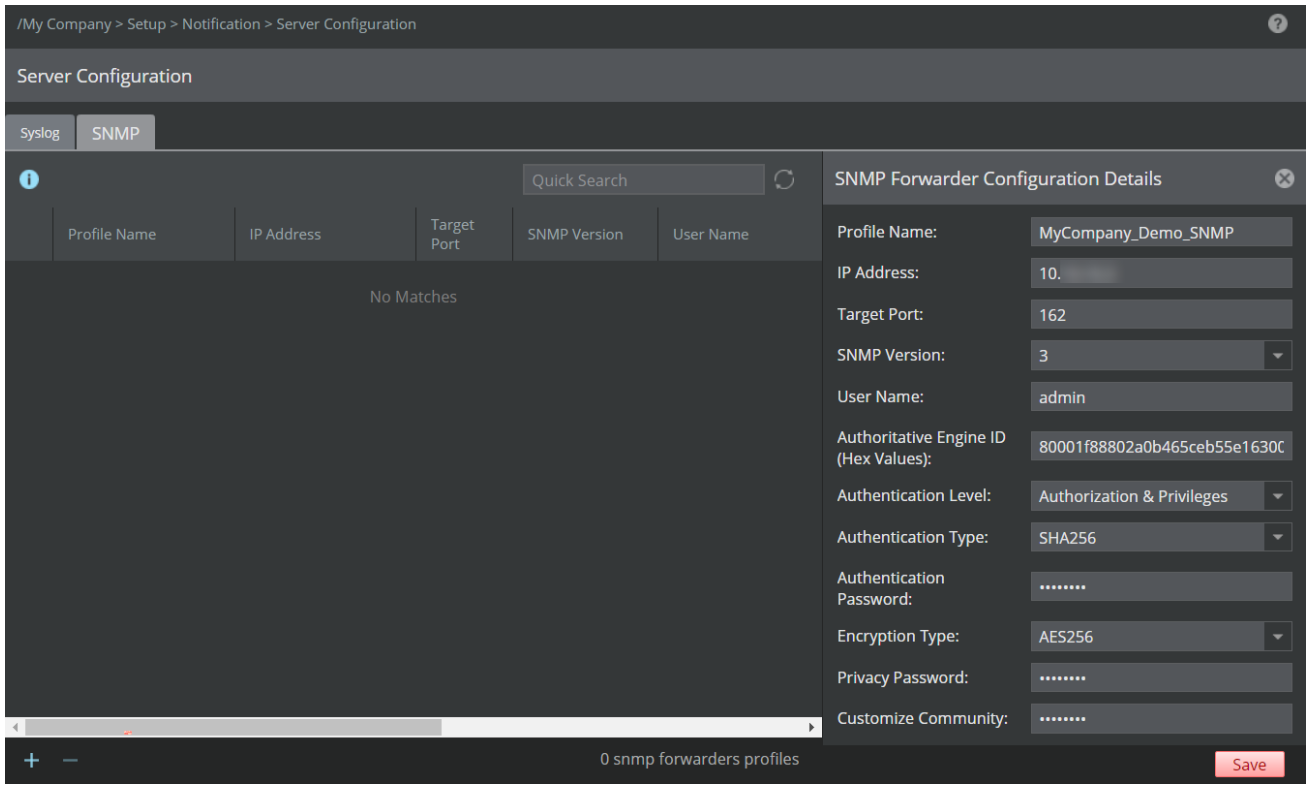


Configure an SNMP Forwarder

Steps:

1. To add an SNMP server, go to the **SNMP** tab and click the + icon at the bottom-left corner of the page.

   The **SNMP Forwarder Configuration Details** panel opens to the right of the page.



2. Specify your options in the appropriate fields.

Field	Description
Profile Name	Specify a profile name for the server addition. This name will be used while configuring the SNMP notification profile. **NOTE** It is recommended to specify the Server Profile Name as **<Domain-Name>_<ServerProfileName>** to avoid confusing with child domains names.
IP Address	IP address of the target SNMP server. This can be an IPv4 or IPv6 address.
Target Port	SNMP listening port of the target server
SNMP Version	The version of SNMP running on your target SNMP server. Version options are **1**, **2c**, **Both 1 and 2c**, and **3**.
Community String	Enter an SNMP community string to protect your Trellix IPS data. SNMP community strings authenticate access to Management Information Base (MIB) objects and functions as embedded passwords.
The following fields appear only when **SNMP Version** 3 is selected.	
Username	Username for authentication

Field	Description
Authoritative Engine ID (Hex Values)	The authoritative (security) engine ID used for SNMP version 3 REQUEST messages by primary Manager. The length of the hex value of the Authoritative Engine ID should be between 10 and 50 hexadecimal characters.
Authoritative Peer Engine ID (Hex Values): **NOTE** The **Authoritative Peer Engine ID** field is available while configuring SNMP version 3 only after successful creation of an MDR pair.	The authoritative (security) engine ID used for SNMP version 3 REQUEST messages by secondary Manager. **NOTE** The Authoritative (security) engine ID for any Manager is unique. At any point of time, the **Authoritative Engine ID** of the Manager is static irrespective of Manager status in case of an MDR pair. That is, when MDR switchover occurs, the authoritative engine ID of the Manager will not change with the status of the Manager. Hence, the alerts generated from the Primary and Secondary Manager will have their respective authoritative engine IDs. **NOTE** After successful deletion of an MDR pair, the Authoritative Engine IDs are retained by the respective Managers.
Authentication Level	This specifies the authentication level and has the following categories: • **No Authorization, No Privileges** — Uses Username match for authentication • **Authorization, No Privileges** — Provides authentication based on the MD5 or SHA algorithms • **Authorization and Privileges** — Provides authentication based on the MD5 or SHA algorithms. It also provides encryption in addition to authentication based on the DES or AES standards.
Customize Community	Enter an SNMP community string to protect your Trellix IPS data. SNMP community strings authenticate access to Management Information Base (MIB) objects and functions as embedded passwords.
The following fields appear only when **Authorization, No Privileges** is selected as **Authentication Level**:	
Authentication Type	The authentication protocol (MD5, SHA, or SHA256) used for authenticating SNMP version 3 messages
Authentication Password	The authentication pass phrase used for authenticating SNMP version 3 messages
The following fields appear only when **Authorization and Privileges** is selected as **Authentication Level**:	
Authentication Type	The authentication protocol (MD5, SHA, or SHA256) used for authenticating SNMP version 3 messages

Field	Description
Authentication Password	The authentication pass phrase used for authenticating SNMP version 3 messages
Encryption Type	The privacy protocol (DES, AES, or AES256) used for encrypting SNMP version 3 messages **NOTE** **AES256** appears in the drop-down menu only when you choose **SHA256** as the **Authentication Type**.
Privacy Password	The privacy pass phrase used for encrypting SNMP version 3 messages

3. Click **Save**.

   The SNMP server is added under the **SNMP** tab.

NOTE

Do not use a broadcast IP address (that is, 255.255.255.255) as the target SNMP server for forwarding alerts.

4. If you want to modify an existing entry, double-click the specific SNMP entry. The **SNMP Forwarder Configuration Details** panel opens where you can update the required fields and save the changes.
5. In case you want to delete an existing server, select the specific entry and click −. You can delete only one server entry at a time.

Forward alerts to an SNMP server

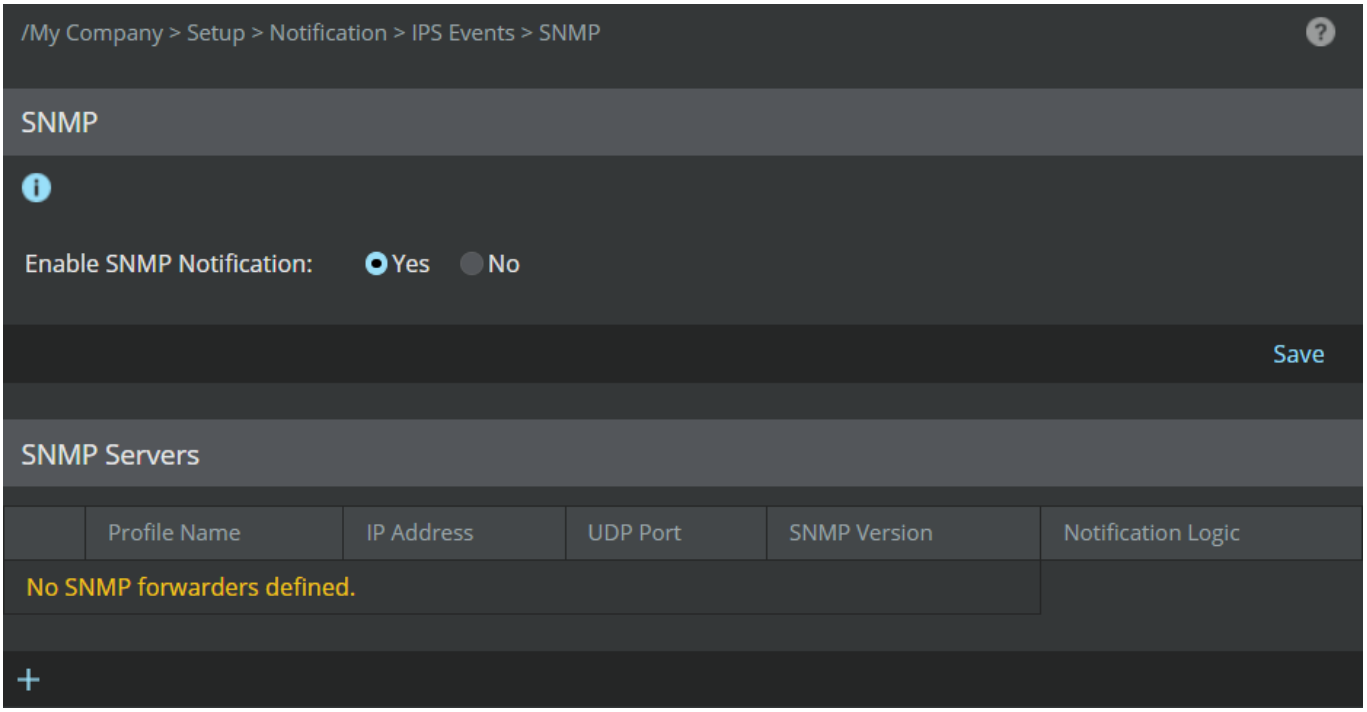
You can configure the SNMP server to which alert information for Sensor or NTBA Appliance is to be sent.

You can configure more than one SNMP server. You can configure the SNMP servers for each admin domain separately. The SNMP server configured for a root admin domain can be different from the SNMP server configured for its child domains. When the **Children** and the **Current** checkboxes are selected while configuring an SNMP server for the root admin domain, the SNMP server configured for the child domain will forward notifications to both the parent and child domain SNMP servers. When the **Children** checkbox is not selected in the root admin domain, then the child domain will use only the SNMP server configured for that domain to forward notifications. The **SNMP Servers** list on the **SNMP** tab displays the SNMP servers you have configured.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS Events/NTBA Events → **SNMP**.

   The **SNMP** tab is displayed where **Enable SNMP Notification** option and the configured **SNMP Servers** list is displayed.



2. Select **Yes** against **Enable SNMP Notification** and click **Save**.
3. The columns displayed under the **SNMP Servers** section are as follows:

Field	Description
Profile Name	The profile name from where notifications are sent
IP Address	IP address of the target server
UDP Port	SNMP listening port of the target server
SNMP Version	The version of SNMP server
Notification Logic	The logic by which the notifications are sent to the target server

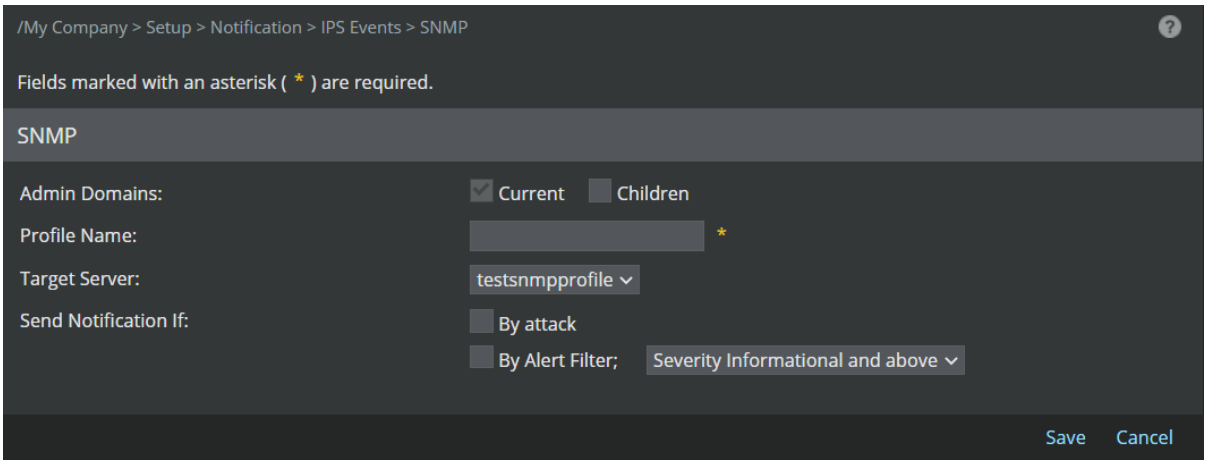
Add an SNMP profile for alert notification

You can configure the SNMP server on the **SNMP** configuration page.

Steps:

1. Click the + button in the SNMP parent page.

   The **SNMP** configuration page is displayed.



2. Specify options in the appropriate fields.

Field	Description
Admin Domains	Specify whether this applies to the child domains as well.
Profile Name	Enter the profile name from where notifications are sent.
Target Server	Choose the target server from the drop-down to which notifications are forwarded.
Send Notification If	**By attack** for Sensor and the attack definition has this notification option explicitly enabled for IPS — Forwards attacks that match customized policy notification settings, which you must set when editing attack responses within the Policy Editor. **By Alert Filter** for Sensor and the following notification filter is matched for NTBA — Sends notification for all, or based on the severity of alerts: • **Severity Informational above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium, and high severity alerts • **Severity High** — Includes only high severity alerts

3. Click **Save**.

   The SNMP server is added to the **SNMP** parent page under the **SNMP Servers** section.

Modify or delete SNMP server settings

You can modify or delete the SNMP server settings at the **Manager** node.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **SNMP.**

   The **SNMP** tab with the **Enable SNMP Notification** option and the **SNMP Servers** list is displayed.

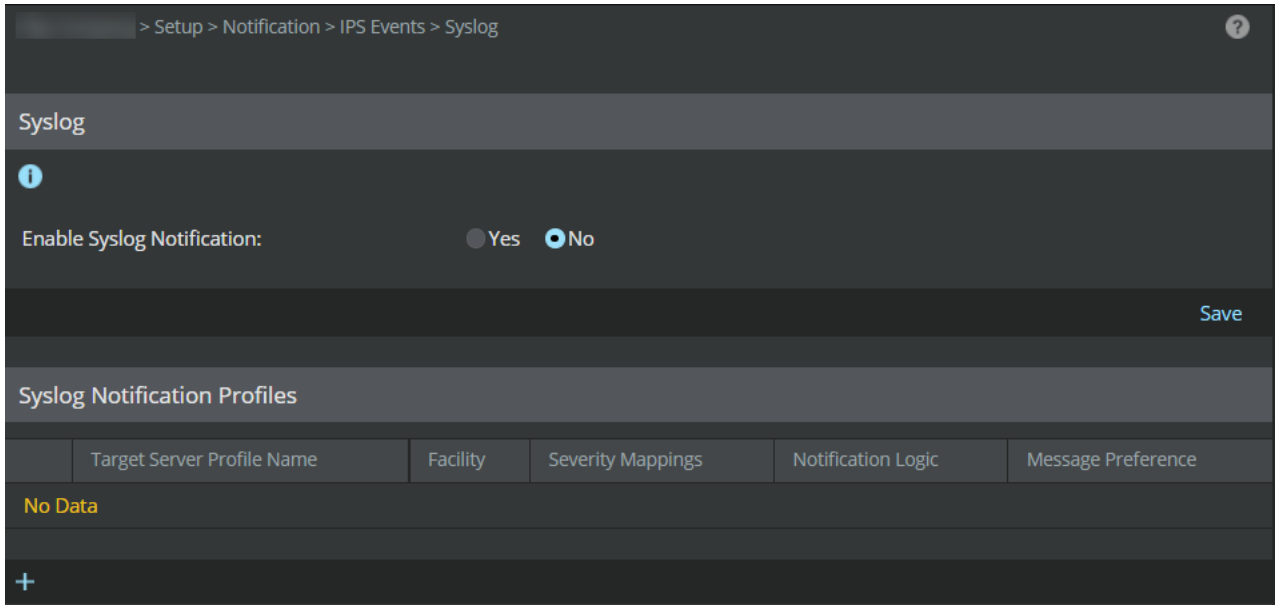
2. Select the configured SNMP server instance from the **SNMP Servers** list.

3. Configure the following:
   a. To edit the settings, click , modify the fields as required, and click **Save**.
   b. To delete the settings, click and click **OK** to confirm deletion.

Forward alert notifications from the Manager to a syslog server

Alerts forwarded from the Manager to a syslog server enable you to view the alerts on the third-party applications that support UDP and TCP over SSL, for example, Syslog NG.

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS Events → **Syslog**.



2. Click **Yes** in **Enable Syslog Notification** to enable syslog forwarding of alerts.
3. Click **Save.**

> **NOTE**
>
> You can forward Sensor alerts to multiple syslog servers by creating new syslog notification profiles. You can forward IPS alerts to syslog servers using UDP or TCP (with or without SSL).

4. The columns displayed under the **Syslog Notification Profiles** section are as follows:

Field	Description
Target Server Profile Name	The profile name of the target server from where notifications are sent
Facility	The facility defined in the **Edit a Syslog Notification Profile** page
Serverity Mappings	The severity mappings defined in the **Edit a Syslog Notification Profile** page
Notification Logic	The logic by which the notifications are sent to the target server
Message Preference	The message preference you defined - **Default** or **Custom**

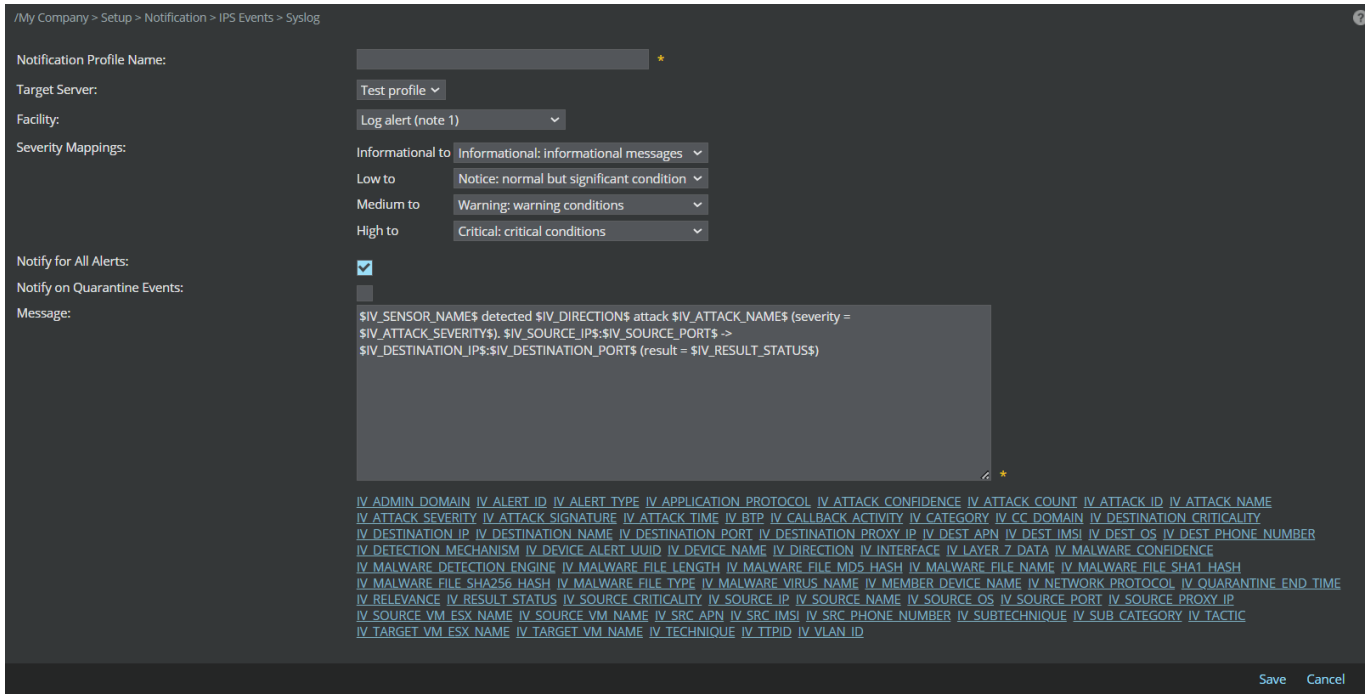
Add a Syslog notification profile to forward alerts

You can add notification profiles that will be displayed in the **Syslog** page.

1. Click + in the **Syslog** page.

   The **Add a Syslog Notification Profile** page is displayed.

2. Specify your options in the corresponding fields.



Field	Description
Admin Domain	• **Current** — Send notifications for alerts in the current domain. Always enabled for current domain by default. • **Children** — Include alerts for all child domains of the current domain (Not applicable to NTBA)
Notification Profile Name	Profile name from where notifications are sent
Target Server	Choose the target server from the drop-down to which notifications are forwarded.

Field	Description
Facility	Standard syslog prioritization value. The choices are as follows: • **Security/authorization (code 4)** • **Security /authorization (code 10)** • **Log audit (note 1)** • **Log alert (note 1)** • **Clock daemon (note 2)** • **Local user 0 (local0)** • **Local user 1 (local1)** • **Local user 2 (local2)** • **Local user 3 (local3)** • **Local user 4 (local4)** • **Local user 5 (local5)** • **Local user 6 (local6)** • **Local user 7 (local7)**
Severity Mappings	You can map each severity (Informational, Low, Medium, or High) to one of the standard syslog severities listed below: • **Emergency** — System is unusable • **Alert** — Action must be taken immediately • **Critical** — Critical conditions • **Error** — Error conditions • **Warning** — Warning conditions • **Notice** — Normal but significant condition • **Informational** — Informational messages • **Debug** — Debug-level messages
Notify for All Alerts	By default, this checkbox will be selected. Notifies for *all* discovered attacks.
The following field is enabled only on deselecting the **Notify for All Alerts** checkbox.	

Field	Description
Only Notify When	**The attack definition has this notification option explicitly enabled** Send notification for attacks that match customized policy notification settings, which you must set when editing attack responses within the policy editor (Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types) → **IPS** based on the following filters: • **Severity High** — Includes only high severity alerts • **Severity Informational and above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium and high severity alerts
Notify on Quarantine Events (not applicable to NTBA Appliance)	Select this checkbox to see quarantine events.
Message	The default message is a quick summary of an alert with the following fields for easy recognition: **Device Name**, **Direction**, **Attack Name**, **Attack Severity**, **Attacker IP: Attacker Port**, **Target IP: Target Port**, and **Result**. A default message reads: IV_SENSOR_NAME detected $IV_DIRECTION$ attack IV_ATTACK_NAME (severity = $IV_ATTACK_SEVERITY$). IV_SOURCE_IP:IV_SOURCE_PORT -> $IV_DESTINATION_IP$:$IV_DESTINATION_PORT$ (result = IV_RESULT_STATUS) **NOTE** For syslog message to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each parameter. Example: $ATTACK_TIME$ Type a message and select (click) the parameters for the wanted alert identification format. You can type custom text in the **Message** field. IV_ADMIN_DOMAIN IV_ALERT_ID IV_ALERT_TYPE IV_APPLICATION_PROTOCOL IV_ATTACK_CONFIDENCE IV_ATTACK_COUNT IV_ATTACK_ID IV_ATTACK_NAME IV_ATTACK_SEVERITY IV_ATTACK_SIGNATURE IV_ATTACK_TIME IV_BTP IV_CALLBACK_ACTIVITY IV_CATEGORY IV_CC_DOMAIN IV_DESTINATION_CRITICALITY IV_DESTINATION_IP IV_DESTINATION_NAME IV_DESTINATION_PORT IV_DESTINATION_PROXY_IP IV_DEST_APN IV_DEST_IMSI IV_DEST_OS IV_DEST_PHONE_NUMBER IV_DETECTION_MECHANISM IV_DEVICE_ALERT_UUID IV_DEVICE_NAME IV_DIRECTION IV_INTERFACE IV_LAYER_7_DATA IV_MALWARE_CONFIDENCE IV_MALWARE_DETECTION_ENGINE IV_MALWARE_FILE_LENGTH IV_MALWARE_FILE_MD5_HASH IV_MALWARE_FILE_NAME IV_MALWARE_FILE_SHA1_HASH IV_MALWARE_FILE_SHA256_HASH IV_MALWARE_FILE_TYPE IV_MALWARE_VIRUS_NAME IV_MEMBER_DEVICE_NAME IV_NETWORK_PROTOCOL IV_QUARANTINE_END_TIME IV_RELEVANCE IV_RESULT_STATUS IV_SOURCE_CRITICALITY IV_SOURCE_IP IV_SOURCE_NAME IV_SOURCE_OS IV_SOURCE_PORT IV_SOURCE_PROXY_IP IV_SOURCE_VM_ESX_NAME IV_SOURCE_VM_NAME IV_SRC_APN IV_SRC_IMSI IV_SRC_PHONE_NUMBER IV_SUBTECHNIQUE IV_SUB_CATEGORY IV_TACTIC IV_TARGET_VM_ESX_NAME IV_TARGET_VM_NAME IV_TECHNIQUE IV_TTPID IV_VLAN_ID **NOTE** Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

3. Click **Save.**

The newly added notification profile will be displayed in the **Syslog** page.

Table 6. Syslog variables for alert notification and the equivalent Attack Log columns

Syslog variable name	Description	Attack Log column
IV_ADMIN_DOMAIN	The domain to which the Sensor that detected the attack belongs	Domain
IV_ALERT_ID	The globally unique ID that the Manager assigns to an alert	Alert ID
IV_ALERT_TYPE	The Sensor decides the type of alert. This is mainly used by the Manager for its internal processing. This is not related to the Attack Category or Attack Sub-category. Some example alert types are signature, statistical anomaly, threshold anomaly, port scan, and host sweep.	Not available
$IV_APPLICATION_PROTOCOL$	The application-layer protocol associated with the attack traffic. This is not related to the Application Identification feature, and this information is displayed even if you have not enabled Application Identification. There could be instances when a Sensor might not be able to detect the protocol.	Not available
$IV_ATTACK_CONFIDENCE$	This is a value between 1 and 7. For example, a confidence level of 7 indicates that there is low possibility of the attack being a false-positive. The attack confidence values are inversely related to the Benign Trigger Probability (BTP) values of attack signatures. • Confidence 1 = BTP 7 (high) • Confidence 2 = BTP 6 (high) • Confidence 3 = BTP 5 (medium) • Confidence 4 = BTP 4 (medium) • Confidence 5 = BTP 3 (medium) • Confidence 6 = BTP 2 (low) • Confidence 7 = BTP 1 (low) **NOTE** When the BTP value is 0, there is no corresponding confidence value for the attack.	Not available
IV_ATTACK_COUNT	The number of types the attack occurred. This information is more relevant for suppressed alerts. Consider you have enabled alert suppression such that the alert is raised only when the attack is seen 5 times within 30 seconds. Subsequently, the Sensor detected this attack 10 times within 30 seconds. Then the attack count for this alert is 10.	Attack Count

Syslog variable name	Description	Attack Log column
IV_ATTACK_ID	Trellix Advanced Research Center assigns a universally unique hexadecimal value to each attack. This field displays the integer value of the hexadecimal ID assigned by Trellix ARC.	The equivalent hexadecimal value is displayed in the **Attack Information & Description** page as **Intrusvert ID**.
IV_ATTACK_NAME	The name assigned by Trellix ARC to an attack	Name
$IV_ATTACK_SEVERITY$	Indicates the severity value of an attack specified in the corresponding attack definition. • 0 - Informational • 1 to 3 - low • 4 to 6 - medium • 7 to 9 - high	Attack Severity (high, medium, low, or informational)
$IV_ATTACK_SIGNATURE$	The ID of the signature that matched the attack traffic	Not available
IV_ATTACK_TIME	The time when the Sensor created the alert	Time
$IV_CALLBACK_ACTIVITY$	The name of the Callback Activity family	Callback Activity
$IV_CATEGORY$	The category to which the attack belongs. This is decided by Trellix ARC. Some examples are exploit, policy violation, and reconnaissance. You can view the attack categories in the IPS Policy Editor when you group by Attack Category.	Attack Category
IV_CC_DOMAIN	The name of the Callback Activity domain	C&C Domain
$IV_DESTINATION_CRITICALITY$	Displays the risk level as High Risk, Medium Risk or Low Risk	Target Risk
$IV_DESTINATION_IP$	The destination IP address to which the attack is destined	Target IP address
$IV_DESTINATION_NAME $	The name of the host to which the attack is destined	Target Hostname
IV_DESTINATION_PORT$	The port number on the destination host to which the attack traffic is sent	Target Port
$IV_DESTINATION_PROXY_IP	The IP address of the proxy server	Target Proxy IP

Syslog variable name	Description	Attack Log column
IV_DEST_APN	This is the destination Access Point Name (APN). This information is part of a mobile subscriber's identity data and is relevant only if you have deployed Sensors to monitor mobile networks. To see this data, you must enable capturing and tagging of mobile subscriber data in the alerts by using the **`set mnsconfig`** Sensor CLI command.	Not available
IV_DEST_IMSI	This is the destination International Mobile Subscriber Identity (IMSI). The details provided for APN apply to this as well.	Not available
IV_DEST_OS	The operating system installed on the destination host	Target OS
$IV_DEST_PHONE_NUMBER$	This is the destination mobile phone number. The details provided for APN above apply to this as well.	Not available
$IV_DETECTION_MECHANISM$	The method the Sensor used to detect the attack. For example, signature, multi-flow-correlation, threshold, and so on. Each method relates to a specific attack category.	Detection (in Alert Details panel)
$IV_DEVICE_ALERT_UUID$	ID assigned to the alert	Alert ID
IV_DEVICE_NAME	Name of the device that detected the attack	Device
$IV_DIRECTION$	Indicates whether the attack traffic originated from your network or the outside network. For example, inbound direction means that the attack traffic originated from the outside network, targeting the hosts on your network.	Direction
$IV_INTERFACE$	The interface or sub-interface on which the Sensor detected the attack traffic	Interface
$IV_LAYER_7_DATA$	Provides the Layer 7 data	Layer 7 Data
$IV_MALWARE_CONFIDENCE$	Confidence level of the malware as detected by the engine	Malware Confidence
$IV_MALWARE_DETECTION_ENGINE$	Engine which detected the malware (Gateway Anti-Malware, Global Threat Intelligence, PDF-JS, etc)	Engine
$IV_MALWARE_FILE_LENGTH$	The length of the malware file	Not available
$IV_MALWARE_FILE_MD5_HASH$	The MD5 hash of the malware file (fingerprint)	File Hash
$IV_MALWARE_FILE_NAME$	The name of the malware file. For SMTP traffic, it displays the file name of the attachment and for HTTP traffic, it displays the URL of the file.	File Name
$IV_MALWARE_FILE_SHA1_HASH$	The SHA1 hash of the malware file (fingerprint)	File Hash
$IV_MALWARE_FILE_SHA256_HASH$	The SHA256 hash of the malware file (fingerprint)	File Hash
$IV_MALWARE_FILE_TYPE$	The file type of the malware file	Not available
$IV_MALWARE_VIRUS_NAME$	The virus name as detected by Gateway Anti-Malware	Not available

Syslog variable name	Description	Attack Log column
$IV_MEMBER_DEVICE_NAME$	Name of the device that detected the attack	Device
$IV_NETWORK_PROTOCOL$	The network protocol, such as TCP, of the attack traffic	Protocol (in Alert Details panel)
$IV_QUARANTINE_END_TIME$	The time when the attacking host will be out of quarantine. This is relevant only if you had enabled **Quarantine** feature.	Not available
$IV_RELEVANCE$	Indicates if the endpoint is vulnerable to this particular attack	Relevance
IV_RESULT_STATUS	Indicates whether the attack traffic reached the victim host	Result
$IV_SOURCE_CRITICALITY$	Displays the risk level as High Risk, Medium Risk or Low Risk	Attacker Risk
$IV_SENSOR_ALERT_UUID$	The universally unique ID assigned by the Sensor for the alert. For a specific alert raised by a specific Sensor, the Central Manager also displays the same ID.	Alert ID
$IV_SENSOR_CLUSTER_MEMBER$	The member Sensor of a HA pair that generated the alert	Not available
IV_SENSOR_NAME	The Sensor that generated the alert	Device
IV_SOURCE_IP	The IP address of the attacking host	Attacker IP address
IV_SOURCE_NAME	Name of the host from where the attack was generated	Attacker Hostname
IV_SOURCE_OS	OS of the attacking host	Attacker OS (in Alert Details panel)
IV_SOURCE_PORT	The port number on the attacking host from which the attack traffic is sent	Attacker Port
$IV_SOURCE_PROXY_IP$	The IP address of the proxy server	Attacker Proxy IP
$IV_SOURCE_VM_NAME$	Name of the virtual machine from where the attack was generated	Attacker VM Name
IV_SRC_APN	This is the source Access Point Name (APN). This information is part of a mobile subscriber's identity data and is relevant only if you have deployed Sensors to monitor mobile networks. To see this data, you must enable capturing and tagging of mobile subscriber data in the alerts by using the **`set mnsconfig`** Sensor CLI command.	Not available
IV_SRC_IMSI	This is the source International Mobile Subscriber Identity (IMSI). The details provided for APN apply to this as well.	Not available
$IV_SRC_PHONE_NUMBER$	This is the source mobile phone number. The details provided for APN apply to this as well.	Not available

Syslog variable name	Description	Attack Log column
$IV_SUBTECHNIQUE$	Name of the corresponding adversarial sub-technique matching with the attack or alert	Sub-Technique
$IV_SUB_CATEGORY$	The subcategory to which the attack belongs. This is decided by Trellix ARC, and is a classification within Attack Category. Some examples are brute-force, buffer-overflow, host-sweep, and restricted-application. You can view the attack subcategories in the IPS policy editor when you group by Attack Subcategory.	Attack Subcategory (in Alert Details panel)
IV_TACTIC	Name of the adversarial tactic matching with the attack or alert	Tactic
$IV_TARGET_VM_NAME$	Name of the virtual machine to which the attack is directed	Target VM Name
$IV_TECHNIQUE$	Name of the corresponding adversarial technique matching with the attack or alert	Technique
IV_TTPID	ID of the specific technique/sub-technique in the<techniqueID.sub-techniqueID> format	Technique/Sub-Technique ID
IV_VLAN_ID	The VLAN ID seen on the attack traffic	VLAN

NOTE

Mitre Attack Details can be currently forwarded through the Manager alone. So, if you plan to forward details such as the **Tactic**, **Technique**, **Sub-Technique**, or **Technique/Sub-Technique ID**, you need to assign the relevant variables only through this page.

Edit or delete a syslog notification profile

You can edit or delete a syslog notification profile by clicking the or in the **Syslog Notification Profiles** section.

Configure email or pager alert notifications

Prerequisite:

You must identify a mail server for email notifications in the **E-mail** page (Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **E-mail**).

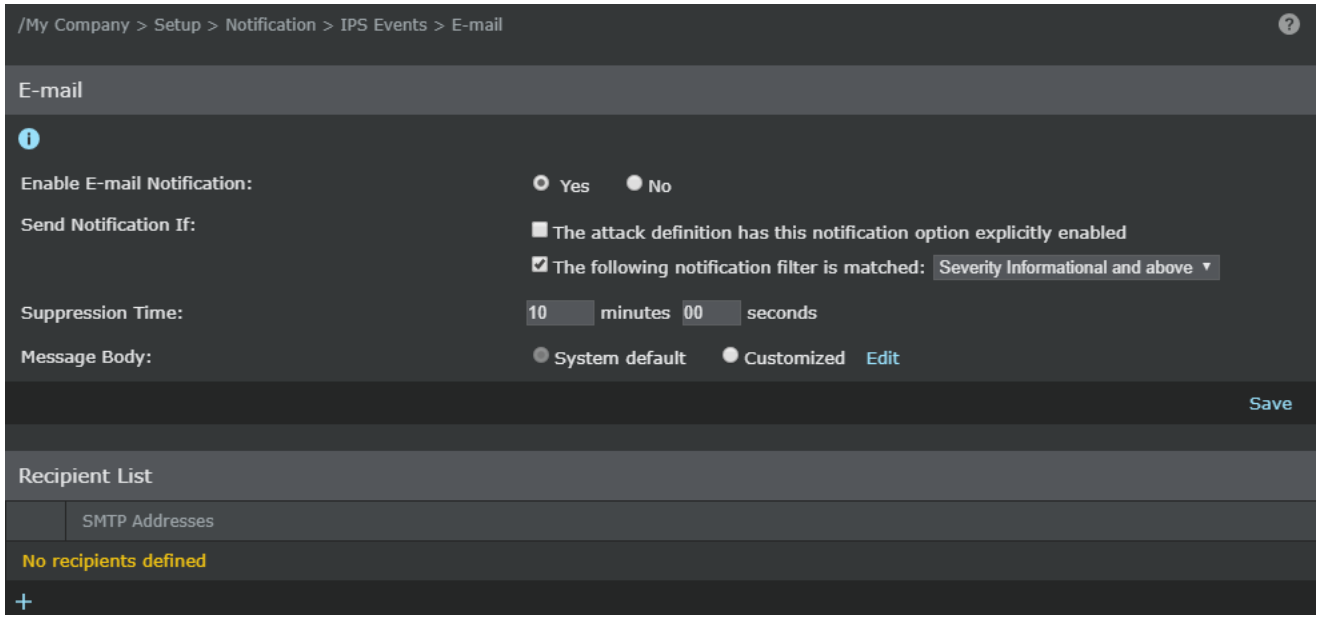
Users can be alerted by email or pager when an alert is generated that matches a chosen severity or customized attack setting.

The procedure for configuring email alerts is described here. The procedure for configuring pager is similar.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **E-mail**.

   The **E-Mail** and **Recipient List** information is displayed under the **E-mail** tab.



2. Specify your options in the corresponding fields.

Field	Description
Enable E-mail Notification	Select **Yes** to enable alert notification through email.
Send Notification If	**The attack definition has this notification option explicitly enabled** — Send notification for attacks that match customized policy notification settings, which you must set when editing attack responses within the policy editor. **The following notification filter is matched** — Send notification based on the following filters: • **Severity Informational and above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium and high severity alerts • **Severity High** — Includes only high severity alerts The table below explains the functional interdependency of the two options.
Suppression Time	Type a **Suppression Time** for the notification. The suppression time is the duration (minutes and seconds) to wait after an alert notification has been sent before sending another alert notification. The default and minimum value is 10 minutes and 0 seconds. Suppression time is useful to avoid sending excessive notifications when there is heavy attack traffic.

Field	Description
Message Body	The *message body* is a preset response sent with the notification with information pertaining to the alert. **System Default** — The system default message provides the notified admin with the most basic attack details so that an immediate response can be made. Details include the attack name, time detected, attack type, severity, the Sensor interface where detected, and the source and/or destination IP addresses. **NOTE** You cannot edit the **System Default** message. **Customized** — Select **Customized** against **Message Body** and click **Edit** to view the **Custom Message** page. You can type custom text in the **Subject** field or **Body** section, as well as click one or more of the provided variable links at **Subject Line Variables** or **Content-Specific Variables**. **NOTE** Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

Notification option explicitly enabled	Notification filter is matched	Functionality
✔		Emails are sent only for the attacks where the notification option is enabled.
	✔	Emails are sent only when the defined severity level is matched and the notification option is disabled.
✔	✔	If the attack matches at least one of the criteria, an email is sent.

3. Click **Save** to return to the email or pager notification settings page.
4. Click + in the **Recipient List** section of the **E-mail** page.

   The **Add a Recipient** page is displayed.
5. Enter the Recipient email address in the **SMTP Address** field and click **Save**.

   The email address is listed under the **Recipient List** on the **E-mail** tab.

   - You can configure pager settings using a similar procedure in the **Pager** page. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **Pager** to view the **Pager** page.
   - Email and pager notifications are configured per admin domain.

Enable alert notification by script

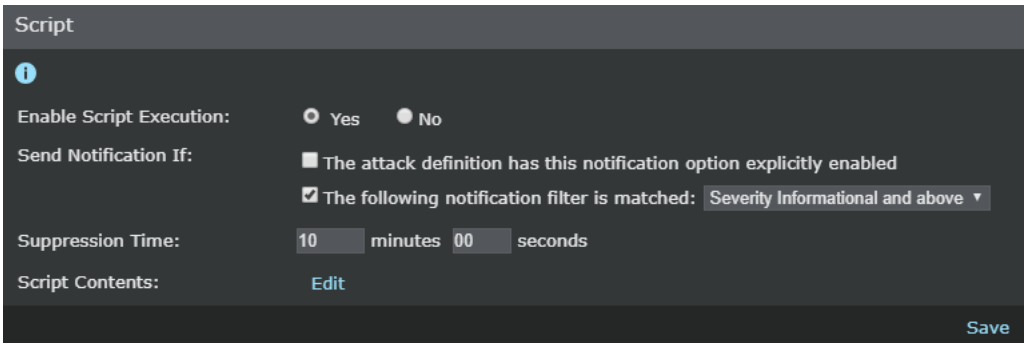
Users can be alerted through an executed script when an alert is generated that matches a chosen severity or customized attack setting.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **Script**.

   The **Script** page is displayed.

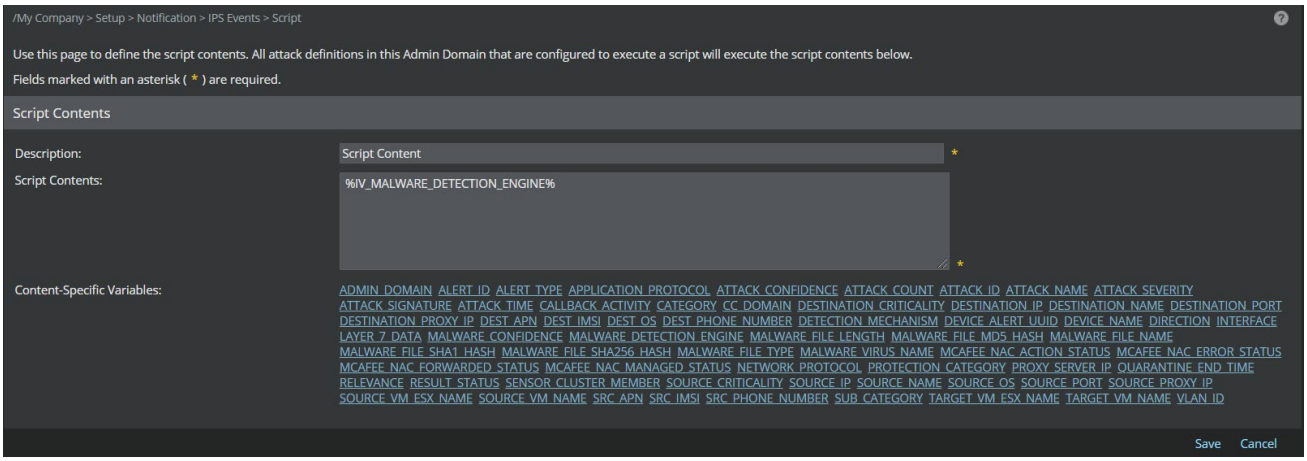
2. Specify the options in the corresponding fields.



Field	Description
Enable Script Execution	Select **Yes** to enable alert notification through an executed script.
Send Notification If	**The attack definition has this notification option explicitly enabled** — send notification for attacks that match customized policy notification settings, which you must set when editing attack responses within the policy editor. **The following notification filter is matched**: • **Severity Informational and above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium and high severity alerts • **Severity High** — Includes only high severity alerts
Suppression Time	Enter a **Suppression Time** for the notification. The suppression time is the amount of time (minutes and seconds) to wait after an alert has been generated before sending the notification. This will prevent alerts being sent through notification in the event an alert has been acknowledged or deleted through the **Attack Log** page within the suppression time. The default and minimum value is 10 minutes and 0 seconds.

3. Click **Edit**.

   The **Script Contents** page is displayed.



- Enter a description in the **Description** field.
- Enter the required text in the **Script Contents** field. Click the links provided against **Content-Specific Variables** to add variables in the **Script Contents** field.

> **NOTE**
>
> Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

4. Click **Save** to return to the **Script** page.
5. Click **Save** to save your settings.
   - The local system user needs to have permission to create the script output file on the Manager installation directory.
   - Notifications are configured per admin domain.

Set up of fault notifications

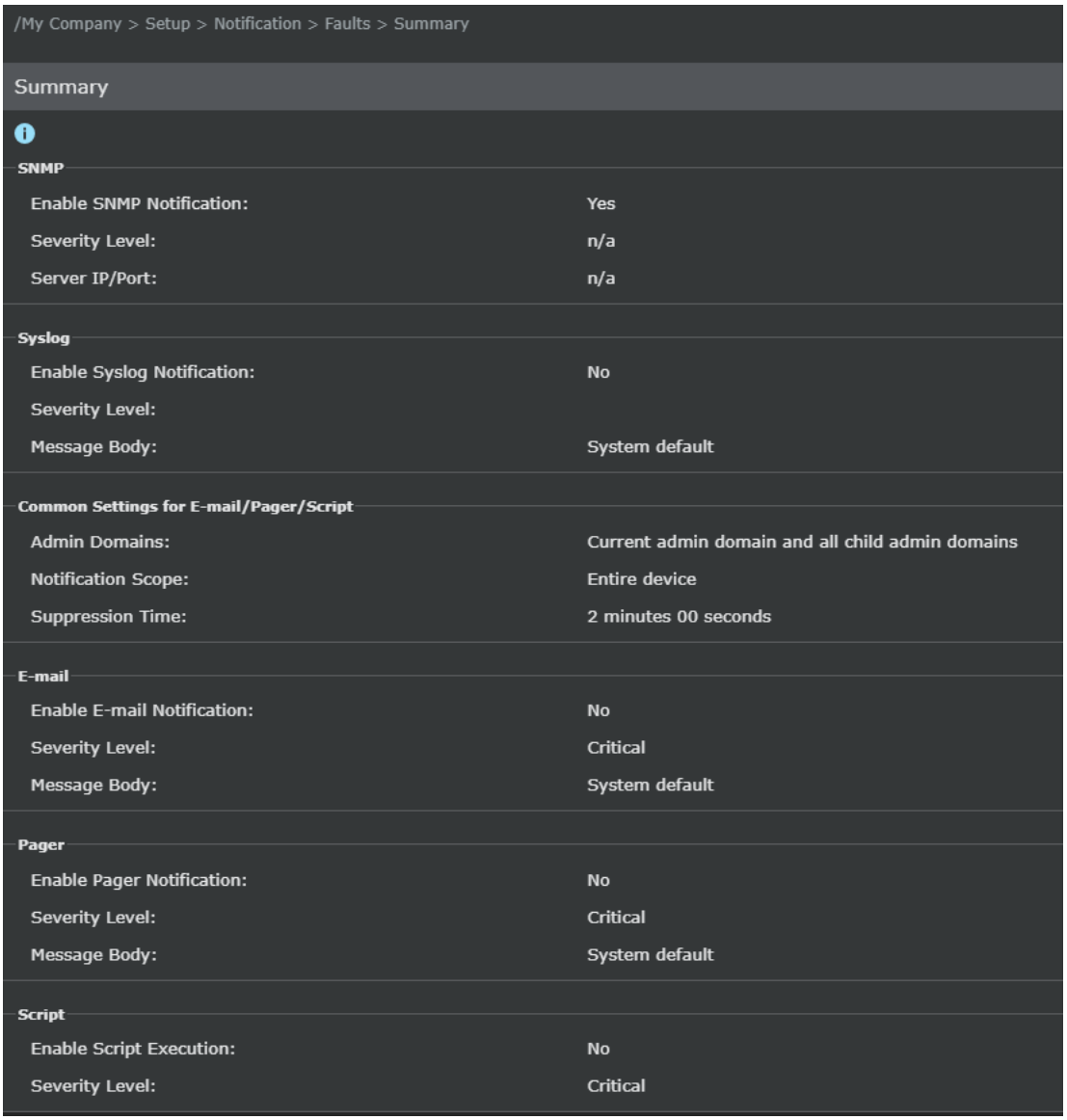
The Manager can send system fault information to third-party machines such as SNMP servers and syslog servers. You can also configure Manager to notify you — via email, pager, or script — for system faults based on fault severity. You can view fault notification details, forward faults to an SNMP or Syslog server, configure fault notification, send alerts to an email or pager, and specify script parameters for fault notifications.

How to view fault notification details

The **Summary** (Manager → <Admin Domain Name> → Setup → Notification → Faults → **Summary**) option displays a summary of configured fault notification settings for the Manager (or Central Manager). The summary reflects configurations made within the other **Fault Notification** group actions.

In case of Central Manager, select Manager → Setup → Notification → Faults → **Summary**.

Figure 42. Fault Notification Details



Forward faults to an SNMP server

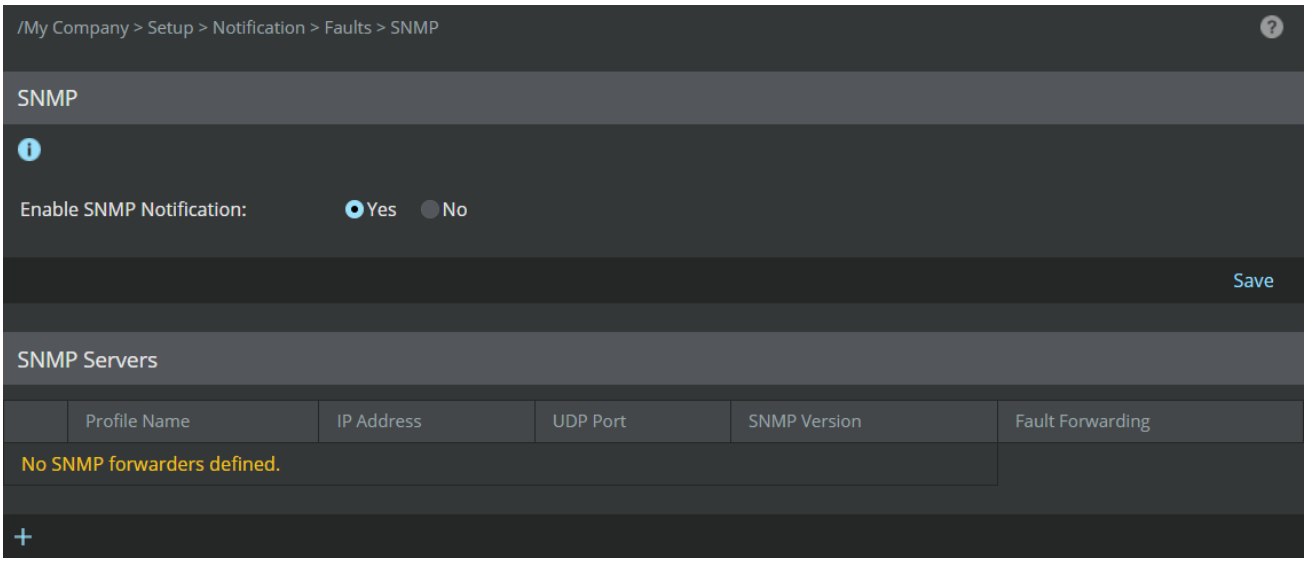
The Manager → <Admin Domain Name> → Setup → Notification → Faults → **SNMP** option enables you to specify an SNMP server to which system fault information will be sent from the Manager. You can configure more than one SNMP server where you want to send fault messages. The SNMP Servers page displays the SNMP servers that have been configured. The fields in this page are described within the configuration steps that follow.

To configure an SNMP server to receive system faults from your Manager, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → Faults → **SNMP**.

   The **SNMP** tab is displayed where **Enable SNMP Notification** option and the configured **SNMP Servers** list is displayed.



2. Select **Yes** against **Enable SNMP Notification** and click **Save**.
3. The fields displayed under the **SNMP Servers** section are as follows:

Field	Description
Profile Name	The profile name from where notifications are sent
IP Address	IP address of the target server
UDP Port	SNMP listening port of the target server
SNMP Version	The version of SNMP server
Fault Forwarding	The logic by which faults are forwarded to the target server

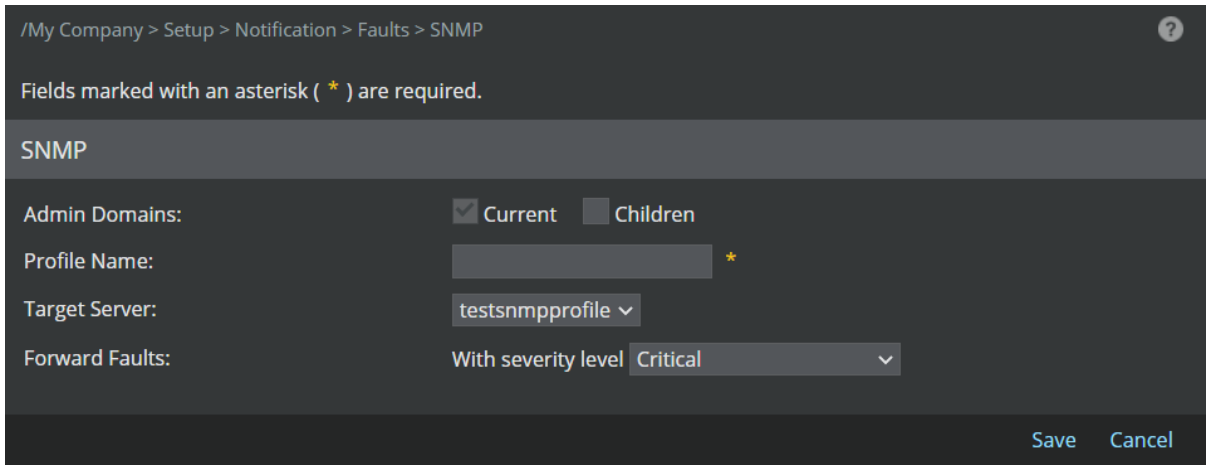
Add an SNMP profile for fault notification

You can configure the SNMP server on the **SNMP** configuration page.

Steps:

1. Click the + button in the SNMP parent page.

   The **SNMP** configuration page is displayed.



2. Specify options in the appropriate fields.

Field	Description
Admin Domains	Specify whether this applies to the child domains as well.
Profile Name	Enter the profile name from where faults are sent.
Target Server	Choose the target server from the drop-down to which faults are forwarded.
Forward Faults	Choose the severity level for forwarding faults. The options are **Critical, Error and above, Warning and above**, and **Informational and above**. Choose the severity of alerts that will have information forwarded. Limiting your alert severities to **Critical** or **Error and above** is recommended for focused analysis.

3. Click **Save**.

   The SNMP server is added to the **SNMP** parent page under the **SNMP Servers** section.

Modify or delete SNMP forwarder settings

To modify or delete SNMP Forwarder settings, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → Faults → **SNMP**.
2. Select the configured SNMP server instance from the SNMP Forwarder list page.
3. Do one of the following:
   a. To edit the settings, click , modify the fields as required, and then click **Save**.
   b. To delete the settings, click and then click **OK** to confirm the deletion.

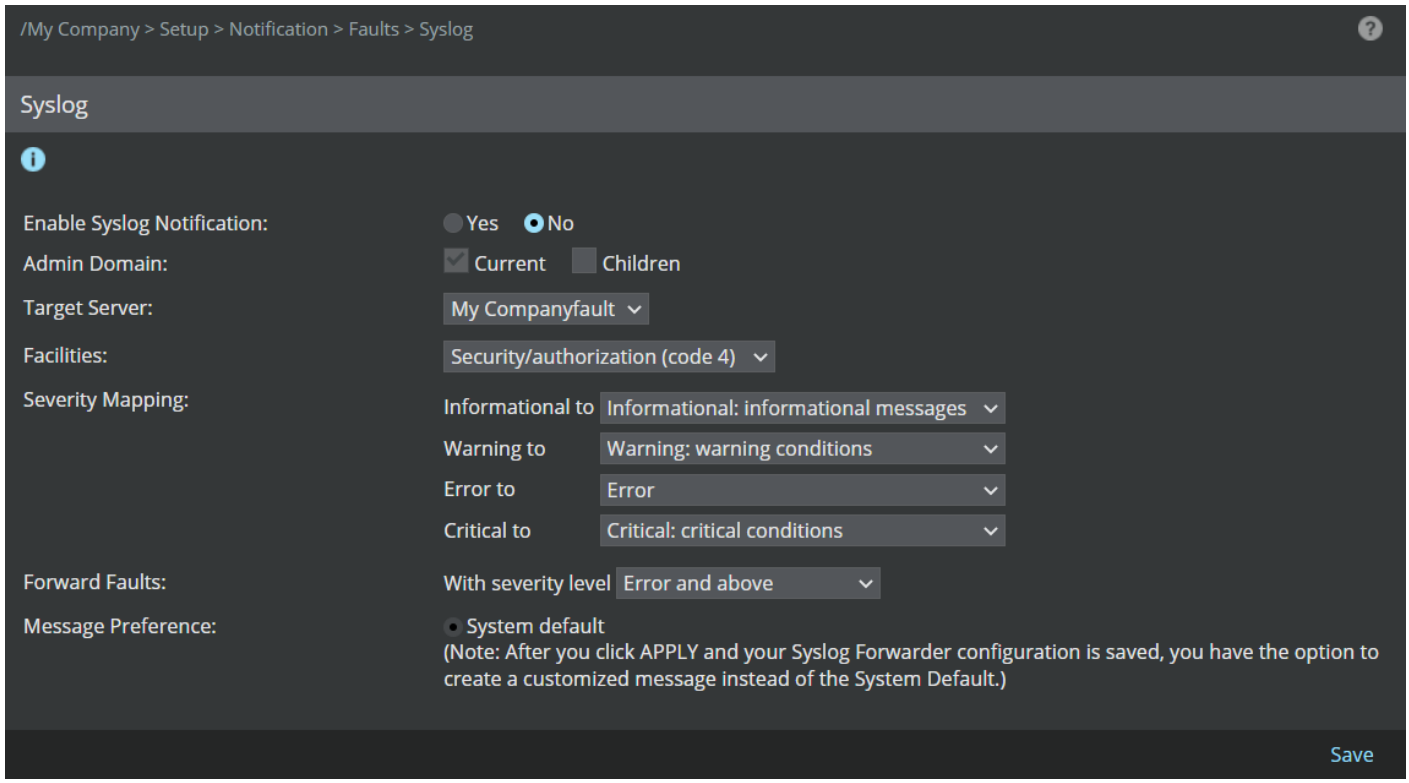
Forward faults to a Syslog server

The Manager → <Admin Domain Name> → Setup → Notification → Faults → **Syslog** option enables the forwarding of Trellix IPS faults to a syslog server. Syslog forwarding enables you to view the forwarded faults via a third-party syslog application. For syslog forwarding, the root domain and parent domains have the option to include faults from all corresponding child domains.

To enable syslog forwarding for fault notification, do the following:

1. Select Manager → <Admin Domain Name> → Setup → Notification → Faults → **Syslog** (same for Central Manager).

   The **Syslog** window is displayed.



2. Configure the following fields:

Field	Description
Enable Syslog Notification	**Yes** is enabled; **No** is disabled
Admin Domain	Select the below options to enable admin domain notification: • **Current**— Send notifications for alerts in the current domain. Always enabled for current domain. • **Children**— Include alerts for all child domains of the current domain. **NOTE** This field is not present for Central Manager.
Target Server	Choose the target server from the drop-down to which faults are forwarded.

Field	Description
Facilities	Standard syslog prioritization value. The choices are as follows: • Security/authorization (code 4) • Security/authorization (code 10) • Log audit (note 1) • Log alert (note 1) • Clock daemon (note 2) • Local user 0 (local0) • Local user 1 (local1) • Local user 2 (local2) • Local user 3 (local3) • Local user 4 (local4) • Local user 5 (local5) • Local user 6 (local6) • Local user 7 (local7)
Severity Mapping	You can map each fault severity (**Informational**, **Error, Warning**, and **Critical**) to one of the standard syslog severities listed below (default severity mappings are noted in parentheses): • **Emergency**— System is unusable • **Alert**— Action must be taken immediately • **Critical**— (HIGH) Critical conditions • **Error**— Error conditions • **Warning**— (MEDIUM) Warning conditions • **Notice**— (LOW) Normal but significant condition • **Informational**— (INFORMATIONAL) Informational messages • **Debug**: Debug-level messages
Forward Faults	Select the severity of the faults that you want to be forwarded to the syslog server. The options are: • **Critical**— Only Critical faults • **Error and above**— Both Error and Critical faults • **Warning and above**— Warning, Error, and Critical faults • **Informational and above**— All faults

3. Click **Save**.

NOTE

You must click **Save** before you will be able to customize the message format sent to your syslog server.

4. Select the **Message Preference** to send as the syslog forwarding message. The choices are:
   - **System Default** — The default message is a quick summary of a fault with two fields for easy recognition: Device Name and Description. A default message reads:

     ```
     Fault : $IV_DEVICE_NAME$: $IV_DESCRIPTION$
     ```

   - **Customized** — Create a custom message. To create a custom message, do the following:
     1. Click **Edit** to create a custom message.
     2. Type a message and select (click) the parameters for the desired alert identification format. The following figure displays a custom message. You can type custom text in the **Message** field as well as click one or more of the provided elements below the field box.
     3. Click **Save** when finished to return to the Syslog page. The **Customized** button is automatically selected after you have customized the **Message Preference**.

     CAUTION

     For syslog information to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each element. Example: $ATTACK_TIME$

Table 7. Syslog variables for fault notification

Syslog variable name	Description
$IV_ACK_INFORMATION$	Displays additional acknowledgment information when a created fault is acknowledged after the hysteresis period.
$IV_ADDITIONAL_TEXT$	Displays additional text for the raised fault.
IV_ADMIN_DOMAIN	Name of the domain.
$IV_DESCRIPTION$	Description of the fault.
IV_DEVICE_NAME	Name of the device.
$IV_FAULT_COMPONENT$	The component for which the fault is generated.
IV_FAULT_LEVEL	Displays the fault level (Manager system level, Sensor level, or Sensor interface level)
IV_FAULT_NAME	The name of the fault.
IV_FAULT_SOURCE	Indicates if the fault is generated by the Manager or sent by the Sensor.
IV_FAULT_TIME	The time at which the fault is generated.
IV_FAULT_TYPE	Indicates if the event is created, acknowledged, or cleared.
$IV_MEMBER_DEVICE_NAME$	Name of the Sensor.
IV_OWNER_ID	ID of the Manager or the Sensor.
$IV_SEVERITY$	The severity of the fault (critical, error, or warning).

5. Click **Save**.

Set up common settings for fault notification

The **Common Settings** option enables you to determine the breadth and detail of fault information that will be sent via email, pager, or script. You can configure a suppression time within which faults are held pending Acknowledge or Delete actions — or automatic clearing events from the source — within Operational Status.

To manage fault notification details, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → Faults → **Common Settings** (same for Central Manager).
2. Fill in the following fields:
   - **Admin Domains**
     - **Current** — Send only faults for the current domain. This is always selected for the current domain.
     - **Children** — Send faults for all child domains of the current domain
   - **Notification Scope**— If Sensor interfaces have been delegated to a child domain, faults can be set to display by the Admin domain in which the delegated interface resides, rather than by the domain where the Sensor is controlled.
     - **Entire Device** — Faults based on Sensor-domain relationship
     - **Individual interface** — Faults based on interface-domain relationship
   - **Suppression Time** — The amount of time to suppress system faults before forwarding. The default and minimum value is 2 minutes.

     NOTE

     Suppression Time can **only** be set within the root admin domain.
3. Click **Save**.

Send alerts to an email or pager

Users can be alerted by email or email pager when a fault occurs that matches a specified severity.

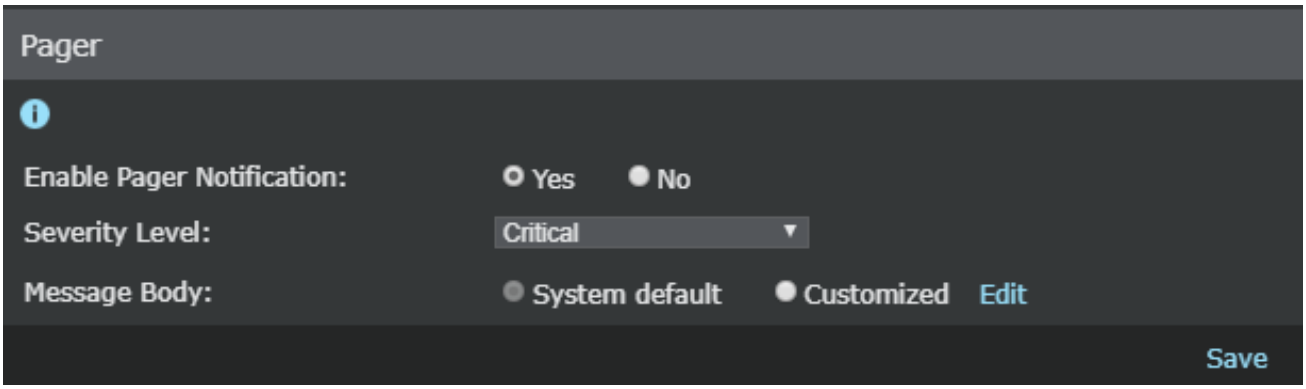
NOTE

You must also identify a mail server for email notifications.

NOTE

Email and pager notifications are configured per admin domain.

Figure 43. Pager notification settings



To enable email or pager fault notification, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → Faults → **E-mail** or Manager → <Admin Domain Name> → Setup → Notification → Faults → **Pager** (same for Central Manager).
2. Select the enabled status (**Enable E-mail / Pager Notification**). **Yes** is enabled; **No** is disabled.
3. Select a fault **Severity Level** to be notified of:

Field	Description
Informational and above	Notifies for *all* faults.
Warning and above	Notifies for Warning, Error, and Critical faults.
Error and above	Notifies for Error and Critical faults.
Critical	Notifies only for Critical faults.

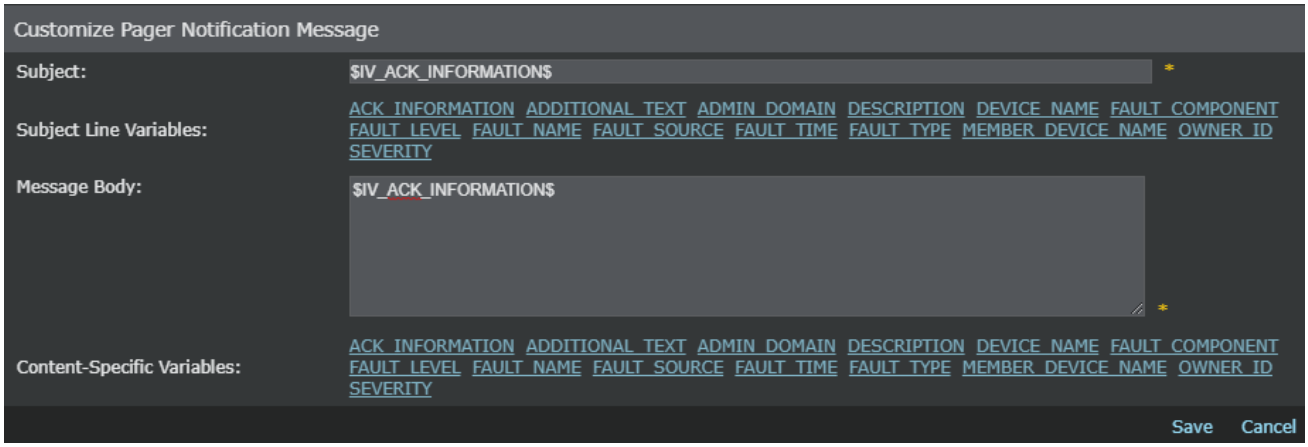
4. Select a **Message body**. The message body is a preset response sent with the notification with information pertaining to the fault.
   - **System Default** — The system default message provides the notified admin with the most basic fault details so that an immediate response can be made. Details include the fault type (severity) and the component source. The subject line of the default message contains the fault name.

     NOTE

     You cannot edit the **System Default** message.

   - **Customized** — Type a message and select (click) the parameters for the desired attack identification format. The following figure displays a custom message. You can type custom text in the **Subject** field or **Message Body** section, as well as click one or more of the provided elements at **Subject Line Variables** or **Content-Specific Variables** to add to the description. When you are finished formatting your message template, click **Save**. The **Customized** button is selected if you have customized the message.

Figure 44. Customize Email Notification Messages window



5. Click **Save**, to save your notification settings.
6. Specify the email or pager address of the intended recipient(s).
7. Scroll to the bottom of the **E-mail** or **Pager** page.
   a. Click +.
   b. In **SMTP Address**, type an email address or email pager address.
   c. Click **Save** when complete.
   d. Repeat steps **a** through **d** to add additional recipient addresses.

Specify script parameters for fault notification

Users can be alerted via executed script when a system fault occurs that matches a configured severity.

> **NOTE**
> Script notifications are configured per admin domain.

To enable alert notification by script, do the following:

1. Select Manager → <Admin Domain Name> → Setup → Notification → Faults → **Script** (Same for Central Manager).
2. Select the enabled status (**Enable Script Execution**). **Yes** is enabled; **No** is disabled.
3. Select a **Severity Level** to be notified of:

Field	Description
Informational and above	Notifies for *all* faults
Warning and above	Notifies for Warning, Error, and Critical faults
Error and above	Notifies for Error and Critical faults
Critical	Notifies only for Critical faults

4. Configure **Script Contents**. This is a preset response sent with the notification with information pertaining to the fault.
   a. Click **Edit**.
   b. Type a name for the script at **Description**.
   c. For the **Script Contents** section, type the text and select the content-specific variables for the attack information you want to see.
   d. Click **Save** to return to the notification form. The script is saved to your installation directory at `<Manager_Install_Dir>\temp\scripts\0\<script-name>`. The script file name is appended with ".bat".

   > **NOTE**
   > The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

5. Click **Save** to save your notification settings.

Management of audit notifications

Every action that is performed by Manager and the Manager server is audited with all information. All audit information contains the following:

- action performed
- result of the action (success or failure)
- time of action
- action message
- user information
- category of the action performed
- admin domain
- comments in detail

Manager can forward this audit information to syslog server.

Forward audit information to SNMP Server

Trellix IPS allows you to configure an SNMP server to which system audit information is sent from the Manager. You can configure more than one SNMP servers where you want to send audit messages. You can configure the SNMP servers for each admin domain separately. The SNMP server configured for a root admin domain can be different from the SNMP server configured for its child domains. When the **Children** and the **Current** checkboxes are selected while configuring an SNMP server for the root admin domain, the SNMP server configured for the child domain will forward notifications to both the parent and child domain SNMP servers. When the **Children** checkbox is not selected in the root admin domain, then the child domain will use only the SNMP server configured for that domain to forward notifications. The IPS Manager displays the SNMP servers that have been configured. The fields in this page are described within the configuration steps that follow.

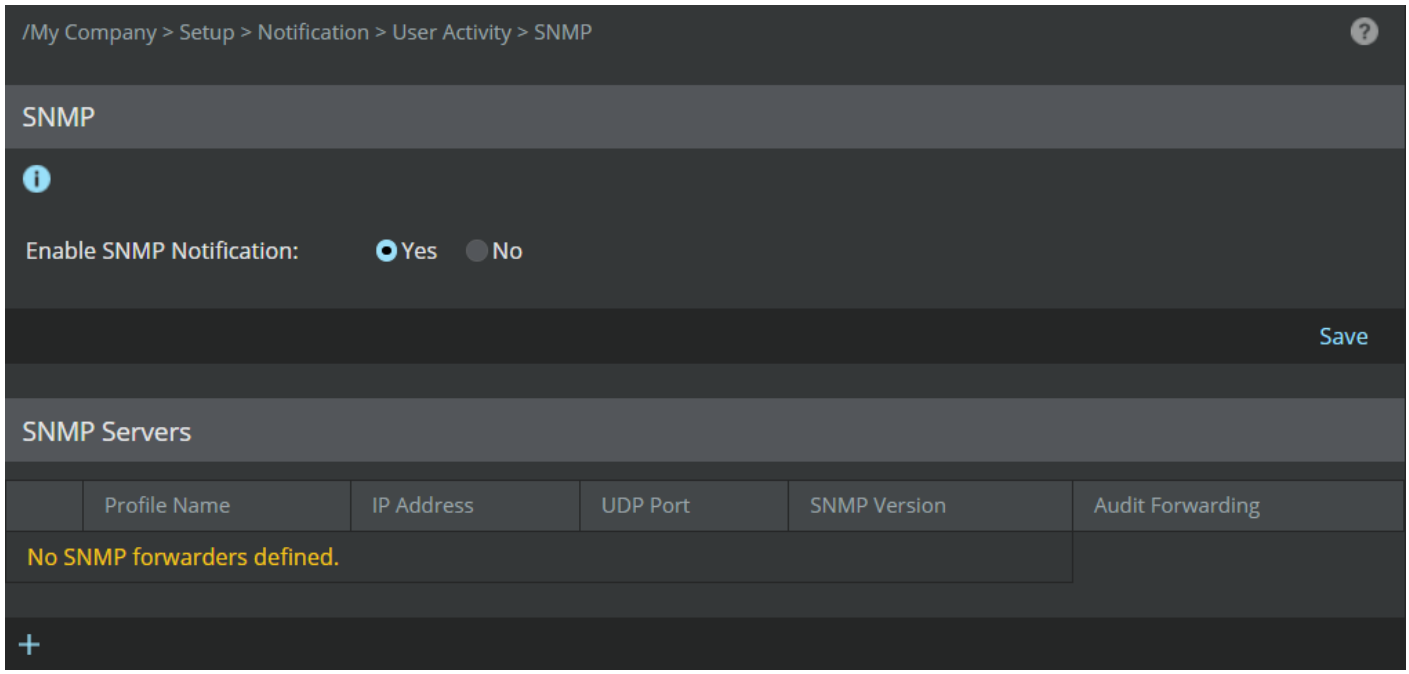
For SNMP forwarding, the root domain and parent domains have the option to include audit information from all corresponding child domains.

To configure an SNMP server from your Manager, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → User Activity → **SNMP**.

   The **SNMP** tab is displayed where **Enable SNMP Notification** option and the configured **SNMP Servers** list is displayed.



2. Select **Yes** against **Enable SNMP Notification** and click **Save**.
3. The columns displayed under the **SNMP Servers** section are as follows:

Field	Description
Profile Name	The profile name from where audit information is sent
IP Address	IP address of the target server
UDP Port	SNMP listening port of the target server
SNMP Version	The version of SNMP server
Audit Forwarding	The logic by which audit information is forwarded to the target server

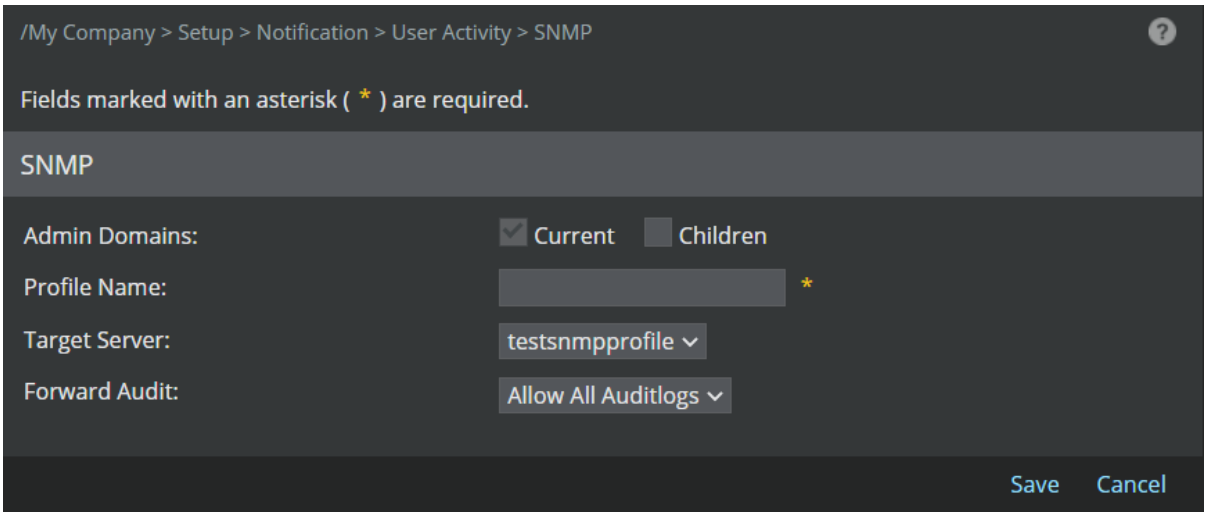
Add an SNMP profile to forward audit information

You can configure the SNMP server on the **SNMP** configuration page.

Steps:

1. Click the + button in the SNMP parent page.

   The **SNMP** configuration page is displayed.



2. The **SNMP** page is displayed. Specify options in the appropriate fields.

Field	Description
Admin Domains	Enables VLAN based reconnaissance
Profile Name	Enter the profile name from where audit information is sent.
Target Server	Choose the target server from the drop-down to which audit information is forwarded.
Forward Audit	Choose the audit logs to be forwarded. The options are **Allow All Auditlogs**, **Failed Only**, **Successful Only**, and **In Progress Only**.

3. Click **Save**.

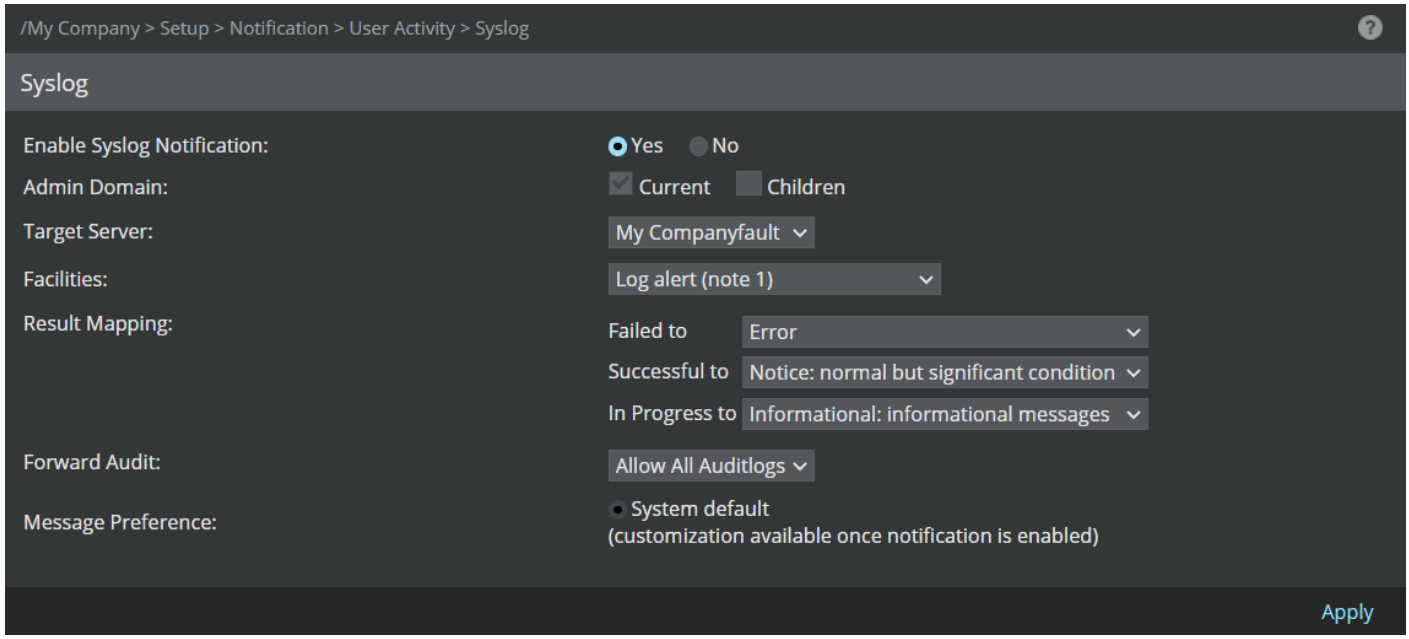
   To edit or delete an SNMP server, select the appropriate server from the list of SNMP servers and use the desired option (or).

Forward audit information to Syslog Server

The **User Activity** option enables the forwarding of Trellix IPS audit information to a syslog server. Syslog forwarding enables you to view the forwarded audit information via a third-party syslog application. For syslog forwarding, the root domain and parent domains have the option to include audit information from all corresponding child domains. To enable syslog forwarding for audit notification, do the following:

1. Select Manager → <Admin Domain Name> → Setup → Notification → User Activity → **Syslog**.

   The **Syslog** page is displayed.



2. Fill in the following fields:

Field	Description
Enable Syslog Notification	**Yes** is enabled; **No** is disabled
Admin Domain	• **Current**— Send notifications for audit information in the current domain. Always enabled for current domain. • **Children**— Include audit information for all child domains of the current domain.
Target Server	Choose the target server from the drop-down to which audit information is forwarded.
Facilities	Standard syslog prioritization value. The choices are as follows: • **Security/authorization (code 4)** • **Security/authorization (code 10)** • **Log audit (note 1)** • **Log alert (note 1)** • **Clock daemon (note 2)** • **Local user 0 (local0)** • **Local user 1 (local1)** • **Local user 2 (local2)** • **Local user 3 (local3)** • **Local user 4 (local4)** • **Local user 5 (local5)** • **Local user 6 (local6)** • **Local user 7 (local7)**

Field	Description
Result Mapping	You can map each audit result (**Failed to**, **Successful to**, and **In Progress to**) to one of the standard syslog severities listed below (default result severities are noted in parentheses): • **Emergency**— System is unusable • **Alert**— Action must be taken immediately • **Critical**— (HIGH) Critical conditions • **Error**— Error conditions • **Warning**— (MEDIUM) Warning conditions • **Notice**— (LOW) Normal but significant condition • **Informational**— (INFORMATIONAL) Informational message • **Debug**— Debug-level messages
Forward Audit	Select the severity of the audit that you want to be forwarded to the syslog server. The options are: • **Allow all Auditlogs** • **Failed only** • **Successful only** • **In Progress only**
Message Preference	Select the preference of the message. The options are: • **System default**— This is available by default • **Customized**— This is available once the notification is enabled

3. Click **Apply**.

> **NOTE**
>
> You must click **Apply** before you will be able to customize the message format sent to your syslog server.

4. Select the **Message Preference** to send as the syslog forwarding message. The choices are:
   - **System Default** — The default message is a quick summary of a fault with three fields for easy recognition: Action, Result, and Time. A default message reads:

     ```
     $IV_AUDIT_ACTION$ $IV_AUDIT_RESULT$ at $IV_AUDIT_TIME$
     ```

   - **Customized** — Create a custom message. To create a custom message, do the following:
     1. Click **Edit** to create a custom message.
     2. Type a message and select (click) the parameters for the desired alert identification format. The following figure displays a custom message. You can type custom text in the **Message** field as well as click one or more of the provided elements below the field box.
     3. Click **Save** when finished to return to the Syslog page. The **Customized** button is automatically selected after you have customized the **Message Preference**.

CAUTION

For syslog information to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each element. Example: $ATTACK_TIME$

Table 8. Syslog variables for audit notification

Syslog variable name	Description
IV_AUDIT_ACTION	The audit action value based on the action ID that was passed.
IV_AUDIT_RESULT	Indicates the stage of auditing (received, succeeded, failed, or ongoing).
IV_AUDIT_TIME	Time stamp of the audit message.
$IV_AUDIT_MESSAGE$	The audit message.
IV_AUDIT_USER	The username for the audit.
$IV_AUDIT_CATEGORY$	The action taken for the audit.
IV_AUDIT_DOMAIN	Name of the domain.
$IV_AUDIT_DETAIL_COMMENT$	Displays committed comments if the audit details are available.
$IV_AUDIT_DETAIL_DELTA$	Displays audit data if the audit details are available.

CAUTION

For syslog message to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each parameter. Example: $ATTACK_TIME$

5. Click **Save**.

Import syslog server certificate

Perform the following steps to import the certificate:

1. Import the CA certificate to the Manager Keystore:
   a. Copy the exported CA certificate CRT file to `<Manager_Install_Dir>\config` folder.

   NOTE

   Replace all `<Manager install directory>` with `%programfiles%\Trellix\IPS Manager\App`.

   b. In the Manager, navigate to Start → **Run** type **cmd**, and press **ENTER**.
   c. Type the following command and press **ENTER** to import the certificate:

   ```
   <Manager install directory>\jre\bin\keytool.exe -import -alias "syslog-server" -keystore <Manager install directory>\config\CustomSecurity\customjssecacerts -file<Manager install directory>\config\CustomSecurity\syslog-server.crt
   ```

d. In the **Password** prompt, type **changeit**, and press **ENTER**.

e. In the **Trust this certificate** prompt, type **yes**.

2. Verify the certificate import:

a. In the Manager, navigate to Start → **Run** type **cmd**, and press **ENTER**.

b. Type the following command to verify:

```
<Manager install directory>\jre\bin\keytool.exe -list -keystore <Manager install directory>\config\CustomSecurity\customjssecacerts
```

3. Restart the Manager service:

a. In the Manager, navigate to Start → **Run** type **cmd**, and press **ENTER**.

b. Click the Trellix IPS icon in the taskbar, and select **Start Manager**.

Customize syslog messages

For customizing syslog message, ensure that **Enable Syslog Notification** is enabled in the page.

1. Go to, Manager → <Admin Domain Name> → Setup → Notification → **Firewall Access Events**.
2. Enter the Server name or IP address.
3. Enter the port number

NOTE

The page displays the message: **Settings successfully saved**.

NOTE

In **Message body**, the default option is selected as **Customized**.

After configuring the syslog forwarder, do the following steps to customize syslog message.

1. Click **Edit**.

   The **Customize Syslog Forwarder Message** page is displayed. By default, the following audit information parameters are included in **Messages**:

   - audit action
   - audit result
   - audit time

   These parameters are displayed as: Audit IV_AUDIT_ACTION IV_AUDIT_RESULT at IV_AUDIT_TIME

2. Type a message and select (click) the parameters that should be included in **Message**. The following are the list parameters that are available in the **Message** field.

Table 9. Syslog variables for audit notification

Syslog variable name	Description
IV_AUDIT_ACTION	The audit action value based on the action ID that was passed.
IV_AUDIT_RESULT	Indicates the stage of auditing (received, succeeded, failed, or ongoing).
IV_AUDIT_TIME	Time stamp of the audit message.
$IV_AUDIT_MESSAGE$	The audit message.
IV_AUDIT_USER	The username for the audit.
$IV_AUDIT_CATEGORY$	The action taken for the audit.
IV_AUDIT_DOMAIN	Name of the domain.
$IV_AUDIT_DETAIL_COMMENT$	Displays committed comments if the audit details are available.
$IV_AUDIT_DETAIL_DELTA$	Displays audit data if the audit details are available.

CAUTION

For syslog message to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each parameter. Example: $ATTACK_TIME$

3. Click **Save** to save the customized syslog message.

Enable log forwarding in Secondary Manager

Users can enable log forwarding in the Secondary Manager within an MDR pair. This can be done by updating the value of **`iv.core.mdr.forwarding`** attribute in the **`ems.properties`** file within the Manager server. The possible values to be updated are **`['A','F','L','C','N'] or [0]`**, where:

A represents Alerts
`F` represents Faults
`L` represents Audit events
`C` represents Access Control Lists
`N` represents NTBA Quarantine events
`0` is the default value set to the attribute, meaning log forwarding is disabled on the Secondary Manager

To edit the **`ems.properties`** file in the Manager, follow these steps:

Windows based Manager server

1. RDP to the Manager server.
2. In the **`ems.properties`** file, locate the following:

   `iv.core.mdr.forwarding=0`

3. Go to **`<Manager_Install_Dir>\config\ems.properties`**

NOTE

The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

4. To enable log forwarding, assign a value associated with the alerts you plan to forward. An example of enabling fault logs is shown below:

   ```
   iv.core.mdr.forwarding=F
   ```

   NOTE

   You can enable single or multiple log types based on your requirement. If you want to enable forwarding multiple log types, enter the values separated by **|**. For example, if you want to enable fault and audit logs, update the attribute as **`iv.core.mdr.forwarding=F|A`**.

   NOTE

   If you later plan to disable log forwarding, assign the value **`0`** or any other positive number to the attribute.

5. Save the changes.
6. Reboot the Manager server.

Linux based Manager server

1. Log in to the Manager shell.
2. Execute the **`edit ems.properties`** command.

   NOTE

   The **`edit`** command will edit the file using **vi-editor**. Trellix recommends you to use **vi_editor** command to perform editing operations on the files.

3. In the **`ems.properties`** file, locate the following:

   ```
   iv.core.mdr.forwarding=0
   ```

4. To enable log forwarding, assign a value associated with the alerts you plan to forward. An example of enabling fault logs is shown below:

   ```
   iv.core.mdr.forwarding=F
   ```

   NOTE

   You can enable single or multiple log types based on your requirement. If you want to enable forwarding multiple log types, enter the values separated by **|**. For example, if you want to enable fault and audit logs, update the attribute as **`iv.core.mdr.forwarding=F|A`**.

   NOTE

   If you later plan to disable log forwarding, assign the value **`0`** or any other positive number to the attribute.

5. Save the changes.
6. Execute the **reboot** command to restart the Manager server.

GUI Access

Configuration of LDAP servers

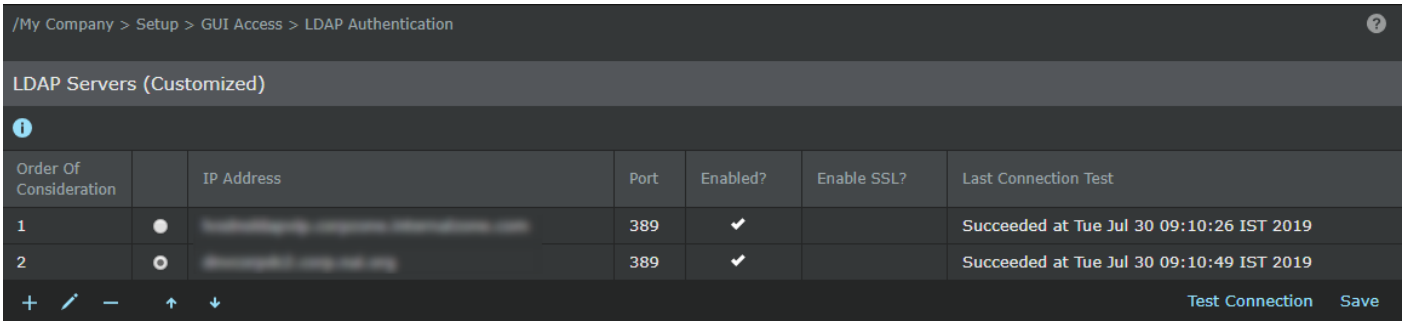
Lightweight Directory Access Protocol (LDAP) is a set of protocols for accessing information directories. LDAP runs on top of TCP/IP, which is necessary for any type of Internet access. LDAP is used to look up encryption certificates, pointers to printers and other services on a network, and provide a single sign-on across many services.

LDAP is appropriate for any kind of directory-like information, where fast lookups and less-frequent updates are the standard.

Using Manager, you can configure a LDAP server at the Manager level. You can configure a maximum of 4 LDAP servers onto Manager. If the first LDAP server is not available for communication due to a network failure, Manager will try to communicate with the second or the third server. If authentication fails at any available servers, the Manager will not communicate with the other available servers.

The LDAP action enables you to use LDAP to authenticate existing users on their LDAP server.

Figure 45. LDAP Server Configuration



You can configure the LDAP server in the Manager/Central Manager from Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.

NOTE

If LDAP servers are configured with Central Manager, and the LDAP servers exist in private networks and Managers exist in public network, the LDAP configuration needs to be customized at the Manager in a way that it reaches the LDAP server through the translated public IP address.

Add an LDAP server

To add the LDAP server configuration in Manager, do the following:

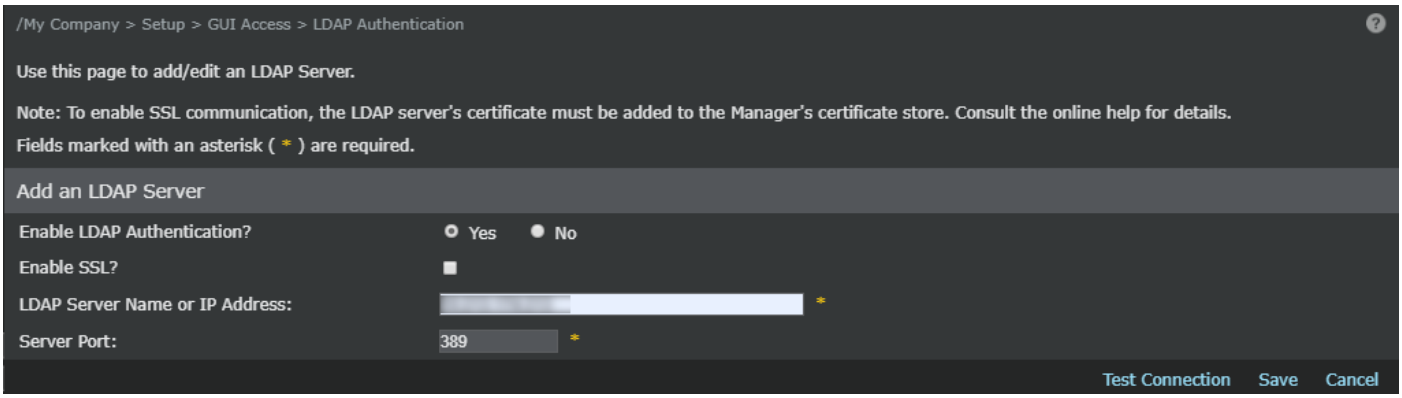
Without SSL enabled

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.

2. Click +.

   The **Add an LDAP Server** page is displayed.

Figure 46. Add an LDAP server



3. Update the following fields to complete adding a new LDAP server:

Option	Definition
Enable LDAP Authentication?	Select **Yes** to continue adding the LDAP server.
Enable SSL?	Not applicable when not using SSL.
LDAP Server Name or IP Address	Type the LDAP server IPv4 or IPv6 address. **⚠ CAUTION** Only use a valid server name, since Trellix IPS does not check to see if the names are valid. A valid server name is the name of the host on which LDAP server is configured.
Server Port	Type the port number between 0 and 65535. Default port is 389.
Test Connection	(Optional) Click to verify that the Manager can connect to the LDAP server.
Save	Click to save the changes.
Cancel	Click to cancel the changes and exit.

With SSL enabled

Prerequisites:

Before enabling SSL, perform the following steps to confirm LDAP over SSL is working in the AD server:

1. In the **Start** menu, select **Run**.
2. Type **`ldp.exe`** and press **ENTER**.

   You see a new window named **Ldp**.
3. Click **Connection**.

   The **Connect** pop-up opens.

4. Enter the Fully Qualified Domain Name (FQDN) of the AD server used to generate the certificate in the **Server** field.

> **NOTE**
>
> If you enable SSL and use a third-party SSL certificate (for example, Verisign, Thawte, etc.), you must provide the same Fully Qualified Domain Name (FQDN) or IP address that is provided in the SSL certificate.

5. Select **SSL**. Confirm that the **Port** is 636, and then click **OK**.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.
2. Click +.

   The **Add an LDAP Server** page is displayed.
3. Update the following fields to complete adding a new LDAP server:

Option	Definition
Enable LDAP Authentication?	Select **Yes** to continue adding the LDAP server.
Enable SSL?	Select the checkbox to enable SSL encryption. **TIP** You have to import the LDAP server's SSL certificate into the Manager keystore for authentication. To import the SSL certificate, see Import certificate (page 211).
LDAP Server Name or IP Address	Type the LDAP server IPv4 or IPv6 address. **CAUTION** Only use a valid server name, since Trellix IPS does not check to see if the names are valid. A valid server name is the name of the host on which LDAP server is configured.
Server Port	Type the port number between 0 and 65535. Default port is 636.
Test Connection	(Optional) Click to verify that the Manager can connect to the LDAP server.
Save	Click to save the changes.
Cancel	Click to cancel the changes and exit.

Import certificate

Perform the following steps to import the certificate.

1. Import the CA certificate to the Manager Keystore:
   a. Copy the exported CA certificate CRT file to `<Manager_Install_Dir>\config` folder.

> **NOTE**
>
> Replace all `<Manager install directory>` with `%programfiles%\Trellix\IPS Manager\App`.

b. In the Manager, navigate to Start → **Run** type **cmd**, and press **ENTER**.

c. Type the following command and press **ENTER** import the certificate:

<Manager_Install_Dir>\jre\bin\keytool.exe -import -alias "LDAP Certificate" -keystore <Manager_Install_Dir>\config\CustomSecurity\customjssecacerts -file<Manager_Install_Dir>\config\CustomSecurity\<file name>.crt

d. In the **Password** prompt, type **changeit**, and press **ENTER**.

e. In the **Trust this certificate** prompt, type **yes**.

2. Verify the certificate import:

a. In the Manager, navigate to Start → **Run** type **cmd**, and press **ENTER**.

b. Type the following to verify:

<Manager_Install_Dir>\jre\bin\keytool.exe -list -keystore <Manager_Install_Dir>\config\CustomSecurity\customjssecacerts

3. Restart the Manager service:

a. In the Manager, navigate to Start → **Run** type **cmd**, and press **ENTER**.

b. Click the Trellix IPS icon in the taskbar, and select **Start Manager**.

Edit an LDAP server

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.

> **NOTE**
>
> To edit an LDAP server in the Central Manager, select Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.

2. Select a server and click .

You can either enable or disable the LDAP server. You can also change the Server Port value and enable or disable SSL.

3. Follow the steps as in Add an LDAP server (page 209).
4. Click **Save**.

Delete an LDAP server

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.

NOTE

To delete an LDAP server in the Central Manager, select Manager → Setup → GUI Access → **LDAP Authentication**.

2. Select a server and click −.
3. Click **OK** in the confirmation page to delete the LDAP server.

   The LDAP server is deleted.

Test connection status

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **LDAP Authentication**.

NOTE

To test the connection status with the LDAP server and Central Manager, select Manager → Setup → GUI Access → **LDAP Authentication**.

2. Select a server and click **Test Connection**.

   Verify that Manager can connect to the LDAP server.

Configuration of RADIUS server in the Manager

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol for applications such as network access.

While connecting to the internet using a modem, you are required to enter a username and password. The information is passed through a Network Access Device (NAD) device, and then to a RADIUS server over the RADIUS protocol. The RADIUS server checks if the information is correct using authentication schemes like PAP, CHAP, and EAP-MD5. If accepted, the server will authorize the access.

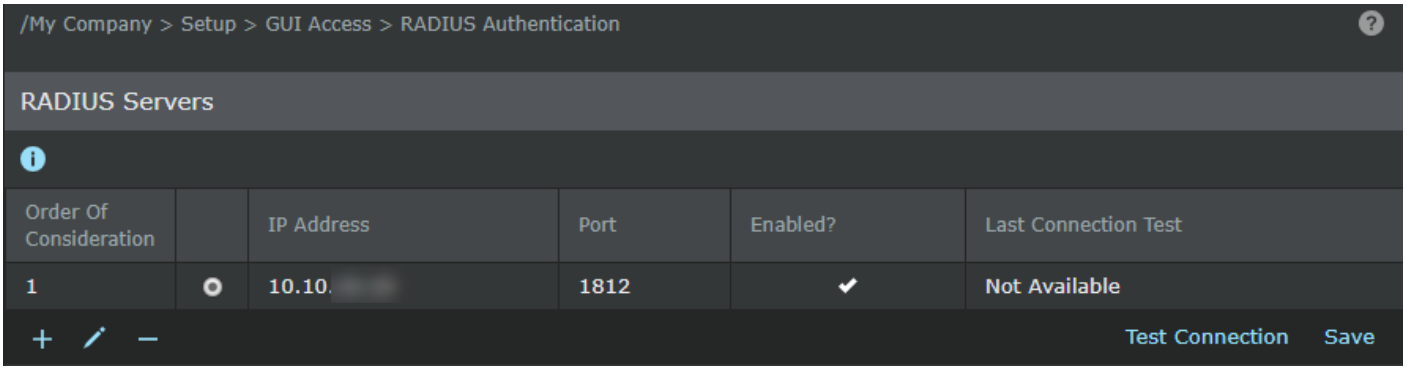
Using Manager, you can configure a RADIUS server at the Manager level. You can configure a maximum of 4 RADIUS servers onto Manager. If the first RADIUS server is not available for communication, due to a network failure, Manager will try to communicate with the second or the third server. If authentication fails at any available servers, then Manager will not communicate with the other available servers.

The RADIUS action enables you to use RADIUS to authenticate existing users on their RADIUS server. Trellix IPS supports the PAP, CHAP, and EAP-MD5 schemes of RADIUS authentication.

NOTE

When EAP-MD5 scheme is selected, the Manager internally authenticates requests that use MS-CHAPv2.

Figure 47. RADIUS Server Configuration



You can configure the RADIUS authentication in the Manager from Manager → <Admin Domain Name> → Setup → GUI Access → **RADIUS Authentication**.

NOTE

For the Central Manager, you can configure RADIUS authentication from Manager → Setup → GUI Access → **RADIUS Authentication**.

Add a RADIUS server

To add the RADIUS server configuration in Manager, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **RADIUS Authentication**.

   NOTE

   To add a RADIUS server in the Central Manager, select Manager → Setup → GUI Access → **RADIUS Authentication**.

2. Click +.

   The **Add a RADIUS Server** page is displayed.

3. Select **Yes** next to **Enable RADIUS Authentication?**.

4. Type the **RADIUS Server Name or IP Address** (IPv4 or IPv6 address).

   CAUTION

   Only use a valid server name, since Trellix IPS does not check to see if the names are valid. A valid server name is the name of the host on which RADIUS server is configured.

   Type the RADIUS **Server Port**. The port number should be between 0 and 65535. (default =1812).

5. Type a **Shared Secret Key** that is required on both the Manager and the RADIUS server. The Shared Secret key is same as entered in the RADIUS server during configuration.

6. Select the **Connection Time Out** (in milliseconds).

   This time determines how long the Manager should wait for authentication. Three attempts are made to connect before timeout occurs, so the value you enter is how long Trellix IPS waits between attempts before timeout (default =6000 milliseconds).

7. (Optional) Click **Test Connection** to verify that the Manager can connect to the RADIUS server.

   NOTE

   If Manager Disaster Recovery (MDR) is enabled, both the Primary and Secondary Manager IP addresses must be registered in the RADIUS server.

8. Click **Save** to save your changes.

   NOTE

   If RADIUS servers are configured with Central Manager, and the RADIUS servers exist in private networks and Managers exist in public network, the RADIUS configuration needs to be customized at Manager in a way that it reaches the RADIUS Server through translated public IP address.

Edit a RADIUS server

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **RADIUS Authentication**.

   NOTE

   To edit RADIUS server settings in the Central Manager, select Manager → Setup → GUI Access → **RADIUS Authentication**.

2. Select a server and click  .

   You can either enable or disable the RADIUS server. You can also change the Server Port or the Connection Time Out value.

3. Follow the steps as in Add a RADIUS server (page 214).

4. Click **Save**.

Delete a RADIUS server

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **RADIUS Authentication**.

   NOTE

   To delete RADIUS server settings in the Central Manager, select Manager → Setup → GUI Access → **RADIUS Authentication**.

2. Select a server and click −.
3. Click **OK** in the confirmation page to delete the RADIUS server.

   The RADIUS server is deleted.

Test connection status

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **RADIUS Authentication**.

   > **NOTE**
   >
   > To test the connection status of RADIUS server settings in the Central Manager, select Manager → Setup → GUI Access → **RADIUS Authentication**.

2. Select a server and click **Test Connection**.

   Verify that the Manager can connect to the RADIUS server.

Authentication of access to the Manager using CAC/PIV

> **NOTE**
>
> This section is not applicable for Common Criteria evaluated configuration.

Common Access Card (CAC) and Personal Identification Verification (PIV) are smart cards that are used for general identification as well as authentication of user access to secure networks. CAC/PIV holds a unique digital certificate and user information, such as photograph, personal identification number (PIN), and signature, to identify each user. Trellix IPS provides an option for authentication of users to log onto the Manager based on their smart card verification.

Authentication to the Manager using CAC/PIV requires a smart card reader connected to the Manager client workstation. The administrator inserts the CAC/PIV into the smart card reader and opens the Manager UI through the web browser. The Manager sends an SSL certificate to the client and requests the user's certificate from the browser. The browser validates if the Manager's certificate is signed by a trusted Certificate Authority. The browser then selects the user's certificate by prompting the user if required. The browser retrieves the selected certificate from the smart card which triggers the CAC/PIV interface software (called middleware) to request the user PIN associated with the smart card. The user must correctly enter the PIN to unlock the smart card.

The Manager validates the following attributes of the user's certificate:

- If the certificate is signed by a trusted Certificate Authority (CA)
- If the certificate is valid and has not been revoked
- When the certificate was last validated

The Manager extracts the common name from the user's certificate and checks for a matching administrator account in the Manager with that common name. If the match is successful, a secure session is established and the user is logged into the Manager.

To validate the user's certificate, the trust chain is validated by two CA certificates. The first validation is that the client's certificate is signed by the intermediary CA. Then the intermediary CA certificate is validated by verifying if it was signed by the root CA which is trusted. The root CA is a self-signed CA that is used to sign the intermediary CA certificates.

At a high level, authenticating user access to the Manager through CAC/PIV can be brought about by a 5-step process:

- Obtain the CA certificates
- Import the CA certificates
- Set up CAC users in the Manager
- Enable the CAC authentication
- Log on to the Manager using the CAC/PIV authentication

Obtain the CA certificates

Obtain the intermediate and root certificates in the certificate chain of your CAC cards. To obtain the CAC certificates, perform the following steps:

Steps:

1. Plugin the CAC card reader in the Windows client machine which is used to access the Manager. The drivers for the smartcard reader are automatically installed and detected. If the drivers are not installed automatically, you have to manually install the drivers for the smartcard reader.

   To troubleshoot problems with CAC card reader installation, see Installing and updating the CAC reader driver/Firmware update/Check services to make sure Smart Card is running.
2. Once the CAC card reader is active, plugin the CAC card.
3. In the Internet Explorer browser, navigate to Internet Options → Content → Certificates → **Personal**.

   The certificates of the card are available in the **Personal** tab. There are three certificates corresponding to the card's user, two for email and one for ID.
4. Select the certificate for ID and click **View**.

   The **Certificate** window with the details of the certificate opens.
5. The **Certification path** tab lists the chain of the certificate.
6. Select the intermediate certificate which is the issuer of the leaf and click **View Certificate** to view the intermediate certificate.
7. Go to the **Details** tab in the **Certificate** window and click **Copy to File**. This allows you to export the certificate. Choose any of the .cer formats and save it to a file. Trellix recommends you to select **Base-64 encoded** option as it is compatible with the Manager. Create a new folder for the certificates as "Saved intermediate and root certificates".
8. Repeat the process for the root certificate and save that to a file as well.

   NOTE

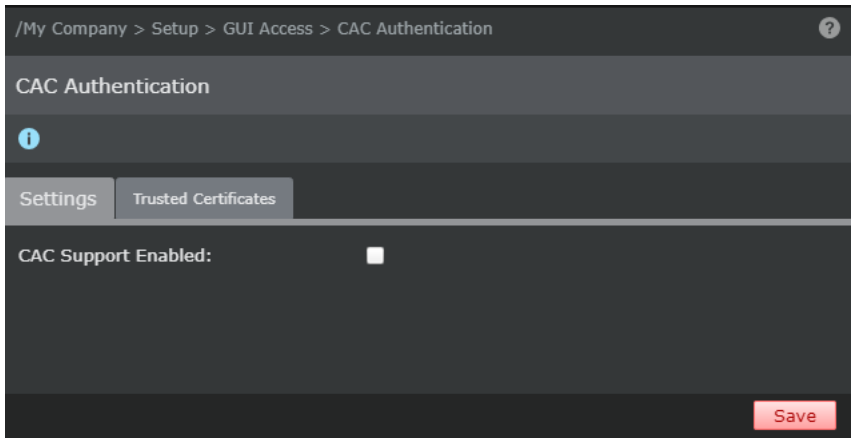
   The root and intermediate certificates can be obtained simultaneously by obtaining the certificate chain.
9. Convert the certificates to .pem format and save them in a separate file.

Import the CA certificates

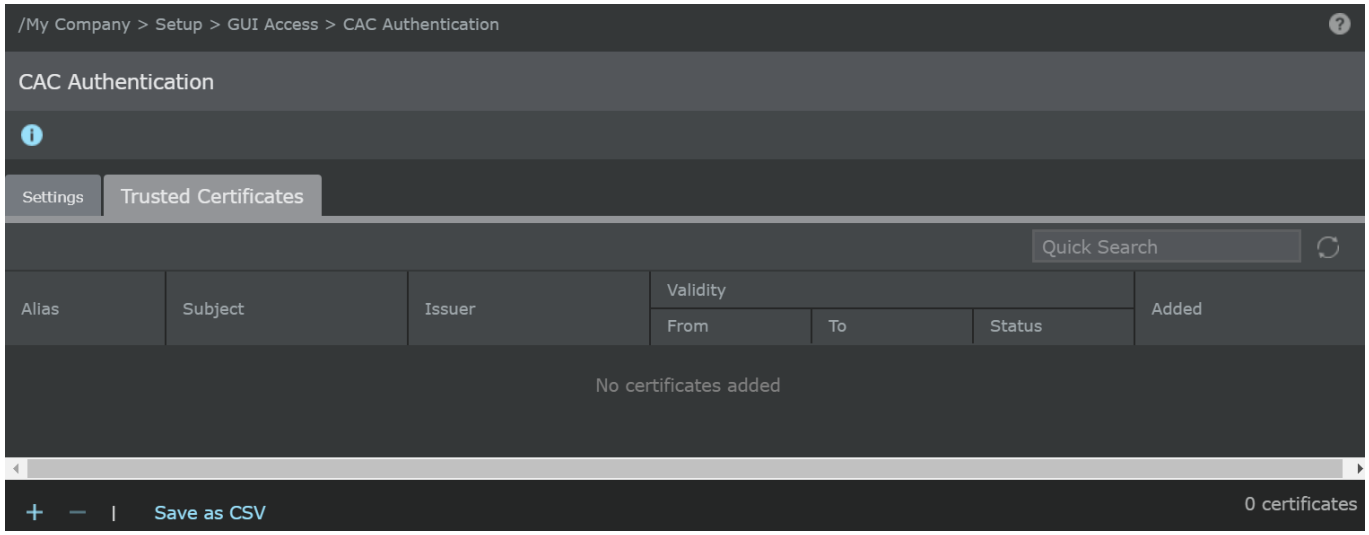
Import the intermediate and root certificates in the certificate chain of your CAC cards to the Manager. To import the CAC certificates, perform the following steps:

1. Log in to the Manager GUI.
2. Go to, Manager → <Admin Domain Name > → Setup → GUI Access → **CAC Authentication**.

   The **CAC Authentication** page opens.



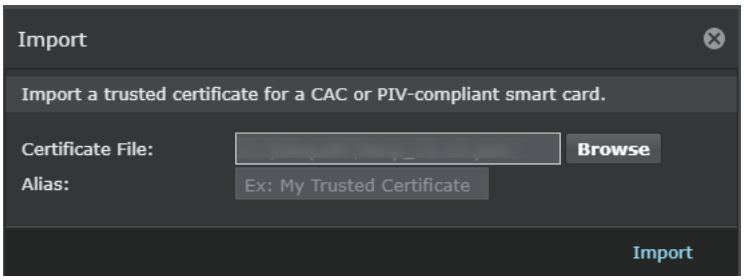
3. In the **Trusted Certificates** tab, click +.



4. In the **Import** dialogue box, click **Browse**.
5. Browse to the directory that contains the certificate chain and click **Open**.

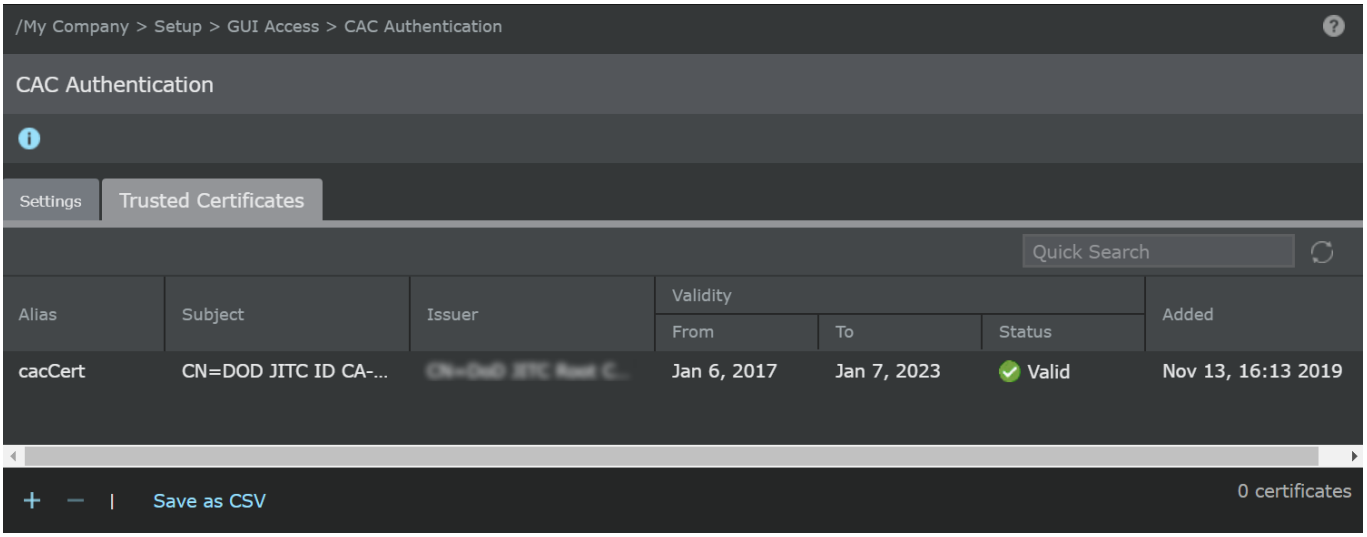
> **NOTE**
>
> The CAC certificate should be in .pem format.

6. Provide an **Alias** for the certificate and click **Import**.



7. Click .

   The Manager imports the certificate to its keystore and the details of the certificate are displayed on the **Trusted Certificates** tab.



> **NOTE**
>
> Click **Save as CSV** to export the trusted certificates details as .csv file.

Set up CAC users in the Manager

Steps:

1. Connect the smart card reader to your Manager client through a USB port.

   The smart card reader can be connected to a Manager server, if the server doubles up as a Manager client.

   - Refer to the card reader manufacturer's recommendations for the necessary device drivers to be installed.
   - Install the **ActivID ActivClient** CAC software on the Manager client.

> **NOTE**
>
> Trellix currently supports integration with smart card reader model SCR3310 from TxSystems. Other smart card readers will also work but have not been tested by Trellix.

2. Insert a card into the card reader.
3. Open the ActivClient software → Smart Card Info → **User Name**.

   User name is available in the **CN** field under **Subject** in the **Certificate** details window. The user name is a combination of alphanumeric characters and a few special characters like "." or spaces. For example, "BROWN.JOHN.MR.0123456789"
4. Log onto the Manager and create a user with the exact same name as provided in the CN field, that is "BROWN.JOHN.MR .0123456789".

> **NOTE**
>
> If you have RADIUS/LDAP servers in your setup for external authentication, an additional field **Authentication Type** will be displayed in the Manager with the following choices: Local, LDAP, RADIUS:PAP, and RADIUS:CHAP.

Enable the CAC authentication

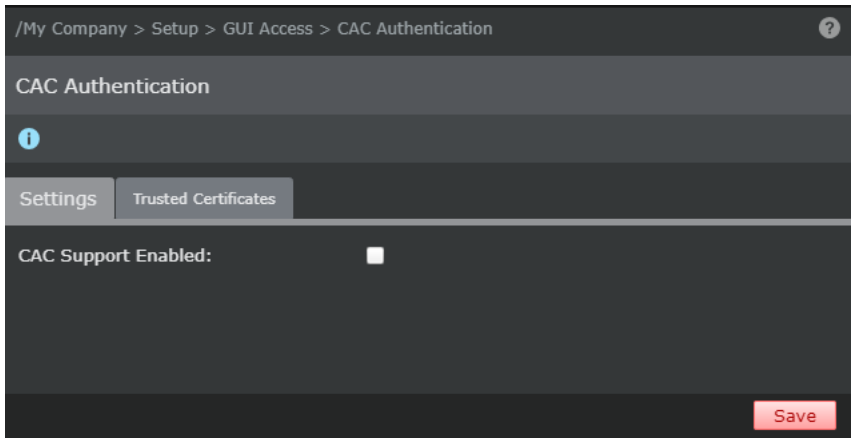
The CAC authentication feature is disabled by default. It is mandatory to set up the CAC user accounts and import the CAC certificates to the Manager, before enabling it.

To enable CAC, do the following:

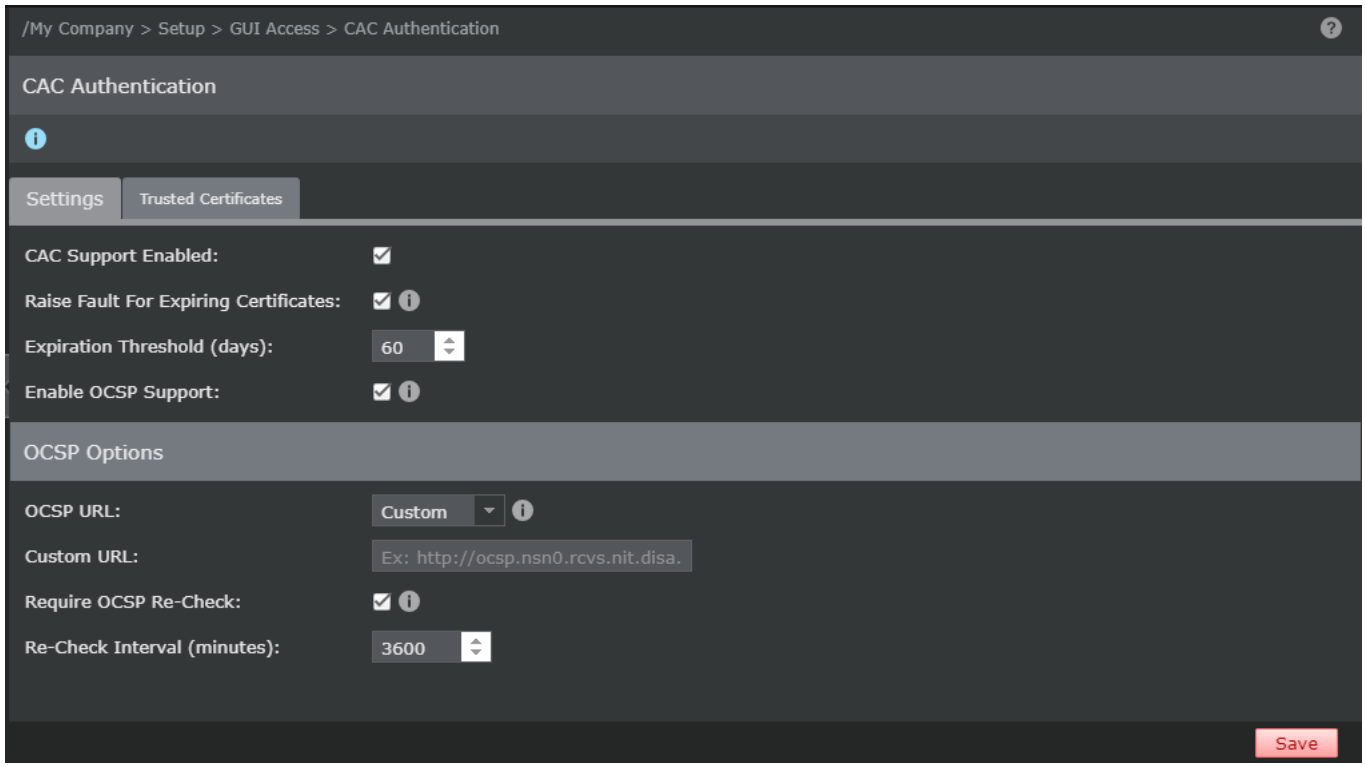
Steps:

1. Log in to the Manager GUI.
2. Go to, Manager → <Admin Domain Name> → Setup → GUI Access → **CAC Authentication**.

   The **CAC Authentication** page opens.



3. In the **Settings** tab, configure the CAC Authentication as needed.



The table below describes the fields available for configuration:

Field	Description
CAC Support Enabled	Select the checkbox to enable CAC Authentication. By default, the CAC Authentication is disabled.
Raise Fault for Expiring Certificates	Select the checkbox to configure the Manager to generate faults when a trusted certificate is about to expire.
Expiration Threshold (days)	Number of days for the trusted certificate expiration when a fault is generated in the Manager. **NOTE** The **Expiration Threshold (days)** can be within the range of 30 to 60 days only. **NOTE** The **Expiration Threshold (days)** can be configured only when the **Raise Fault for Expiring Certificate** option is enabled.
Enable OCSP Support	Select the checkbox to enable OCSP Support. By default, the OCSP Support is disabled.
OCSP Options	

Field	Description
OCSP URL	Select **Default** to use the OCSP URL defined in the trusted certificate or **Custom** to configure a unified OCSP URL for all trusted certificates in the Manager.
Custom URL	Specify the OCSP URL for authenticating the trusted certificates. **NOTE** The **Custom URL** field is available only when you have the **OCSP URL** option set to **Custom**.
Require OCSP Re-Check	Select **Yes** to verify the authenticity of the trusted certificate after a definite interval.
Re-Check Interval (minutes)	Specify the duratin in minutes after which the authenticity of the trusted certificate is re-checked. **NOTE** The **Re-Check Interval (minutes)** can be within the range of 30 to 1440 minutes only. **NOTE** The **Re-Check Interval (minutes)** can be configured only when the **Require OCSP Re-Check** option is enabled.

4. Click **Save**.
5. Log in to the Manager shell.
6. Stop the Manager service using the **`manager stop`** command.
7. Restart the Manager service using the **`manager start`** command.

Log on to the Manager using the CAC/PIV authentication

Steps:

1. Insert a card into the card reader.
2. Start a fresh browser session for the Manager.

   You are prompted to choose the CAC/PIV certificate.
3. Select the certificate.

   You are prompted to enter the PIN.
4. Enter the PIN.

   A maximum of 3 attempts is allowed while entering PIN, following which, the user will be locked out. It is impossible to unlock a CAC/PIV card that is locked and the card has to be replaced.

   If the user name, certificate, and PIN match, you are directly given access to the Manager Home Page.

Delete a trusted certificate from the Manager

You can delete a previously added trusted certificate from the Manager.

Steps:

1. Log in to the Manager.
2. Go to Manager → <Admin Domain Name > → GUI Access → **CAC Authentication**.

   The **CAC Authentication** page opens.
3. Click **Trusted Certificates**.
4. Select the certificate from the **Trusted Certificates** section.
5. Click −.

   The **Confirmation** dialog box opens.
6. Click **OK** to confirm deletion.

Troubleshooting tips

- If the card is not inserted in the card reader, the Manager will not be accessible in this setup.
- When authenticating users through CAC, you do not have to enter your Manager user name and password while logging on.
- If you have imported a CA certificate to the Trusted Certificates in the Manager, you can't reimport the same certificate to the Manager.
- You are loading a CA certificate to the Manager, and yet you are unable to import it, then verify the validity of the certificate and make sure it is not expired.
- You have imported the relevant CA into the Manager, and yet you are unable to view the Manager Login page, then check whether a firewall is blocking your access to destination port 443 on the Manager server.
- If you are able to view the Manager Login page but are unable to log onto the Manager, it means that the user name on the CAC card does not match the user name in the Manager database. To remedy the problem, verify that the user name on the CAC card exactly matches the Manager user name.

Authorization for Manager access

By default, any host can access Manager/Central Manager from any IP address. You can allow access to specific hosts by enabling **GUI Access** from Manager → <Admin Domain Name> → **Setup** menu and defining the list of authorized hosts/networks.

> **NOTE**
>
> You need to have at least one authorized host to enable GUI Access.

All attempts by authorized and unauthorized hosts to access your Manager are logged in the user activity log, which you can access from the **View User Activity Audit Log** link in the page.

Enable GUI Access

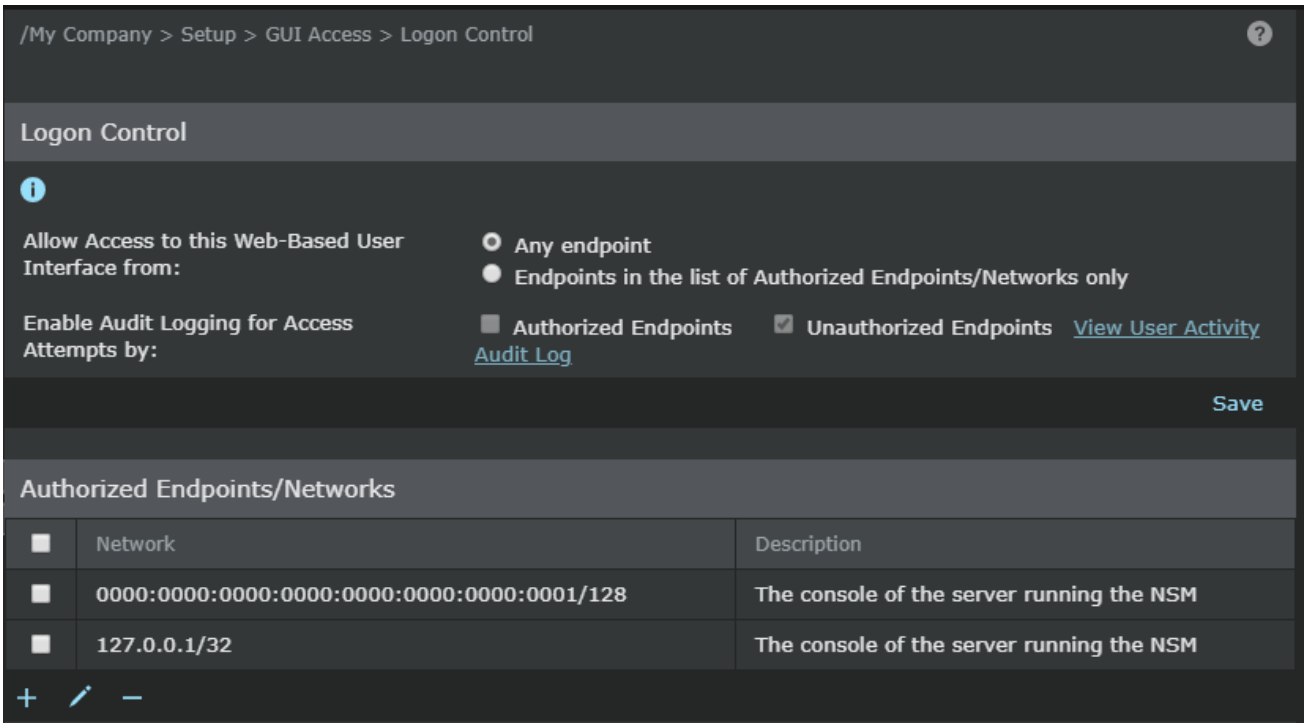
In the Manager, to configure authorized hosts:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **Logon Control**.

> **NOTE**
>
> In the Central Manager, select Manager → Setup → GUI Access → **Logon Control**. The fields displayed are similar to that in Manager, explained below.

Figure 48. GUI Access Control Configuration



2. Select **Any endpoint** at **Allow Access to this Web-Based User Interface from**. (default is Any endpoint)

   The **Enable Audit Logging for Access Attempts by** option is highlighted. Select **Authorized Endpoints** or **Unauthorized Endpoints** and click on **View User Activity Audit Log** link to see audit log messages.

3. Click **Save**.

   You can now define the list of hosts to access your Manager. You can do this by adding, editing and deleting CIDR networks.

Add a network from Logon Control

You can enter IPv4 or IPv6 address in the **Logon Control** page in Manager.

To add a network in the **Logon Control** page, do the following:

Steps:

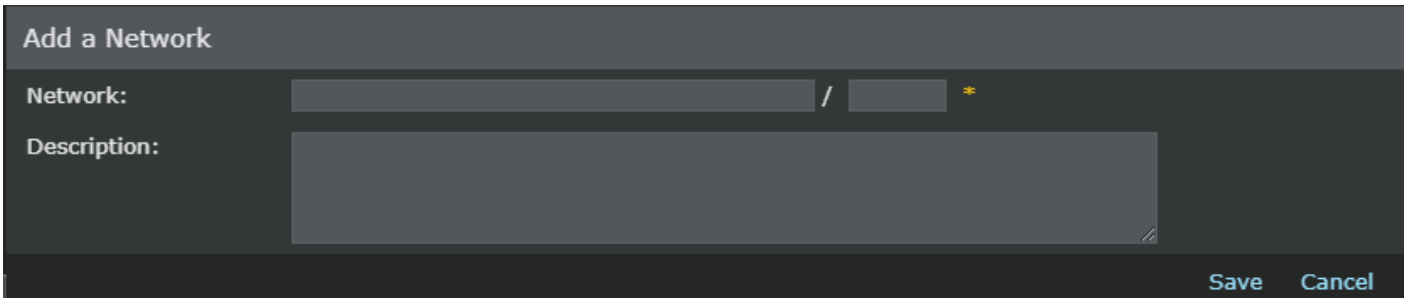
1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **Logon Control**.

> **NOTE**
>
> In the Central Manager, select Central Manager → Setup → GUI Access → **Logon Control**. The fields displayed are similar to that in Manager, explained below.

2. Click +.

   The **Add a Network** page is displayed.

Figure 49. Add a Network Dialog



3. In **Network**, enter the IP address (IPv4 or IPv6) and the prefix length.

   Enter a **Description** (optional).

4. Click **Save**.

Edit a CIDR network

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **Logon Control**.

> **NOTE**
>
> In the Central Manager, select Manager → Setup → GUI Access → **Logon Control**. The fields displayed are similar to that in Manager, explained below.

2. Select a CIDR network and click ✎.

   The **Edit the Network** page is displayed.

3. Edit the changes and click **Save**.

Delete a CIDR network

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **Logon Control**.

NOTE

In the Central Manager, select Manager → Setup → GUI Access → **Logon Control**. The fields displayed are similar to that in Manager, explained below.

2. Select a CIDR network and click −.
3. Click **OK** in the confirmation page to delete CIDR network.

   The CIDR network is deleted.

User activity log error messages

Fault	Fault Description	Category
Authorized end-points	User "<user name>" with login id "<login ID>" successfully logged into the Manager from "<IP address>". Login URI: <login URI>, URI referrer: <referrer>, protocol: <protocol>.	User
Unauthorized end-points	User "<user name>" failed to log into Manager from "<IP address>". Login URI: <login URI>, URI referrer: <referrer>, protocol: <protocol>.	User

Add a Manager logon banner

The logon banner option enables you to upload your company logo (or any other relevant image) and customized text on the Manager logon page.

The size of the banner image must be 100x35 pixels and only .jpeg and .png files are supported. Banner image of different sizes will be resized to 100x35.

To upload a logon banner, do the following:

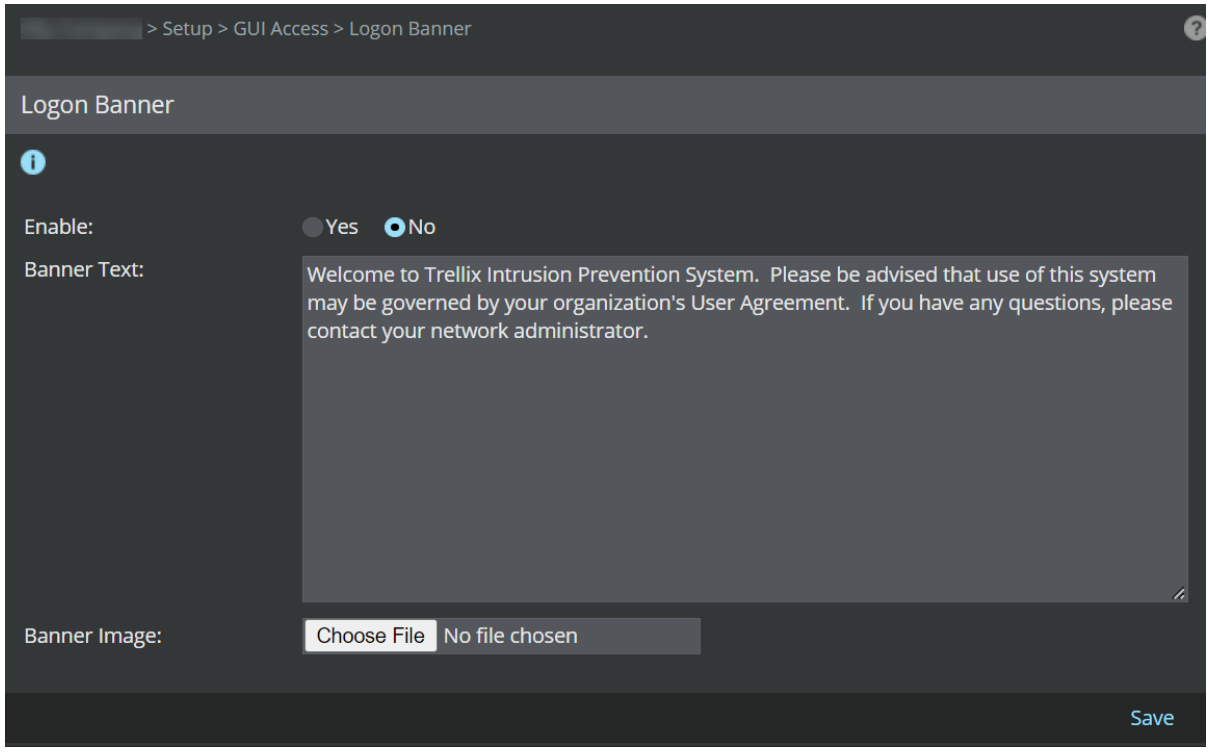
Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **Logon Banner**

NOTE

In the Central Manager, select Manager → Setup → GUI Access → **Logon Banner**. The fields displayed are similar to that in Manager, explained below.

Figure 50. Logon Banner



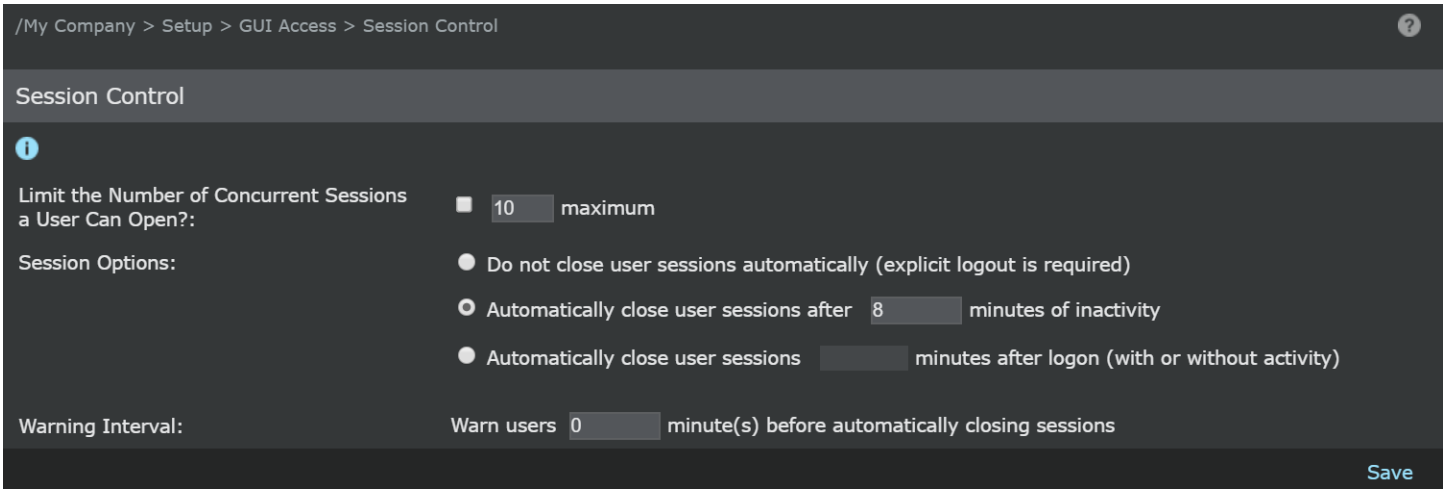
2. Provide the following information:
   - **Enable** — Select **Yes** to allow the logon banner to be displayed and select **No** not to display the logon banner.
   - **Banner Text** — Type the required text to be displayed.
   - **Banner Image** — Browse to select the banner image that you want to upload.
   - **Current banner Image** — Specifies the current banner image.
3. Click **Save** to save the changes.

Configure session control settings

The Session Control provides the option to automatically close Manager/Central Manager sessions.

Only events constitute for a key stroke activity. For example, Session timeout is applicable even when there is an activity in the **Add a User** page. Only when you click **Submit**, it is considered as an activity. Accessing the Port Settings and IPS Policies are considered as events.

Figure 51. Inactivity timeout duration and message setup



Perform the following steps to set this option:

- Select Manager → <Admin Domain Name> → Setup → GUI Access → **Session Control**.

> **NOTE**
>
> In the Central Manager, select Manager → Setup → GUI Access → **Session Control**. The fields displayed are similar to that in Manager, explained below.

- Set the following options:

Field	Description
Limit the Number of Concurrent Sessions a User Can Open?	Select this option and set the maximum value to 1.
Session Options	The session control options help you to configure your security requirements for monitoring user activity on currently open Manager sessions. User Activity is defined as the mouse clicks or keyboard usage not in use for X minutes on the Manager. Select **Automatically close user sessions after X minutes of inactivity**. Set the time to 15 minutes.

Field	Description
Warning Interval	This option appears only if you have opted to automatically close a user session after a set period. Set a value between 1-43,200 minutes as per your site's policy. The Administrator is warned before the session is timed out due to inactivity or time limit. **NOTE** The warning interval value must be lesser than the set timeout activity.

Customize inactivity timeout via the Manager shell

Perform the following steps to configure the inactivity timeout for a local session via Manager shell:

1. In the shell, open the file named **`profile`** located in **`etc`** directory using any text editor.
2. Add the following lines at the end of the file:

   ```
   TMOUT = < inactivity time period (in seconds) >
   readyonly TMOUT
   export TMOUT
   ```

3. Save the configuration and re-login.

Configure password complexity settings

The **Password Control** page allows administrators to set password requirements such as **Password Strength**, **Password History**, **Password Expiration**, and **Account Lockout**.

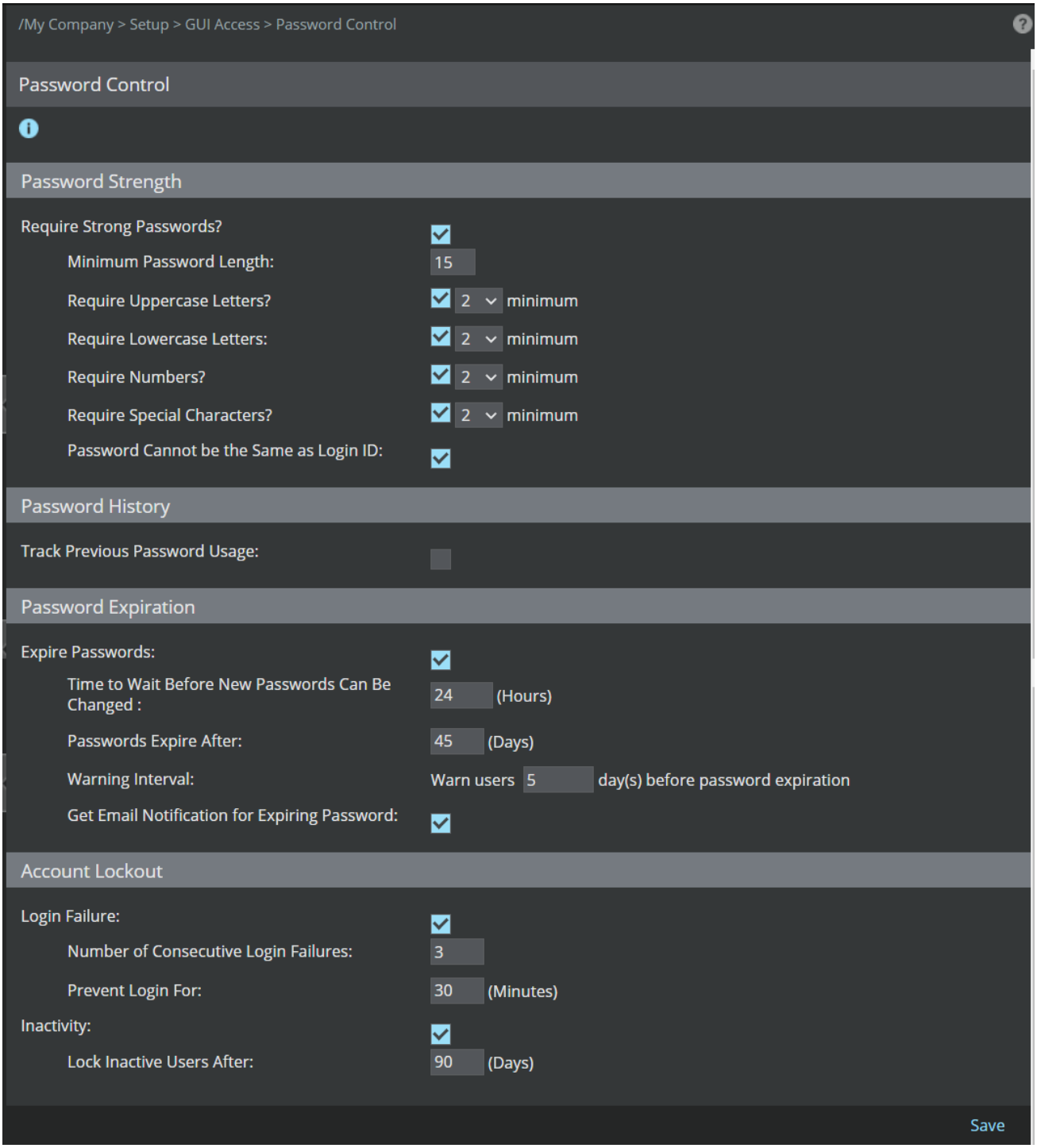
Select Manager → <Admin Domain Name> → Setup → GUI Access → **Session Control**.

NOTE

In the Central Manager, select Manager → Setup → GUI Access → **Password Control**. The fields displayed are similar to that in Manager, explained below.

The **Password Control** page appears.

Figure 52. Password Control page



NOTE

The local administrator cannot be locked out to ensure that administrative access is always maintained.

Password strength

Ensure the **Require Strong Passwords?** check box is selected. To strengthen your password use the fields in this section to set parameters.

Field	Description
Minimum Password Length	Set the minimum password length to 15 characters.
Require Uppercase Letters	Select this option and set the minimum value to 2.
Require Lowercase Letters	Select this option and set the minimum value to 2.
Require Numbers	Select this option and set the minimum value to 2.
Require Special Characters	Select this option and set the minimum value to 2.
Password Cannot be the Same as Login ID	Select this option to ensure that the user does not enter the same set of characters as **Login ID** and **Password**. For example: If the **Login ID** is admin1, the Manager must disallow the user from entering the password as 'admin1'.

Password History

Ensure the **Track Previous Password Usage:** check box is selected. Use the fields in this section to ensure that the previously set passwords are not repeatedly used:

Field	Description
Number of Characters that must be Changed	Set the number of characters that must be changed between 1 and 8.
Number of Previous Passwords to Track	Set the number of passwords to track to 10.

Password Expiration

If you try to log on after your password has expired, the following message is displayed:

Login failed: Account has been locked due to password expiration, contact your Administrator.

Ensure the **Expire Passwords:** check box is selected. Use the fields in this section to ensure that the passwords are changed at regular intervals:

Field	Description
Time to Wait Before New Passwords Can Be Changed	Set the time to wait before new passwords can be changed between 0 and 72 hours.
Passwords Expire After	Set the passwords expiry period between 1 and 180 days.

Field	Description
Warning Interval	Set the warning interval as per your requirement. **NOTE** The warning interval you set should be at least 1 day less than the password expiry period. For example, if the password is expiring after 5 days, the warning interval should be set between 1 and 4 days. That way, if you are setting the password to expire in 1 day, you should set the warning interval to 0 days.
Get Email Notification for Expiring Password	Select this check box to enable email notifications for expiring passwords. The Manager sends these email notifications to the users when their passwords are about to expire. These emails are sent every day until the last day of expiry. For example, if you set the warning interval as 4 days, the user receives 1 email everyday for 4 days before the password expires. **NOTE** The emails are sent to the user's email ID which was specified during user creation. **NOTE** This feature works only when the E-mail Server is configured. **NOTE** • In case of a Central Manager setup that manages multiple Managers, the Central Manager sends the email notifications to the users added in it. • In case of a Manager Disaster Recovery (MDR) setup that involves a primary and a secondary Manager, users will receive email notifications from only one of the Managers in the MDR pair.

Set up account lockout parameters

Ensure the **Login Failure** and/or **Inactivity** check boxes are selected. Use the fields in this section to set the parameters based on which a user account would be locked:

Field	Description
Number of Consecutive Login Failures	Set the maximum number of unsuccessful login attempts to 3.
Prevent Login For	Set the duration of lock out field between 1 and 1440 minutes.

Field	Description
Lock Inactive Users After	Set the number of days to lock the inactive users between 1 and 180 days. **NOTE** Admin user can never be marked as inactive.

After selecting the required parameters, any new user created henceforth will comply with the password policy enabled. The password policy can be enabled only at the root admin domain level.

NOTE

The local administrator cannot be locked out to ensure that administrative access is always maintained.

Customize the unlock time and maximum authentication attempts

To customize the amount of time to unlock a locked out account in the Manager, go to the Manager shell and modify the unlock time in **`unlock_time=<value in seconds>`** within the files **`/etc/pam.d/system-auth`** and **`/etc/pam.d/password-auth`**.

To customize the maximum number of authentication attempts permitted per connection in the Sensor, go to the Sensor shell and modify the value in **`MaxAuthTries=<value>`** within the **`/etc/ssh/sshd_config`** file.

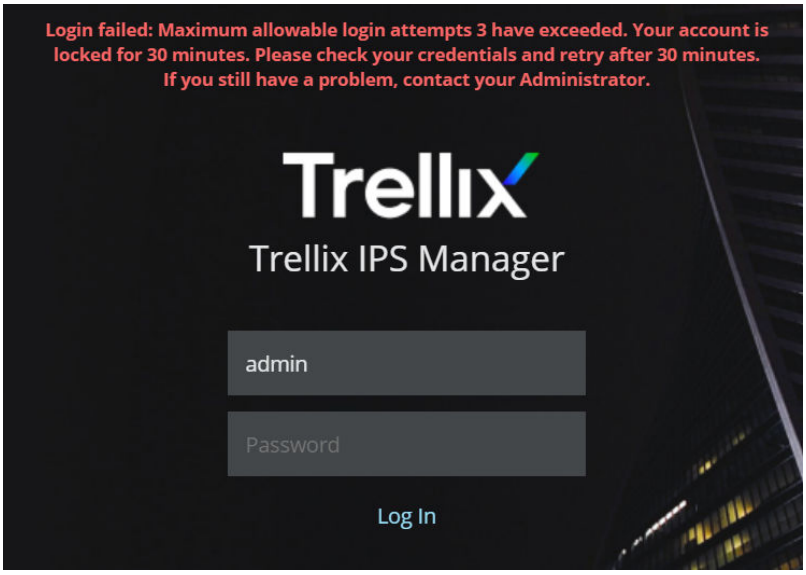
Display account lockout message

Enter the **Login ID** and **Password** and if you have exceeded the login attempts, the following message is displayed.

Login failed: Maximum allowable login attempts <number of login attempts configured> have exceeded. Your account is locked for <duration configured> minutes. Please check your credentials and retry after <duration configured> minutes. If you still have a problem, contact your Administrator.

A similar message appears for password expiration and account locked for timeout.

Figure 53. Sample Account Lock Message



Set up audit log parameters

Setting audit log parameters enables you to determine what information to display in relation to a user's activities. You can choose whether to view actions performed on admin domains and users (creation, editing, role assignment), the Manager (backups, Update Server settings), Sensor (addition, port configuration), and so on. By disabling any of the categories, you will not see user actions in regard to those resources.

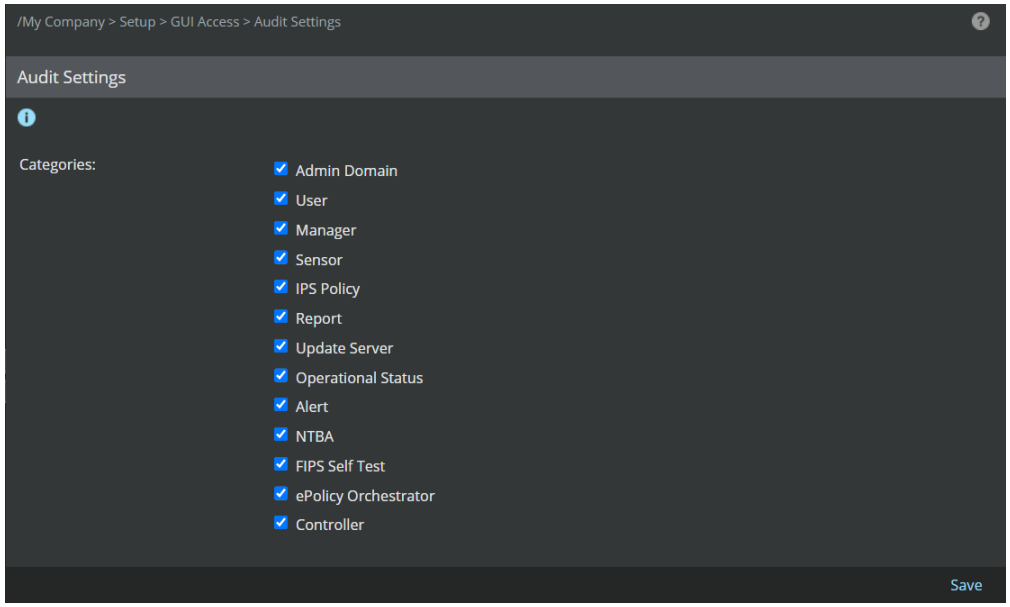
To choose user audit parameters, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Setup → GUI Access → **Audit Settings**.

> **NOTE**
>
> In the Central Manager, select Manager → Setup → GUI Access → **Audit Settings**. The fields displayed are similar to that in Manager, explained below.

Figure 54. Audit Log Parameters



Following Audit Log categories are displayed:

- Admin Domain
- User
- Manager
- Sensor
- IPS Policy
- Report
- Update Server
- Operational Status
- Alert
- NTBA
- FIPS Self Test
- ePolicy Orchestrator
- Controller

2. Select the categories you want to enable.
3. Click **Save** to save the changes.

Active Directory Servers

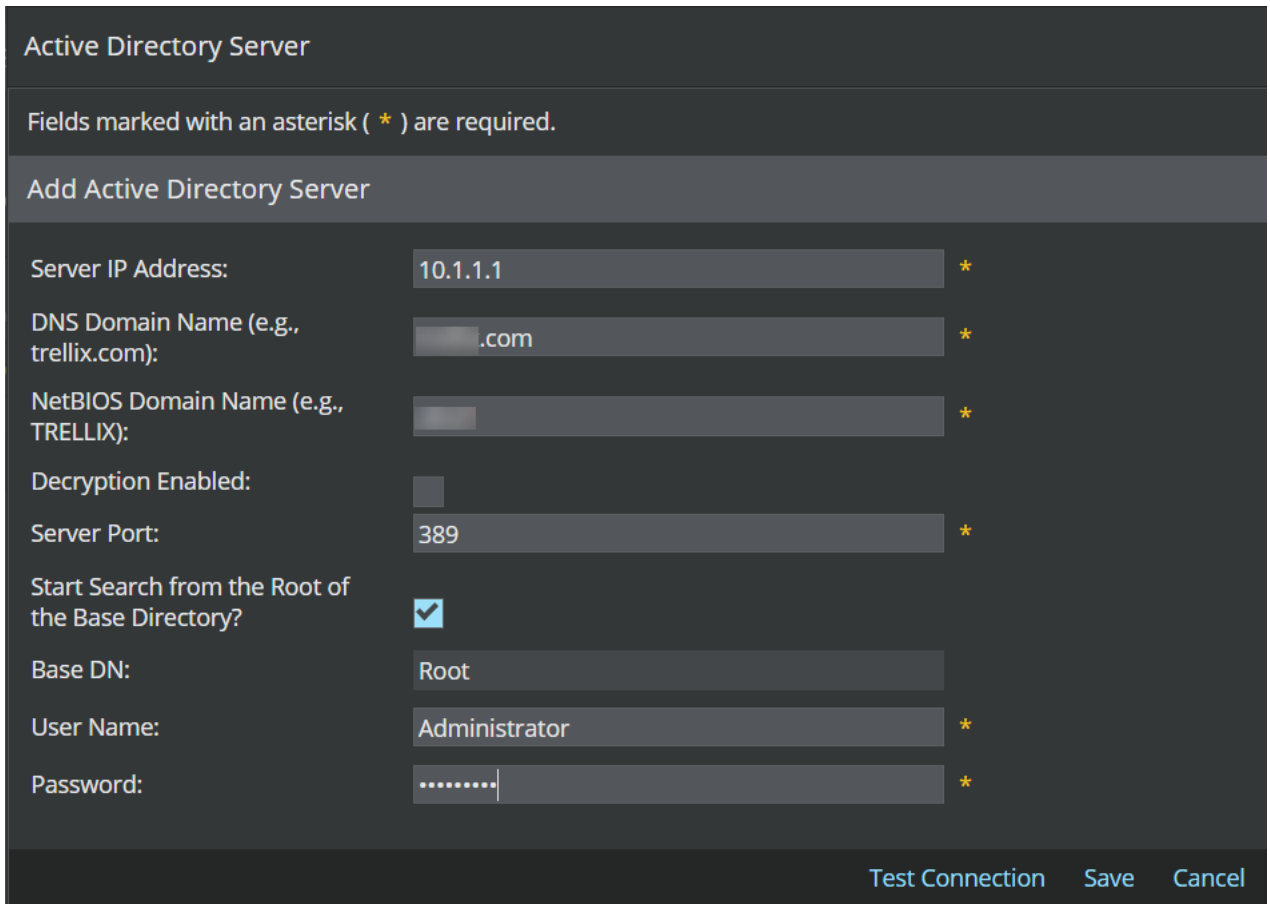
A list of Active Directory servers are used in Manager to enforce firewall rules when Require Authentication is enabled as the primary response action. When authentication is required by the firewall rule, the Sensor initially attempts to obtain the username transparently by snooping login attempts from the list of Trusted Domain Controllers. If the username cannot be obtained transparently, the Sensor redirects the browser to the guest portal. The Active Directory servers are then used to authenticate the user's credentials entered in the guest portal.

Add Active Directory servers

Steps:

1. Go to, Manager → <Admin Domain Name> → Setup → Intrusion Prevention → **Active Directory Servers**.
2. Click ➕.

Figure 55. Add an Active Directory Server



> **NOTE**
>
> When the **Active Directory Servers** tab is accessed from child admin domains, the **Inherit Settings?** option is available. The ➕ button is visible only if you deselect **Inherit Settings?**.

3. In **Add Active Directory Server** window, enter the AD server details in the appropriate fields:

Option	Definition
Server IP Address	Enter the IPv4 IP address of the Active Directory server.

Option	Definition
DNS Domain Name	Enter the Active Directory domain name, like Trellix.com.
NetBIOS Domain Name	Enter the NetBIOS domain name of the Active Directory; for example, Trellix.
Decryption Enabled	Select this option if you want to enable SSL connection for secure data communication.
Server Port	The Active Directory server port. If you select **Decryption Enabled**, the port automatically changes to the default value, 636. Else the default value is 389.
Start Search from the Root of the Base Directory?	Select this option if you want Trellix IPS to check user information from the root node of the Active Directory tree. When you select this option, the value of the next field **Base DN** is displayed as **Root**, by default.
Base DN	Base DN represents the intermediate node name in the Active Directory tree. If you want Trellix IPS to check user information from an intermediate node in the Active Directory tree, enter the corresponding node name in Base DN.
User Name	Active Directory login name for the domain.
Password	Password for the Active Directory login.
Test Connection	Click to test whether the connection with the configured Active Directory Server is working fine. If the connection is successful, a message is displayed for the same.
Save	Saves the configuration in the Manager database. The Manager attempts to verify the details that you provided before creating the record. Even if the Manager is unable to verify the details currently, you can go ahead and create the record. The added Server is listed in the **Active Directory Servers** list.

Notes:

- In **Active Directory Servers** list, if the configuration needs to be inherited to the child admin domains, you can optionally check **Make Settings Visible to Child Admin Domains?** option.
- You are prompted to add the Active Directory server that you created to the list of trusted domain controllers automatically.
- If you configure multiple Active Directory servers, the Manager considers them in a top-down fashion. If two servers from the same domain are listed, the second is only consulted if the one above it cannot be reached.

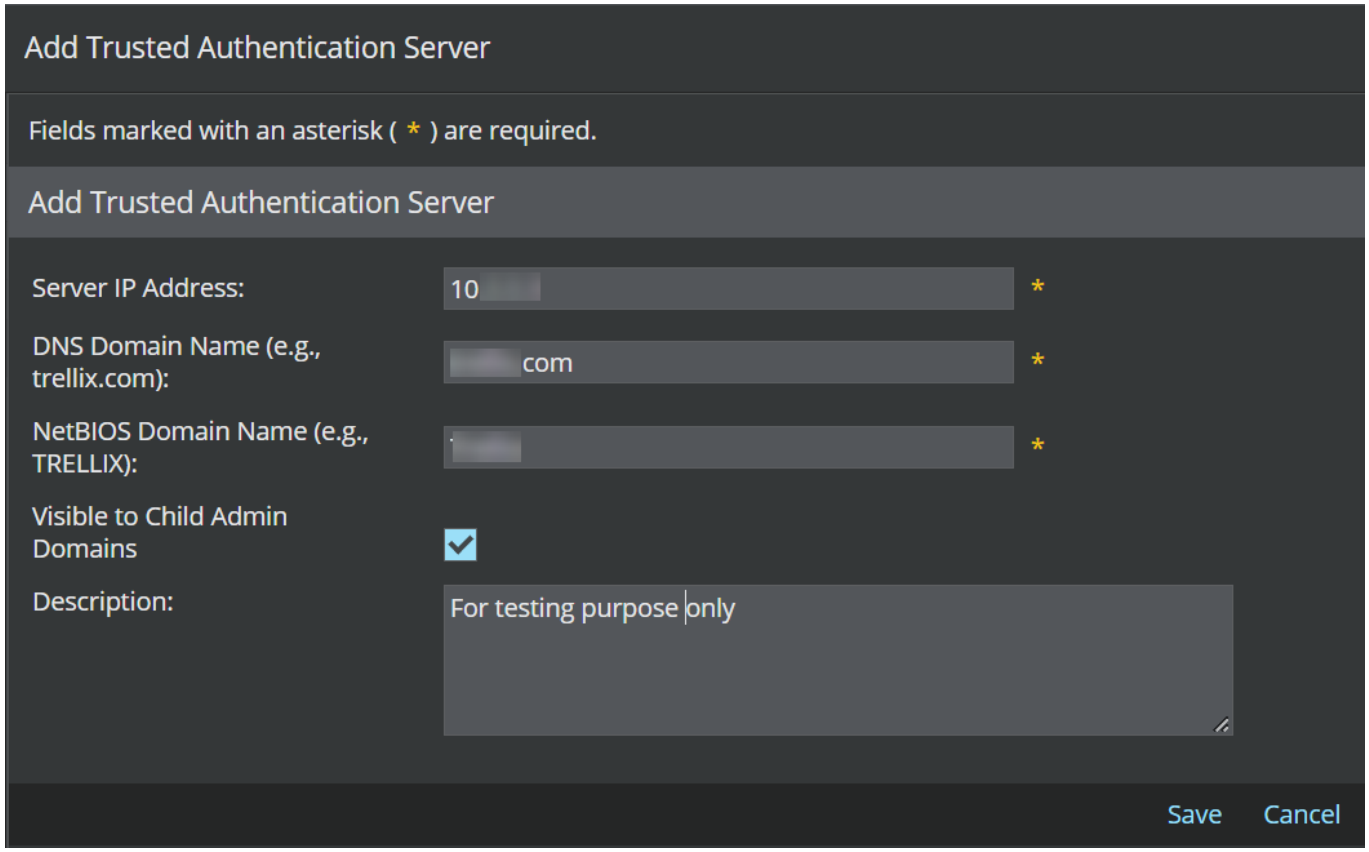
Add Trusted Domain Controllers

When you add the Active Directory servers for an admin domain, you are prompted to automatically create the Trusted Domain Controllers using the same information. If you have done so, you can just verify the list of Trusted Domain Controllers.

Steps:

1. Go to, Manager → <Admin Domain Name> → Setup → Intrusion Prevention → **Trusted Domain Controllers**.
2. Click +.

Figure 56. Add Trusted Domain Controllers



3. In the **Add Trusted Authentication Server** window, enter the Trusted Domain Controller details in the appropriate fields.

Option	Definition
Server IP Address	Enter the IPv4 IP address of the Active Directory server.
DNS Domain Name	Enter the Active Directory domain name, like Trellix.com.
NetBIOS Domain Name	Enter the NetBIOS domain name of the Active Directory; for example, Trellix.
Visible to Child Admin Domain	Select if the configuration needs to be inherited by the child admin domains.
Description	Optionally enter additional information about the Trusted Domain Controller.
Save	Saves the configuration in the Manager database.
Cancel	Clears the details you have entered in the **Add Trusted Authentication Server** window.

Guest Portal settings

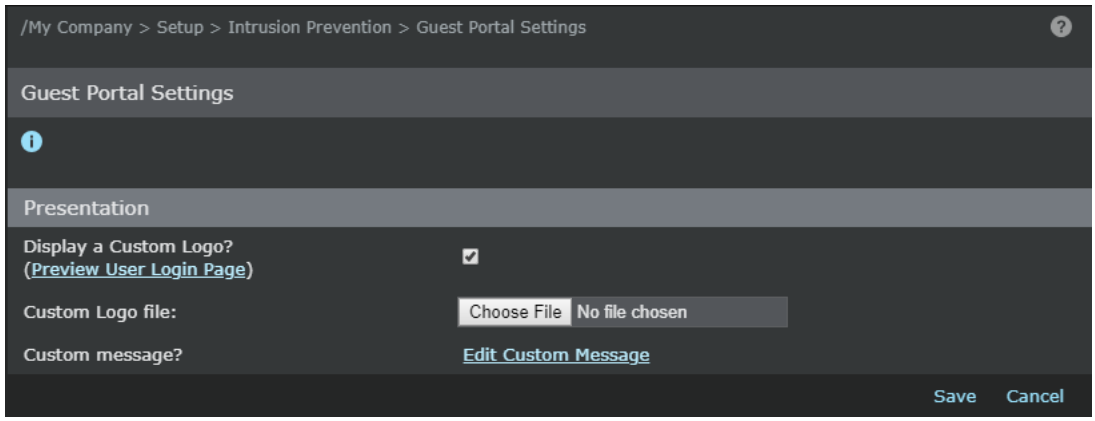
The Guest Portal Settings page allows you to display a custom logo and a custom message for the guest portal.

To display a custom logo and a custom message in the guest portal in the Manager, do the following:

Steps:

1. Go to Manager → Admin Domain Name → Setup → Intrusion Prevention → Guest Portal Settings.

Figure 57. Guest Portal Settings in the Manager



2. Check the required settings for **Presentation**.
3. To save the Guest Portal settings, click **Save**.

Reporting

Report Generation

Trellix IPS provides you report generation options for three types of reports: next generation reports, traditional reports, and configuration reports.

- Click Manager → <Admin Domain Name> → Reporting → **Configuration Reports** to open the configuration reports.
- Click Analysis → <Admin Domain Name> → **Event Reporting** to open the next generation and traditional reports.

Access to the reports is based on user roles. By definition, report generation is available for Super User, Security Expert, and Operator roles. Access is also restricted by admin domain; for example, a user with access to a child domain only cannot view data or templates that require root or higher-level domain access.

Reporting menu

The Manager → <Admin Domain Name> → **Reporting** menu allows you to generate configuration reports, schedule reports, and set report preferences.

The following options are available:

- **Configuration Reports** — These are based on specific type of information like the configuration of Manager, policies, alerts, and summaries of current Manager and Sensor software versions. These reports provide an updated result of the different configurations set on Manager and Sensors.
- **Report Automation** — Schedule report to run automatically and mail to recipients on a daily or weekly basis.
- **Preferences** — Edit report header footer, schedule for running the report, and recipient's list for sending the generated reports.

The report generation time is the time displayed when a report generation is initiated. This is displayed according to the time zone.

NOTE

Click **Back** to navigate to the Configuration Reports list from a generated report page.

Localization of Reports

The Manager supports report generation in the following languages:

- English
- Chinese Simplified
- Chinese Traditional
- Japanese
- Korean

You can configure, schedule, and view the generated reports in all the five languages mentioned.

You can select the language from Manager → <Admin Domain Name> → Reporting → Preferences → **Language** drop-down list. The **Configuration Reports** page is displayed in English the first time you access it. Subsequently, it is displayed in the language that you last chose.

NOTE

If you are accessing Manager from a client machine, you need to install East Asian characters; else such characters in the reports appear as square boxes or question marks. To install the East Asian characters, select Settings → Control Panel → Regional and Language options → **Languages** and select **Install files for East Asian languages**, Install **Asian Language Characters** and then restart the machine.

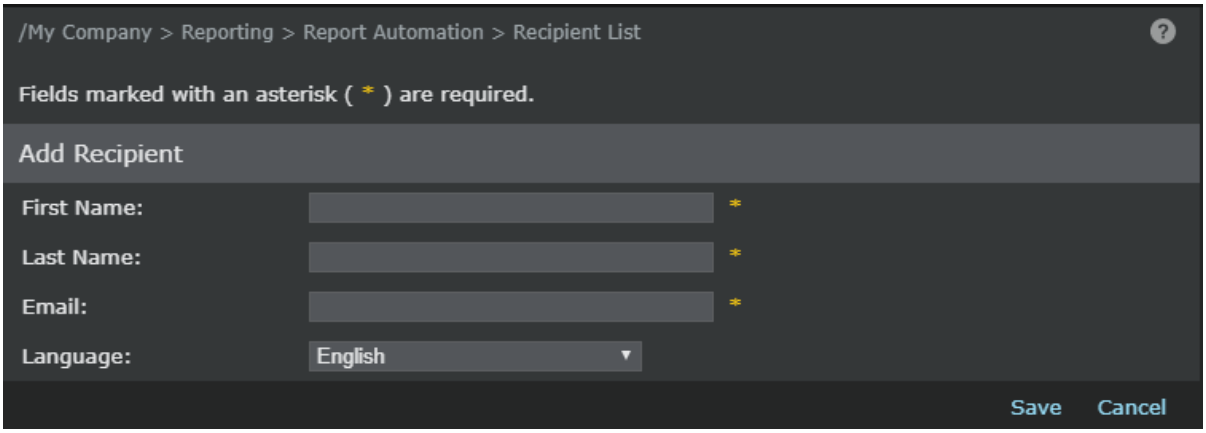
NOTE

To view the PDF version of the localized reports, you need the required fonts in your Acrobat Reader. The first time you attempt to view the PDF version, Acrobat Reader attempts to update with the required fonts.

You can specify the language for the recipients of scheduled reports, and the scheduled reports are generated in those languages. For example, if you have scheduled the Executive Summary Report with five recipients (one recipient for each language including English), this report is generated in all the five languages at the specified time and the appropriate version is emailed to the recipients. That is, the Japanese recipient receives the Japanese version of the report.

The data retrieved from the database is displayed in the language in which it is stored in the database, and this data is independent of the language that you choose in the **Reporting** menu. For example, if a saved report was generated in English, you cannot view it in Japanese by choosing Japanese in the **Language** page. To do this, you need to add another recipient for this report with the language as Japanese.

Figure 58. Add Recipient



The Language column in the Sent Reports page indicates the language in which the reports were generated. Also, for saved reports that are not in English, you can identify the language through the last two letters of the report name:

"ja" indicates Japanese, "ko" indicates Korean, "CN" indicates Chinese Simplified, and "TW" indicates Chinese Traditional.

In the following pages, you can enter text in the language that you had chosen:

- Add Report Template (Description)
- Edit Report Template (Description)
- Add Recipient (First Name and Last Name)
- Edit Recipient (First Name and Last Name)

The following table provides the extent of localization in the Reports module:

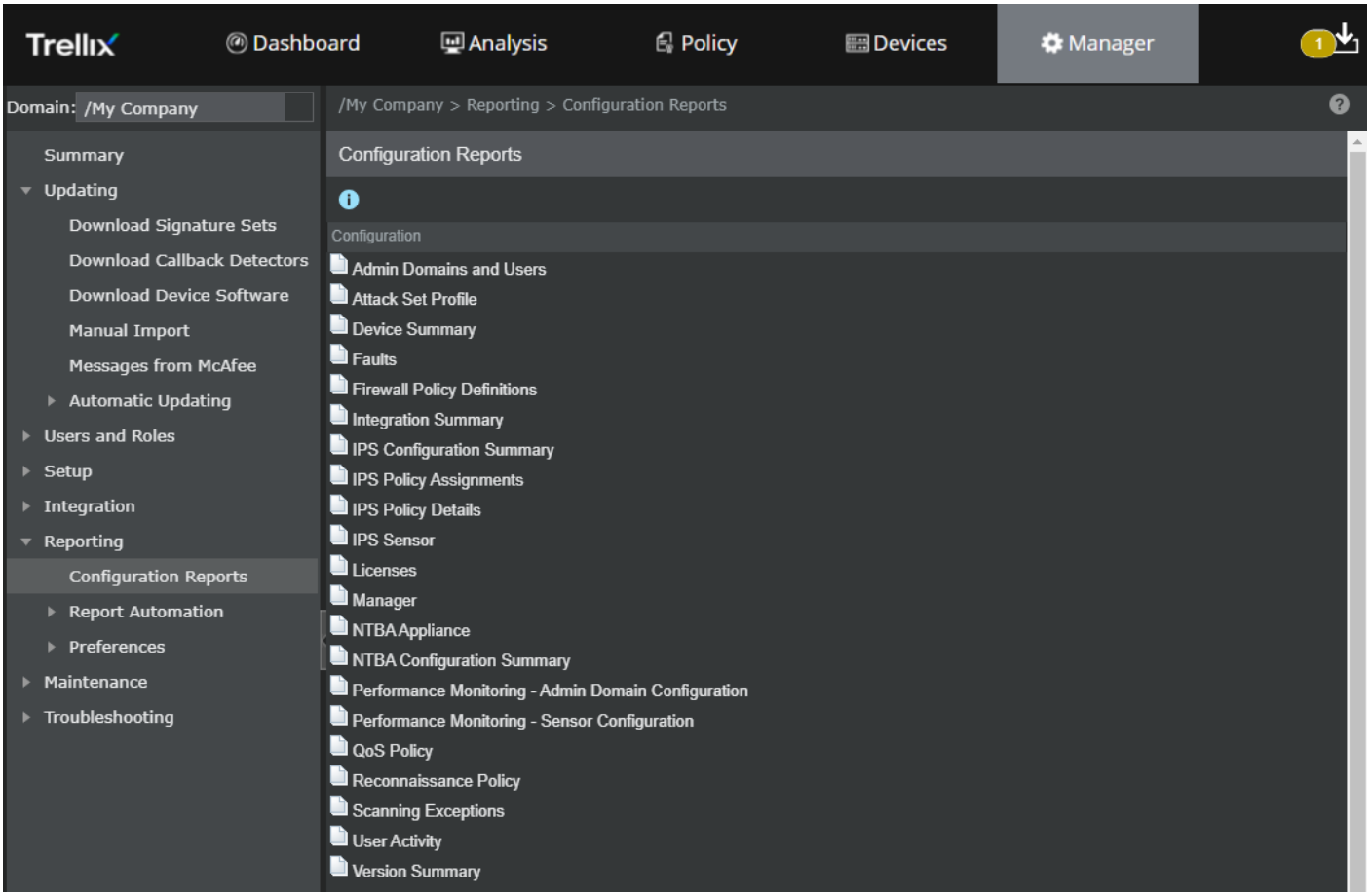
Category	Extent of Localization
User-configurable data retrieved from the database	Not localized
Data that is not user-configurable	Fully localized
Informational messages	Fully localized
Error messages	Fully localized
Online Help	Available in English only by default. The localized online help can be requested for separately, which can be manually installed in your Manager setup.
Text in charts and graphs	Partially localized
Dates	Fully localized
Calendar	Fully localized
Numeric, monetary, and metric	Partially localized
Data input through keyboard	Partially localized

Configuration Reports

Configuration Reports are based on pre-defined conditions and detail your system configuration settings. The Configuration reports are available in Manager → <Admin Domain Name> → Reporting → **Configuration Reports**.

You can generate these reports to view your current software and signature versions, the configuration and status of a Sensor, policy settings, and so forth. The report generation time is the time displayed when a report has been executed. This is displayed according to the time zone. Several pre-formatted reports are provided for simple information gathering.

Figure 59. Configuration Reports



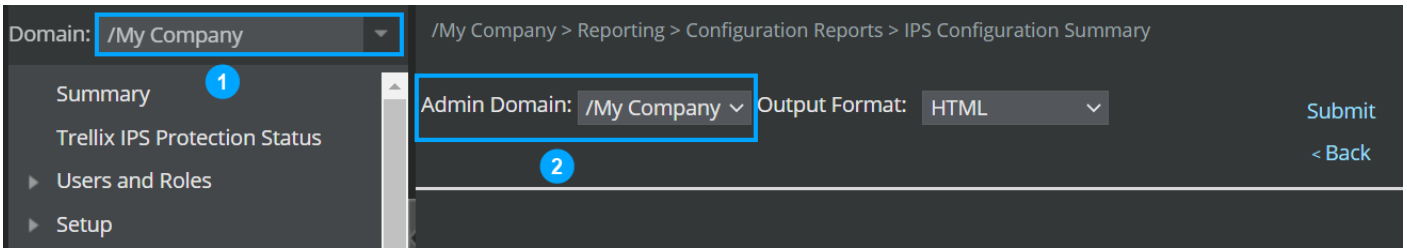
The available configuration reports are:

- Admin Domain and Users Report — Information on the admin domains and users controlled through your Manager.
- Attack Set Profile Report — Information on all of the attack sets available for application.
- Device Summary Report — Information about all the devices configured.
- Faults Report — Information on Manager and Sensor fault logs.
- Firewall Policy Definitions Report — Provides a detailed view of the selected Firewall policy, its Access Rules, and the Sensor resources to which it is assigned.
- Integration Summary Report — Provides a summary of configurations done in the Manager to integrate with other Trellix products, such as Trellix ePO - On-prem.

- IPS Configuration Summary Report — Provides a detailed view of the IPS configuration settings made by the user.
- IPS Policy Assignment Report — Provides a detailed view of the IPS policies available for application.
- IPS Policy Details Report — Provides a detailed view of the IPS policies available for application.
- IPS Sensor Report — Information on the policies applied to one or more Sensors.
- Licenses— Information about the System Licenses, Proxy Decryption Licenses, and Virtual Sensors licenses.
- Manager Report — Configuration information related to the notification mail server, proxy server, and MDR.
- Performance Monitoring - Admin Domain Configuration Report — Displays information on admin domain wise configuration made in the Manager
- Performance Monitoring - Sensor Configuration Report — Displays information on Sensor configuration settings made in the Manager
- QoS Policy — Information on all the Quality of Services (QoS) policies available for application.
- Reconnaissance Policy Report — Information on all the Reconnaissance policies available for application.
- Scanning Exceptions Report — Displays information of the scanning exceptions that are configured on the Sensor's VLAN, TCP, or UDP port.
- User Activity Report — Information on the actions performed by Trellix IPS users.
- Version Summary Report — Information on the versions of software and signatures in use.

This figure shows the difference between the admin domain filter available in the left pane, and the admin domain filter for the reports.

Figure 60. Admin Domain Filters



1 — This admin domain filter has no impact on the reports generated.

2 — This is the admin domain filter that you can use to generate the report based on the admin domain selected.

Saving Configuration reports

To save a Configuration report, select the **Output Format**:**HTML**, **PDF Portrait**, **PDF Landscape**, **Save as CSV** or **Save as HTML**. You can then click **Save** and specify a location where to save the file.

If you select either **PDF Portrait** or **PDF Landscape**, a PDF file format displays on the **Report** page. You need Adobe Acrobat 7.0 or later to view reports in PDF. The recommended viewing size for the PDF version of a report is "Actual Size" or 100%. If you want to save the PDF of a report, Trellix recommends customizing the file name for easy recognition. If you want to keep the generated file name, check the length of the name. If you had de-selected Day/Time Detected from the Fields of Interest section of a report generation template, the default file name will be **ViewReport.pdf**.

If you select **Save as CSV**, a dialog box is displayed prompting you for the file name and location. You can specify an appropriate file name and location and click **Save** to save the report in CSV format and you can open the file using Microsoft Excel.

Generate Admin Domain and Users reports

The Admin Domain and Users report provides information on the admin domains and users created and configured using the Manager. Information presented reflects the basic settings for each resource (admin domain and user).

To generate an Admin Domain and User Report, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Reporting → Configuration Reports → **Admin Domains and Users**.
2. Select the **Output Format**.
3. Click **Submit**.

   The field descriptions for each table in this report are as follows:

   Admin Domain Information

   - Name— Name of an admin domain.
   - Contact Information— The name and email of the main user to contact for the domain.
   - Child Admin Domain Allowed?— Whether a child domain can be configured for the domain. A tick mark indicates that child domain configuration is allowed. For the root admin domain, this is always allowed.
   - Add Device Allowed?— Whether a Sensor can be added to the domain. A tick mark indicates that Sensors can be added to the domain. For the root admin domain, this is always allowed.
   - Default IPS Policy— The IPS Policy applied to the domain.
   - Default Reconnaissance Policy— The Reconnaissance Policy applied to the domain.

   User Information

   - Name— Name of a user.
   - Contact Information— Email address for the user.
   - Creator Domain— The admin domain where the user was created.
   - Login ID— The user's ID for logging into Manager.
   - Role(s)— The user's role(s) with the corresponding domains in parentheses.

   Undefined SNMP Forwarder Information

   - Admin Domain— All current domains.
   - IP Address— The address of the target SNMP server.
   - Destination Port Number— The target server's SNMP listening port.
   - SNMP Version— The version supported by your SNMP server. Version options are 1, 2c, Both 1 and 2c or 3.
   - Notification for All Child Admin Domains— A tick mark indicates that notifications generated for all the child admin domains are also factored in for this report.

NOTE

The SNMP Forwarder information is displayed only for those domains for which SNMP Trap Receivers have been configured.

Fault Syslog Forwarder Information

- Admin Domain— All current domains.
- Syslog Forwarder Enabled— Syslog forwarder has been enabled or disabled.
- Child Domain Notification Enabled— whether child notification has been enabled.
- Syslog Server (Host Name or IP Address)— Syslog server is enabled.
- Port— Port on which it is forwarded.

User Activity Audit Syslog Information

- Admin Domain— All current domains.
- Syslog Forwarder Enabled— Syslog forwarder has been enabled or disabled.
- Child Domain Notification Enabled— Whether child notification has been enabled.
- Syslog Server (Host Name or IP Address)— Syslog server is enabled.
- Port— The port of the Audit Syslog server.
- Facilities— Standard syslog prioritization value.
- Result Mapping— Informational messages of the mapped results. It is categorized into: Failed, In progress, and Success.
- Forward Audit— Severity of the audit log forwarded to the syslog server.
- Message Preference— Preference of the message.

Proxy Server Settings

- Admin Domain— All current domains.
- Use Parent Settings?— Whether parent settings are inherited.
- Use Proxy Server?— Whether proxy server is enabled or disabled.
- Proxy Server Name or IP Address— The address of the target proxy server.
- Port Number— The proxy server's port.
- User Name— Name of a user.

Generate Device Summary report

The Device Summary report contains information regarding all the IPS, Virtual IPS, NTBA, and Virtual NTBA devices configured. It provides a summary of information per device irrespective of the number of similar Sensor models configured. The device count provides a summarized count of all the devices configured.

To generate a Device Summary report, do the following:

1. Click the **Manager** tab.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Device Summary**.

3. Select the **Output Format**.
4. Click **Submit**.

The field descriptions in this report are as follows:

Summary

- Device model — Provides the Sensor models configured
- Count — Displays a summarized count of the similar Sensor models

Sensor Name (IPS, Virtual IPS, NTBA, Virtual NTBA)

Field Name	Description	Applicable to Sensor model
Name	Displays the name of the Sensor.	IPS, Virtual IPS, NTBA, Virtual NTBA
Model	Displays the Sensor model number.	IPS, Virtual IPS, NTBA, Virtual NTBA
Serial Number	Displays the serial number specified on the physical Sensor.	IPS, NTBA, Virtual NTBA
Software Version	Displays the current software version configured on the Sensor.	IPS, Virtual IPS, NTBA, Virtual NTBA
Contact Information	Displays the contact information provided by the user at the time of configuration of the Sensor.	IPS, Virtual IPS, NTBA, Virtual NTBA
Location	Displays the geographical location provided by the user at the time of configuration of the Sensor.	IPS, Virtual IPS, NTBA, Virtual NTBA
Updating Mode	Displays the mode of configuration update for the Sensor. It can be updated online or offline.	IPS, Virtual IPS
Signature Version	Displays the current signature version configured on the Sensor.	IPS, Virtual IPS
Hardware Version	Displays the current hardware version running on the Sensor.	IPS
Gateway Anti-Malware DAT Version	Displays the current version of the Gateway Anti-Malware DAT file.	IPS (NS Series), Virtual IPS, NTBA, Virtual NTBA
Gateway Anti-Malware Engine Version	Displays the current version of the Gateway Anti-Malware Engine.	IPS (NS Series), Virtual IPS, NTBA, Virtual NTBA
Anti-Virus DAT Version	Displays the current version of the Anti-Virus DAT file.	IPS (NS Series), Virtual IPS, NTBA, Virtual NTBA
Anti-Malware Engine Version	Displays the current version of the Anti-Malware Engine.	IPS (NS Series), Virtual IPS, NTBA, Virtual NTBA
IP Address Connected to the Manager	Displays the IP address used by the Sensor to connect with the Manager.	IPS, Virtual IPS, NTBA, Virtual NTBA
Subnet Mask	Displays the subnet mask IP address.	IPS, Virtual IPS
Default Gateway	Displays the IP address of the default gateway.	IPS, Virtual IPS

Field Name	Description	Applicable to Sensor model
Up Time	Displays the time period from when the Sensor started running.	IPS, Virtual IPS, NTBA, Virtual NTBA
Last Reboot	Displays the date and time of the previous reboot.	IPS, Virtual IPS, NTBA, Virtual NTBA
Last Signature Set Update	Displays the date and time of the previous signature set update.	IPS, Virtual IPS, NTBA, Virtual NTBA
FIPS Mode	Displays if FIPS mode is enabled or disabled.	IPS, Virtual IPS

Generate Faults reports

The **Faults Report** enables you to see the details of Sensor and Manager faults that have occurred in the past. Reports can be generated based on the fault name, its creation time, its fault severity, or by the Sensor ID.

To generate a Faults report, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Faults**.
3. Specify the following to narrow down the scope of your report:
   - **Fault Source** — Select **Sensor** and/or **Trellix IPS Manager** to find faults on your Sensor and/or Manager, respectively.
   - **Admin Domain** — Select an admin domain on which to run the report. This is enabled only if the selected **Fault Source** is **Sensor**.

     NOTE

     The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

   - **Include Child Admin Domains** — If you have selected **Include Child Admin Domains**, Sensors in the child admin domains of the selected admin domain are also displayed. This is enabled only if the selected **Fault Source** as **Sensor**.
   - **Sensor** — Select one or all devices on which to run the report.
   - **Fault Severity** — Select one or more of the following:
     - **Informational**
     - **Warning**
     - **Error**
     - **Critical**
   - **Fault State** — Select one of the following:

- **All Faults**
- **Active Faults**
- **Deleted Faults**
- **Acknowledged Faults**

- **Faults** — Select from one of the following time options:
  - **Select Faults for this day (yyyy/mm/dd)** — Displays faults for a selected day.
  - **Select Faults between these dates (yyyy/mm/dd hh:mm:ss)** — Displays faults between the **Begin Date** and the **End Date**.
  - **Select Faults in the past** — Displays faults for the specified period and ending at the specified time. The default is the current time.

> **NOTE**
>
> Faults with creation date previous to the Begin date may get displayed too, implying that the particular fault had occurred before the begin data and re-occurred again between the Begin and End date.

- **Report Format** — Select any of the following format for the report:
  - **HTML**
  - **PDF Portrait**
  - **PDF landscape**
  - **Save as CSV**
  - **Save as HTML**
- **Organized by** — Specify how you want the information to be organized in the report. Choices are **Severity**, **Fault Name**, **Sensor**, or **Create Time**. For example, if you choose Severity, then the information is organized by fault name in the reverse alphabetical order. Create Time is the fault generation time.

4. Click **Run Report** to generate the report.

> **NOTE**
>
> Only 5000 faults can be processed for a report. If more than 5000 faults are involved, a note is displayed recommending you to narrow down the scope of your report.

The field descriptions in this report are as follows:

Field Name	Description
Time	The time at which the fault was generated.
Duration	The length of time the fault lasted. For example, in the case of a performance fault, this is the number of minutes between when the performance first went over its threshold and when it subsequently fell below its reset threshold.
Source	The source of the fault.

Field Name	Description
Criticality	Specifies the severity level of the fault.
Undefined	Specifies the name of the fault that is undefined.
Description	A detailed description of the fault.
Type	The type of fault.
Acknowledged	Indicates whether the fault is acknowledged or not.
Deleted	Indicates whether the fault is deleted or not.
Last Updated	The time at which the fault was last modified. This time stamp gets updated when the fault is acknowledged.

Generate Firewall Policy Definition report

The Firewall Policy Definition Report provides a detailed view of the selected Firewall policy, its Access Rules, and the Sensor resources to which it is assigned.

Steps:

1. Click the **Manager** tab.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Firewall Policy Definitions**.
3. Select a filter from the **Admin Domain** drop-down list.

> **NOTE**
>
> The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

4. Select the **Firewall Policy**.
5. Select the **Output Format**.
6. Click **Submit**.

Generate Integration Summary reports

The Integration Summary report provides a summary of configurations done in the Manager to integrate with other products such as, Trellix ePO - On-prem and Trellix Global Threat Intelligence Configuration.

To generate an Integrated Summary Report, do the following:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Integration Summary**.
3. Select the **Output Format**.
4. Click **Submit**.

The Integration Summary Report displays the following details:

1. ePO DB Configuration
2. Telemetry Submission
3. Technical Contact Information
4. Trellix Global Threat Intelligence

ePO DB Configuration

The integration between the Manager and the ePO server is done with the help of an extension file. After the installation of the extension file, the detail is listed in this report and its fields are described in the following table:

Field Name	Description
Admin Domain	The selected admin domain for the summary report to be generated.
Endpoint Summary Queries	Displays details of the Endpoint Summary Queries which can be enabled or disabled.
Endpoint Lookup	Displays details of the Endpoint Queries which can be enabled or disabled.
Endpoint Tagging	
Server Name or IP Address	The name or the IP of the ePO server running the extension file. Note that this ePO server should have the details of the hosts covered by the admin domain. Contact your ePO administrator for the server name and IP.
Server Port	Specify the HTTPS listening port on the ePO server that will be used for the Manager-ePO communication. Contact your ePO administrator for the port number.
User Name	The username to be used while connecting to the ePO server. Trellix recommends you use a local ePO user account with View-only permissions.

For more information on ePO, refer to [ePO documentation].

NOTE

If you update the IP address of ePO from the Manager in the Manager → <Admin Domain Name> → Integration → **ePO Integration** page, you should reboot the Manager.

Telemetry Submission

The details of what has actually been sent to Trellix are described in the following table:

Field Name	Description
Alert Data Details	This field shows the details of the Alert data sent to Trellix for each attack.
Only send data for following alert severities (Filter)	This field helps to configure the levels of severities.
Alert Data Summary	This field shows the alert summary information sent hourly to Trellix like List of Trellix IPS attack IDs seen.
General Setup	This field shows the general setup information sent daily to Trellix like Manager software version and active signature set version.

Field Name	Description
Feature Usage	This field shows the feature information sent daily to Trellix like the number of default policies in use.

Technical Contact Information

The details of your contact information that are provided to Trellix ARC are described in the following table:

Field Name	Description
Send Technical contact information	Technical contact information is gathered to communicate End of Life and other key milestones.
First Name	The first name of the contact person.
Last Name	The last name of the contact person.
Street Address	The street address of the contact person.
Phone Number	The phone number of the contact person.
E-mail Address	The email address of the contact person.

Global Threat Intelligence

The details of private TI cloud integration are described in the following table:

Field Name	Description
Private GTI Cloud Integration	Displays if the private GTI cloud integration is enabled or disabled.
Private GTI Cloud Server IP	Displays the server IP of the private GTI cloud.

Generate IPS Configuration Summary reports

The IPS Configuration Summary report provides a detailed view of the IPS configuration settings made by the user. This includes SNMP Forwarder Information, Alert Syslog Forwarder Information, Firewall Syslog Forwarder Information, Quarantine information, Network Objects, Quarantine Zones, Syslog Forwarding, Remediation Portal, IPS Settings and Quarantine. Information can be displayed for any selected admin domain in either .html, .pdf or .csv file formats.

To generate an IPS Configuration Summary report for an admin domain, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **IPS Configuration Summary**.
3. Select a filter from the **Admin Domain** drop-down list.

> **NOTE**
>
> The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

4. Select the **Output Format**.
5. Click **Submit**.

For the selected Admin Domain, IPS Configuration Summary report gives the following IPS configuration details:

IPS Events SNMP Forwarder Information

SNMP Forwarder Information specifies the server to which alert information will be sent from Manager. You can configure more than one SNMP server to where you want to send alert messages. The field details are described in the following table:

Field Name	Description
IP Address	IP address of the target SNMP server which can be IPv4 or IPv6 address.
Destination Port Number	The target server's SNMP listening port.
SNMP Version	Version of SNMP running on the target SNMP server. Version options are 1, 2c, Both 1 and 2c, and 3.
SNMP Forwarder Information	The SNMP server to where you want to send alert messages.

Alert Syslog

Alert Syslog Forwarder Information enables the forwarding of Trellix IPS alerts to a Syslog Server. The field detail is described in the following table:

Field Name	Description
Syslog Forwarder Enabled	Syslog forwarder has been enabled or disabled.

Alert Syslog Forwarder Information

Alert Syslog Forwarder Information enables the forwarding of Trellix IPS alerts to a Syslog Server. The Syslog forwarding enables you to view the forwarded alerts from a third-party Syslog application. The field details are described in the following table:

Field Name	Description
Child Domain Notification Enabled	Child notification has been enabled.
Notification Profile Name	Name of the notification profile.
Syslog Server (Host Name Or IP Address)/Port	Syslog server or port on which it is enabled.
Protocol	Syslog server using UDP or TCP connection
Use SSL	Use SSL when syslog server uses TCP
Quarantine Enabled	Quarantine enabled or disabled.

Firewall Notification Information

It is an optional Firewall feature that will log packets that are dropped or permitted based on your Access Rules. You can configure the Sensor to forward Firewall logs to Manager, where they are formatted and converted to Syslog messages and sent to the configured Syslog server. You can also configure the Sensor to directly send logs to the configured Syslog server. The field details are described in the following table:

Field Name	Description
Syslog Forwarder Enabled	Syslog forwarder has been enabled or disabled.
Child Domain Notification Enabled	Child notification has been enabled.
Syslog Server (Host Name Or IP Address)	Syslog server is enabled.
Port	Port on which it is forwarded.

Quarantine

To protect your network from security threats, Trellix IPS provides the Quarantine feature which quarantine and remediate the non-compliant network devices (or hosts) connecting to your network.

Rule Objects

Rule objects provide a convenient way of grouping together IP addresses, VLAN, CIDR or MAC addresses. The field details are described in the following table:

Field Name	Description
Name	Name of the rule object.
Type	This indicates the four different types of network address types that can be listed together in a network object. • IP Address • Network Address (CIDR) • MAC Address • VLAN
Value	Enter the Value for the Type selected.

Quarantine Zones

Quarantine Zones are a set of ACL rules that define the zone of network access provided to a host subjected to Quarantine.

The field details are described in the following table:

Field Name	Description
Name	The name of the Quarantine Zone.
Description	The description of the Quarantine Zone.

Syslog Forwarding

The **Alert Notification Syslog** action enables the forwarding of Trellix IPS alerts to a Syslog Server. Syslog forwarding enables you to view the forwarded alerts from a third-party Syslog application. For Syslog forwarding, the root domain and parent domains have the option to include alerts from all applicable child domains.

Field Name	Description
Syslog	Syslog forwarder has been enabled or disabled.
Name	Host Name of the Syslog Server where alerts will be sent.

Field Name	Description
Facility	Standard Syslog prioritization value. The choices are as follow: • Security/authorization (code 4) • Security/authorization (code 10) • Log audit (note 1) • Log alert (note 1) • Clock daemon (note 2) • Local user 0 (local0) • Local user 1 (local1) • Local user 2 (local2) • Local user 3 (local3) • Local user 4 (local4) • Local user 5 (local5) • Local user 6 (local6) • Local user 7 (local7)
Priority	The severity level of a higher or lesser priority.

Remediation Portal

To make the quarantined host clean of malicious traffic and thus compliant to the security policies of the network, Trellix IPS provides remediation by re-directing the HTTP traffic from the host to a Remediation Portal.

Field Name	Description
Remediation Portal State	Enable the redirection of HTTP traffic to the Remediation Portal.
Remediation Portal IP Address	Configure the Remediation Portal, by specifying the Remediation Portal IP Address.
Remediation Portal URL	Configure the Remediation Portal, by specifying the Remediation Portal URL

IPS Settings

The IPS Settings node in each admin domain facilitates actions related to configuration and management of IPS related policies configuration on the Trellix IPS.

Quarantine

Field Name	Description
State	Whether Quarantine is enabled or not.
Quarantine Zone	The quarantine zone selected.
Release Logic	Whether the Sensor is configured to release the endpoint from quarantine automatically after a set timing or whether you have to manually release the endpoint from quarantine.
Release After	If the Sensor is configured to release the endpoint, what is the time duration after which the endpoint is released.

Field Name	Description
Browser Message	How is the browser message enabled.

Quarantine Exceptions

You can exclude certain hosts or network from being quarantined. This can be configured from the **Quarantine Exceptions** page of the Quarantine Configuration Wizard.

Field Name	Description
Type	The IP address, IPv4 Network, or Rule Object.
Value	Enter the Value for the Type selected.
Description	The description of the hosts or network.

File Reputation

The File Reputation Report provides you details of Trellix ePO™ (GTI) IP Reputation-related alerts such as Dirtiness Level, Matched fingerprint, Sensor Source IP, Source Port, etc.

Fingerprints - GTI

Field Name	Description
Maximum file size scanned	4194304 bytes (for signature set 10.8 and higher) - fixed size up to which malware files are detected.
Primary DNS Server	The main DNS server - configured first.
Secondary DNS Server	The backup DNS server – configured next and if main DNS server fails to respond.
Response Action	Detect/Allow (Alert only), block, block and send TCP resets.
Sensitivity	The severity of malware to block can be controlled.

Fingerprints - Custom

Field Name	Description
Number of custom fingerprints	The number of custom finger prints that are added.
Maximum file size scanned	4194304 bytes (for signature set 10.8 and higher)- fixed size up to which malware files are detected.
Response Action	Detect/Allow (Alert only), block, block and send TCP resets.

File types supported

Field Name	Description
GTI	The Portable Executable (PE) files.
Custom	File types based on custom signatures.

IVX Integration - Integration with IVX Appliance

Field Name	Description
Enable IVX Integration	IVX appliance Integration has been enabled or disabled.
Enabled Integration with	Integration has been enabled with IVX.
IP Address	IP address of the IVX broker(s) integrated with Trellix IPS.
Manager to IVX Communication Port (TCP)	Manager-to-IVX Appliance Communication Port number.

IVX Integration - Integration with IVX Cloud

Field Name	Description
Enable IVX Cloud Integration	IVX Cloud Integration has been enabled or disabled.
Enabled Integration with	Integration has been enabled with IVX Cloud.
Host Name	Host name for the IVX Cloud service. The default host name is **`feapi.marketplace.apps.fireeye.com`**.
Manager to IVX Cloud Communication Port	Manager-to-IVX Cloud Communication Port number.

Trellix Intelligent Sandbox Integration

Field Name	Description
Enable Trellix Intelligent Sandbox Integration	Trellix Intelligent Sandbox Integration has been enabled or disabled.
Trellix Intelligent Sandbox IP Address	IP address of Trellix Intelligent Sandbox integrated with Trellix IPS.
Sensor-to-Intelligent Sandbox Communication Port (TCP)	Sensor-to-Intelligent Sandbox Communication Port number.
Manager-to-Intelligent Sandbox Communication Port (TCP)	Manager-to-Intelligent Sandbox Communication Port number.

Generate IPS Policy Assignment reports

The IPS Policy Assignment provides a detailed view of the policies - Exploit, Reconnaissance, and DoS - applied to one or more Sensors. Policy information includes severity, responses, thresholds, notifications, and other information configured for each attack whether from a pre-configured or user-customized policy. Also, you can view attack set profile, and DoS ID settings for all of the policies applied within a Sensor. The **Customized Attacks** option consolidates all user-customized attacks into one section for easy viewing.

To generate an IPS Policy Assignment report for a Sensor, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **IPS Policy Assignments**.
3. Select one or more **Devices**.

> **TIP**
>
> Sensor Policy Configuration Reports can be very long when multiple Sensors are selected. Trellix recommends selecting a single Sensor for ease of readability.

4. Select one or more of the following based on what information you want to see in the report:
   - **Reconnaissance Policy**
   - **Exploit/DoS Policy**
     - IPS Policy Detail
     - DoS Detail
     - Attack Set Profile Detail
     - Recon Attacks
   - **Customized Attacks**
5. Select the **Output Format**.
6. Click **Submit**.

Generate IPS Policy Details reports

The IPS Policy Details provides a detailed view of the IPS policies available for application. This includes any user-created or user-cloned policies. Policy information includes severity, responses, thresholds, notifications, and other information configured for each attack from a policy. Also, you can view attack set profile and DoS settings for all of the policies applied within an admin domain.

To generate an IPS Policy Details report, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **IPS Policy Details**.
3. Select one or more **Policies**.

> **TIP**
>
> IPS Policy Reports can be very long when multiple policies are selected. Trellix recommends selecting a single policy for ease of readability.

4. Select one or more of the following based on what information you want to see in the report:
   - IPS Policy Detail
   - DoS Detail
   - Attack Set Profile Detail
   - Customized Attacks: Consolidates all user-customized attacks into one section
   - Recon Attacks: This is enabled only if the selected policy is Trellix Global IDS.

5. Select the **Output Format**.
6. Click **Submit**.

Generate IPS Sensor reports

The Physical Sensor report provides information on the current software/signature versions, the status of a Sensor's ports, as well as configured settings such as non-standard ports.

To generate a Physical Sensor report, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **IPS Sensor**.
3. Select one or more **Sensors**.

> **TIP**
>
> Sensor Reports can be very long when multiple Sensors are selected. Trellix recommends selecting a single Sensor for ease of readability.

4. Select one or more of the following based on what information you want to see in the report:
   - **Device Information**
   - **Port Configuration**
   - **Interface Configuration**
   - **TCP/IP Settings**
   - **Non-standard Ports**
   - **Alerting Options**
   - **Trellix Intelligent Sandbox Integration**
   - **TIE Integration**
   - **L2 Switch & SSL Configuration**
   - **TACACS+ Authentication Settings**
   - **NMS Configuration**
   - **Exception Details**
   - **NTBA Configuration**
   - **CLI Auditing**
   - **Quarantine Information**
   - **L7 Data Capture Settings**
   - **NTP Server Details**
   - **Performance Monitoring**

- **IVX Integration**

5. Select the **Output Format**.
6. Click **Submit**.

Generate Manager Report

Manager Report provides a quick view of the notification mail server and/or proxy server settings configured using Manager.

To generate a Physical Sensor Report, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Manager**.
3. Select the **Output Format**.
4. Click **Submit**.

   The field descriptions for each table in this report are as follows:

   - **Notification Mail Server Settings**
     - Hostname/IP— Hostname or IP address of the mail server.
     - From Address for Messages— "From:" address appended to notification emails.
     - Login Name— The optional login ID used for mail server access.
   - **Proxy Server Settings**
     - Use Proxy Server?— If proxy server is used.
     - Proxy Server Name or IP Address— Hostname or IP address of proxy server.
     - Port Number— Port number where proxy server receives requests from Manager.
     - User Name— Name of the Proxy Server.
   - **MDR Information For Trellix IPS Manager**
     - Manager Status— Administrative status of Manager you are logged on. "Primary" indicates that Manager is in active mode, and "Secondary" indicates that Manager is in standby mode.
     - Out of Band (OOB) Manager to Manager Communication— Whether OOB communication is enabled between Managers in the MDR pair.
     - OOB Peer Manager IP— The IP used for OOB communication by the peer Manager comprising the MDR pair.
     - Operation Status— Operative status of Manager you are logged on.
     - Peer IP Address— Hostname or IP address of the peer Manager.
     - Peer Manager Status— Administrative status of the peer Manager.
     - Peer Manager Operation Status— Operative status of the peer Manager.

   NOTE

   The hostnames and IP addresses for the peer Manager are specified in Manager Disaster Recovery Details page. For information, see Preparations for Manager Disaster Recovery (MDR) (page 125).

- **Access Control**
  - Allow Access to this Web-Based User Interface from— Permit the user to Web-based user interface from authorized or any host.
  - Audit Logging for Access Attempts by Authorized Endpoints— Permit the user to log from authorized host.
  - Audit Logging for Access Attempts by Unauthorized Endpoints— Permit the user to log from unauthorized host.
- **Authorized Hosts / Networks**
  - Network— Displays the authorized network.
  - Description— Displays the description for the authorized host name.
- **Authentication Details**
  - **RADIUS Configuration**
    - Server Enabled— Displays if RADIUS is enabled or displayed.
    - IP Address— Displays the host name or IP address.
    - Port— Displays the configured port.
  - **LDAP Configuration**
    - Server Enabled— Displays if LDAP is enabled or displayed.
    - IP Address— Displays the host name or IP address
    - Port— Displays the configured port.
    - Decryption Enabled— Displays if decryption is enabled or displayed.

View NTBA Appliance reports

The NTBA Appliance report displays information on the selected NTBA Appliance. Information includes device name, serial number, port configuration, flow information, general settings, IP settings to the interfaces, exporters settings, SNMP settings, list of NTBA interfaces, list of inside zones, list of outside zones, and zone elements.

Follow this procedure to view the NTBA Appliance report:

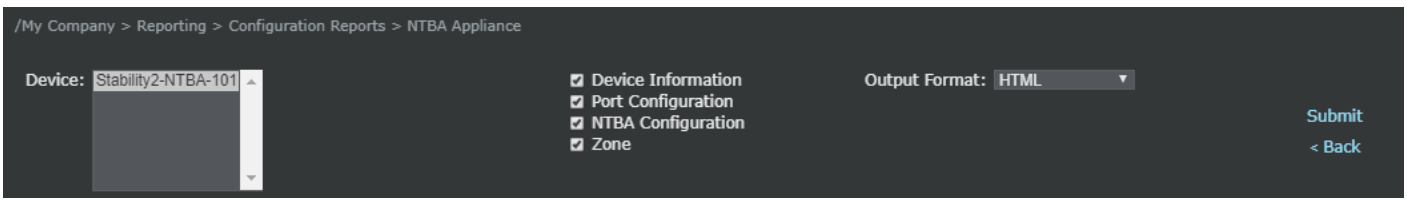
Steps:

1. Select Manager → <Admin Domain Name> → Reporting → **Configuration Reports**.

   The **Configuration Reports** page is displayed.
2. Click the **NTBA Appliance** link.

   The **NTBA Appliance** report page with the configuration options is displayed.

Figure 61. NTBA Appliance report page



3. Configure the following:
   - Select the device for which you want to generate the report from the **Device** field.
   - Select the required checkboxes against **Device Information**, **Port Configuration**, **NTBA Configuration**, and **Zone**.
   - Select the required **Output Format** from the **Output Format** drop-down list.
   - Click **Submit**.

   For the selected admin domain, the NTBA Appliance report displays the following device configuration details:

   1. NTBA Appliance Information for <Device Name>
      a. Name
      b. Model
      c. Serial Number
      d. Software Version
      e. NTBA Appliance Signature Version
      f. Last Signature Set Update
      g. IP Address
      h. Subnet Mask
      i. Default Gateway
      j. Uptime
      k. Last Reboot Time
      l. Contact Information
      m. Location
      n. Gateway Anti-Malware DAT Version
      o. Gateway Anti-Malware Engine Version
      p. Anti-Virus DAT Version
      q. Anti-Malware Engine Version
   2. Current NTBA Port Configuration for device <Device Name>:
      a. Port Settings
         i. Port #
         ii. Port Type
         iii. Configuration
            A. Speed
            B. Duplex
         iv. Administrative Status
         v. Operational Status
   3. Flow Information
      a. Flow Protocol Supported

4. Proxy Server Settings
    a. Use Parent Settings?
    b. Use Proxy Server?
    c. Proxy Server Name or IP Address
    d. Port Number
    e. User Name
5. NTBA General Settings
    a. Use Global Settings?
    b. NTBA listening port for flow records
    c. Enable De-duplication?
6. IP Settings to the NTBA interfaces
    a. IP Address
    b. Network Mask
    c. Gateway IP
7. Exporters
    a. Name
    b. IP Address
    c. Type
    d. Enabled
    e. Description
    f. Flow Type and Version
8. SNMP Settings for exporter
    a. Use Global settings?
    b. UDP Port
    c. SNMP Version
    d. Read-Only Community String
    e. SNMP Polling Interval Time
9. List of NTBA-ready Interface
    a. Enabled
    b. Name
    c. External?
    d. Description
10. Gateway Anti-Malware Engine Updating
    a. Use Parent Settings?
    b. Enabled ?
    c. Update Interval

11. Active Device Profiling
    a. Enabled ?
    b. Available Zones
    c. Selected Zones
    d. CIDR Blocks
    e. TCP/UDP Ports
    f. Profiling Frequency Schedule
    g. Profiling Frequency Days
    h. Profile Expiration (days)
12. EIA Integration
    a. Use Parent Settings?
    b. Enabled ?
    c. NTBA Listening Port
13. ePO Settings
    a. ePO Server IP Address
    b. ePO Server Port
    c. ePO Server Username
14. Auto Classification Settings
    a. Automatically Allow Executables Signed by a Trusted Certificate Authority?
    b. Automatically Allow Executables Found on the GTI Allow List?
    c. Automatically Block Executables Found on the GTI Block List?
15. Summary of list of inside zones
    a. Name
    b. Description
16. Summary of list of outside zones
    a. Name
    b. Description
17. Zone elements of inside Zones
    a. Zone
    b. Element
    c. Type
18. Zone elements of outside Zones
    a. Zone
    b. Element
    c. Type

View NTBA Configuration Summary reports

The NTBA Configuration Summary report displays information on NTBA Appliance configuration. The settings include spambot detection, Manager Presentation, services, collector details, and exporter settings.

Steps:

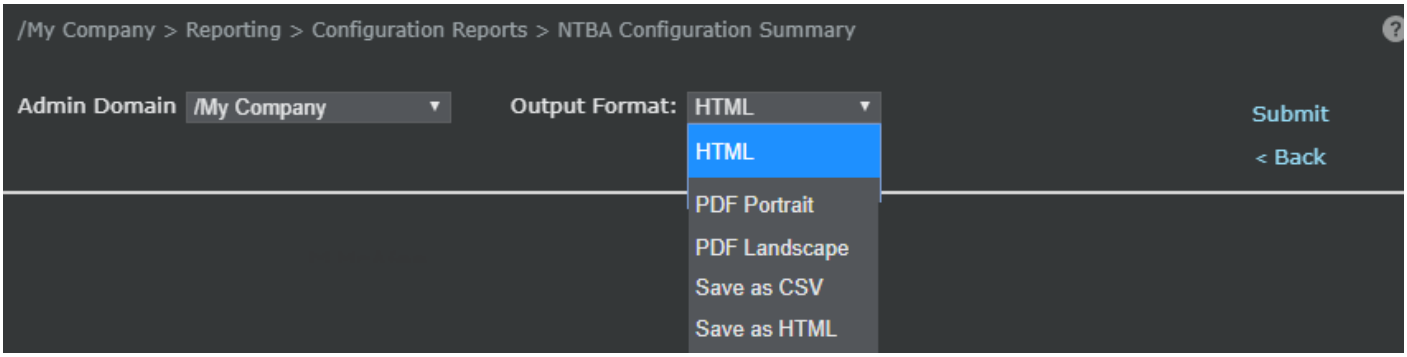
1. Select Manager → <Admin Domain Name> → Reporting → **Configuration Reports**.

   The **Configuration Reports** page is displayed.

2. Click **NTBA Configuration Summary** link.

   The **NTBA Configuration Summary** report page with the configuration options is displayed.

Figure 62. NTBA Configuration Summary report page



3. Configure the following:

   - Select the **Admin Domain** for which you want to generate the report from the drop-down list.

     NOTE

     The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

   - Select the **Output Format** from the drop-down list.
   - Click **Submit**.

   For the selected Admin Domain, the **NTBA Configuration Summary report** is displayed with the following configuration details:

   1. **Spambot Detection**
      a. Email Domain
   2. **Manager Presentation**
      a. The Value of N in Top N lists
      b. Consider Endpoints/Protocols "New" if Seen for First Time Within (days)
      c. Consider Endpoints/Protocols "New" if Seen for First Time With Reference Days As (days)

d. Consider Endpoints/Protocols "Active" if Seen for First Time Within (days)

3. **Services**
   a. Name
   b. Enabled?
   c. Service Details
4. **Collector Details**
   a. Listen for flow information on UDP Port
   b. Enable De-duplication
   c. Primary Name Server
   d. Secondary Name Server
   e. Refresh Interval (hours)
5. **Exporter Settings**
   a. UDP Port
   b. SNMP Version
   c. Read Only Community String
   d. SNMP Polling Interval Time

Generate Performance Monitoring - Admin Domain Configuration reports

The **Performance Monitoring - Admin Domain Configuration** report displays information on admin domain wise configuration made in the Manager.

Follow this procedure to generate the admin domain report.

Steps:

1. Click the **Manager** tab from the Manager home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Performance Monitoring - Admin Domain Configuration**.

   The configuration options of the **Performance Monitoring - Admin Domain Configuration** is displayed.
3. Select a filter from the **Admin Domain** drop down list.

   NOTE

   The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.
4. Select or clear the checkboxes against **Metrics**, **Thresholds** and **Display**.
5. Select the **Output Format**.
6. Click **Submit**.

   The **Performance Monitoring - Admin Domain Configuration** report is generated.

Generate Performance Monitoring - Sensor Configuration reports

The **Performance Monitoring - Sensor Configuration** report displays information on Sensor configuration settings made in the Manager.

Steps:

1. Click the **Manager** tab from the Manager home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Performance Monitoring - Sensor Configuration**.

   The configuration options of **Performance Monitoring - Sensor Configuration** report is displayed.
3. Select the Sensors to be included against Sensors. Select or clear checkboxes against **Metrics** and **Thresholds**.
4. Select the **Output Format**.
5. Click **Submit**.

   The **Performance Monitoring - Sensor Configuration** report is generated.

Generate QoS Policy Report

The QoS Policy Report details the configuration information for each port on the Sensor.

To generate a report for the QoS policies, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **QoS Policy**.
3. Select a filter from the **Admin Domain** drop-down list.

   NOTE

   The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.
4. Select **QoS Policy**.
5. Select the **Output Format**.
6. Click **Submit**.

Generate Reconnaissance Policy reports

Th Reconnaissance Policy report allows users to see their Reconnaissance attack list and their customization done on selected policies. Users can select multiple reconnaissance policies at the same time.

NOTE

Only Reconnaissance policies visible to the admin domain are shown.

To generate a report displaying all current policies in the Reconnaissance Policy Editor, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Reconnaissance Policy**.
3. Select one or more Reconnaissance Policies.

   > **TIP**
   >
   > Reconnaissance Policy Reports can be very long when multiple policies are selected. Trellix recommends selecting a single policy for ease of readability.

4. Select one or more of the following based on what information you want to see in the report:
   - **Customized Attacks**— Consolidates all user-customized attacks into one section
   - **Recon Attacks**— This is enabled only if the selected policy is Trellix Global IDS.
5. Select the **Output Format**.
6. Click **Submit**.

   The **Reconnaissance Policy** report is generated.

Generate Attack Set Profile reports

The attack set profile report provides a detailed view of the attack set profiles available for the application. This includes any user-created or user-cloned attack set profiles. Attack set profile information includes severity, responses, notifications, and other information configured for each Exploit attack, whether from a pre-configured or user-customized attack set profile.

To generate a report displaying all current attack set profiles in the Attack Set Profile Editor, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Attack Set Profile**.
3. Select one or more **Attack Set Profiles**.

   > **TIP**
   >
   > Attack set profile Reports can be very long when multiple attack set profiles are selected. Trellix recommends selecting a single attack set profile for ease of readability.

4. Select the **Output Format**.
5. Click **Submit**.

Generate Scanning Exception reports

The Scanning Exceptions report provides a detailed view of the scanning exceptions that are configured on the device's VLAN, TCP, or UDP port. Scanning exceptions information includes the type of exception and the assigned interface.

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Scanning Exceptions**.
3. Select the **Devices**.
4. Select one or more exceptions — VLAN, TCP, and UDP.
5. Select the **Output Format**.
6. Click **Submit**.

Generate User Activity reports

The Audit report enables you to view the actions performed by Trellix IPS users. Similar to the generating a user activities audit option, this report allows you to view the actions of all users or a single user in one or more admin domains.

> **NOTE**
>
> You can create report templates and also schedule report generation on a daily or weekly basis for the Audit report.

To generate an audit report, do the following:

Steps:

1. On the Manager Home page, click the **Manager** tab.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **User Activity**.
3. Select a filter from the **Admin Domain** drop-down list.

   > **NOTE**
   >
   > The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

4. Select whether or not to include audit data from all child domains of the selected domain. (**Include All Child Admin Domain Audit Data**)
5. Select "All Users" or a single user to audit. (**Select User(s) to Audit**)
6. Select one or more **Audit Categories**. By default, all categories except Unspecified are selected. Audit categories are areas/resources where users can perform actions. Choose from the following (examples of each provided):
   - Unspecified — All actions not covered by the other categories
   - Admin Domain — Created an admin domain, generated a system log
   - User — Logged into the system, created a user, assigned a role to a user

- Manager — Configured proxy server settings
- Sensor — Configured ports, pushed configuration changes
- IPS Policy — Created a policy, cloned a attack set profile
- Report — Designed a scheduled report template, generated a report
- Update Server — Configured Update Server settings, downloaded software
- Operational Status — Delete Manager or Sensor related faults.
- Alert — Acknowledge alerts, delete alerts.
- NTBA — Reports all the network threat behavior analysis
- FIPS Self Test — Reports all the audits related to FIPS mode crypto activity
- ePolicy Orchestrator — Audit events related to ePO
- Controller — Checks the Controller-Manager registration status

7. Select **Show Details** to include detailed audit information in the report output, such as Date and Time when a change was made, username against each change, etc.
8. Type the number of audit messages to show. The default is 10 messages. (**Show x messages**)
9. Select from one of the following time options:
   - **Up to Current Time** — Displays the requested number of most recent messages
   - **Ending (All messages before this date will be displayed)** — Displays the requested number of messages starting from this time and proceeding backwards
   - **Select Messages Between These Dates** — Select the desired range of dates for activity by a user.
10. Select the **Output Format**.
11. Click **Run Report** to start the audit.
    - The fields displayed in the audit result are as follows:
      - Date — When an action was performed
      - Admin Domain — The domain in which the action was performed
      - User — Who performed the action
      - Attack Category — Audit category. That is, area/resource, where action was performed.
      - Action — Short description of the performed action
      - Result — Status of the performed action as either "Success" or "Failure"
      - Description — Verbose description of the performed action
    - The following additional fields are displayed if **Show Details** is selected:
      - Commit Comments — Comments that the user entered before committing the policy changes
      - Audit Data Details — Details of the changes made

Generate Version Summary reports

The Version report provides information on the software and signatures versions currently loaded on the Manager and all devices. Signature and software versions do not run in parallel and may not be similar.

To generate an Version Summary report, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Version Summary**.
3. Select the **Output Format**.
4. Click **Submit**. The **Version Summary** report is displayed.

   The Version Summary report gives the following details:

   - **Version Information for Intrusion Prevention System Manager**

   The field details are described in the following table:

Field Name	Description
Trellix IPS Manager Version	Currently running Manager software version.
Current Signature Set Version	Latest signature version available on Manager for download to Sensors for policy enforcement. **NOTE** The latest signature version may be available on Manager and not yet loaded to the Sensor.
Current Callback Detectors Version	Latest version of callback detectors.

   - **Software Ready for Installation**— The Sensor software version last downloaded to the Manager from Trellix IPS Update Server. This version may or may not have been applied to your devices. Different device platforms may have different available software versions.
   - **Device Version Information**

   The field details are described in the following table:

Field Name	Description
Device (Failover Pairs)	Names of Sensors/failover pairs currently deployed.
Model	Names of the models.
Signature Set Version	The signature set version loaded and running on a device. The signature version on the device may be different than the latest available on the Manager.
Callback Detectors Version	The callback detector's version loaded and running on a device.
Software Version	The software version loaded and running on a device. The software version on the device may be different than the latest available on the Manager.
Gateway Anti-Malware	The current versions of the Gateway Anti-Malware DAT and Engine.
Anti-Malware	The current versions of the Anti-Malware DAT and Engine.

Generate the Licenses report

The licenses report list the **Trellix Virtual IPS Licenses**, **Managed Trellix Virtual IPS Sensors**, **Proxy Decryption Licenses**, **Proxy Decryption License Usage Per Sensor Model**, **Sensors with missing System Licenses**, and **System License**.

Steps:

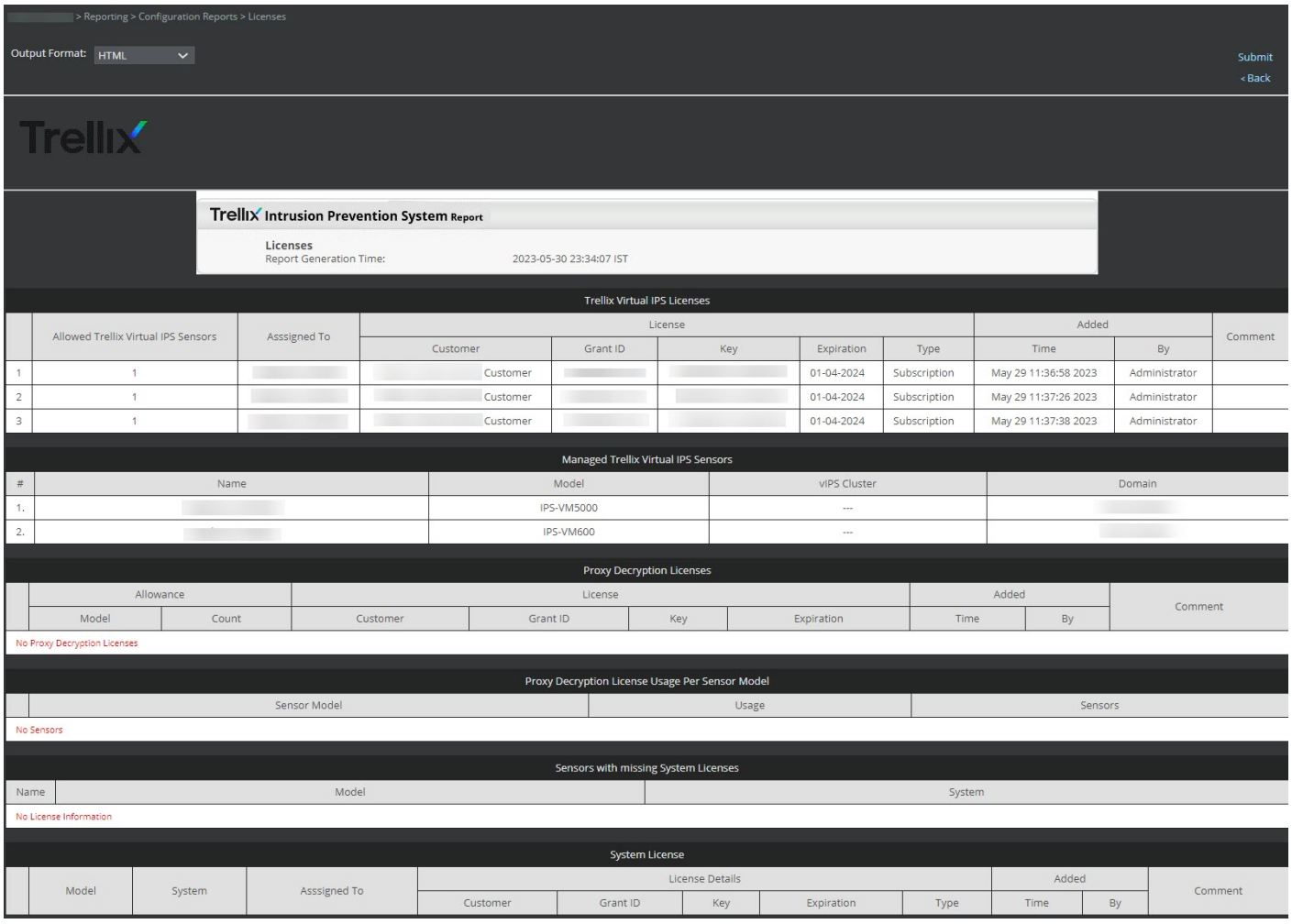
1. In the Manager, go to Manager → <Admin Domain Name> → Reporting → **Configuration Reports**.
2. Click **Licenses**.
3. Select the **Output Format**.
4. Click **Submit**.

   The field descriptions for each table in this report are as follows:

   - **Trellix Virtual IPS Licenses**
     - Allowed Trellix Virtual IPS Sensors - Displays the details of allowed vIPS Sensors.
     - Assigned To - Displays the Sensor name.
     - License
       - Customer - Displays the name of the associated customer.
       - Grant ID - Displays the details of grant ID.
       - Key - Displays the key details.
       - Expiration - Displays the timestamp of expiry.
       - Type - Displays the type of subscription
     - Added
       - Time - Displays the timestamp.
       - By - Displays the name of the user.
     - Comment
   - **Managed Trellix Virtual IPS Sensors**
     - #
     - Name - Displays the name.
     - Model - Displays the model details of the Sensor.
     - vIPS Cluster - Displays the details of the associated cluster.
     - Domain - Displays the domain name details.
   - **Proxy Decryption Licenses**
     - Allowance
       - Model - Displays the model details of the Sensor.
       - Count - - Displays the total count.
     - License
       - Customer - Displays the name of the associated customer.
       - Grant ID - Displays the details of grant ID.

        - Key - Displays the key details.
        - Expiration - Displays the timestamp of expiry.
    - Added
        - Time - Displays the timestamp.
        - By - Displays the name of the user.
    - Comment
- **Proxy Decryption License Usage Per Sensor Model**
    - Sensor Model - Displays the model details of the Sensor.
    - Usage - Displays the usage details of the proxy decryption license.
    - Sensors - Displays the domain details of Sensors.
- **Sensors with missing System Licenses**
    - Name - Displays the name of the Sensor.
    - Model - Displays the model details of the Sensor.
    - System - Displays the rate in Gbps.
- **System License**
    - Model - Displays the model details of the Sensor.
    - System - Displays the rate in Gbps.
    - AssignedTo - - Displays the domain details of an assignee.
    - License Details
        - Customer - Displays the name of the associated customer.
        - Grant ID - Displays the details of grant ID.
        - Key - Displays the key details.
        - Expiration - Displays the timestamp of expiry.
        - Type - Displays the type of subscription.
    - Added
        - Time - Displays the timestamp.
        - By - Displays the name of the user.
    - Comment

The **Licenses** report is generated.



> Reporting > Configuration Reports > Licenses

Output Format: HTML

Submit
< Back

Trellix

Trellix Intrusion Prevention System Report

Licenses
Report Generation Time: 2023-05-30 23:34:07 IST

Trellix Virtual IPS Licenses

	Allowed Trellix Virtual IPS Sensors	Asssigned To	License					Added		Comment
			Customer	Grant ID	Key	Expiration	Type	Time	By	
1	1		Customer			01-04-2024	Subscription	May 29 11:36:58 2023	Administrator	
2	1		Customer			01-04-2024	Subscription	May 29 11:37:26 2023	Administrator	
3	1		Customer			01-04-2024	Subscription	May 29 11:37:38 2023	Administrator	

Managed Trellix Virtual IPS Sensors

#	Name	Model	vIPS Cluster	Domain
1.		IPS-VM5000	---	
2.		IPS-VM600	---	

Proxy Decryption Licenses

	Allowance		License				Added		Comment
	Model	Count	Customer	Grant ID	Key	Expiration	Time	By	

No Proxy Decryption Licenses

Proxy Decryption License Usage Per Sensor Model

	Sensor Model	Usage	Sensors

No Sensors

Sensors with missing System Licenses

Name	Model	System

No License Information

System License

	Model	System	Asssigned To	License Details					Added		Comment
				Customer	Grant ID	Key	Expiration	Type	Time	By	

Automation of reports

You can schedule reports to be automatically generated and emailed on a daily or weekly basis. You can schedule the IPS Reports as well as Configuration Reports. This enables convenient and regular forensic analysis of the alerts and user-activity details.

After a scheduled report is generated, it is emailed to the list of recipients that you can specify. The generated report is also saved in Manager server for viewing.

NOTE

The scheduling of reports in the Central Manager is similar to that in the Manager.

Scheduling reports

Click the **Manager** tab on the Home page and select <Admin Domain Name> → Reporting → Report Automation → **Automation Settings**.

The **Automation Settings** page enables you to do the following:

- Add, or edit, or delete scheduled report template
- Edit report scheduler

You can click **Recipient List** link to add recipients for a scheduled report.

Field Name	Description
State	Displays the state of report. A green tick mark indicates that the report is enabled. A red cross mark indicates that the report is disabled.
Name	Displays the name of report.
Report Type	Displays the type of report.
Last Modified	Displays the date and time of the latest modification done on the report.
Frequency	Indicates the frequency report to be generated(Weekly or Daily).
E-mail To	Displays the email address of the recipient receiving the report.

Add automated reports

You can add a scheduled report template which enables you to schedule a new report that generates automatically and emailed regularly. You can schedule a report for any of the IPS Reports and Configuration Reports. When you schedule a report, you need to specify the parameters for the report (Example: **Admin Domain**, **Sensor**).

To schedule a report:

Steps:

1. Click the **Manager** icon from the Home page.
2. Select <Admin Domain Name> → Reporting → Report Automation → **Automation Settings**.

   The **Automation Settings** page is displayed.
3. Click  .

   The **Add an Automated Report** page is displayed.

   The **Enable?** field is enabled by default.

   1. Select the **Report Category** — **IPS Events** or **Configuration Reports**.
   2. Select the **Report Type**. Based on this selection, the template fields change to fit the elements of the selected report. Only those fields that are common to all report types are described in this section.
      - Traditional-IPS Event reports
        - Big Movers report
        - Executive Summary report
        - Reconnaissance Attacks report
        - Top N Attacks report
        - Trend Analysis report

        - User Defined report
    - Traditional-Configuration reports
        - Attack Set Profile report
        - Device Summary Report
        - Faults report
        - Firewall Policy Definitions report
        - IPS Policy Assignment report
        - IPS Policy Details report
        - IPS Sensor report
        - Licenses
        - NTBA Appliance report
        - NTBA Configuration Summary report
        - Performance Monitoring - Admin Domain Configuration report
        - Performance Monitoring - Sensor Configuration report
        - QoS Policy
        - Reconnaissance Policy report
        - Scanning Exceptions
        - User Activity report
        - Version Summary
3. For Configuration reports
    - Type a **Template Name**.
    - Type a **Description** that summarizes the report. The maximum length is 254 characters. This is for future reference.
    - Choose a **Report Frequency** as either **Hourly, Daily**, **Weekly** or **Monthly**. The default is **Weekly**.
    - Select a required **Attack Set Profile**.
    - Select **Report Format**. The options are:
        - **PDF Portrait**
        - **PDF Landscape**
        - **Save as HTML**
        - **Save as CSV**

    For IPS Events
    - Type a **Template Name**.
    - Type a **Description** that summarizes the report. This is for future reference.
    - Choose a **Report Frequency** as either **Hourly, Daily**, **Weekly** or **Monthly**. The default is **Weekly**.
    - Select the **Admin Domain**.
    - Select a device in the **Sensor**.

- Select **All Devices** to displays all devices.
- Select **By Device** to display individual devices.
- Checking the check box for **Include Child Admin Domains** displays all the devices in the child domain (By default the check box is unchecked).

- **Attack Severity** — Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities which relate to attack impact.
- **Ranking Basis** — Select one of the following:
  - Percentage change in attack count
  - Change in attack account value
- **Direction** — Select one of the following directions of how alerts occurred should be displayed:
  - **Upward Movers only**
  - **Upward and Downward Movers**
  - **Downward Movers only**
- **Maximum Movers** — Enter the value of maximum occurred alerts to be displayed.
- **Comparison Interval** — Enter the time period. The time period is in days.
- Select **Report Format**. The options are:
  - **PDF Portrait**
  - **PDF Landscape**
  - **Save as HTML**
  - **Save as CSV**

> **NOTE**
>
> The **PDF** option appears disabled if you had selected the **Report Frequency** as **Monthly**.

4. Click **Next**. The **Select Recipients** page appears.
5. Select the recipients from the grid.
6. Click **Finish**.

Add or edit scheduled report settings

When you schedule a report, you set a time and day (for weekly reports) when you want the report to be generated (to schedule a report, select Reporting → Report Automation → **Report Scheduler**). The report is then generated on a recurring basis for the set time/day. The Edit action in the **Automation Settings** page enables you to enable/disable and set global generation times for your daily, weekly and monthly reports.

> **NOTE**
>
> When scheduling weekly and daily reports, make sure to give 2 hours between the times when weekly and daily reports are generated. For example, if you schedule daily reports to run at 9:00 AM, set your weekly reports to run either before 7:00 AM or after 11:00 AM. This will save Manager processing cycles.

To modify report schedule settings:

Steps:

1. Click the **Manager** tab from the Home page.
2. Select <Admin Domain Name> → Reporting → Report Automation → **Automation Settings**.
3. Click .

   The **Report Scheduler** page is displayed.
4. Select **Yes** to enable hourly, daily, weekly or monthly reporting.

   NOTE

   Select **No** and click **Save** to disable daily, weekly or monthly reporting.
5. Select the **Report Generation Time**. For **Weekly** reports, also select the day of the week.

   For the **Monthly** reports, select the day of the month. For example, if you configure monthly scheduler with date selected is 01 and the hour as 8:00, the monthly report gets generated on 1st of every month at 8:00 am in the morning.
6. Click **Save**.

Add recipient lists for a scheduled report

You can maintain a global list of email addresses for all scheduled reports functions. You must add email entries for all individuals or groups you want to receive scheduled report information. After the email entry is added, you can then apply the email address to receive a generated scheduled report.

To add a recipient email to the list, do the following:

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Report Automation → **Recipient List**.

   The **Recipient List** page is displayed.
3. Click .

   The **Add Recipient** page is displayed.
4. Type a **First Name**, **Last Name**, and **Email** address for the new recipient.
5. Select the **Language** from the list.
6. Click **Save**. The added recipient and email address appears in the **Recipient List** table. You can now apply a recipient to a scheduled report.

View scheduled reports

You can view a list of reports that are generated and mailed as part of the report scheduling process. Do the following steps to view the sent reports.

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Report Automation → **Automatically-Generated Reports**.

   The **Automatically-Generated Reports** page is displayed.
3. Select a sent report and do one of the following:
   - Click **Email Now** to view the recipients list in **Recipient List** page. For more information on **Recipient list** page see, Adding recipient list for scheduled report (page 277).
   - Click **View in** to view the report.
   - Click **Delete** to remove the report.

Configure preferences

You can configure header, footer, output limits, and language from the Manager or Central Manager.

NOTE

The fields in the **Preferences** sub-menu in the Central Manager are similar to the ones in the Manager.

Set headers and footers

To edit the header & footer settings:

Steps:

1. Select Manager → <Admin Domain Name> → Reporting → Preferences → **Header and Footer**.
2. Click
3. Select **Text** from the drop down list to add text that you want to display in the report header.
4. Click **Edit Logo** to change the logo in the header. The Trellix logo is displayed by default.
5. Select the text that you want to display in the report footer. The options are:
   - Page Number
   - Date/Time
   - Text
6. Click **Save**.

Set language preference

The **Language** sub-menu allows you to set the language preference.

To set the language preference:

Steps:

1. Select Manager → <Admin Domain Name> → Reporting → Preferences → **Language**.

   The **Language** page is displayed.

2. Select a **Language** from the list.
3. Click **Save**. The selected language will be applied across all pages.

Configure Output Limits

To edit the output limits settings:

Steps:

1. Select Manager → <Admin Domain Name> → Reporting → Preferences → **Output Limits**.
2. Set a limit for **Maximum number of records return per query**
3. Click **Save**.

Maintenance

Managing your Trellix IPS Manager database

Network security is an ongoing process that requires a long-term plan for archiving and maintaining your database for the alerts and packet logs generated by your deployed Sensors. Archiving this information is necessary for historical analysis of alerts that may help you better protect your network in the future.

All sizing estimates are based on tests of various alert/log generation frequencies. Multiple frequency and file size parameters are offered to help you better prepare your database for long-term maintenance.

As alerts and packet logs gradually accumulate in your database, the disk space allotted to your Trellix IPS processes will require thoughtful planning and maintenance to keep up with the frequency and size of incoming data. Depending on your archiving needs, it is essential that you understand the database space required to maintain an efficient system.

One question to ask yourself is: "If my Sensors generate one alert every ten seconds for a year, how much database space will I need to maintain all of these alerts?"

With that question in mind, the following topics are presented to help you get the most out of Trellix IPS Manager and database:

- Capacity planning— Ensure that resource requirements are met for optimal performance.
- Database maintenance and tuning— Perform regular database tuning to ensure optimal performance.
- Database backup and recovery— Backup and archive to protect against hardware/software failure.
- Maintenance tab in Manager— File pruning of the generated log data and files.
- Using the Database Admin Tool— A standalone tool for maintaining your Manager database.

Capacity planning for Manager database

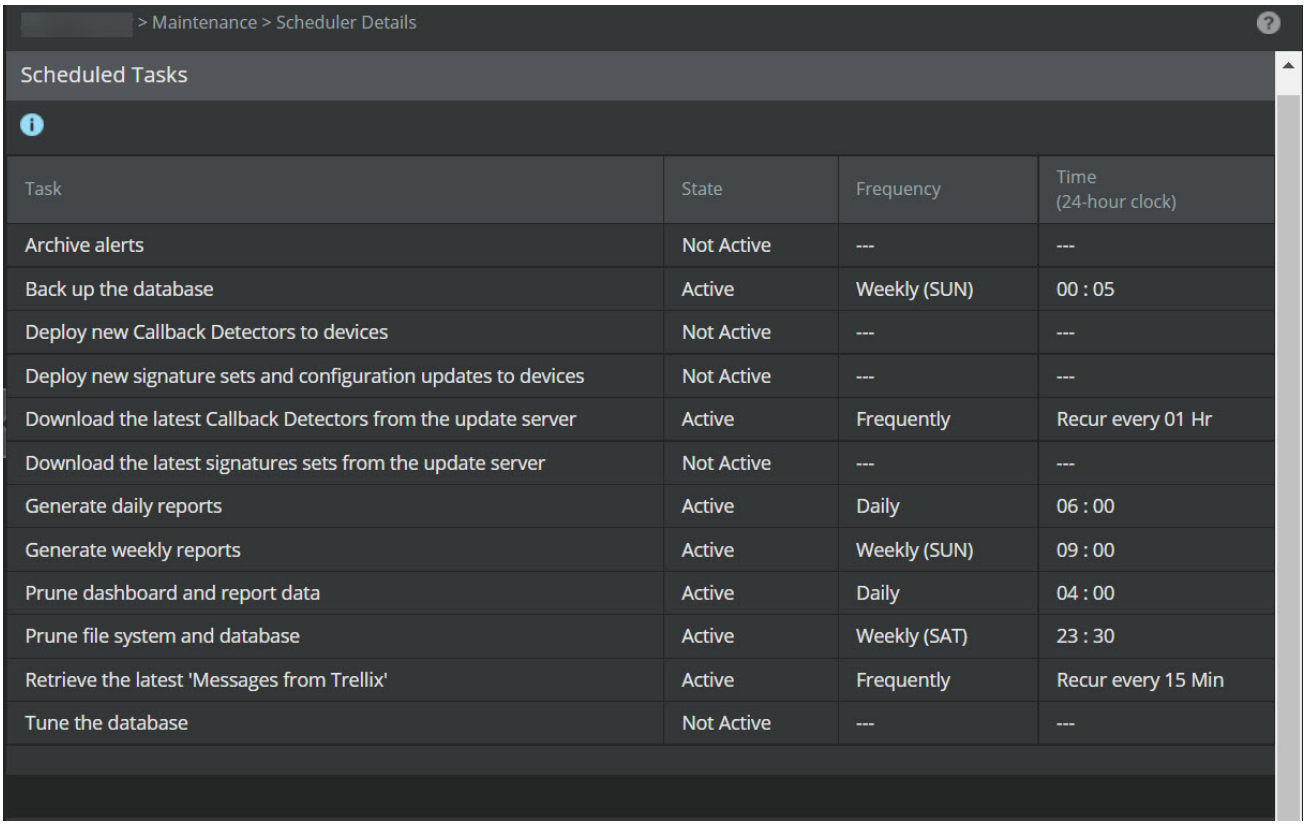
One of the first tasks to complete when you are deploying Trellix IPS is the installation and setup of your database. The database houses the alert and packet log data generated by the Sensors. The integrity and availability of this data is essential to a complete Trellix IPS experience.

Scheduler Details

The **Scheduler Details** provides the details of overall scheduled processes in the Manager. You can view these details from Manager → Admin Domain Name → Manitenance → **Scheduler Details**. It includes data backups, database maintenance, file

maintenance, and other actions. Based on this information, you can choose an appropriate time for the backup you are currently scheduling.

Figure 63. Scheduler Details



Data archive options

The **Archiving** option presents actions that enable you to save alerts and packet logs from the database on demand or by a set schedule.

You can also restore archived alerts and packet logs on the client or another Manager. The procedure for archiving data relating to Sensor and NTBA Appliance is similar.

The archiving action for the Sensor and the NTBA Appliance is done from the Manager → <Admin Domain Name> → Maintenance → **Data Archiving** option of the **Manager** tab tree.

Archive alerts and packet logs

The **Archive Now** action enables you to archive alerts and packet logs on demand into an archival file for future restoration. This process reads alerts and packet logs for the given time range from the database and writes them into a zip file.

NOTE

Archive your alerts and packet logs regularly. We recommend that you archive your alert data monthly, and that you discard alert and packet log information from your database every 90 days to manage your database size. There is a 1 GB size limitation for restoration (import of the file in the Manager) of a single archive file. However, you can extract an archive zip file greater than 4 GB in size but in that case the archived file cannot be restored.

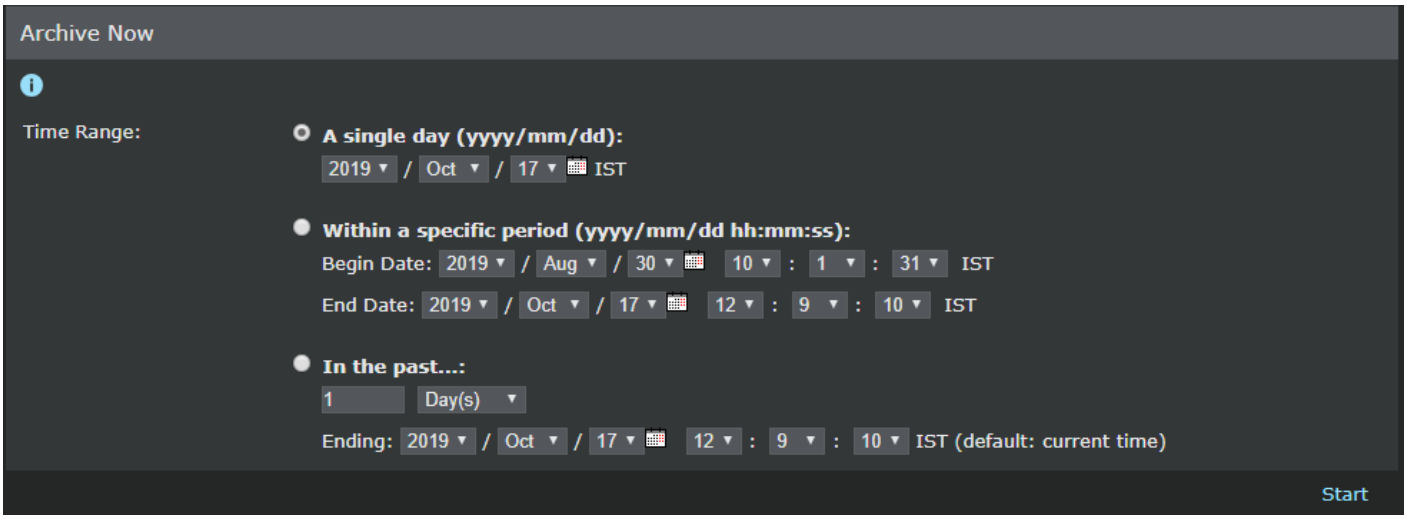
Archived files less than 4GB in size are saved locally to the Manager, and can be exported to your client.

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Data Archiving → IPS → **Archive Now** (Manager → Maintenance → Alerts → Archiving → NTBA → **Archive Now** for the **NTBA Appliance**).

   The **Archive Now** page is displayed.

Figure 64. Archive Now page



2. Choose one of the following time spans in **Time Range**:
   - **A single day (yyyy/mm/dd)** — Select alerts and packet logs for a single day in the format **yyyy/mm/dd**. Default is the Manager system date.
   - **Within a specific period (yyyy/mm/dd hh:mm:ss)** — Select alerts and packet logs between the begin and end dates in the format **yyyy/mm/dd hh:mm:ss**. Default **Begin Date** is the oldest alert detected time and default **End Date** is the Manager system time.
   - **In the past** — Selects alerts from a point in the past relative to the current time. This time in the past can be months, weeks, days (default), or hours. Select a time (**yyyy/mm/dd hh:mm:ss**) when the span of reporting time ends (default is the Manager system time).

3. Click **Start**.

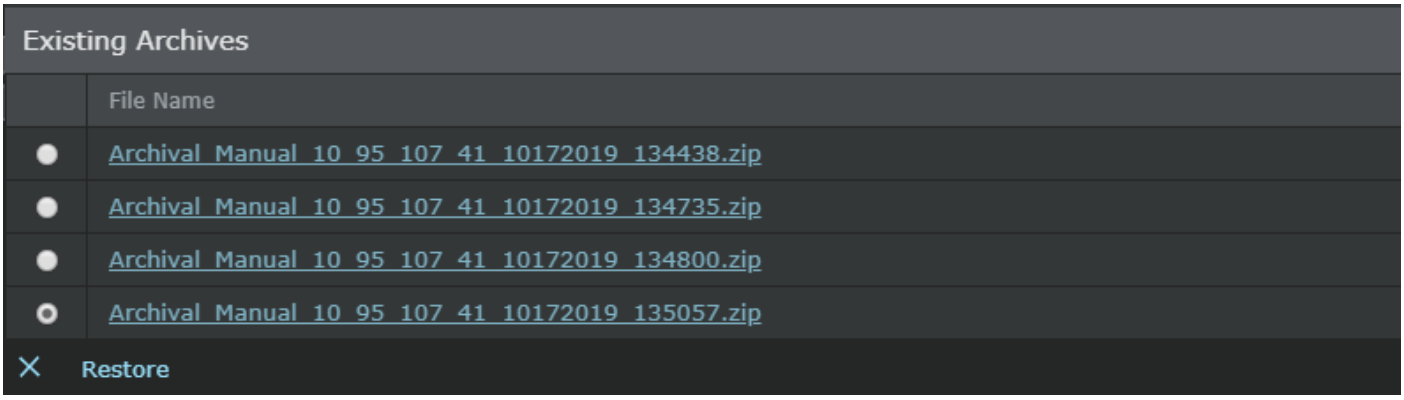
   When the archival process is complete, the file is saved to `<Manager_Install_Dir>\alertarchival`

   The files also appear in the **Existing Archives** page.

   NOTE

   The default Manager installation directory is **`%programfiles%\Trellix\IPS Manager\App`**.

   Figure 65. Existing Archives page

   You can click an archived file listed in the **Existing Archives** page to view the details in the **Archived File Info** page.

4. Optionally, select an archived file in the **Existing Archives** page and click **Export** to download that file from the Manager to your client.

   NOTE

   You can import an exported file into another Manager, such as a test Manager.

Schedule automatic archival

The **Automated Archival** action enables you to set a schedule by which alerts and packet logs are automatically archived.

The scheduled archival process archives alerts and packet logs daily, weekly, or monthly depending on the frequency you select.

If you choose **Weekly** and select a day of the week from the drop-down list, the archival begins from the previous week for the selected day. For example, if you choose **Weekly** and choose **Sunday** as the day of the week, logs from the previous Sunday through Saturday are archived.

If you choose **Monthly**, the archive frequency is the 1st of every month and the logs for the month are archived.

If you choose **Daily**, the logs from the hour 00:00:00 through 23.59.59 from 2 days back are archived. For example, if you set the **Scheduler** to **Daily** on 3-Sep, then the logs from 1-Sep are archived.

NOTE

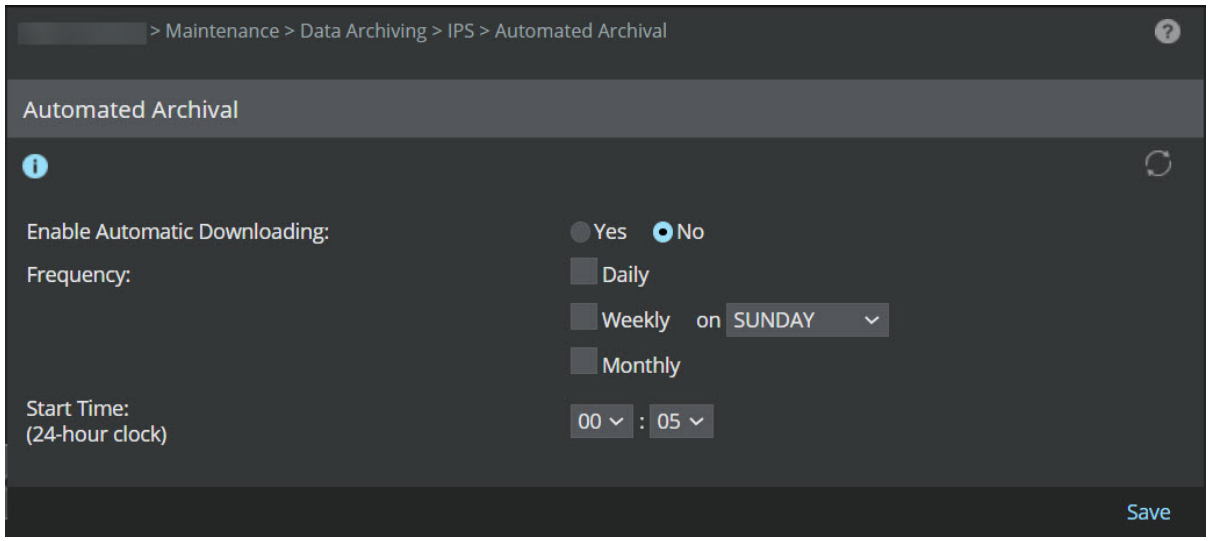
When scheduling archival, set a time when no other scheduled functions (backups, database tuning) are running. The time should be a minimum of an hour after/before other scheduled actions.

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Data Archiving → IPS → **Automated Archival**.

   The **Automated Archival** page is displayed.

Figure 66. Automated Archival page



2. Select **Yes** against **Enable Automatic Downloading** to turn on the scheduling process.
3. Select values for any of the following against **Frequency**:
   - **Daily**
   - **Weekly** — Select the day of the week.
   - **Monthly**
   - **Start Time** — Hours: Minutes (24 hour clock)
4. Click **Save**. Every time the process runs, finished archival is saved to `<Manager_Install_Dir>\alertarchival`

   NOTE

   The default Manager installation directory is **`%programfiles%\Trellix\IPS Manager\App`**.

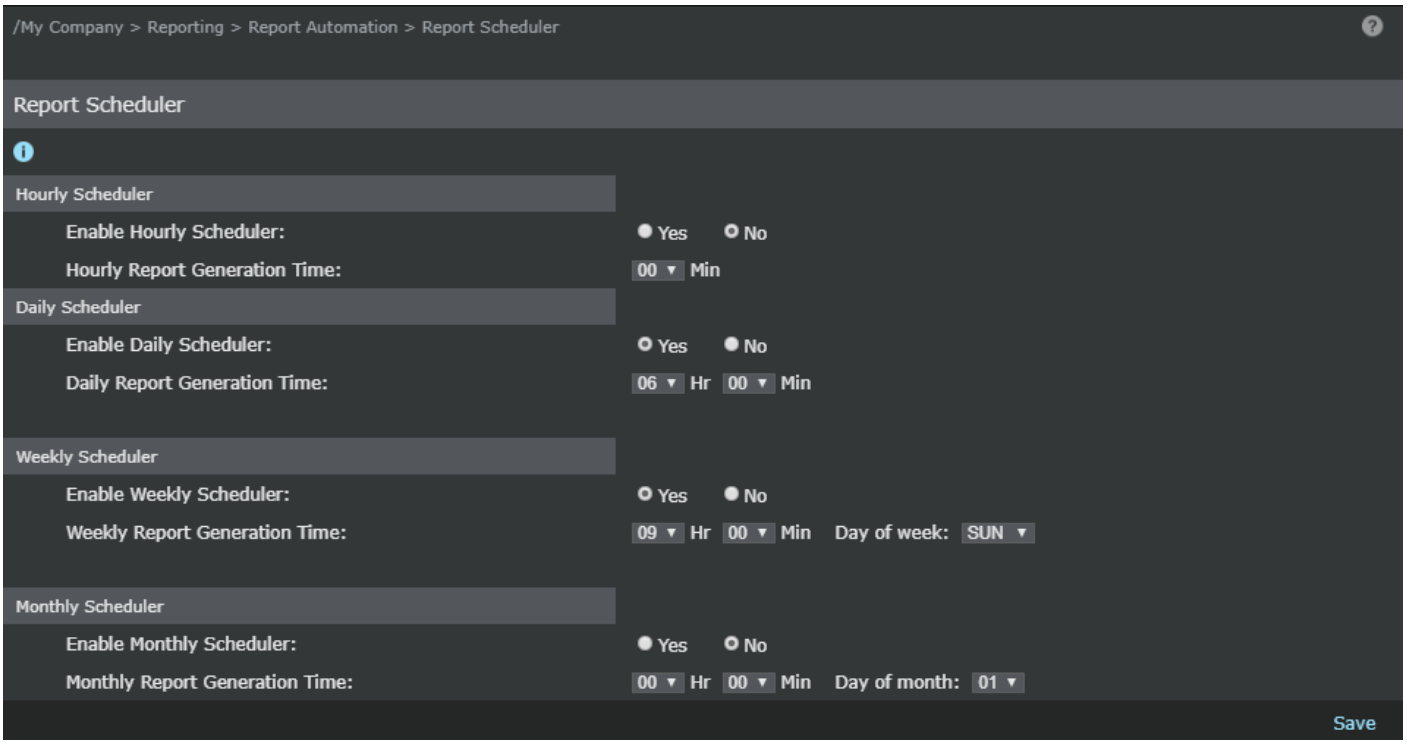
5. Optional:
   - Click to reset the settings to those last applied. This is helpful when you started to make changes but forgot what the last settings were.

- You can also check the present settings for all scheduled processes (including backups, database maintenance, and file maintenance actions) in **Scheduler Details**. To access **Scheduler Details** go to Manager → <Admin Domain Name> → Maintenance → **Scheduler Details**.

How to view scheduled actions

The **Report Scheduler** action enables you to view the settings for the Archival Scheduler as well as the other schedulers configurable within the Manager.

Figure 67. Report Scheduler page



Export an archive

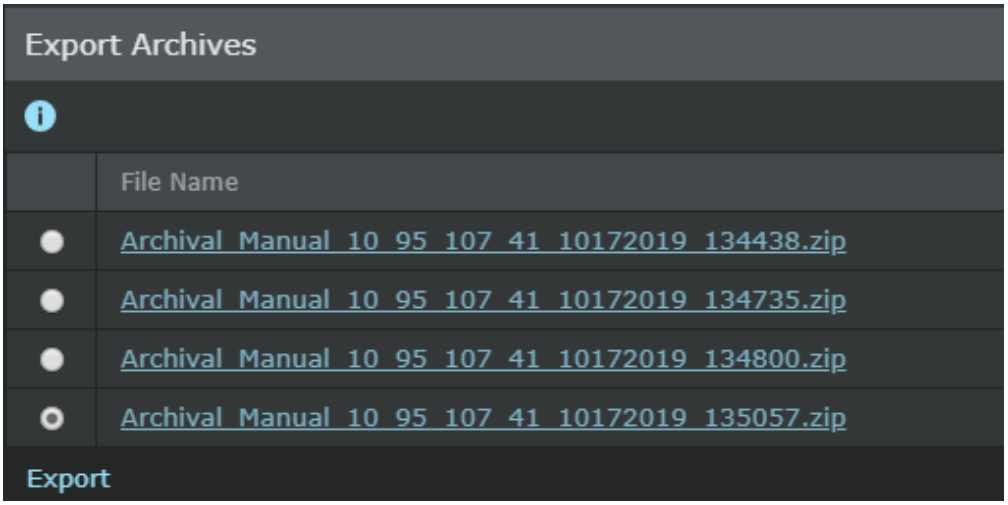
The **Export Archives** action enables you to export an archive from the Manager to your client, or to a location reachable by your client. You can take the exported archival and import (that is, restore) it into another Manager, such as a test Manager.

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Data Archiving → IPS → **Export Archives**.

   The **Export Archives** page is displayed.

Figure 68. Export Archives page



2. Select an archive to export from the list.
3. Click **Export**.

   The **File Download** window of your client machine is displayed.
4. Click **Save** to save the file to a location in your client machine.

Restore an archive

The **Restore** action enables you to restore an archived alerts and packet log files to the Manager. When restoring an archival to a target Manager, the archive must be copied to a directory on the target Manager or a network directory that Manager can access. The **Restore** feature also enables you to filter through the alerts in the archival.

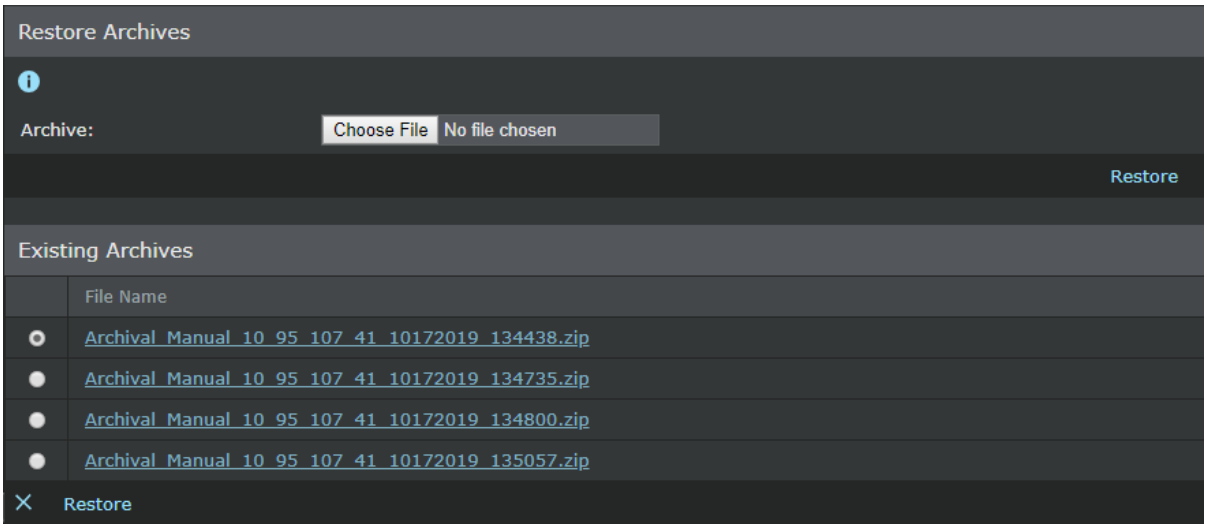
> **NOTE**
>
> To import the file in the Manager, make sure the file size is within 1 GB.

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Data Archiving → IPS → **Restore Archives**.

   The **Restore** page with **Restore Archives** option and **Existing Archives** list is displayed.

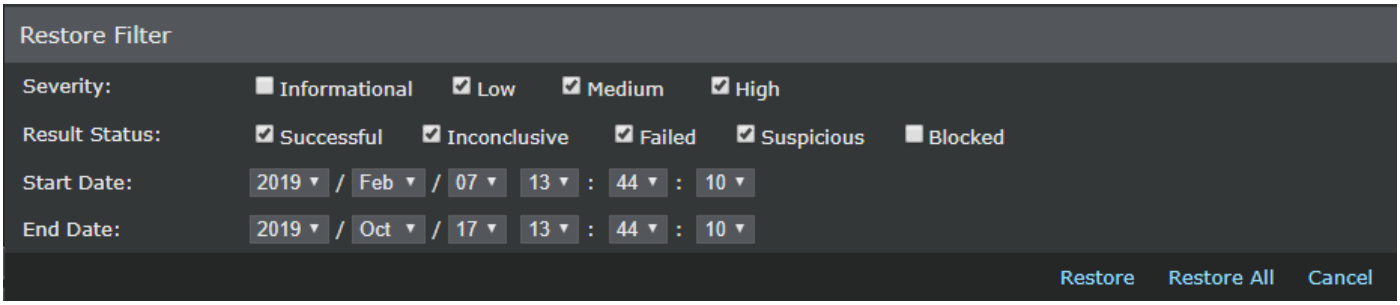
Figure 69. Restore page



2. Do one of the following:
   a. Click **Choose File** to locate the archival or enter the absolute path of the archived file and click **Restore**.
   b. Select an archival listed under **Existing Archives**, and then click **Restore**.

   The **Restore Filter** page is displayed.

Figure 70. Restore Filter page



3. Filter alerts by the following parameters:
   - **Severity** — Select one or more severities to keep.
   - **Result Status** — Select one or more results to keep.
   - **Start Date** — Keep only the alerts and packet logs starting from the designated time.
   - **End Date** — Keep only the alerts and packet logs up to the designated time.
4. Click **Restore**.

> **NOTE**
>
> Click **Restore All** to restore all alerts without any filtering.

NOTE

Manager only permits 300,000 alerts to be restored at a time if filtering is applied. If your archive contains more than 300,000 alerts, you need to perform the restoration process multiple times. For example, if your archival still contains 750,000 alerts after filtering parameters have been met, you will have to restore three times: 1) 300,000 2) 300,000 3) 150,000.

5. To see the alerts restored in attack log, run solr import.

NOTE

To run solr import, refer to *Trellix Intrusion Prevention System Installation Guide*.

Delete archives from the Manager

You can delete archives from the Manager.

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Data Archiving → IPS → **Restore Archives**.
2. Scroll down the page to the list of **Existing Archives**.
3. Select an archival and click .
4. Click **OK** to confirm deletion.

Archive alerts using dbadmin.bat

You can archive alerts and packet logs from either the Trellix IPS user interface or from the standalone database admin tool. However, you can avoid the additional workload on Manager server by using the database admin tool. The archived data is stored in a .zip file at `%programfiles%\Trellix\IPS Manager\App\alertarchival`. Note that data from the following tables are archived:

- iv_alert
- iv_alert_data
- iv_packetlog

Note the following before attempting to archive alerts:

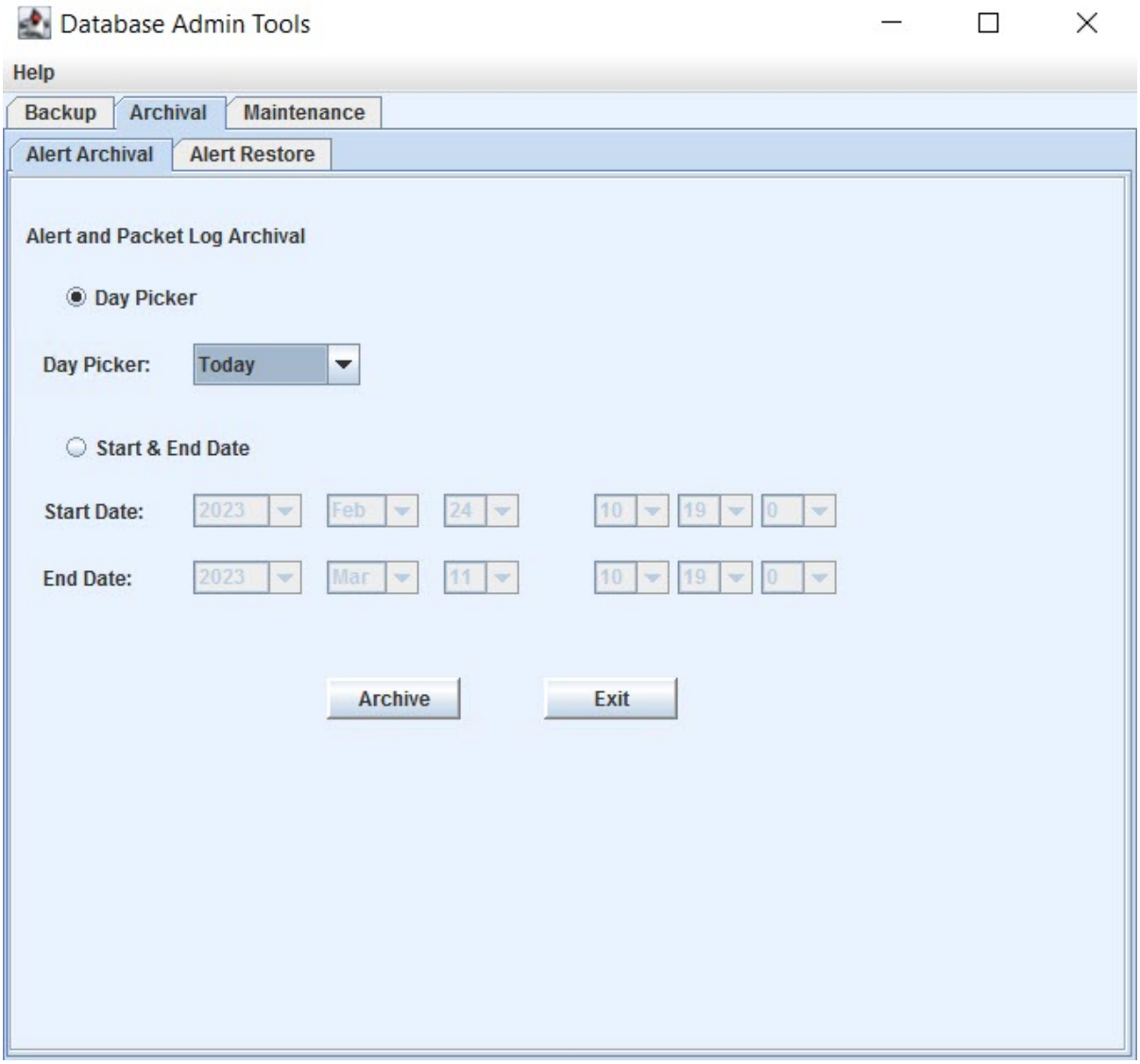
- You can restore alerts only if the major versions of the backed up Manager and the present Manager match. For example, a backup from any 10.1 Manager version can be restored on any other 10.1 Manager version. A backup from a 10.1 Manager cannot be restored on a 11.1 Manager.
- You cannot restore alerts of a later version of the Manager on an earlier version of the Manager. For example, you cannot back up alerts from Manager version 10.1.7.65 and restore it on Manager version 10.1.7.50.

To archive alerts and packet logs using the standalone Database admin tool:

Steps:

1. Navigate to `%programfiles%\Trellix\IPS Manager\App\bin`.
2. Execute the **dbadmin.bat** file. The standalone tool opens.
3. Select Archival → **Alert Archival**.

Figure 71. Database Admin Tools - Alert Archival Settings



4. Specify the time period of the data to be archived either by using the **Day Picker** or by specifying the start date and time and the end date and time.
5. Click **Archive**. Archive Confirmation dialog pop-up appears. Click **Yes**.

   When the process is complete, the archived file is saved to `%programfiles%\Trellix\IPS Manager\App\alertarchival`. This file will also be listed in a table when you restore files using this tool or Manager.

Restore alerts using dbadmin.bat

You can restore archived alerts and packet logs from either the Trellix IPS user interface or from the standalone Database Admin tool. However, you can avoid the additional workload on Manager by using the Database Admin tool.

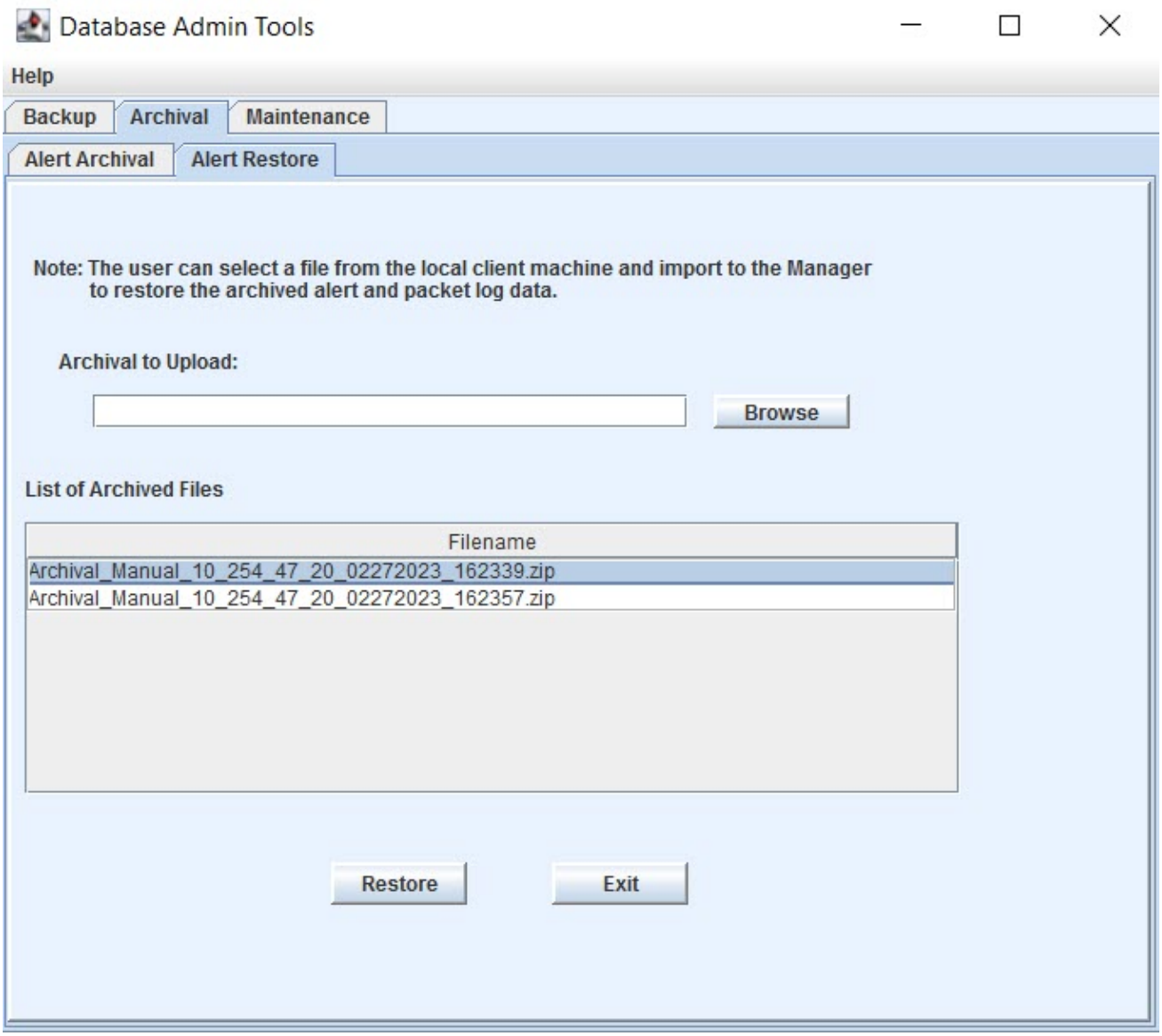
To restore data, the archived data should either be in Manager server or in a computer that is accessible from Manager server. You can also filter data from an archived file and restore just the filtered data. Suppose that there is an archived file containing data generated between Jan 1 and Jan 10. Then you can filter the data generated between Jan 1 and Jan 5 from the archived file and restore just this data.

To restore alerts and packet logs using the standalone Database Admin tool:

Steps:

1. Navigate to `%programfiles%\Trellix\IPS Manager\App\bin`.
2. Execute the **dbadmin.bat** file. The standalone tool opens.
3. Select Archival → **Alert Restore**.

Figure 72. Database Admin Tools - Archival Alert Restore tab



4. Do the following:
   a. Click **Browse** to locate the archival or type the file's absolute path name.
   b. Select the archived file from the **List of Archived Files** and then click **Restore**.

> **NOTE**
>
> Archived data in the `%programfiles%\Trellix\IPS Manager\App\alertarchival` are listed under **List of Archived Files**.

5. Filter the data in the archived file by specifying the start date and time and the end date and time. Only those alerts and packet logs generated during this time frame are restored from the archived file.

NOTE

The start date and time and the end date and time displayed by default in this window indicate the time frame of the archived data that you have selected to restore. Therefore, if you choose the default dates and times, all the data in the archived file will be restored.

6. Click **Restore**.
7. Enter your database user name and password to complete the restoration process.

NOTE

Manager server only permits 300,000 alerts to be restored at a time if filtering is applied. If your archive contains more than 300,000 alerts and you set filtering parameters, you will need to perform the restoration process multiple times. For example, if your archival still contains 750,000 alerts after filtering parameters have been met, you will have to restore three times: 1) 300,000 2) 300,000 3) 150,000.

8. To see the alerts restored in attack log, run solr import.

NOTE

To run solr import, refer to *Trellix Intrusion Prevention System Installation Guide*.

Capacity planning

Every network has slight architectural differences that make each deployment unique. When deploying a network IPS, you must take into consideration the following factors when planning the capacity of your database:

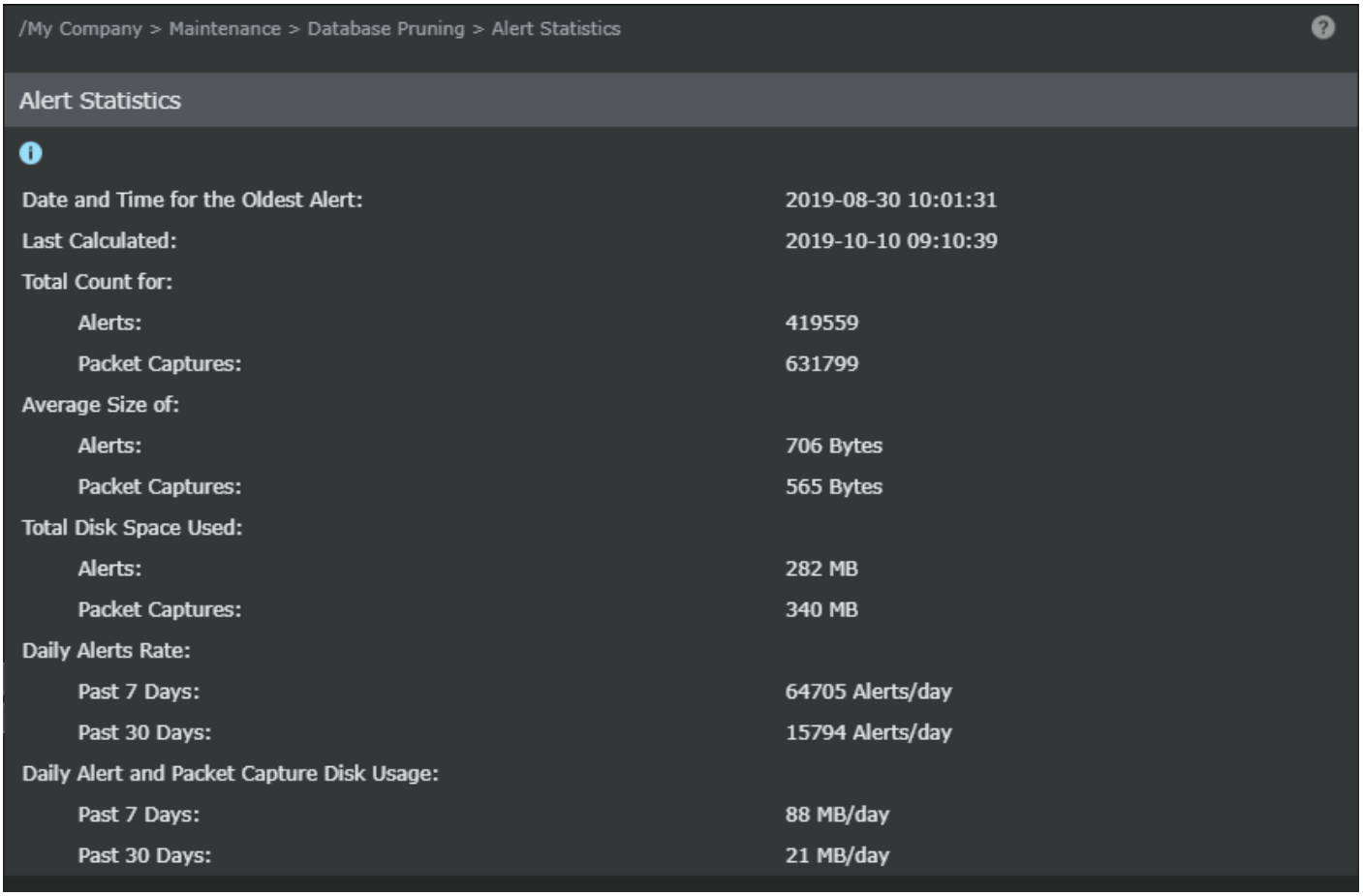
- **Aggregate Alert and Packet Log Volume From All Sensors**— What is the volume in your network? A higher volume will require additional storage capacity.
- **Lifetime of Alert And Packet Log Data**— How long should you archive an alert? Maintaining your data for a long period of time (for example, one year) will require additional storage capacity to accommodate both old and new data.

The following subsections provide useful information for determining the necessary capacity for alerts and packet logs in your database.

Alert Statistics

The **Alert Statistics** option in Manager displays information that helps you track the historical trend of database space usage on a weekly and monthly basis, and also the rate at which data is being inserted into your database. By analyzing the trend of the load factors on your database and your hardware, you can set the threshold for the amount of historical data that you want to store at any given time.

Figure 73. Alert Statistics page



The Manager retrieves and displays the following data from the underlying database:

- Date and Time for the Oldest Alert: displays the date and time
- Last Calculated
- Total Count for
    - Alerts
    - Packet Captures
- Average Size of
    - Alerts
    - Packet Captures
- Total Disk Space Used
    - Alerts
    - Packet Captures
- Daily Alerts Rate
    - Past 7 days

    - Past 30 days
- Daily Alert and Packet Capture Disk Usage
    - Past 7 days
    - Past 30 days

These data are retrieved and displayed to enable timely action for avoiding degradation in performance due to issues like storage limitation or volume of data.

Alert and packet log sizes

Alert frequency is the first factor to consider when planning database capacity. This is separate from packet log frequency since not every alert has an accompanying packet log by default. (Only TCP- and UDP-based attacks generate packet logs by default; you must manually set packet logging for all other Exploit attacks.)

To help you plan your capacity needs, the following statistics have been determined from lab and live environment testing (based on 30,000,000 alerts):

- Alert with no packet log = 200 bytes (average)
- Alert with packet log = 650 bytes (average)

Space for packet logs must also be allocated in your database. The frequency of generated logs is typically less than that of alerts, but a packet log is generally larger in size than an alert. The average size of a packet log is approximately 450 bytes (based on 30,000,000 logs).

Determine average alert rate-weekly

A good reference point for determining your required database capacity based on the volume of alerts and packet logs is to find the average alert rate for a week, then multiply by a longer time frame such as 12 weeks, one year (52 weeks), and so forth. To do this, generate an Executive Summary Report using a one-week time horizon.

Steps:

1. Click Analysis → Event Reporting → **Traditional Reports**.
2. From the IPS Events list, select **Executive Summary**. The **Configure Executive Summary Report** page is displayed.
3. Fill in the following fields to determine the average weekly alert rate:
    - **Admin Domain**— Select the root admin domain (default).
    - **Sensor**— Select All Devices (default if you have more than one Sensor).
    - **Attack Severity**— Make sure all three severities (**Low**, **Medium**, **High**) are checked. When all three are selected, Informational alerts are also included.
    - **Alert State**— Select **View All Alerts**. Both acknowledged and unacknowledged alerts are included for the specified time frame.
    - **Attacks**— Choose **Select Attacks in the past: 1 Week(s)**. You do not need to adjust the "Ending" time fields.
    - **Get summary of**— You do not have to adjust this field.
    - **Report Format**— Select a view of the report information from the following: **HTML**, **PDF** and **Save as CSV**.

4. Click **Run Report** once all of the above fields are set.

   This report displays your alert data in a presentation-style format (that is, tables and colored pie charts). The first pie chart details the "Total Alerts Per Sensor." Simply add the totals from each Sensor to determine the amount for one week.

Database sizing requirements

Based on the average size of an alert without packet, the following graph and table are provided to help you determine the database size required to store alert data for one year based on the number of alerts generated by your Sensors over a one week period.

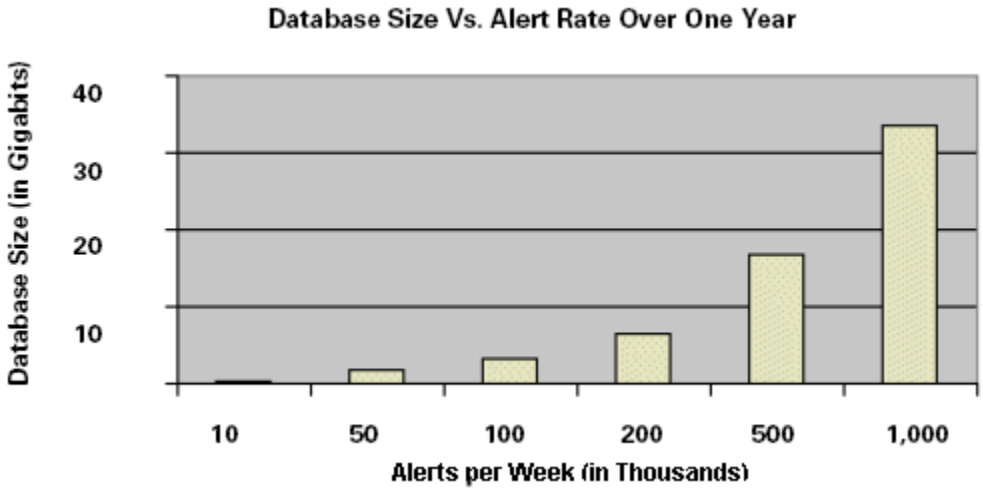
NOTE

For comparison, generation of 10,000 alerts per week is low, while 1,000,000 alerts per week is high. If you are generating 1,000,000 alerts per week, it is recommended that you check your applied Trellix IPS policies to determine if you are applying a policy that is an "exact" match for your protected network environment.

NOTE

The following graph and table estimate size based on alerts both with and without associated packet logs. Thus, the size of alert data has been estimated from both lab and live environments.

Figure 74. Database Sizing - Graphical view



Alerts/Week	DB Size (One Year) in GB
10,000	0.3
50,000	1.7
100,000	3.3
200,000	6.7

Alerts/Week	DB Size (One Year) in GB
500,000	16.7
1,000,000	33.4
30,000,000	1002

Database alert threshold

By default, the Manager determines alert capacity based on the pre-defined limit of 10,000,000 alerts. When varying percentages of this capacity is reached, a system fault is raised alerting you of the reached threshold. System faults are raised at 80-90%, 90-95%, 95-99% of the alert capacity to let you know that you are approaching the 10,000,000 alert threshold. You can view and configure this threshold by opening the Manager's System Configuration interface, selecting the **Manager** tab's **Maintenance** menu. This is seen in configuration steps as Manager → <Admin Domain Name> → Maintenance → Database Pruning → **Alert Pruning**.

NOTE

This threshold is purely for capacity planning purposes and does not re-configure the size of your database.

Alert Pruning

The **Alert Pruning** option enables you to manage the database space required for the alerts generated by your Trellix IPS Sensors. Alert pruning is an important, ongoing task that must be performed for optimal Manager and database performance. If your database were to grow unchecked with millions of stored alerts, analysis using the **Attack Log** page or Reports would slowdown considerably.

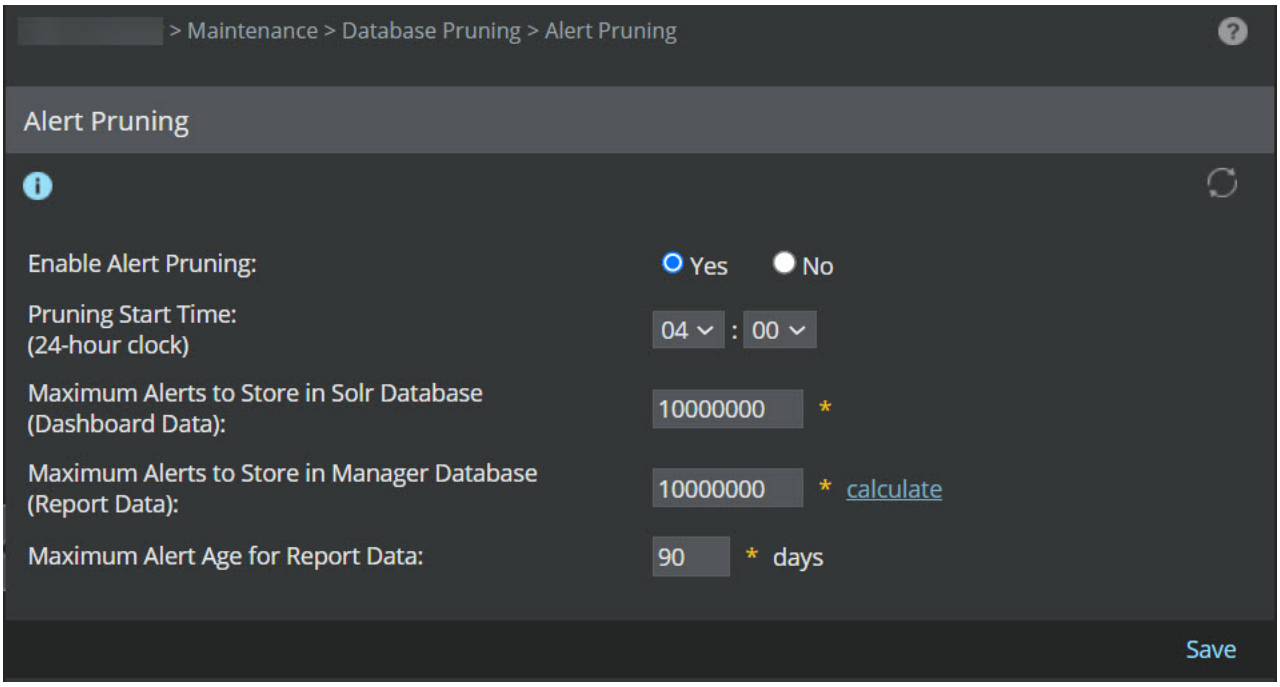
The Manager uses database which has a pre-defined alert capacity of 10,000,000 alerts. This means Manager will generate system fault messages when your database is nearing or exceeding the 10,000,000 limit by issuing warnings at 80-90%, 90-95%, 95-100%, >100% interval ranges. This value is purely for capacity planning and not an actual constraining limit on your database. You can customize this limit to properly manage your capacity needs.

In addition, the Manager uses an open-source search application called Solr, which stores alerts within a flat file. The alert capacity correlates directly with the amount of memory installed in the Manager server. If you have the minimum memory of 16GB, Solr supports up to 10 million alerts. If you have memory of 32 GB or higher, Solr supports up to 20 million alerts.

NOTE

Trellix recommends that you delete items, such as alerts and other system-generated files, at scheduled intervals to create more disk space.

Figure 75. Alert Pruning page



To plan Manager database capacity, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Database Pruning → **Alert Pruning**.
   - **Enable Alert Pruning**: Select Yes to delete all alerts and packet logs in the database that are older than the number of days set in **Maximum Alert Age for Report Data**.

     For Alert & Packet Log Data, Trellix strongly recommends entering a large value (such as 90, as 90 days is the default) in **Maximum Alert Age for Report Data**. You may want to perform long-term analysis using the information in your database, and having alerts and packet logs deleted, for example, every 10 days would be detrimental.

     NOTE

     The scheduled maintenance deletes all alerts older than the value entered in the Retain Alerts by Max number of days field or exceeding the alert count specified in the Max Alert Quantity field. This helps you automate database cleaning based on the alert threshold count.

     NOTE

     If after deleting alert and packet log by number of days, the number of alerts are still more than the set threshold value, Manager starts deleting all old alerts till the alert count falls below the Max Alert Quantity value.

   - Set the time (**Pruning Start Time:** At Hour and Minutes) for the selected day when you want scheduled maintenance to occur.

2. Type a number greater than or equal to 10,000 in **Maximum Alerts to Store in Solr Database (Dashboard Data)**.

> **NOTE**
>
> You must set this value depending on the amount of memory in your Manager server. If you have the minimum memory of 16GB, Solr supports up to 10 million alerts. If you have memory of 32 GB or higher, Solr supports up to 20 million alerts.

3. Do one of the following for **Maximum Alerts to Store in Manager Database (Report Data)**:
   - To allocate more disk space for your calculations, type a number greater than 10,000,000 (ten million).
   - To allocate less disk space for your calculations, type a number less than 10,000,000.
   - To calculate disk space capacity, click **Calculate**. This calculator has specific fields related to determining the database allocation space required to maintain your alerts and packet logs.

   Do the following in **Calculate Maximum Alert Quantity** window.

   a. Type the gigabytes allocated to the database at **Desired Disk Space Allocation**.

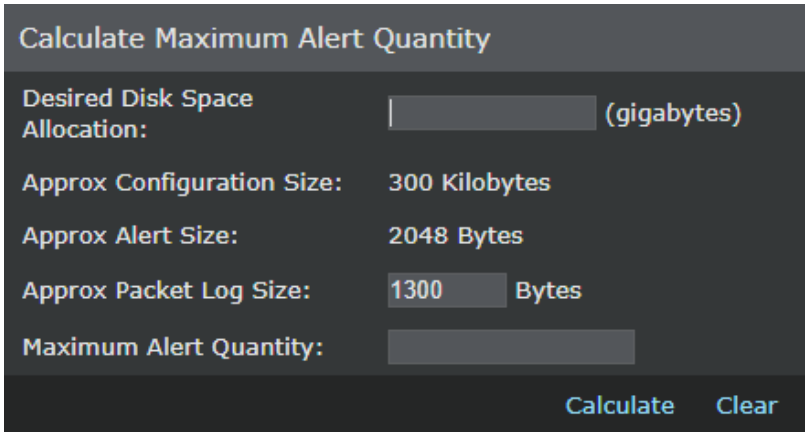
   b. (Optional) Type an approximate size for each packet log in your database (at **Approx Packet Log Size**).

   c. Enter **Maximum Alert Quantity**.

   d. Click **Calculate**. The number of alerts your database can maintain is listed in the **# of Alerts** field.

   e. (Optional) Click **Clear** to start a new calculation.

Figure 76. Calculate Maximum Alert Quantity dialog



4. Type the age of the alerts that can be deleted **(Maximum Alert Age for Report Data)**.
5. Do one of the following:
   - Click **Save** to save your changes.
   - Click to revert back to the previously saved values, thus aborting any current changes.

Delete alerts and packet logs from the database using purge.bat

An alternative to using the **Alert Pruning** action for alert and packet log deletion is to delete these files using **purge.bat**. To do this, perform the following steps:

1. Stop the Manager service.

   Follow one of these methods to stop the Manager service:

   - Right-click on the Manager icon at the bottom-right corner of your server and stop the service.
   - Select Windows Control Panel → Administrative Tools → **Services**. Then right-click on Trellix IPS Manager and select **Stop**.

2. Do one of the following:

   - Open your Trellix IPS installation folder and run **`purge.bat`** from`<Manager_Install_Dir>\bin\purge.bat`

     NOTE

     The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

   - Open a DOS prompt and type **`<Manager_Install_Dir>\bin\purge.bat`**

     NOTE

     Purge.bat also has the option to remove records flagged for deletion. This can significantly increase the amount of time it takes to finish, depending on the size of the database.

3. Answer the following questions:

   a. Is the Manager Down or Off-Line (Y/N)?

      NOTE

      The Manager service must be disabled prior to using **purge.bat**. If the service is not disabled, the purge will not continue.

   b. Do You Wish To Perform DB Tuning After The Purge Operation (Y/N)?

      TIP

      You can perform DB tuning separately from the purge operation.

   Alert and packet log data alert

   a. Enter the Number of days of Alerts and Packet Log data to be preserved. For example, to delete alerts/packet logs older than 90 days, type 90.

   b. Enter the Number of Alerts to be preserved.

   c. You Are About To Delete Alerts And PacketLog Data Older Than X Days. Type **Y** to continue.

   d. Do You Wish To Purge Alerts / Packet Logs That Have Been 'Marked For Delete' Through The Attack Manager? Type **Y** to continue

   Host event data

   a. Number of days of Host Event data to be preserved

b. Number of Host Entries to be preserved

c. You Are About To Delete Host Event Data Older Than X Days. Type **Y** to continue.

d. If The Number of Remaining Hosts Is Still More Than XXX, Deletion Will Be Continued Until It Reaches XXX. Type **Y** to continue.

e. Do You Wish To Purge Performance Monitoring Data [Y/N]. Type **Y** to continue.

Sensor performance data

a. Number of days of Raw performance data to be preserved

b. Number of days of Hourly performance data to be preserved

c. Number of days of Daily performance data to be preserved

d. Number of weeks of weekly performance data to be preserved

e. Number of months of monthly performance data to be preserved

f. You Are About To Delete Raw Performance Data Older Than X Days, Hourly Data Older than X Days, Daily Data Older than X Days, Weekly Data Older Than X Weeks, Monthly Data Older Than X Months. Are you sure you want to proceed (Y/N): Type **Y** to delete.

Application Visualization data

a. Number of days of Raw Application Visualization data to be preserved

b. Number of days of Hourly Application Visualization data to be preserved

c. Number of days of Daily Application Visualization data to be preserved

d. Number of weeks of weekly Application Visualization data to be preserved

e. Number of months of monthly Application Visualization data to be preserved

f. You Are About To Delete Raw Application Visualization Data Older Than X Days, Hourly Data Older than X Days, Daily Data Older than X Days, Weekly Data Older Than X Weeks, Monthly Data Older Than X Months. Are you sure you want to proceed (Y/N): Type **Y** to delete.

- Restart the Manager service after completion.

Database backup and recovery

Protecting your database against hardware and software failures is essential for ensuring the availability and integrity of configuration and/or forensic data. Trellix IPS provides backup functionality under the Manager → <Admin Domain Name> → Maintenance → **Database Backup** within the Trellix IPS Manager Configuration page, or through a standalone tool called the "Database Backup and Restore Tool" (`%programfiles%\Trellix\IPS Manager\App\bin\dbadmin.bat`).

> **NOTE**
>
> You can also use dbbackup.bat to back up and restore data. However, strongly encourages you to use **dbadmin.bat** for all your database administration tasks.

In the Manager, backups can be performed by a set schedule (**Automation**) or on demand (**Now**). The standalone tool can also perform backups, and is the only area wherein restoration of a backup can be executed.

When performing a backup, you can back up the following tables (**Backup Types**):

- **All Tables** — Back up all information, including configurations, alerts, and audits. This option is **not enabled** by default due to disk space consideration. When backing up All Tables, use the **Now** action.

  TIP

  Saving your **All Tables** settings **monthly** is strongly recommended.

- **Config Tables** — Back up only tabled information relating to configured tasks. This option is **enabled** by default to occur every Saturday night. This is set within the **Schedule** action.

  TIP

  Saving your configuration settings **weekly** is strongly recommended.

- **Audit Tables** — Back up only information on user activity and alert information. Backing up this data is useful for offline analysis. This option is **not enabled** by default. Use the **Now** action.
- **Event Tables** — Back up only information on alert, packetlog, host and Sensor performance events.
- **Trend Tables** — Back up only information on trend patterns (daily, weekly, monthly) of alerts and Sensor performance events. The backup also includes the first-seen attack statistics.

Database archival

Archiving your database is also recommended for protection against hardware and software failures. Once saved, the archival is available for future or third-party (such as Crystal Reports) retrieval.

NOTE

An archived database can be sent to Technical Support in the event of database issues.

Trellix recommends archiving your database to one of the following for added redundancy of system data, and to save Manager server disk space:

- A network-mapped drive
- CD-ROM/ DVD-ROM
- Multi-disc RAID storage on Manager server
- Database Replication
- Secure FTP

Protecting your backups

To ensure the availability of a backup, Trellix recommends the following testing backup restoration on a staging or non-production Manager server on a systematic basis.

To ensure the integrity of backups, Trellix recommends creating a digital "fingerprint" of all backup files using one-way hash functions such as MD5/SHA– 1 to detect tampering.

The following are general rules for protecting your backups:

- Avoid creating additional database user accounts.
- Block remote access to the database.
- Restrict access to physical data files in the database install directory.

Backing up data and settings

The **Database Backup** menu enables you to back up your Trellix IPS data on-demand or by a set schedule. Regularly backing up your data (alerts, saved reports, logs) and configuration settings is strongly recommended to maintain the integrity of your system.

> **NOTE**
>
> Restoration of stored data must be performed using the standalone **Database Admin tool**. This tool is explained in this section.

The **Database Backup** menu and the standalone tool provide the following functions:

- Backing up your Manager data— Save your data to your Manager server, a network server, or a device such as a zip drive.
- Automating a backup for your Manager— Set a frequency for backing up the Manager data.
- Using the Database Admin Tool— Backup and restore via the standalone Database Admin tool.
  - Backing Up Using the Database Admin Tool
  - Restoring Data Using the Database Admin Tool

> **NOTE**
>
> Before an **All Tables** or **Audit Tables** backup, it is recommended that you shut down the Manager. Therefore, Trellix recommends using the standalone Database Admin tool rather than your Manager for such backups.

> **NOTE**
>
> Data restore can only be performed using the standalone tool.

Backup and restore best practices

Note the following suggestions for successful backup and restore of Trellix IPS data:

- Protect your backups from tampering by creating a digital fingerprint of the file using a hash function such as MD5 or SHA-1.
- Back up your configuration data after major changes, such as created admin domains, Sensor addition, port configuration, and policy additions/modifications.

- The **All Tables** and **Audit Tables** options can be rather large in size, depending upon the amount of alert data in your database. Trellix recommends saving these types of backups to an alternate location, preferably an alternate system.
- When scheduling backups, set a unique time when no other scheduled functions (archivals, database tuning) are running. The time should be a minimum of an hour after/before other scheduled actions.
- When restoring your data, note that all related table information in the database is overwritten. For example, restoring a **Config Tables** backup overwrites all current information in the configuration table of the database. Thus, any changes not backed up are erased in favor of the restored backup.
- While a MariaDB backup is performed, the tables being backed up are placed in a READ LOCAL LOCK state. New records can be inserted in these tables while the backup is in progress, although these new records will not show up in the backup. However updates/modifications of existing records are not allowed during the backup. While a backup is in progress, you will not be able to perform the following activities:
  - Modify the configuration
  - Acknowledge and delete alerts
  - Acknowledge and delete faults
  - Add audit log entries
  - Purge the alert and packet logs
  - Perform database tuning.
- New alerts and packet logs will continue to be added to the database during the backup.
- In case of problems during database backup or restore, try after you complete the following tasks:
  - Exclude the following MariaDB directories from anti-virus scanning:
    - data
    - innodbdata
  - Create a new directory like c:\mariadbtmp, which will act as temporary directory for database. If the system has multiple physical disks, then Trellix recommends that you create this directory on a drive different than where Trellix IPS and MariaDB are installed to spread the load effectively.
  - Include the following entry in the `%programfiles%\Trellix\IPS Manager\MariaDB\my.ini` file under [mariadbd] section: **tmpdir=c:/mariadbtmp**
  - Restart both Trellix IPS and MariaDB services.

Back up your Manager (or Central Manager) data

You can back up your Manager data to your Manager server, or another media connected to your Manager, such as a tape drive. The backup file is saved by default within Manager program installation folder at **`<Manager_Install_Dir>\App\Backups.`**

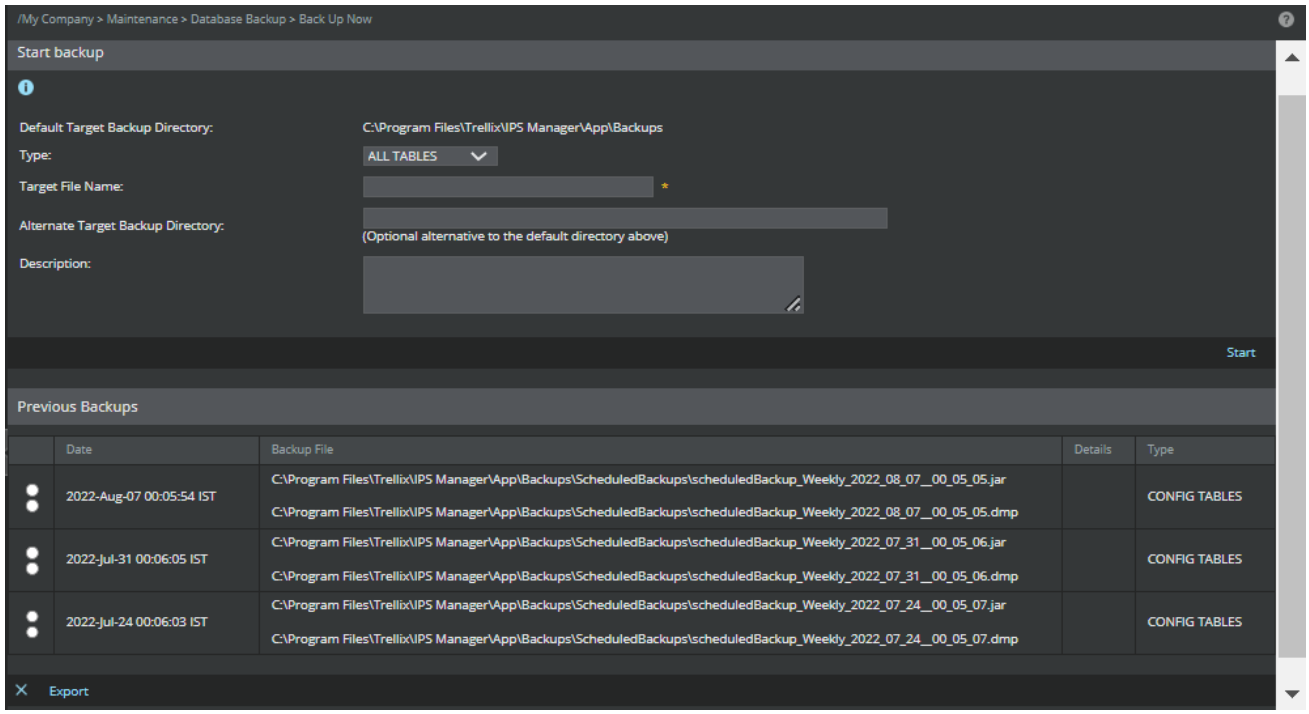
The above is applicable to Trellix IPS Central Manager as well.

To back up your Manager data using Manager server:

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Database Backup → **Back Up Now**.

Figure 77. Back Up Now page



NOTE

To backup your Central Manager data, select Manager → Maintenance → Database Backup → **Back Up Now**. The fields displayed are similar to that of Manager described below.

2. Select one of the following **Type** choices.
   - **All Tables**— Provides backup for the entire database, that is, all configurations, user activity, and alert information.
   - **Audit Tables**— Provides backup information related to user activity and Manager Health Status.
   - **Config Tables**— Provides backup for the Manager configuration.
   - **Event Tables**— Will backup alert, packetlog, host and Sensor performance events.
   - **Trend Tables**— Will backup the trend patterns (daily/weekly/monthly) of alerts and Sensor performance events. The backup also includes the first-seen attack statistics.

   CAUTION

   Do not make modifications to existing database records while doing an **All Tables** or **Audit Tables** backup, since such modifications are not allowed while a backup is occurring.

3. Type a **Target File Name**. You can use alphanumeric characters including hyphens and underscores (for example, **backup_01-10-03**).
4. (Optional) Type a location different from the default to be your **Alternate Target Backup Directory**.

5. (Optional) Type a description of your backup in **Description**.
6. Click **Start**.

   After a few moments, the following message appears: "Successfully backed-up data." The backup information appears in the List of **Previous Backups**. At the backup location, an XML file with the backup file name contains the description entered in the **Details** field.

> **NOTE**
>
> Previous backups can be exported to a desired location by selecting the radio button against the backup in the **Previous Backups** list and clicking the **Export** button. The selected Backup in the Previous Backup list be deleted using the ✕ button.

Automate backup of your Manager (or Central Manager) data

The **Automated Backups** option enables you to schedule the backup of your system configuration. Setting a schedule also allows you to work on other configurations without having to worry constantly about manually saving your work. Scheduled backups are saved by default to your installation folder:

`<Manager_Install_Dir>\App\Backups\ScheduledBackups`

> **NOTE**
>
> By default, your **Config Tables** are scheduled for back up every Sunday at 0 Hrs 5 Min. Each scheduled backups is saved to the default scheduled back up folder.

To schedule a backup, do the following:

1. Select Manager → <Admin Domain Name> → Maintenance → Database Backup → **Automated Backups**.

   > **NOTE**
   >
   > To run the database backup automation for your Central Manager data, select Manager → Maintenance → Database Backup → **Automated Backups**. The fields displayed are similar to that of Manager described below.

   Default Target Backup Directory: displays the location of the backup directory.
2. Note **Yes** is selected by default at **Schedule a Backup?**.

   Select **No** at any time to turn off the scheduled backup.
3. Select a backup **Frequency**:
   - **Daily**— Select the daily time to backup.
   - **Weekly**— Select the day and time to backup.

   > **NOTE**
   >
   > If you want an immediate backup of Manager data, perform the **Back Up Now** action.

> **NOTE**
>
> You can access **Scheduler Details** from Manager → <Admin Domain Name> → **Maintenance** to see when the processes are scheduled. These processes can include data backups, database maintenance, and file maintenance actions. Based on this information, you can choose an appropriate time for the backup you are currently scheduling.

4. **Start Time** — Set the time (Hour and Minutes)
5. Select the backup **Type** from the following:

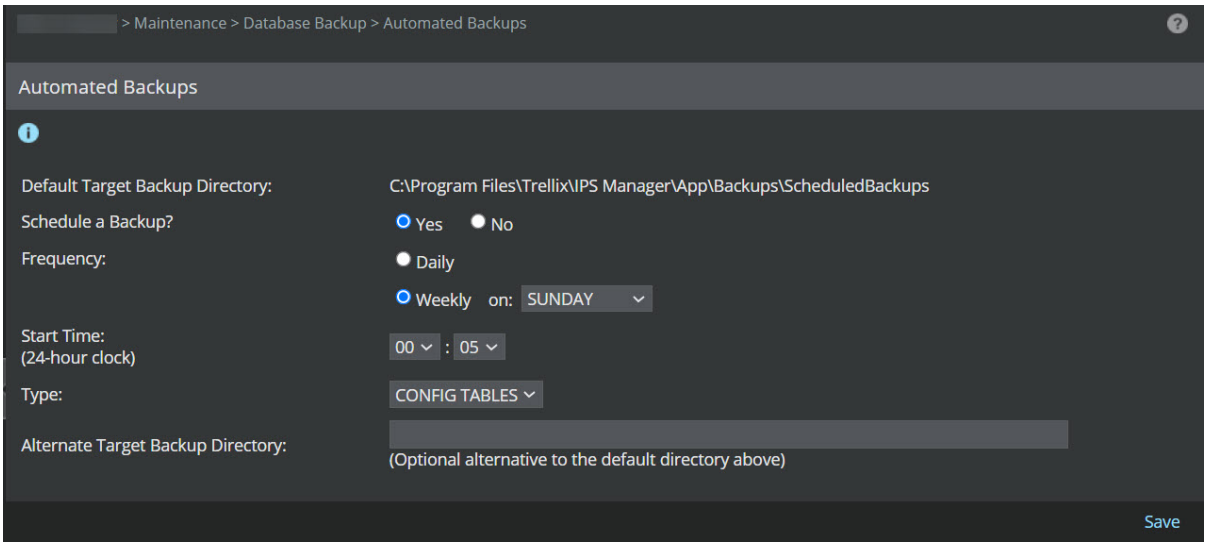
> **NOTE**
>
> You can only set a schedule for one backup **Type** at any given time.

- **All Tables**— All configuration, audit and alert information.
- **Audit Tables**— Backup information related to user activity and Manager Health Status.
- **Config Tables**— Only tabled information for the Manager configuration.
- **Event Tables**— Information on alert, packet log, host and Sensor performance events.
- **Trend Tables**— Trend patterns (daily/weekly/monthly) of alerts and Sensor performance events. The backup also includes the first-seen attack statistics.

> **CAUTION**
>
> Do not make modifications to existing database records while doing an **All Tables** or **Audit Tables** backup since such modifications are not allowed.

6. (Optional) Type the location of the **Alternate Target Backup Directory** if different from the default directory.
7. Click **Save**.

Figure 78. Back Up Scheduler



Database maintenance and tuning

Once you have determined the necessary database capacity for archiving your alerts and packet logs, as well as other Trellix IPS generated logs and files, you should consider a maintenance plan that keeps your database performing at an optimal level. Deleting old, unwanted alerts, packet log entries, and other files (for example, backups, saved reports) ensures adequate capacity for future data.

For database maintenance, Trellix IPS offers two solutions:

- File pruning action (Manager → <Admin Domain Name> → Maintenance → Database Pruning → **File and Database Pruning**) enables you to set a schedule by which Trellix IPS generated logs and files are deleted from Trellix IPS (Manager) and database. File pruning allows you to delete Trellix IPS data that has reached a set age (number of days old). Data is deleted according to a weekly schedule; this time, seen as **Enable File and Database Pruning?**, **Recur every**, and **Start Time (24-hour clock)**, must be enabled to operate.

  If you plan to use Alert Pruning (Manager → <Admin Domain Name> → Maintenance → Database Pruning → **Alert Pruning**) to delete alert and packet log data, Trellix recommends entering a value — such as 90, as in 90 days — in the **Maximum Alert Age for Report Data** field. This allows for long-term analysis of alerts and packet logs without overburdening your database with millions of records, which may affect long-term and overall database performance. By setting the value to 90 days, all alerts and packet logs older than 90 days are deleted at the scheduled time every day.

  Suppose you set a value of 90 days for the **Maximum Alert Age for Report Data** field and a value of 10000 for the **Maximum Alerts to Store in Solr Database (Dashboard Data)** field. Then at the scheduled time, Manager deletes all alerts that are older than 90 days and then checks if the number of alerts and packet logs is less than or equal to 10000. If it is more than 10000, it deletes the oldest alerts and packet logs until the number is less than or equal to 10000.

  You can also delete alerts in the Attack Log. This, however, only marks alerts for deletion in the database. To permanently delete these alerts from the database, you need to use the DB Purge feature in the dbadmin.bat utility or the purge.bat utility. Scheduled alert and packet log purge as part of Alert Pruning (Manager → <Admin Domain Name> → Maintenance → Database Pruning → **Alert Pruning**) has no effect on the alerts marked for deletion. Deleting alerts marked for deletion is a time-consuming process. Therefore, to delete alerts marked for deletion that are less than the age specified in the **Maximum Alert Age for Report Data** field, you need to use the dbadmin.bat or the purge.bat utility and manually delete these alerts. Also, note that the Manager has to be stopped to run the dbadmin.bat.

  NOTE

  Entering a very large value (such as 500, as in 500 days) is not recommended due to the capacity required to archive 500 days worth of alerts. Your requirements will determine the number of days you need to maintain alerts. If you must keep alerts for several hundred days, ensure that you have the necessary hard drive space on your Manager server, or back up your alert tables regularly.

TIP

You can use the purge.bat utility or the dbadmin.bat utility for alert and packet log data maintenance. Thus, if possible, do not schedule disk space maintenance with respect to alert and packet logs.

- Purge.bat utility: Provided with your Manager installation is the alert and packet log data maintenance utility named purge.bat (`%programfiles%\Trellix\IPS Manager\App\bin\purge.bat`). This utility enables on-demand deletion of

alerts and packet log data from your database. Alerts and packet logs can be deleted that are older than a specified number of days. Using purge.bat, you can automatically start the database tuning utility, dbtuning.bat, immediately after the purge is completed. This utility ensures your database is properly maintained for optimal continued use.

Database tuning

Over time, a relational database can experience performance issues if the data is not re-tuned on a recurring basis. By regularly diagnosing, repairing, and tuning your database internals, you can ensure optimal database performance. Trellix provides a set of Manager interface options (Manager → <Admin Domain Name> → Maintenance → **Database Tuning**) and a standalone utility, called **dbadmin.bat**, to maintain database performance.

NOTE

You can also use **dbtuning.bat** to tune your Trellix IPS database. However, Trellix strongly encourages you to use **dbadmin.bat** for all your database administration tasks.

The database tuning feature does the following:

- Defragments tables where rows/columns are split or have been deleted
- Re-sorts indexes
- Updates index statistics
- Computes query optimizer statistics
- Checks and repairs tables

On a regular basis (minimum recommendation: one month), perform database tuning on your Manager server. Completion time is dependent on the number of alerts/packet logs in the database and the performance of your Manager server's physical hardware platform.

NOTE

When you perform off-line database tuning, you must shut down the Manager service for proper performance. Trellix recommends scheduling this downtime for whenever you plan to re-tune the database. Your Sensor can continue to operate and generate alerts because of built-in alert buffers.

Tuning the Manager database

The Manager → <Admin Domain Name> → Maintenance → **Database Tuning** options provide actions for enabling you to schedule or initiate tuning of the database.

Trellix recommends tuning your database once per month at a minimum. For optimal performance, tuning once a week provides best results.

TIP

Ensure at any point of time the free space available in the database directory is at least one and a half times that of the maximum size occupied by a table (generally **Event Tables** and **Trend Tables**).

Viewing current database tuning status

The **Tuning Status** option (Manager → <Admin Domain Name> → Maintenance → Database Tuning → **Tuning Status**) provides the current database tuning operation status for the Manager or Central Manager.

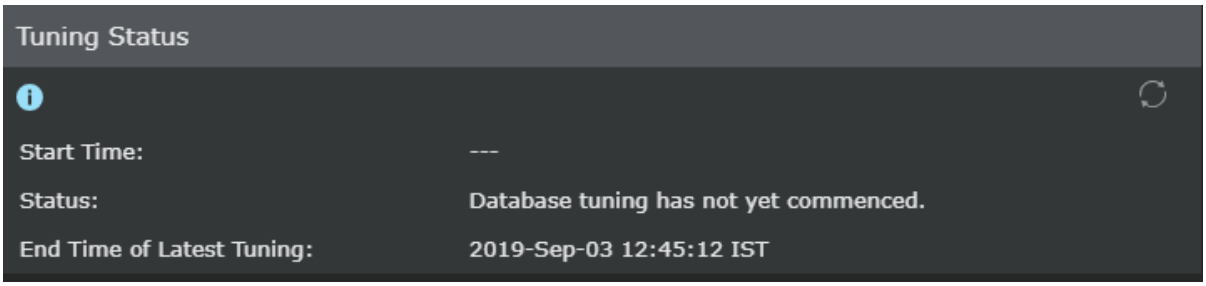
For the Central Manager, tuning status can be viewed from Manager → Maintenance → Database Tuning → **Tuning Status**.

This dialog box displays one or more of the following:

- **Start Time**— The time in-progress tuning started.
- **Status**— Displays if tuning has yet been initiated, is in progress, or is idle.
- **End Time of Latest Tuning**— Time when database was last tuned.

Clicking updates the dialog to provide you with the latest status (thus if another user initiated tuning since you opened the dialog, you could see the status after refreshing).

Figure 79. Database Tuning Status Dialog



Tune your database on-demand

For on-demand database tuning of Manager database, do the following:

1. Select Manager → <Admin Domain Name> → Maintenance → Database Tuning → **Tune Now**.

   NOTE

   For on-demand database tuning of Central Manager, select Manager → Maintenance → Database Tuning → **Tune Now**.

2. Select which tables to tune, either **All Tables** or only the **Event Tables**.

   NOTE

   Selecting **All Tables** will tune the entire database, that is, all configurations, user activity, and alert information, whereas selecting **Event Tables** tunes alert, host and Sensor performance events.

NOTE

The **iv_packetlog** table is not tuned in this method. You need to tune the database using **dbadmin.bat** or **dbtuning.bat** to tune this table. For more information on tuning the database using dbadmin.bat, refer to *Using the database admin tool* (page 318) and *Tune your database using dbadmin.bat* (page 327).

3. Click **Start**.

Automate database tuning

When scheduling database tuning, set a time when no other scheduled functions (archivals, backups, file maintenance) are running. The time should be a minimum of an hour after/before other scheduled actions.

To schedule database tuning, do the following:

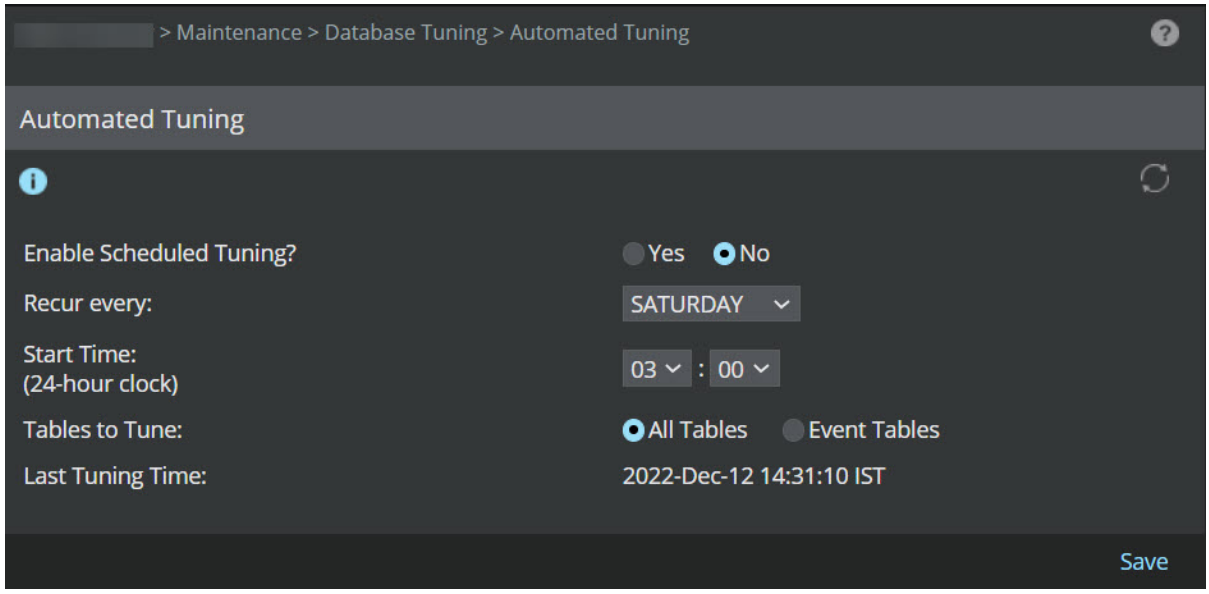
Steps:

1. Go to Manager → <Admin Domain Name> → Maintenance → Database Tuning → **Automated Tuning**.

NOTE

To schedule database tuning in Central Manager, select Manager → Maintenance → Database Tuning → **Automated Tuning**.

Figure 80. Database Tuning Scheduler



2. Select **Yes** at **Enable Scheduled Tuning?**
3. Select the day of the week when database tuning will occur (**Recur every**).
4. Use the **Hr** and **Min** drop-down menus to select the process start time.
5. Select which tables to tune, either **All Tables** or only the **Event Tables**.

Note the **Last Tuning time**. This indicates the last time the database tuning process occurred.

6. Click **Save**.

   The database tuning process is now enabled to start automatically on the configured day and time.

7. (Optional) Click  to clear current changes and view the last saved configuration.
8. (Optional) Go to Manager → <Admin Domain Name> → Maintenance → **Scheduler Details** to view the overall scheduled tasks in the Manager.
9. Click **Back** to return to the **Automated Tuning** page.

Database maintenance best practices

Trellix recommends the following best practices for database backup and tuning:

- Perform regular manual backups of your database using the Backup feature in the Manager software. Your configuration tables are saved by default once a week on Sunday.
- Database backups are cumulative and the size of a backup file can become quite large. Perform regular file maintenance to prevent disk space issues.

  CAUTION

  A database left untuned can lead to performance issues over time.

- Online database tuning operation causes the creation of temporary alerts and packet log tables; if you are using an agent that queries the database, your agent may attempt to interact with these tables during tuning.

  TIP

  During tuning, the SQL query might return empty results. If this occurs, simply retry the query once the tuning is complete.

  Further information on the impact of online database tuning of the Manager database will be sent to the third-party vendors that are directly accessing this database. If you have any specific questions, contact Technical Support. Also note that there is no change in database SQL query behavior if online database tuning is disabled.

- Make a regular practice of defragmenting the disk of the Manager server, as disk fragmentation can lead to database inefficiency.

  TIP

  Ensure at any point of time the free space available in the database directory is at least one and a half times that of the maximum size occupied by a table (generally **Event Tables** and **Trend Tables**).

- When scheduling certain Manager actions (backups, file maintenance, archives, database tuning), set a time for each that is unique and is a minimum of an hour after/before other scheduled actions. Do not run scheduled actions concurrently.

Backup of data and configurations

For the back up of Trellix IPS data and configurations, following best practices are recommended:

- Back up Manager data either within the Manager server (`%programfiles%\Trellix\IPS Manager\App\Backups` folder) or preferably on any external media.
- Back up all information, including configurations, alerts, and audits.
- Implement a schedule for backups using the Backup scheduler. Backing up config tables weekly is recommended. (Be sure to schedule this at a time when other processes will not be running concurrently.)
- As the **All Tables** and **Event Tables** options can be rather large in size (depending upon the amount of alert data in the database) these types of backups should be saved off the Manager server.
- Saving the **All Tables** settings on a monthly basis is strongly recommended.
- Protect backups from tampering by creating a digital fingerprint of the file using a hash function such as MD5 or SHA-1.
- Test restoration of backups periodically to ensure that a backup was successful and valid. The best way to do this is to perform a "test" restore of the backup on a secondary, non-production Manager.
- The **Config Tables** option backs up only tabled information relating to configured tasks. This option is enabled by default to occur every Sunday night. This is set within the Backup Scheduler action.
- Save actual configurations of Sensors (not just the config tables) using the Export option under the **Sensor_Name** tab. This creates an XML file (no attempt to read this file should be made) that can be imported to any Sensor of the same type in the future. Save actual Sensor configurations once a week.

Alerts and Disk space maintenance best practices

Disk space maintenance is an important task that must be completed to ensure efficient running of the Manager.

In order to develop best practices for database maintenance, it is important to understand the lifecycle of an alert.

Archiving alerts

Archive your alerts and packet logs regularly, using the Data Archival feature. Trellix recommends that you archive your alert data monthly, and that you discard alert and packet log information from your database every 90 days to manage your database size. Note that there is currently a 4 GB size limitation for a single archive file.

Scripts for disk space maintenance

If you have a large amount of data and wish to do your tuning offline, it is a best practice to use the purge and database tuning features in the **dbadmin.bat** utility. To do this, you must stop the Manager and run the scripts.

A best practice suggestion is to wait for 97 days of data and then, on a recurring 7-day period, run the purge and the database tuning features in the **dbadmin.bat** utility.

Using File Maintenance Scheduler

Databases can be substantially overloaded with all alerts, packet logs, any incident reports that have been generated, and audit and fault logs. Maintenance of this data can be accomplished automatically using the File Maintenance scheduler.

If automatic File Maintenance is used to delete alert and packet log data it is recommended that a large value, such as 90 (as in 90 days), is entered in the "Scheduled Deletion" column for the Alert & Packet Log Data option. This allows for long-term analysis of alerts and logs without overloading your database with millions of alerts, which may affect long-term and overall database performance. By setting the value to 90 days, all alerts and packet logs older than 90 days are deleted at the weekly maintenance scheduler time.

Apart from the database data, Manager creates a group of administration files that must be maintained regularly. These include Diagnostic files, DoS files (profiles) and Data Mining files (for Trend Reporting) among others. It is a best practice to schedule the deletion of the oldest of these files on an on-going basis. This can be accomplished using the Maintenance scheduler.

Viewing Manager server disk usage statistics

When the Manager database or disk space becomes full, the Manager cannot process any new alerts or packet logs. In addition, the Manager may not be able to process any configuration changes, including policy changes and alert acknowledgment. There is also a chance that the Manager may stop functioning completely.

Trellix therefore recommends that you monitor the disk space on a continuous basis to prevent this from happening. Health checks can be performed by navigating to the **Health Check** page in Manager → <Admin Domain Name> → Troubleshooting → **Health Check**. Use the **Health Check** page to view details, such as the percentage of space used, its total capacity, and the amount of disk space used.

NOTE

A fault type warning will be generated when the Manager disk space reaches 80-90%, 90-95%, 95-100%, >100% of interval ranges. By default, the frequency is 24 hrs.

Maintenance of system data and files

The Manager → <Admin Domain Name> → Maintenance → Database Pruning → **File and Database Pruning** option enables the following:

Setting a schedule for File pruning: Schedule deletion of the system data and files (logs, diagnostics, and so on) generated by System Configuration actions.

Set up a schedule for file pruning

The **File and Database Pruning** option enables you to set a schedule by which generated log data and files are deleted from your Manager/database. These data/files are admin created through various System Configuration actions, and each details a different aspect of system functionality. These system files get larger as more data is added over time. File pruning allows you to delete the data in a log or an entire static file either at the next scheduled time or in a set number of days. Regular deletion saves disk space on Manager server, thus improving overall performance.

The deletion scheduler works as follows: First, you set a daily time when you want File pruning (that is deletion) to take place; this is under the **Maintenance Scheduler** setting. Next, for each file type, you set a number of days/file size **(Scheduled Deletion)** after which you want a file that has reached the set age/size to be deleted. On the day a file is to be deleted, deletion takes place at the set daily time.

NOTE

When scheduling File pruning, set a time when no other scheduled functions (archives, backups, database tuning) are running. The time should be a minimum of an hour after/before other scheduled actions.

To schedule deletion for Manager and database files, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → Database Pruning → **File and Database Pruning**.

   NOTE

   To schedule file pruning action in the Central Manager, select Manager → Maintenance → Database Pruning → **File and Database Pruning**.

2. Select **Yes** against **Enable File and Database Pruning?** to enable automatic file pruning.

   This overrides the enabled status of individual file types from the table.

3. Select the day (**Recur every**) on which automatic file pruning will occur. Saturday is the default.
4. Set the time (**Start Time**: At Hr and Min) for the selected day when you want scheduled maintenance to occur. The default is 23:30 hours.
5. View the list of files/logs for which you can set maintenance:

   NOTE

   The default enabled status for each file/log is listed in parentheses after each description that follows.

   - Manager Files
     - **Diagnostics** — Files created by performing the steps in Uploading a diagnostics trace from a Sensor to your Manager. (Yes)
     - **Sig Files (*.bin)** — Files created during signature files update from the Manager to the Sensor by performing the steps in Updating the configuration of all Sensors. (No)
     - **DoS Files** — Denial of service (DoS) profiles uploaded from your Sensors. These files are downloaded by performing the steps in Managing DoS Learning Mode profiles on a Sensor. (Yes)
     - **Backup Files** — Saved Manager configuration, audit, and/or alert data as created by performing the steps in Backing up and restoring data. (Yes)
     - **Saved Reports** — All saved scheduled reports created by performing the steps in Scheduling a report. (Yes)
     - **Daily Archival** — Those archivals scheduled as **Daily** when Scheduling automatic archival.
     - **Weekly Archival** — Those archivals scheduled as **Weekly** when Scheduling automatic archival.
     - **Monthly Archival** — Those archivals scheduled as **Monthly** when Scheduling automatic archival.
     - **Packet Capture Files** — Manager can be configured to capture traffic on any port for a particular duration or size. These captured files reside under Packet Capture Files.

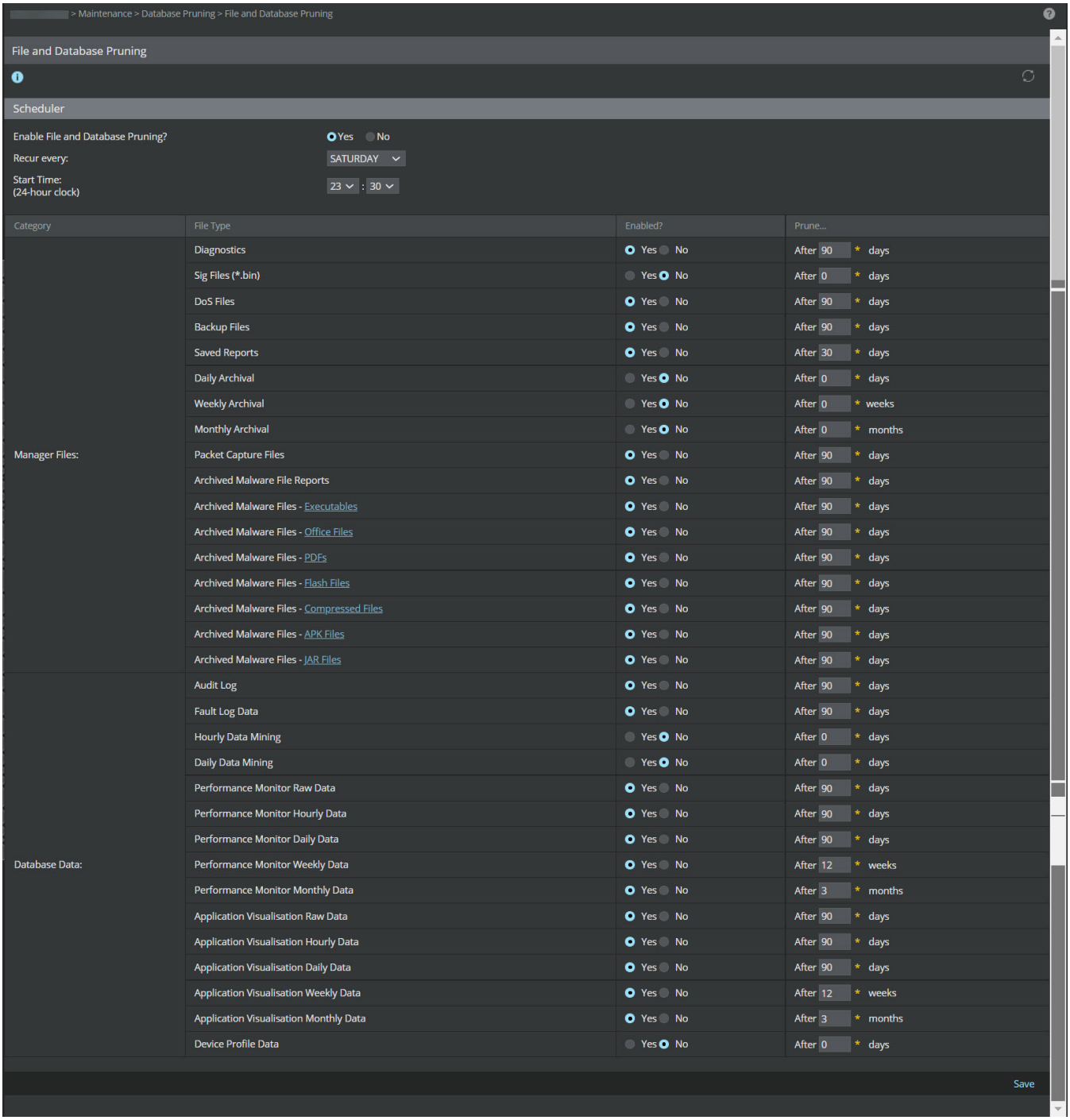
- **Archived Malware File Reports** — All reports fetched from IVX and Intelligent Sandbox
- **Archived Malware Files - Executables** — All executable malware files
- **Arachived Malware Files - Office Files** — All the office files like Excel, Word, and so on
- **Archived Malware Files - PDFs** — All the PDF files
- **Archived Malware Files - Flash Files** — All the flash files
- **Archived Malware Files - Compressed Files** — All compressed files
- **Archived Malware Files - APK Files** — All APK files
- **Archived Malware Files - JAR Files** — All JAR files

- Database Data
  - **Audit Log** — Log detailing user activity. Data is deleted by timestamp; the file itself is never deleted. This file can be viewed by performing the steps in Generating a User Activities Audit. (Yes)
  - **Fault Log Data** — Log detailing system faults. Data is deleted by timestamp; the file itself is never deleted. (Yes)
  - **Hourly Data Mining** — Deletes trend data collected for trend analysis resources on an hourly basis. (No)
  - **Daily Data Mining** — Deletes trend data collected for trend analysis on daily basis. (No)
  - **Performance Monitor Raw Data** — Raw data relating to performance monitoring (data polled from the Sensor every 3 minutes).
  - **Performance Monitor Hourly Data** — Data pertaining to performance monitoring. The data is captured hourly.
  - **Performance Monitor Daily Data** — Data pertaining to performance monitoring. The data is captured daily.
  - **Performance Monitor Weekly Data** — Data pertaining to performance monitoring. The data is captured weekly.
  - **Performance Monitor Monthly Data** — Data pertaining to performance monitoring. The data is captured monthly.
  - **Application Visualisation Raw Data** — Raw data relating to Application Visualisation.
  - **Application Visualisation Hourly Data** — Data pertaining to Application Visualisation. The data is captured hourly.
  - **Application Visualisation Daily Data** — Data pertaining to Application Visualisation. The data is captured daily.
  - **Application Visualisation Weekly Data** — Data pertaining to Application Visualisation. The data is captured weekly.
  - **Application Visualisation Monthly Data** — Data pertaining to Application Visualisation. The data is captured monthly.
  - **Device Profile Data** —Data relating to any remote computing device to decipher its operating system and device type. The remote computing device can be any endpoint inside or outside the network.
  - **Incident Data** — All generated incidents in the system marked as incident. The reported attacks are logged as incidents.

6. Select **Yes** for those file types that you want to be deleted at the scheduled time.

7. For those file types for which you have enabled deletion, type the time duration after which you want the files to be deleted.
8. Click **Save** when you are done with your changes.
9. (Optional) Click to update the information displayed in the page. Go to Manager → <Admin Domain Name> → Maintenance → **Scheduler Details** to view the overall scheduled tasks in the Manager.

Figure 81. File Maintenance Scheduler Settings



NOTE

Data on performance monitoring is displayed only when it is enabled from Devices → <Admin Domain Name> → Global → Common Device Settings → Performace Monitoring → **Enable**.

NOTE

By default, pruning is enabled for application visualization data, malware data, and performance monitor data and the default duration will be 90 days, 12 weeks, and 3 months respectively.

NOTE

When you upgrade from earlier versions of the Manager, the default values will be applied to application visualization data, malware data, and performance monitor data. If you had pruning enabled with a set duration in the earlier version of Manager, the values will get migrated to the latest Manager. If pruning was not enabled in the previous version, it will be enabled after the upgrade with the default values.

Archive malware files

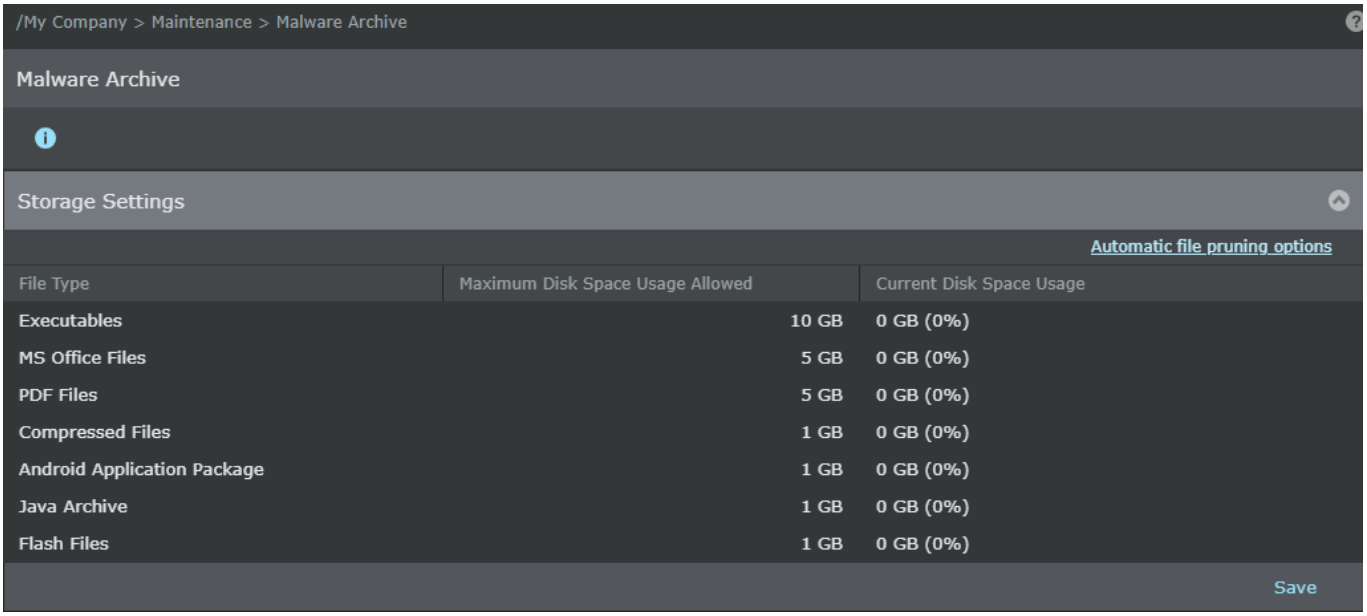
The malware policy has configuration settings to archive downloaded files based on various characteristics. These downloaded files are archived on the Manager server as encrypted files. You can configure the location and maximum disk space that can be used to store the archives. The configuration for disk usage is defined at the Global Manager level. The Manager also provides configuration to prune files that are stored for more than a specified period of time.

Perform the following steps to maintain the malware files saved to the Manager.

Steps:

1. Select Manager → <Admin Domain Name> → Maintenance → **Malware Archive**.
2. The **Storage Settings** are displayed for each file type. Click the **Maximum Disk Space Usage Allowed** to modify it as per your requirement.

Figure 82. File storage settings



3. To prune the file storage, click **Automatic file pruning options**.

   File pruning option allows you to determine the interval at which the Manager prunes older data to make sure its file system and database have adequate space for new data.

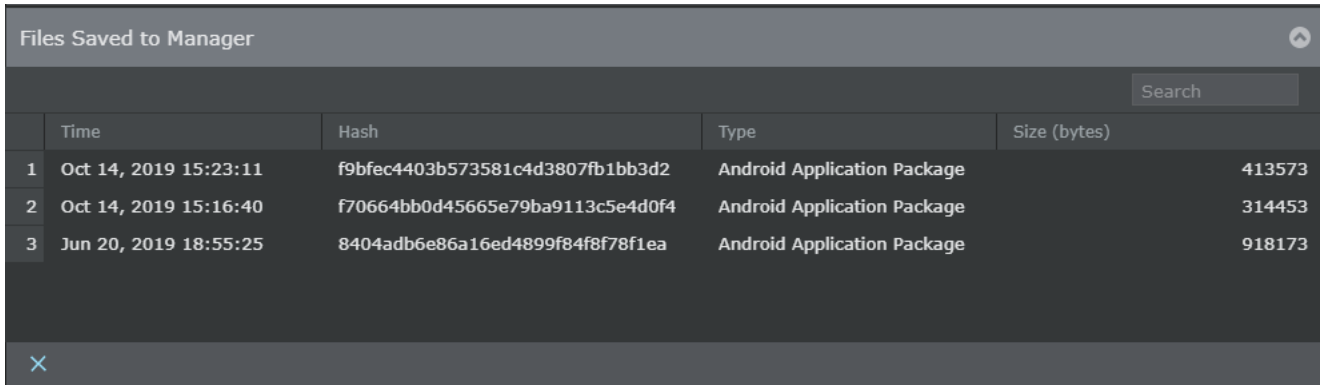
4. Click **Save**.

   The Manager warns you when the allocated disk space to a malware file type reaches 70%, 80%, 90%, and 100% of the maximum allowed. When the maximum space limit is reached, new malware files of that type are not stored until space is freed.

   The default location of these files in the Manager server is `%programfiles%\Trellix\IPS Manager\App\temp\tftpin\malware`. The list of files currently archived on the Manager are displayed with the following details.

   - **Time**— Indicates the date and time when the file was saved
   - **Hash** — Displays the MD5 hash of the file
   - **Type** — The type of the saved file
   - **Size** — The size of the file saved

Figure 83. Details on stored files



5. To delete the archived files, select the required ones and click ✕

Using the database admin tool

The database admin tool (dbadmin.bat) is a standalone tool that can:

- Backup and restore Trellix IPS data from the database.
- Archive and restore alerts and packet logs.
- Tune your Trellix IPS database and purge unwanted data from it.
- Change the password of your Trellix IPS database (this is **not** the database root password).

You need to shut down the Manager before performing the following tasks:

- Data backup
- Data backup restore
- Data purge
- Database tuning
- Database password change

You can perform the following activities in the database admin tool regardless of Manager status:

- Alert archival
- Alert restore

The DB Admin tool is available on the Manager server at `<Manager_Install_Dir>\App\bin\dbadmin.bat`. Note that you need to execute the tool from the same location as well.

You can also use the Manager to perform some of the tasks mentioned above. Some of these tasks can be time consuming and resource intensive. Because of the standalone nature of this tool, there will be no additional workload on the Manager when you use the tool to perform these tasks.

NOTE

If you are using the tool, then you will need your database user name and password to complete the tasks that would result in changes to the database.

NOTE

You will need database root password if you are changing the database user password using the Database Admin tool.

NOTE

The Database Admin tool displays all activity console messages as well as error messages for tracking purposes.

Back up data using dbadmin.bat

You can back up Trellix IPS data using either the Manager server or the standalone Database Admin tool. However, you can avoid the additional workload on the Manager server by using the tool.

Note the following before attempting to backup data:

- You can restore **Config Tables** or **All Tables** only if the major versions of the backed up Manager and the present Manager match. For example, a backup from any 10.1 Manager can be restored on any other 10.1 Manager and not on 11.1 Manager.
- You cannot restore **Config Tables** or **All Tables** of a later version of the Manager on an earlier version of the Manager. For example, you cannot back up the **Config Tables** from Manager version 10.1.7.65 and restore it on Manager version 10.1.7.50.

To backup using the standalone Database Admin tool:

Steps:

1. Stop the Manager service.

   You can stop the Manager service by any of the following methods:

   a. Right-click on the Manager icon at the bottom-right corner of your Windows server and stop the service.

   b. Select Windows Control Panel → Administrative Tools → **Services** and right-click on **Trellix IPS Manager** and select **Stop**.

2. Navigate to `<Manager_Install_Dir>\bin`.

   NOTE

   The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`

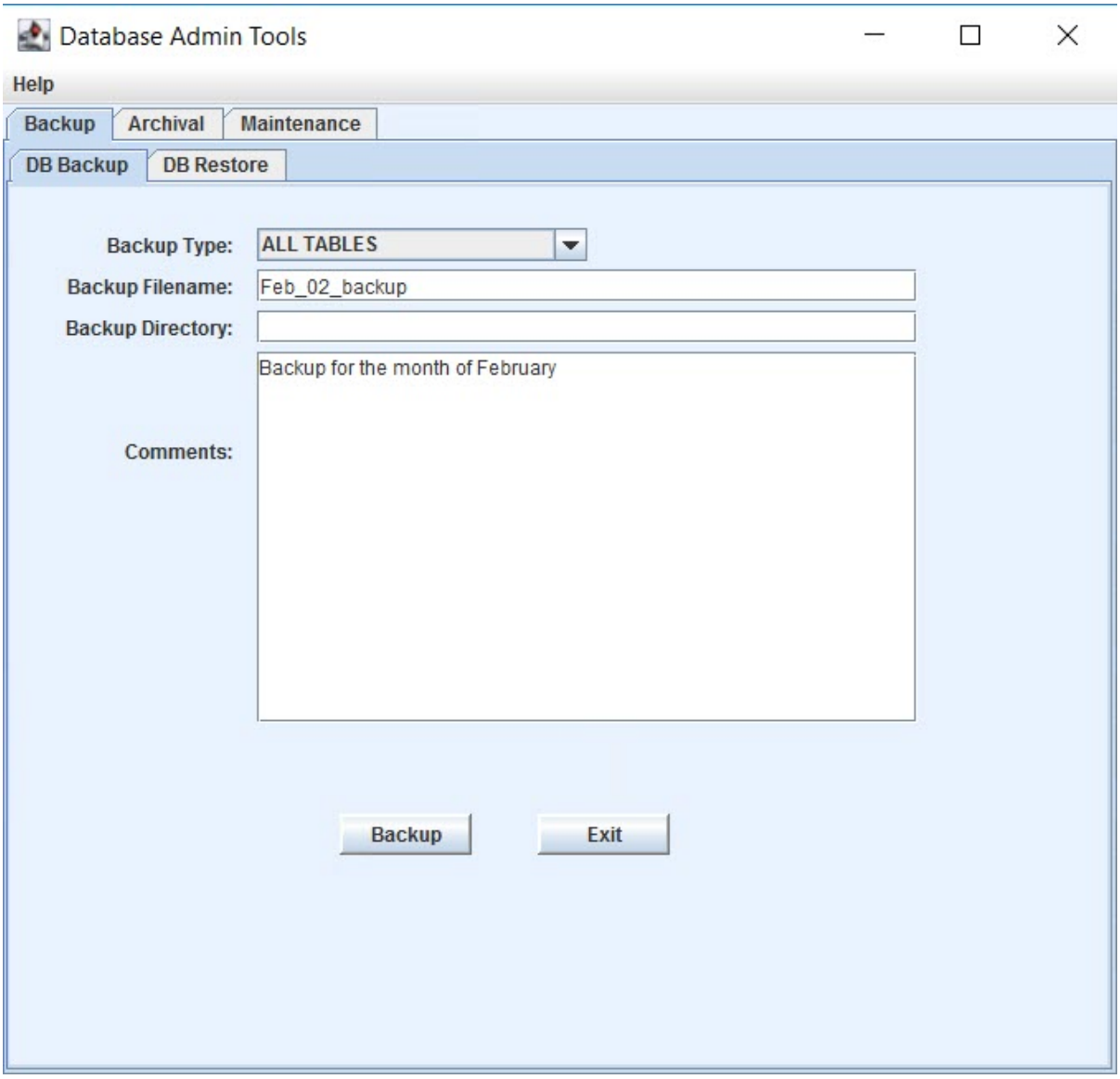
3. Execute the **dbadmin.bat** file.

   The standalone tool opens.

   NOTE

   You can also use dbbackup.bat to back up and restore data. However, you will be directed to use dbadmin.bat for all your database administration tasks.

Figure 84. Database Admin Tools - DB Backup Tab



4. Select one of the following backup **Type** choices from the drop down:
   - **All Tables**— The entire Manager database consisting of configuration, user activity, event and trend tables.
   - **Config Tables**— Information regarding Manager configuration.
   - **Audit Tables**— Information regarding user activity.
   - **Event Tables**— Information regarding events such as, alerts, packetlogs, hosts and Sensor performance.
   - **Trend Tables**— Trend patterns (daily/weekly/monthly) of alerts and Sensor performance events.

> ⚠ **CAUTION**
>
> Backup of Event table and All table option can be large in size depending upon the amount of event data (i.e. alert/ host/ Sensor performance metrics data) in your database.

5. Type a backup **Filename**. You can use alphanumeric characters including hyphens and underscores (for example, **back-up_01-10-03**).
6. Optionally type the backup **Directory** where you want the backup to be stored.

   If you do not specify a backup directory, then the backup is stored in the default backup directory at `<Manager_Install_Dir>\Backups`. It creates a new directory under `<Manager_Install_Dir>` if the Backups directory does not already exist.
7. Optionally type a description of your backup in **Comments**.
8. Click **Backup**. After a few moments, the following message appears: "Database backup successful."

   You can see the backup information by clicking the **DB Restore** tab. In the backup directory, you will find an XML file (JAR format) and the other with the file extension .dmp with the backup file name that you specified.
9. Back up the .jar and .dmp files to a safe location.

Restore data using dbadmin.bat

Restoring your backed up data means you want to return to a previous configuration of your Trellix IPS, or to a previous collection of alert data, or both, which may include different Sensor port configurations, policy applications, and so forth. Note that the Manager server must be shut down during a restore; thus, all Manager activities must be stopped to complete a restore.

When restoring configuration tables (All Tables or Config Tables), you must de-install your Sensors using the Sensor CLI command **`deinstall`**, then re-install your Sensors using the **`set sensor sharedsecretkey`** command.

If your Sensor or interface configurations have changed since the last backup, you may need to re-wire your segments to match the backed up configuration's monitoring settings. Test restoration of backups periodically to ensure that a backup was successful and valid. The best way to do this is to perform a "test" restore of the backup on a Secondary, non-production Manager.

Note the following before attempting to restore a backup:

- Manager Version: You can restore database backup from an older version of the Manager to a newer version of the Manager if they belong to the same major version. For example a back up from an older version of the 11.1 manager can be restored on a newer 11.1 Manager version.
- Config Tables version
  - You can restore the **Config Tables** only if the major versions of the backed up Manager and the present Manager match. For example, a backup from any 10.1 Manager version can be restored on any other 10.1 Manager version. A backup from a 10.1 Manager cannot be restored on a 11.1 Manager.
  - You cannot restore the **Config Tables** of a later version of the Manager on an earlier version of the Manager. For example, you cannot back up the **Config Tables** from Manager version 10.1.7.65 and restore it on Manager version 10.1.7.50.
- All Tables version: You can restore **All Tables** only if the versions of the backed up Manager and the present Manager match exactly (all four digits).

To restore using the standalone Database Admin tool, do the following:

Steps:

1. Stop the Manager server service.

   Follow one of the following methods to stop the Manager service:

   - Right-click on the Manager icon at the bottom-right corner of your server and stop the service.
   - Select Windows Control Panel → Administrative Tools → **Services**. Then right-click on Trellix IPS Manager service and select **Stop**.

2. Navigate to `<Manager_Install_Dir>\bin`.

   NOTE

   The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

3. Execute the **dbadmin.bat** file. The standalone tool opens.

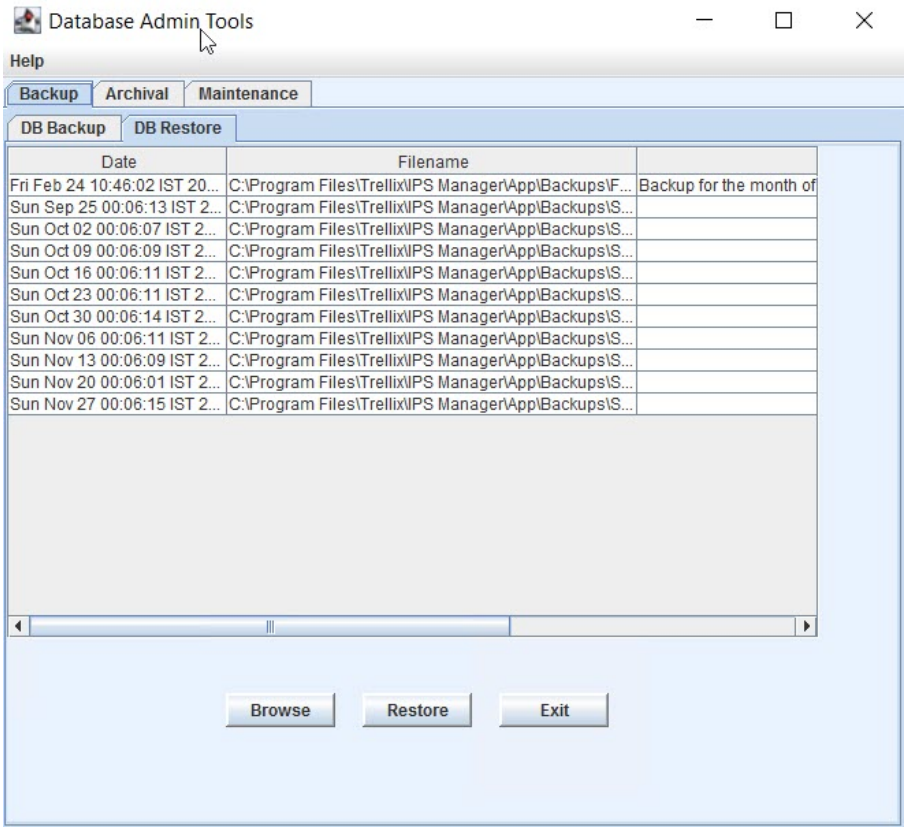
   NOTE

   You can also use dbbackup.bat to back up and restore data. However, you will be directed to use dbadmin.bat for all your database administration tasks.

   You see the **Database Admin Tools** window.

4. Click the **DB Restore** tab.

Figure 85. Database Admin Tools - DB Restore Tab



5. Select a backup from the table.

   All the backups taken through the DB Admin tool are displayed (that is, the backup file copied from another directory is not displayed). Place the mouse cursor over a backup to view file information in a pop-up.

   NOTE

   If the backup file is stored at a location different from the default one, use the **Browse** button to locate it.

6. Click **Restore**.

   NOTE

   During a restore, Manager needs to be shutdown. Since Manager is closed to all communications, no alert data sent from the Sensors is received. Manager system log and ems.log will note "Restore in Progress" faults during this process.

   A pop-up prompts you for the database user name and password.

7. Type the database **User Name** and **Password**. This information was entered during Manager installation.

   NOTE

   For MariaDB, this is **not** the MariaDB root administrator password.

8. After the restore process is complete, the following message is displayed: "Database restore successful, Restart Manager Service." Ensure that all Java processes are terminated and then restart Manager service (on Manager server). Wait a few seconds for Manager service to restart before attempting to log in.

   CAUTION

   Ensure that no Java processes are running when restarting Manager service. Otherwise, Manager may experience errors.

   NOTE

   If the Manager is running on software version 10.1.7.40 or below, you must run the Apache Solr script after restoring database in the Manager to view the alerts in the **Attack Log** page. For more information, refer to the section [Run the Apache Solr Scripts] in [Trellix Intrusion Prevention System Installation Guide]. If the Manager is running on software version 10.1.7.44 or above, it should be able to import the Solr data automatically. In case you do not see the alerts appearing in the **Attack Log** page even after restoring the database, you need to run SolrDB import manually in the Manager. For more information, refer to the section Alerts do not show up in Attack Log or on dashboards after upgrading the Manager (page 2373).

Archive alerts using dbadmin.bat

You can archive alerts and packet logs from either the Trellix IPS user interface or from the standalone database admin tool. However, you can avoid the additional workload on Manager server by using the database admin tool. The archived data

is stored in a .zip file at `%programfiles%\Trellix\IPS Manager\App\alertarchival`. Note that data from the following tables are archived:

- iv_alert
- iv_alert_data
- iv_packetlog

Note the following before attempting to archive alerts:

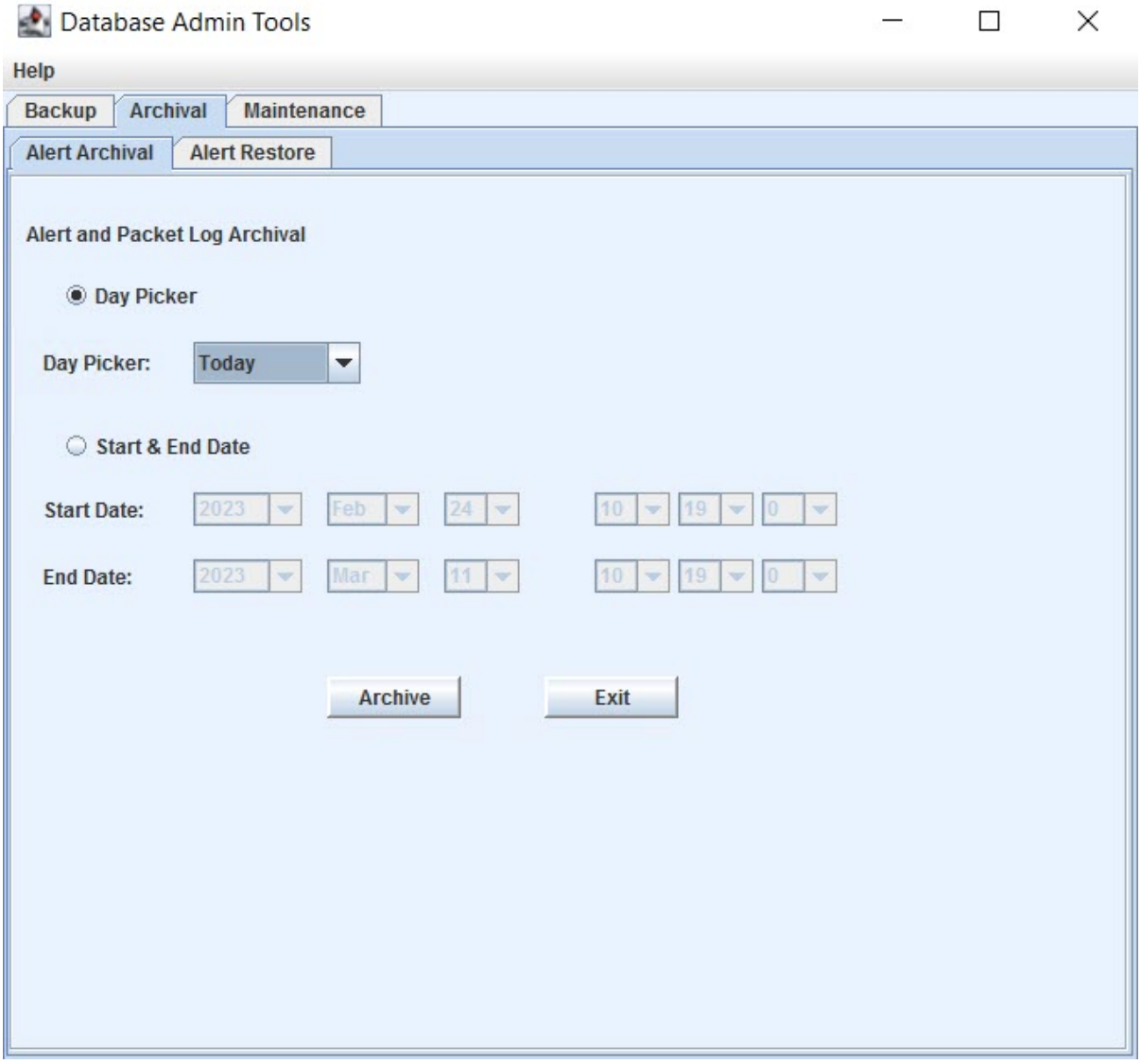
- You can restore alerts only if the major versions of the backed up Manager and the present Manager match. For example, a backup from any 10.1 Manager version can be restored on any other 10.1 Manager version. A backup from a 10.1 Manager cannot be restored on a 11.1 Manager.
- You cannot restore alerts of a later version of the Manager on an earlier version of the Manager. For example, you cannot back up alerts from Manager version 10.1.7.65 and restore it on Manager version 10.1.7.50.

To archive alerts and packet logs using the standalone Database admin tool:

Steps:

1. Navigate to `%programfiles%\Trellix\IPS Manager\App\bin`.
2. Execute the **dbadmin.bat** file. The standalone tool opens.
3. Select Archival → **Alert Archival**.

Figure 86. Database Admin Tools - Alert Archival Settings



4. Specify the time period of the data to be archived either by using the **Day Picker** or by specifying the start date and time and the end date and time.
5. Click **Archive**. Archive Confirmation dialog pop-up appears. Click **Yes**.

   When the process is complete, the archived file is saved to `%programfiles%\Trellix\IPS Manager\App\alertarchival`. This file will also be listed in a table when you restore files using this tool or Manager.

Restore alerts using dbadmin.bat

You can restore archived alerts and packet logs from either the Trellix IPS user interface or from the standalone Database Admin tool. However, you can avoid the additional workload on Manager by using the Database Admin tool.

To restore data, the archived data should either be in Manager server or in a computer that is accessible from Manager server. You can also filter data from an archived file and restore just the filtered data. Suppose that there is an archived file containing

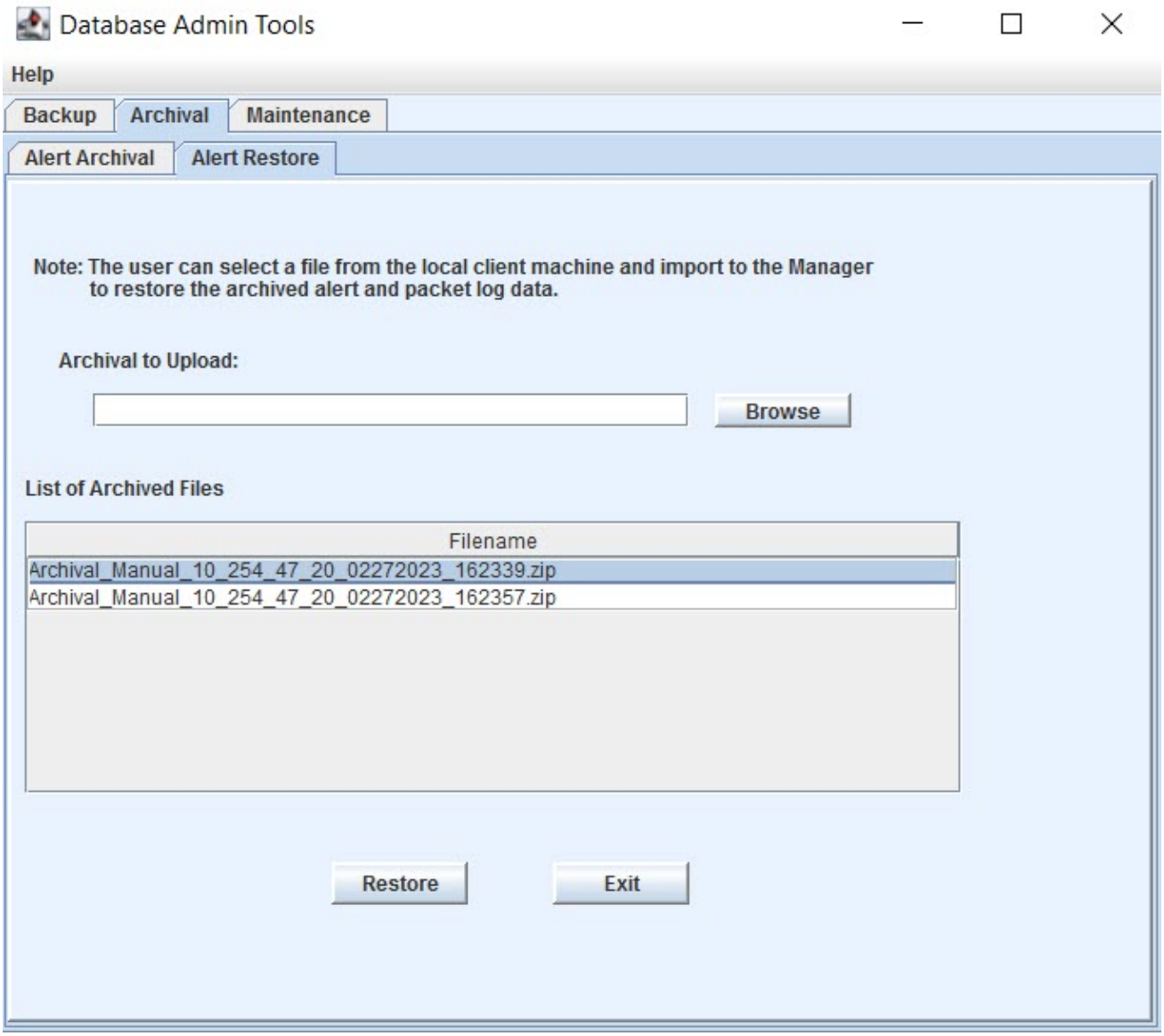
data generated between Jan 1 and Jan 10. Then you can filter the data generated between Jan 1 and Jan 5 from the archived file and restore just this data.

To restore alerts and packet logs using the standalone Database Admin tool:

Steps:

1. Navigate to `%programfiles%\Trellix\IPS Manager\App\bin`.
2. Execute the **dbadmin.bat** file. The standalone tool opens.
3. Select Archival → **Alert Restore**.

Figure 87. Database Admin Tools - Archival Alert Restore tab



4. Do the following:
   a. Click **Browse** to locate the archival or type the file's absolute path name.

b. Select the archived file from the **List of Archived Files** and then click **Restore**.

> **NOTE**
>
> Archived data in the `%programfiles%\Trellix\IPS Manager\App\alertarchival` are listed under **List of Archived Files**.

5. Filter the data in the archived file by specifying the start date and time and the end date and time. Only those alerts and packet logs generated during this time frame are restored from the archived file.

> **NOTE**
>
> The start date and time and the end date and time displayed by default in this window indicate the time frame of the archived data that you have selected to restore. Therefore, if you choose the default dates and times, all the data in the archived file will be restored.

6. Click **Restore**.
7. Enter your database user name and password to complete the restoration process.

> **NOTE**
>
> Manager server only permits 300,000 alerts to be restored at a time if filtering is applied. If your archive contains more than 300,000 alerts and you set filtering parameters, you will need to perform the restoration process multiple times. For example, if your archival still contains 750,000 alerts after filtering parameters have been met, you will have to restore three times: 1) 300,000 2) 300,000 3) 150,000.

8. To see the alerts restored in attack log, run solr import.

> **NOTE**
>
> To run solr import, refer to *Trellix Intrusion Prevention System Installation Guide*.

Tune your database using dbadmin.bat

You can tune your Trellix IPS database using either the Manager or the standalone Database Admin tool. However, you can avoid the additional workload on Manager by using the tool. However, note that when you use Manager, you have the option of tuning all the tables or just the data tables.

> **NOTE**
>
> You can also use **dbtuning.bat** to tune your Trellix IPS database. However, you will be directed to use **dbadmin.bat** for all your database administration tasks.

To tune your Trellix IPS database using the standalone Database Admin tool:

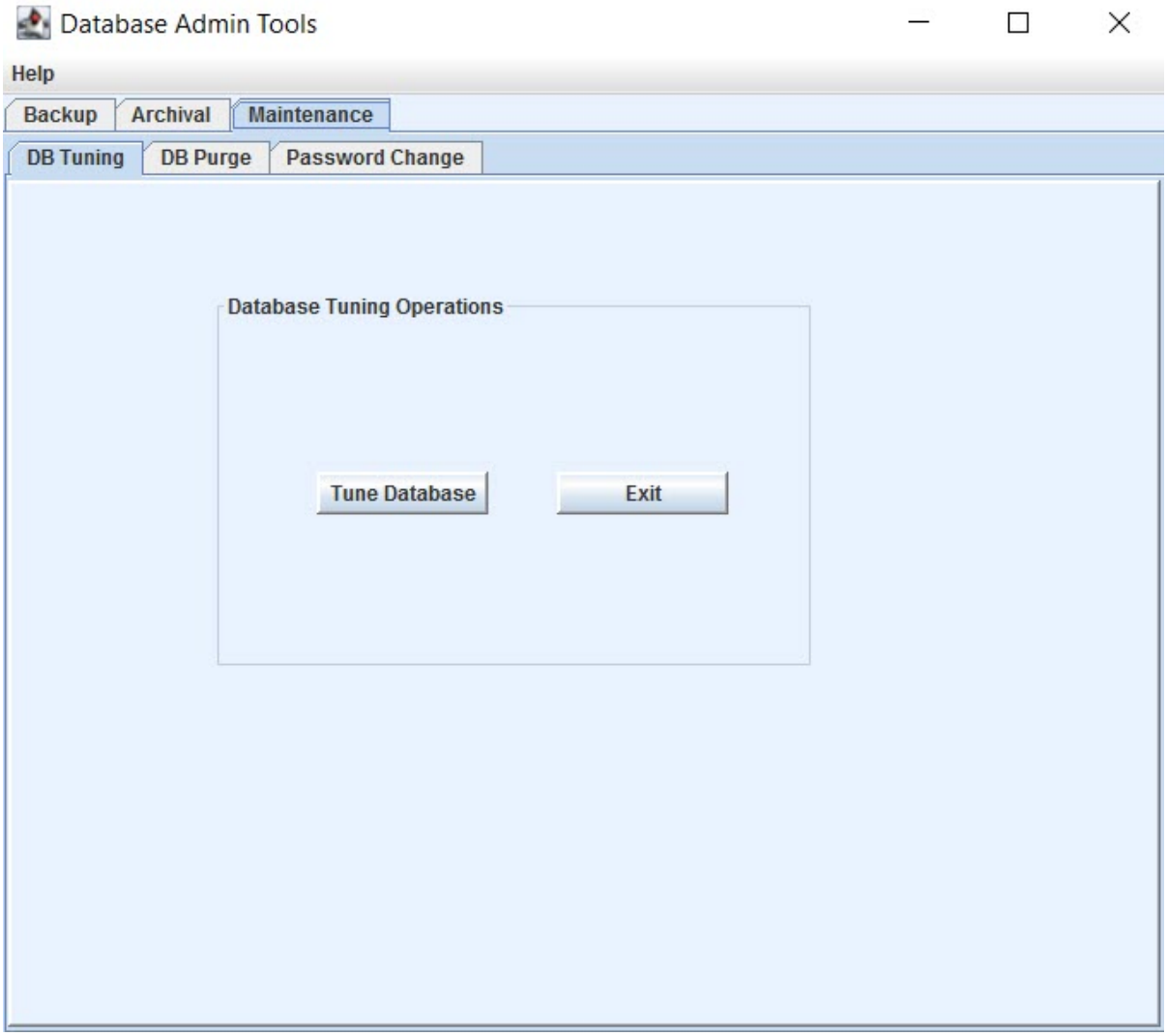
Steps:

1. Navigate to `<Manager_Install_Dir>\bin`.

> **NOTE**
>
> The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

2. Execute the **dbadmin.bat** file. The standalone tool opens.
3. Select **Maintenance**. The **Database Tuning Operations** window is displayed.

Figure 88. Database Admin Tools - DB Tuning



4. Click **Tune Database**. The message "Database Tuning Completed" is displayed to indicate successful tuning.

Delete alerts and packet logs from the database using purge.bat

An alternative to using the **Alert Pruning** action for alert and packet log deletion is to delete these files using **purge.bat**. To do this, perform the following steps:

1. Stop the Manager service.

   Follow one of these methods to stop the Manager service:

   - Right-click on the Manager icon at the bottom-right corner of your server and stop the service.
   - Select Windows Control Panel → Administrative Tools → **Services**. Then right-click on Trellix IPS Manager and select **Stop**.

2. Do one of the following:

   - Open your Trellix IPS installation folder and run **`purge.bat`** from`<Manager_Install_Dir>\bin\purge.bat`

     NOTE

     The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

   - Open a DOS prompt and type **`<Manager_Install_Dir>\bin\purge.bat`**

   NOTE

   Purge.bat also has the option to remove records flagged for deletion. This can significantly increase the amount of time it takes to finish, depending on the size of the database.

3. Answer the following questions:

   a. Is the Manager Down or Off-Line (Y/N)?

   NOTE

   The Manager service must be disabled prior to using **purge.bat**. If the service is not disabled, the purge will not continue.

   b. Do You Wish To Perform DB Tuning After The Purge Operation (Y/N)?

   TIP

   You can perform DB tuning separately from the purge operation.

   Alert and packet log data alert

   a. Enter the Number of days of Alerts and Packet Log data to be preserved. For example, to delete alerts/packet logs older than 90 days, type 90.

   b. Enter the Number of Alerts to be preserved.

   c. You Are About To Delete Alerts And PacketLog Data Older Than X Days. Type **Y** to continue.

   d. Do You Wish To Purge Alerts / Packet Logs That Have Been 'Marked For Delete' Through The Attack Manager? Type **Y** to continue

   Host event data

   a. Number of days of Host Event data to be preserved

b. Number of Host Entries to be preserved

c. You Are About To Delete Host Event Data Older Than X Days. Type **Y** to continue.

d. If The Number of Remaining Hosts Is Still More Than XXX, Deletion Will Be Continued Until It Reaches XXX. Type **Y** to continue.

e. Do You Wish To Purge Performance Monitoring Data [Y/N]. Type **Y** to continue.

Sensor performance data

a. Number of days of Raw performance data to be preserved

b. Number of days of Hourly performance data to be preserved

c. Number of days of Daily performance data to be preserved

d. Number of weeks of weekly performance data to be preserved

e. Number of months of monthly performance data to be preserved

f. You Are About To Delete Raw Performance Data Older Than X Days, Hourly Data Older than X Days, Daily Data Older than X Days, Weekly Data Older Than X Weeks, Monthly Data Older Than X Months. Are you sure you want to proceed (Y/N): Type **Y** to delete.

Application Visualization data

a. Number of days of Raw Application Visualization data to be preserved

b. Number of days of Hourly Application Visualization data to be preserved

c. Number of days of Daily Application Visualization data to be preserved

d. Number of weeks of weekly Application Visualization data to be preserved

e. Number of months of monthly Application Visualization data to be preserved

f. You Are About To Delete Raw Application Visualization Data Older Than X Days, Hourly Data Older than X Days, Daily Data Older than X Days, Weekly Data Older Than X Weeks, Monthly Data Older Than X Months. Are you sure you want to proceed (Y/N): Type **Y** to delete.

- Restart the Manager service after completion.

Delete unwanted data using dbadmin.bat

You can delete any redundant data including alerts and packet logs from your Trellix IPS database using the standalone database admin tool. You can also delete data using Manager. For details, see the **Maintenance** tab section.

To purge unwanted data from your Trellix IPS database using the standalone Database Admin tool:

Steps:

1. Make sure the Manager is shutdown.
2. Navigate to `<Manager_Install_Dir>\bin`.

> **NOTE**
>
> The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

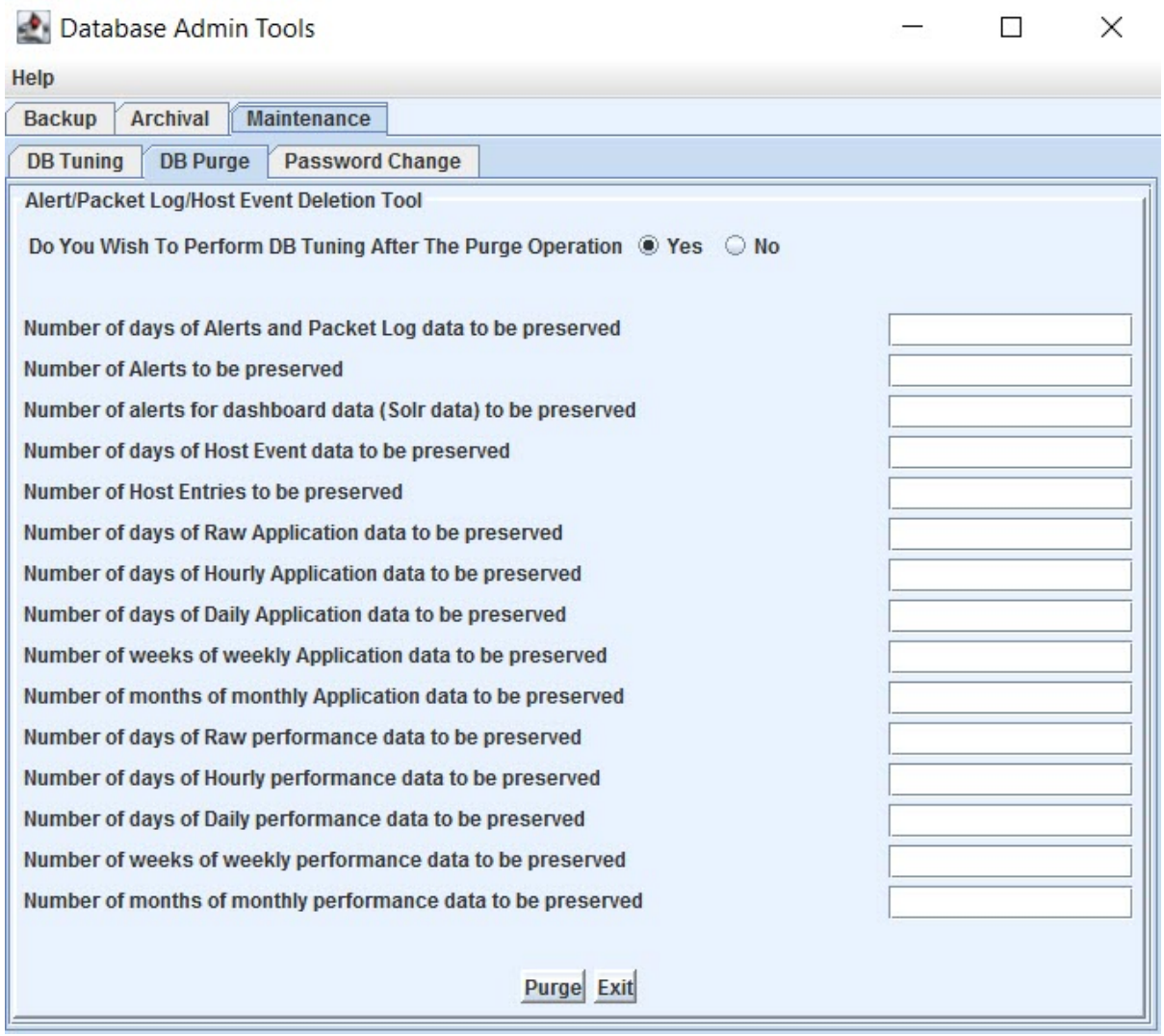
3. Execute the **dbadmin.bat** file. The standalone Database Admin tool opens.

> **NOTE**
>
> You can also use dbpurge.bat to delete unwanted data from your Trellix IPS database. However, Trellix strongly encourages you to use dbadmin.bat for all your database administration tasks.

4. Select Maintenance → **DB Purge**.

   The **Alert and Packet Log/Host Event Deletion Tool** window is displayed.

Figure 89. Database Admin Tools - DB Purge Tab



5. Specify if you want to **Perform DB Tuning after the Purge Operation**. You can perform database tuning separately from the purge operation.

   Alert and Packet Log data

   1. Type the **Number of days of Alerts and Packet Log data to be preserved**. For example, to delete alerts and packet logs older than 90 days, enter 90. You can specify a value between 0 and 9999.

2. Type the **Number of Alerts to be preserved** in the database. You can specify a value between 0 and 1,000,000.

   For example, if you enter **Number of days of Alerts and Packet Log data to be preserved** as 30 and **Number of Alerts to be preserved** as 2000, then only the latest 2000 alerts and packet logs generated over the last 30 days are retained in the database.

Host Event data

1. Type the **Number of days of Host Event data to be preserved:** You can specify a value between 0 and 9999.
2. Type the **Number of Host Entries to be preserved**: Describes the number of quarantined host entries that can be preserved. You can specify a value between 0 and 9999.

For example, enter **Number of days of Host Event data to be preserved** as 60 and **Number of Host Entries to be preserved** as 6000. Assume that the Manager database contains host event data for 100 days. When you click **Purge**, host events of the oldest 40 days will be removed first. Out of the remaining host events for the most recent 60 days, if there are 8000 host entries, 2000 host entries will be removed. If there are only 5000 entries, all the entries will be preserved.

IMPORTANT

The tool considers the value entered in **Number of days of Host Event data to be preserved** first irrespective of the value entered in **Number of Host Entries to be preserved.**

Application Data

Specify the Application data that you want to preserve using the following fields:

1. **Number of days of Raw Application data to be preserved**
2. **Number of days of Hourly Application data to be preserved**
3. **Number of days of Daily Application data to be preserved**
4. **Number of weeks of weekly Application data to be preserved**
5. **Number of months of monthly Application data to be preserved**

Sensor Performance data

Specify the Sensor performance data that you want to preserve using the following fields:

1. **Number of days of Raw performance data to be preserved**
2. **Number of days of Hourly performance data to be preserved**
3. **Number of days of Daily performance data to be preserved**
4. **Number of weeks of weekly performance data to be preserved**
5. **Number of months of monthly performance data to be preserved**

You can specify a value between 0 and 9999.

Once you have completed specifying the amount of data to be preserved, click **Purge**.

NOTE

In cases where purging is aborted for some reason, data that has already been purged is not recovered.

If you have chosen to tune after purge, then the database is tuned after the purge is complete.

Change your database password

You can change your Trellix IPS database password using the standalone Database Admin tool. Note that this is **not** the MariaDB Root password.

> **NOTE**
>
> The Manager has to be stopped when the password is being changed.

To change your Trellix IPS database password:

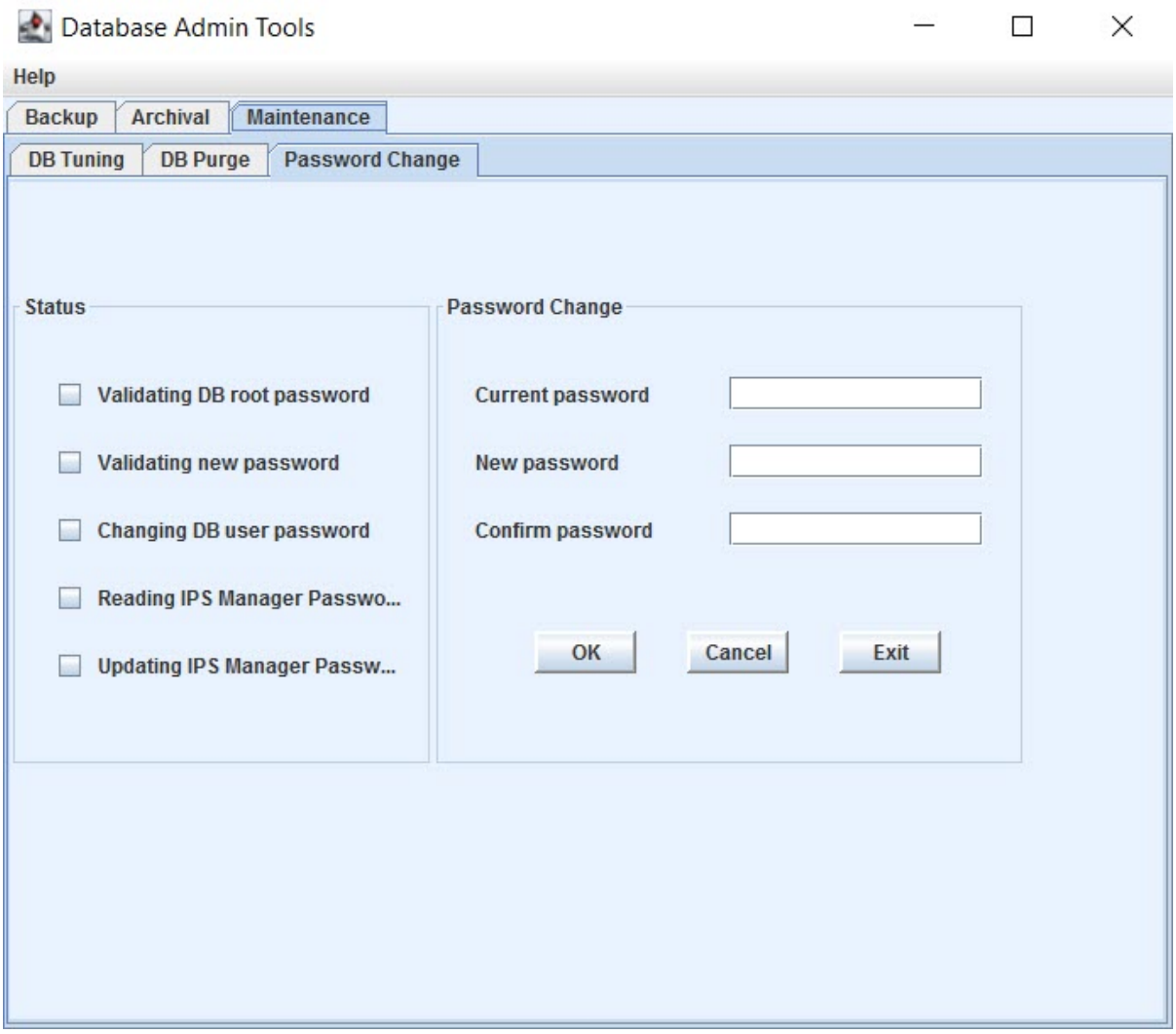
Steps:

1. Navigate to `<Manager_Install_Dir>\bin`.

   > **NOTE**
   >
   > The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

2. Execute the **dbadmin.bat** file. The standalone tool opens.
3. Select Maintenance → **Password Change**.

Figure 90. Database Admin Tools - Password Change Tab



4. Enter the current and new passwords in their respective fields.

   Ensure that you do not leave the password fields blank or reenter the current password as the new password again.
5. Confirm the new password by entering it in the **Confirm password** field.
6. Click **OK**.
7. Enter the MariaDB Root Password (that you specified during Manager installation).
8. Click **OK**.

Troubleshooting

Manager health checks

A set of checks can be performed to diagnose the Manager's health. The checks range from gathering the basic information, such as viewing the active signature set version, to more advanced checks, such as the number of low memory detections in the Manager.

Health checks provide real-time visibility into the health of the Manager, diagnose for known issues, and present the results in a format that can be easily understood by administrators. The results can be exported for further analysis. Health checks not only simplify troubleshooting, but also provides a way to check that the Manager runs smoothly.

NOTE

The Manager health checks can only be run in the root admin domain.

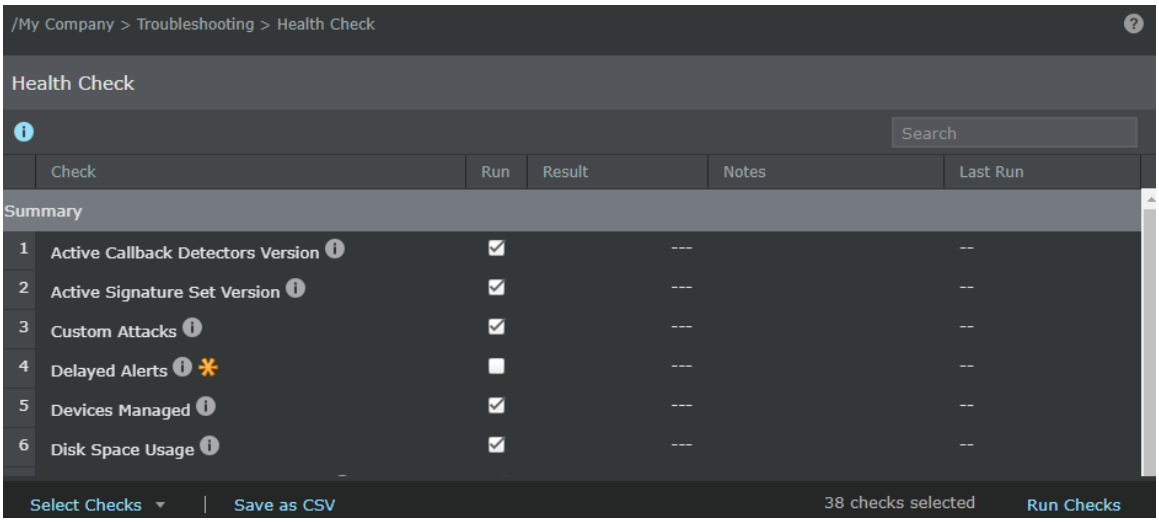
Health check provides a pass/fail indicator for some checks like **Alert Delays** check. For some health checks like **Manager Software Version** check, displays only the requested information. By just having a glance on the **Health Check** page, you can quickly analyze whether the Manager is running smoothly or whether it is experiencing any trouble.

Run health check in the Manager

Use the health check results for further analysis or for troubleshooting purposes.

Steps:

1. Select Manager → <Admin Domain Name> → Troubleshooting → **Health Check**. The **Health Check** page is displayed.



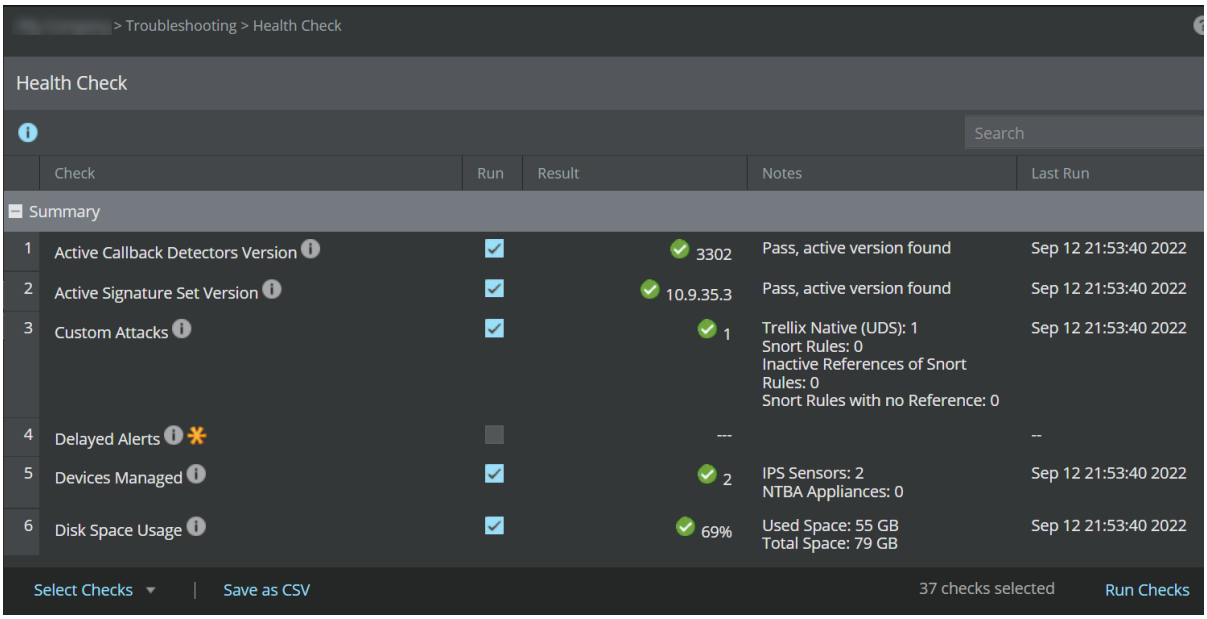
The **Health Check** page displays with the following fields.

Field Name	Description
Check	Displays the list of health checks available in the Manager. The health checks lists are grouped into the following categories: • **Summary** - Checks on basic summary of Manager's performance, for example, the memory currently free in the Manager • **Database check** - Checks the database, for example, the number of alerts that are stored in the database • **Connectivity checks** - Checks the connectivity status, for example, Manager's connectivity with its MDR peer Place the mouse pointer over the icon to view the description of the health check. The icon indicates that the health check is an advanced health check.
Run	Health checks are performed in the Manager only for those health checks that are enabled by selecting the checkboxes in the **Run** column. By default, the checkboxes for default health checks are selected before running a health check for the first time.
Result	Displays the summary of the latest health check result
Notes	Displays any information in addition to the result summary that might be required, for example, when MDR is enabled, the check also displays the peer IP address and last synchronized time in the **Notes** column.
Last Run	Displays the time stamp of the latest health check that was performed. Example: Jul 03 12:14 GMT+05:30 2015.

NOTE

You can adjust the column width for any field by dragging the column line to customize the display of column width.

2. Click **Select Checks** and select the health check options. The following are the available options.
   - **Default (exclude advanced)** - This option is selected by default. Standard checks are those checks that can run quickly, for example, **Manager Software Version** and **Last Reboot**.
   - **All (include advanced)** - This option is selected to include all checks, including advanced checks like **Delayed Alerts**. Advanced checks take more time to execute and can possibly have an impact on the Manager performance.
   - **Summary Only** - This option selects only the summary checks which check on basic summary of the Manager's performance.
   - **Database Checks Only** - This option selects only database checks which check the database health.
   - **Connectivity Checks Only** - This option selects only connectivity checks which check the Manager's connectivity status.
   - **None** - This option is used to unselect all the selected health checks in the **Run** column.
3. Click **Run Checks**. The **Result**, **Notes**, and **Last Run** columns display the health checks details.



> **NOTE**
>
> Running a health check might display an error if none of the checkboxes are enabled in the **Run** column.

You can search and view a specific health check detail in the **Search** text field. Type the first few letters of any detail in any column and the health check matching with the search criteria is filtered and displayed. For example, to search for health check on GTI Server connectivity, type **`gti`** in the **Search** text field.

The filtering is based on the values in the **Check**, **Result**, and **Notes** columns. Apart from these filtering options, you can also filter based on the description given for each health check.

A green icon in the **Result** column indicates that the check has passed. A red icon is a pointer that indicates that the check has failed.

4. Click **Save as CSV** to save the health check result data in CSV format.

Monitoring System Faults

System Faults provide the functional status for all of your installed Trellix IPS components. Messages are generated to detail the system faults experienced by Trellix IPS.

Enable alert relevance

By default, you will find alert relevance enabled in the Manager. If you want to alter alert relevance settings in the Manager at any time, perform the following steps.

1. Select Manager → <Admin Domain Name> → Troubleshooting → **Alert Relevance**.

   The **Alert Relevance** page appears.

2. Select the **Alert Relevance Analysis?** checkbox.

3. Click **Save**.

Manager Policy Cache

The **Manager Policy Cache** option (Manager → <Admin Domain Name> → Troubleshooting → **Manager Policy Cache** or Manager → Troubleshooting → **Manager Policy Cache** in the case of Central Manager) allows you to clear the attack and policy caches without shutting down and restarting Manager. The policy cache may get out of sync with the database due to server errors, database errors, or client/server communication errors. Once you clear the caches, it may take a few minutes to open a policy in **IPS**, because the applied policy must be re-cached. The **Manager Policy Cache** window displays the following information:

- **Cached IPS Policies**— The number of policies in Manager cache.
- **IPS Policy Names**— The names of policies in Manager cache.

To clear the Manager Cache, do the following:

Steps:

1. Select Manager → <Admin Domain Name> → Troubleshooting → **Manager Policy Cache** (or Manager → Troubleshooting → **Manager Policy Cache** in the case of Central Manager).
2. Click **Clear Caches**.

Monitoring traffic in NTBA Appliance

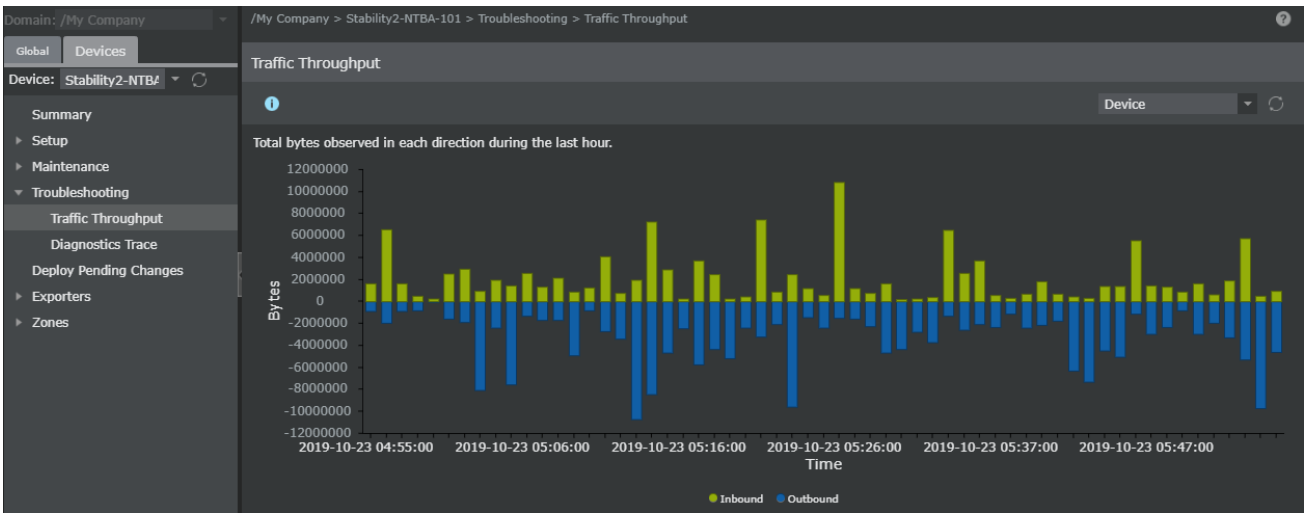
You can monitor traffic per NTBA Appliance to check if traffic is going through the device, zone, or its exporter's interface.

Steps:

1. Select Devices → Devices → <NTBA Appliance> → Troubleshooting → **Traffic Throughput**.

   The **Traffic Throughput** page is displayed. By default **Device** is selected.

Figure 91. Traffic throughput for NTBA Appliances



2. Select **Device** to generate a bar graph showing the total bytes observed in each direction for the last hour.
3. Select **Zones** to display the throughput for each zone in each direction with the time when the last packet was seen on that zone.

   You can use the **Search** field to search by a particular zone of the device.
4. Select **Exporters** to display the combination of exporter and interface, its line speed, and the utilization percentage in each direction.

   You can use the **Search** field to search by a particular zone of the device.

Logs

The Manager → <Admin Domain Name> → Troubleshooting → **Logs** (Manager → Troubleshooting → **Logs** in case of Central Manager) option enables a privileged user to view information like faults, system files, background tasks, user activities, and MDR events. The information displayed in the **Logs** page are from different log files available in the Manager database, thus providing a beneficial resource for analysis and/or problem-solving.

The different tabs available in the **Logs** page are as follows:

- **Faults**: Displays system faults information
- **System Files**: Displays system logs information based on user activity or general system information
- **Background Tasks**: Displays status of long running processes in your system
- **User Activities**: Displays all user actions in the Manager
- **MDR Events**: Displays previous MDR activities

Filter logs

You can filter logs based on the period in which the logs were generated. The **Custom Time Period** option lets you customize the time period. When the [time period] option is selected, the logs are displayed for the chosen time period. By default, the logs for [last 7 days] are displayed.

When looking for a particular log, you can enter the keyword for the log in the **Quick Search** field and the results are automatically displayed in the log. Click **Clear All Filters** to undo all filters applied. The button color and the column header color changes to orange which indicates that a filter is active, and that the particular logs tab is not displaying all entries.

The entries in different tabs of the **Logs** page are not refreshed automatically. Use the refresh icon to view new logs generated. Use the arrow keys at the bottom of the page to navigate back and forth between the pages in a tab.

Sort, group, and filter logs

The tabs in the **Logs** page display thousands of log items and it consumes time to search for specific type of log item. To enable you to find a particular log item, the sorting, grouping, and filtering feature is available for each tab in the **Logs** page. Using this feature you can group and filter the logs based on specific fields and sort the logs in ascending or descending order.

The different options available in each column are as follows:

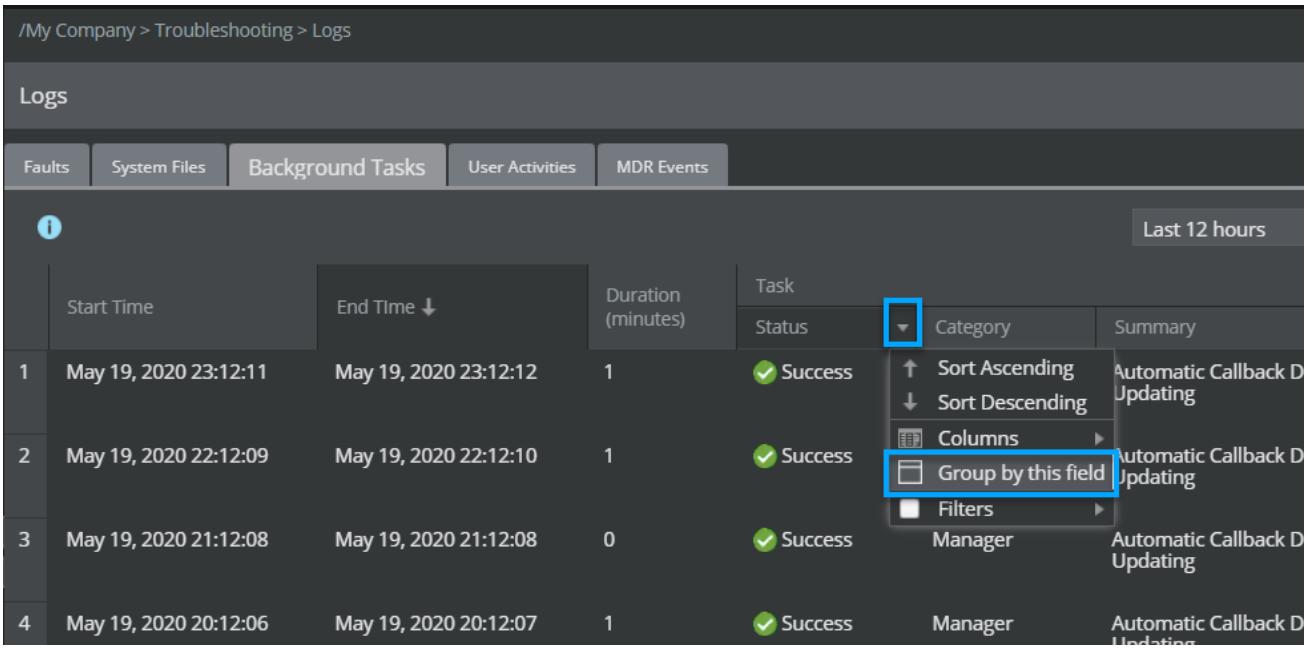
Options	Definition
Sort Ascending	Sorts the logs table in ascending order with the column header as core attribute

Options	Definition
Sort Descending	Sorts the logs table in descending order with the column header as core attribute
Columns	Allows you to select the columns to be displayed on a particular tab
Group by this field	Allows you to consolidate and view a group of log entries based on specific fields in the column for a particular tab. For more information about how to group the log entries, refer to [View grouped logs]. **NOTE** The options in the **Group by this field** vary across the columns on a tab.
Filters	Allows you to apply filters to specific columns on a tab **NOTE** The options in the **Filters** vary across the columns on a tab.

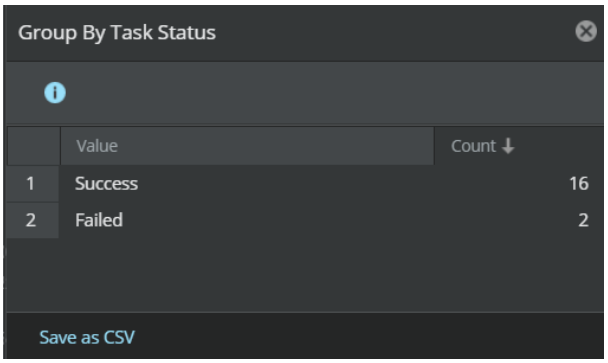
View grouped logs

You can consolidate and view a group of logs based on specific fields on each tab of the **Logs** page. To view a consolidated group of logs, perform the following steps:

1. Select Manager → <Admin Domain Name> → Troubleshooting → **Logs**.
2. In the **Logs** page, select the tab you want to view a group of logs for.
3. Click the arrow in the triangular icon in the column header of the field by which you want to group the logs and select **Group by this field**.



A window is displayed for the selected field. For example, if you select the **Group by this field** option for the **Status** field, the **Group By Task Status** window is displayed.

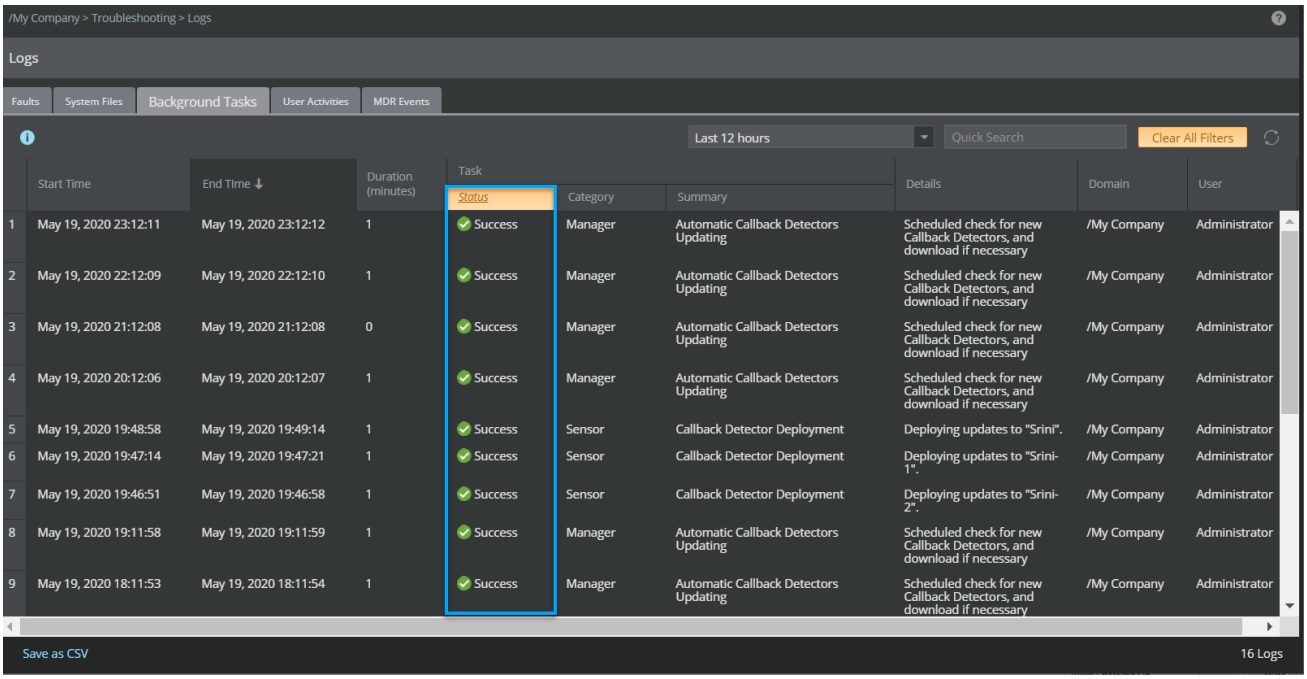


The following options are available in the **Group By <field name>** window.

Option	Definition
Value	Displays the list of items available for the selected field. For example, the **Group By Task Status** window displays the following items: • **Success** • **Failed**
Count	Displays the total count of the logs for each group
Save as CSV	Saves a copy of the list of items available and the total count for the selected field

You can further sort the logs in **Group By <field name>** window by sorting the columns in ascending or descending order.

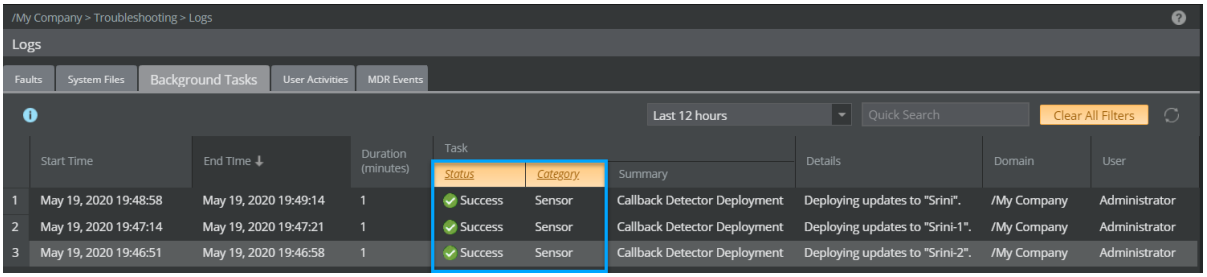
4. In the window, double-click on the row of the item you want to view the grouped logs for. The window closes and the grouped logs are displayed in the **Logs** page.



NOTE

The column header color changes to orange, which indicates that the logs are grouped by that option and only those logs are displayed in this page.

In this example, after grouping the logs, you can further group them to the next level of grouping by selecting the **Group by this field** option on any other column header where this option is available. For example, after grouping the logs based on **Success** from the **Status** field in the **Task** column, you can further filter the group based on **Sensor** from the **Category** field in the **Task** column. As a result, the **Logs** page displays only those logs which have **Status** as **Success** and **Category** as **Sensor**.



Logs can be grouped by all fields in the **Logs** page, except for the following columns:

- **Faults**: **Time**, **Summary** under **Faults** column, **Details**, **Recommended Action**, and **Duration**
- **System Files**: **Time** and **Message**
- **Background Tasks**: **Start Time**, **End Time**, **Duration (Minutes)**, and **Details**
- **User Activities**: **Time** and **Details**
- **MDR Events**: **Time** and **Details**

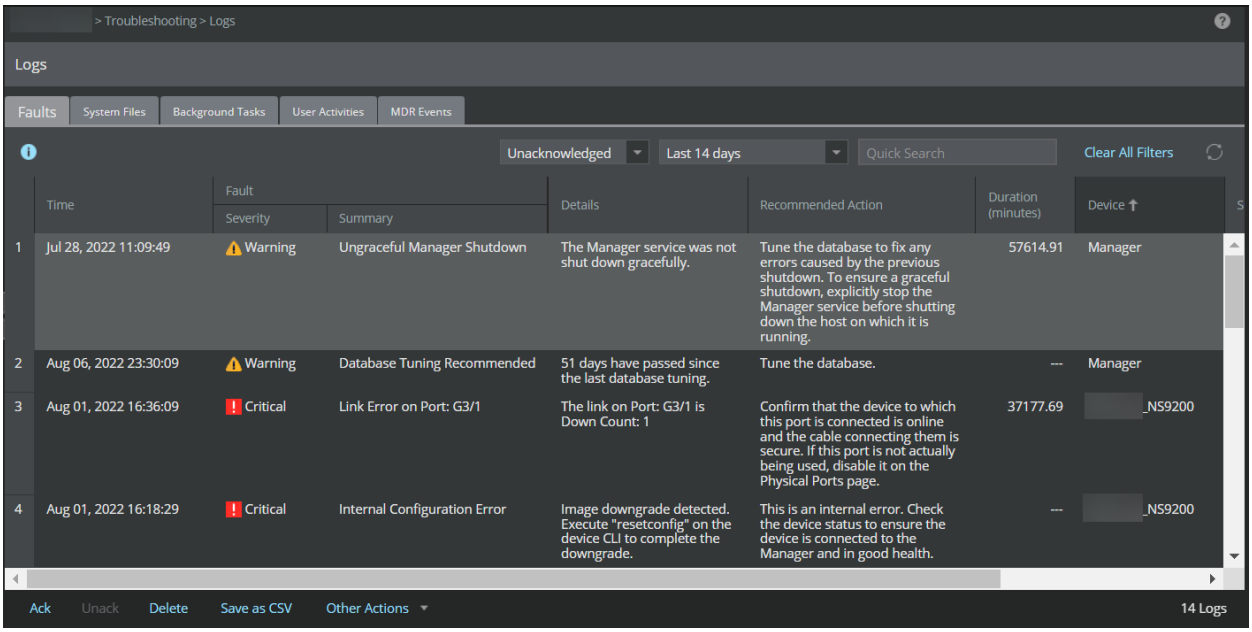
To remove the filtering of grouped logs, click **Clear All Filters**.

Faults

The Faults tab page displays messages that are generated to detail the system faults experienced by Trellix IPS.

To view the faults, follow the steps below:

1. Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** and select **Faults** tab to view the system faults.



The data displayed in the table is based on the time frame of the core attribute in the faults table. By default, the logs for [last 7 days] are displayed. The data can be filtered for the time period of your preference using the **Custom Time Period** option.

The following table lists the fields on the **Faults** tab:

Options	Definition
✔	Displays when a fault is acknowledged **NOTE** By default, acknowledge column is hidden.
Time	Displays date and time of fault occurrence

Options	Definition
Fault	Displays severity and summary of the activity • **Severity**: Displays severity level of the activity. Different severity levels are as follows: • **Informational** • **Warning** • **Error** • **Critical** • **Summary**: Displays brief summary of the activity
Details	Displays brief report on nature of the activity
Recommended Actions	Displays the action to be performed to remediate the faults
Duration	Displays the time length of fault condition **NOTE** The **Duration** option is not applicable for all faults.
Device	Displays the device name for which the fault is generated **NOTE** For Central Manager, the Manager name is displayed for which fault is generated.

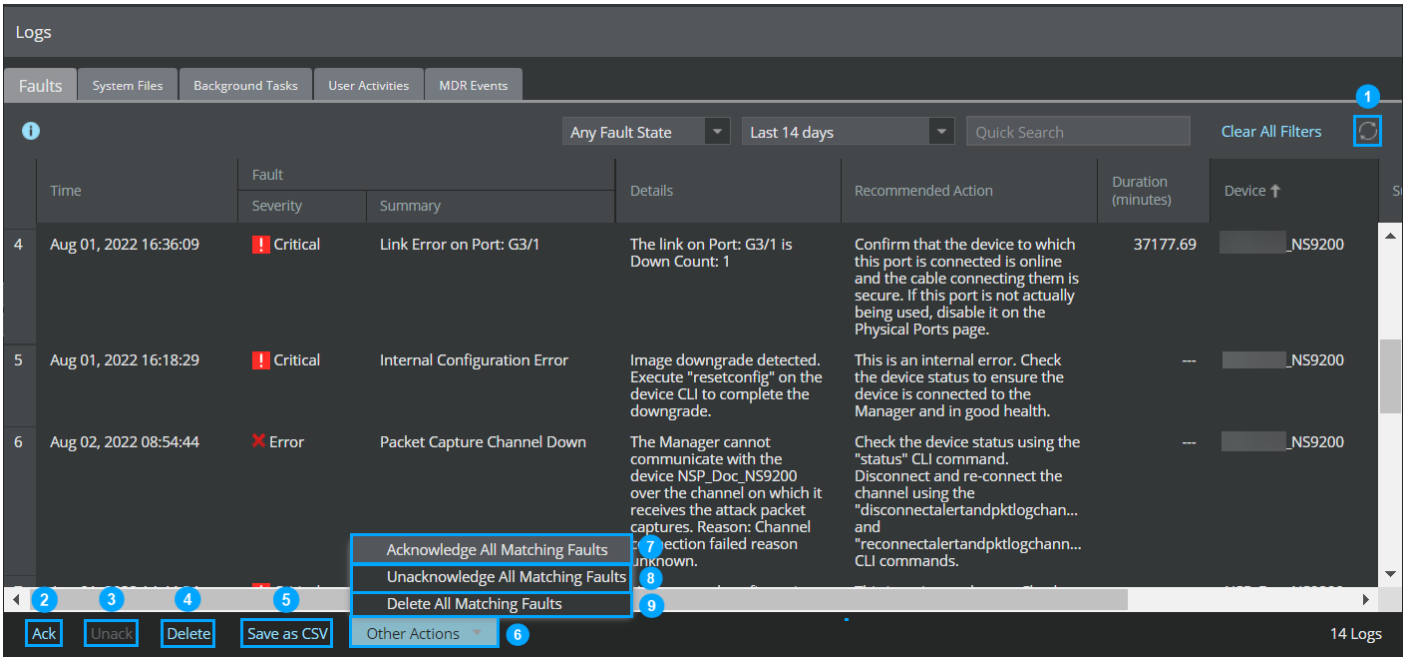
2. You can save a copy of faults by clicking **Save as CSV**.

NOTE

The **Save as CSV** option saves a copy of system faults based on the filters applied. To save a copy of all system faults, clear all filters before saving it as **Save as CSV**.

Faults tab action buttons

The following action buttons are available in the **Faults** tab:



Callout	Action button
1	**Refresh**—Updates the Manager faults log with new faults from the database.
2	**Acknowledge**— Marks the fault as acknowledged/read. Acknowledging a fault means that you are aware of its existence and plan to take appropriate action. The **Ack.** field displays a checkmark on manual acknowledgment. When you acknowledge a fault, the fault will still be available in the Manager which can be used for analysis later.
3	**Unacknowledge**— Marks the faults as unrecognized and the **Ack.** field is blank. By default, all logs are unacknowledged. You can unacknowledge an acknowledged log.
4	**Delete**— Deletes the selected faults from the Manager.
5	**Save as CSV**— Saves a copy of the faults displayed with filters applied.
6	**Other Actions**— You can perform further actions on the faults using the option available under **Other Actions**. The **Other Actions** has the following options: • Acknowledge All Matching Faults • Unacknowledge All Matching Faults • Delete All Matching Faults
7	**Acknowledge All Matching Faults**— Acknowledges all faults of the same type for the selected filter range.
8	**Unacknowledge All Matching Faults**— Unacknowledges all faults of the same type for the selected filter range.
9	**Delete All Matching Faults**— Deletes all faults of the same type for the selected filter range.

For a complete listing of system fault messages and their interpretation, see the [Troubleshooting] section.

System Files

The **System Files** tab enables a privileged user to view system information either by user activity or general system information. The **System Files** tab pulls user-activity information from the database and system-activity information from the log files (such as ems.log files), thus providing a beneficial resource for analysis and/or problem-solving.

How to view and export Manager activity log

The **System Log** option enables you to view and export system activity entries immediately in the Manager log files. By default, this information includes performed actions, system faults, and debug data. You can customize the log query to display only the data you want to see, such as debug data only or Warning-level faults only. Each log file is numbered incrementally based on the recorded data. Once the files exceed 3MB, a backup file is created (ems.log.1, ems.log.2, etc.) and the latest logs are available in the ems.log file.

By default, the log files are located at `<Manager_Install_Dir>/app/logs/<all log files>`.

NOTE

For more information on System Log files, see System Files (page 346).

Note that in Central Manager, the **System Log** option functions are similar to that in Manager described above.

NOTE

Only Super Users, System Administrators, and Security Experts can view the system log.

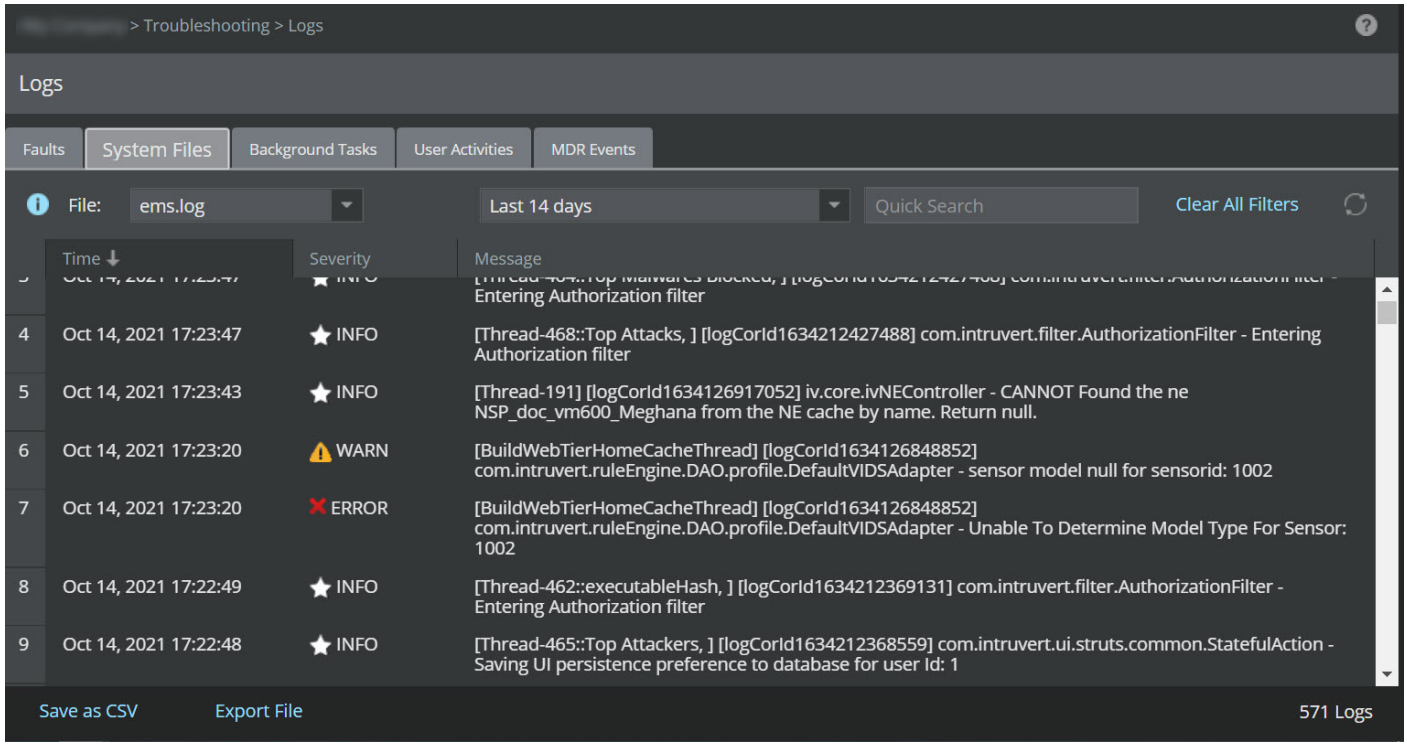
NOTE

Only log files smaller than 4 MB can be viewed or exported from within the user interface. Larger files must be accessed directly via the file system.

View system events information

Steps:

1. Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** and select **System Files** tab.
2. Select a **File** from the drop-down list.
3. The **System Files** table is displayed with logs for the selected file type.



NOTE

The maximum number of logs displayed in any system file is 50,000.

The following is table lists the information displayed in the **System Files** table:

Column	Description
Time	Displays date and time of event occurrence.
Severity	Displays severity of the event. The different severity levels are as follows: • **ALL**— All actions performed/recorded by the system. • **DEBUG**— Only debug information for the system. • **INFO**— Only configuration information, such as when an action is performed. • **WARN**— Only system warning (medium severity) information. • **ERROR**— Only system error (high severity) information. • **FATAL**— Only crash/failure information.

Column	Description
Message	Displays the following information for the activity. • **Status**— Displays the status of the activity. The activity will be in **Successful**, **Failed**, or **In-progress** state. • **Category**— Displays category of the activity. • **Summary**— Displays brief summary on nature of the activity.

Export system files

Steps:

1. Select **System Files** tab in Manager → <Admin Domain Name> → Troubleshooting → **Logs**.
2. Select a **File** which you want to export.
3. Click **Export**.

> **NOTE**
>
> The file selected is copied to your local machine. The exported log file contains all events without any filters.

Background Tasks

The **Running Tasks** monitor of the **Dashboard** page displays the status of currently In-Progress activities on your system that Trellix IPS identifies as long running processes.

When a long running process is taking place in your Manager, the status is displayed as "In progress" in the **Running Tasks** monitor. You can also go to **Logs** page and select **Background Tasks** tab to view long running processes. Once the activity is completed, the entry for that activity is removed from the **Running Tasks** monitor and displayed only under **Background Tasks** tab in the **Logs** page.

Management of long running processes

Trellix IPS helps you identify long running processes, including in-progress and completed activities within your active Manager (or Central Manager). You can view/track scheduled processes as well as user initiated processes for activities. The long running processes that you can view in Manager are the ones that Trellix recommends you keep a track of.

If a long running activity includes several sub-activities, then Trellix IPS provides an activity log for each of the sub-activities. For example, an activity like signature update involves two long running sub-activities: downloading the signature set, and updating the signature set on all the Sensors that have the real time update enabled. These sub-activities are tracked separately and the status for each is displayed separately as well.

Trellix IPS identifies the following as long-running activities:

- Signature set download from Trellix IPS Update Server

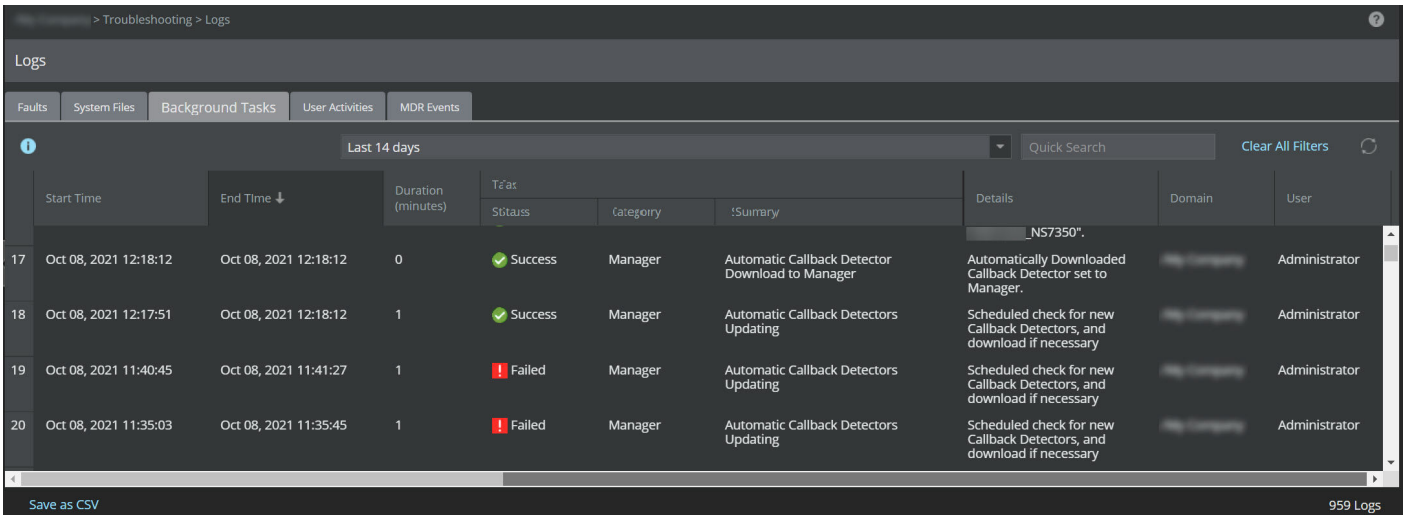
- Signature set update on all active Sensors
- Sensor software download from Trellix IPS Update Server
- Sensor software update on all Sensors
- Cumulative policies update due to signature set download or editing of overriding rules
- Custom Attack Editor export to the Manager
- Report generation
- Data Backup using the Manager
- Data Restore using the Manager
- Database dump transfer/import for an MDR pair
- Database tuning using the Manager
- File maintenance
- Alert archival using the Manager
- Archived alerts restore using the Manager
- Alert data purge using the Manager

NOTE

Trellix IPS records the above mentioned activities for both scheduled as well as user initiated processes.

How to view long running processes

Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** page and select **Background Tasks** tab.



NOTE

The display of long running processes is governed by the admin domain ownership. For example, if your Manager setup has a child admin domain, go to Manager → <Child Admin Domain> → Troubleshooting → **Logs** and select **Background Tasks** to view the long running processes for that child admin domain.

Trellix IPS logs the long running processes against the **<Owner Admin Domain>** and the user who performs the activity. The result for each activity is displayed as "Failure," "Success," or "In Progress" (if still running). You can also view a summary of the activity in the **Details** field.

Once an activity is completed, the entry for that long running activity is removed from the **Running Tasks** monitor in **Dashboard** page and displayed under **Background Tasks** tab in the **Logs** page.

The following table lists the information displayed in the **Background Tasks** tab:

Options	Definition
Start Time	Displays time and date of the task initiation.
End Time	Displays time and date of the task completion.
Duration	Displays time taken by the activity to be completed. **NOTE** The duration is always displayed in minutes.
Task	Displays the following information for an activity. • **Status**— Displays the status of the activity. The activity will either be **Successful**, **Failed**, or **In-progress** state. • **Category**— Displays the category of the activity. • **Summary**— Displays brief summary on nature of the activity.
Details	Brief report of the activity.
Domain	Name of the admin domain where the activity is performed.
User	Name of the user initiating the activity.

User Activities

The User Activities tab enables the admin to view all user actions in the management system. An audit can help to determine what a user has done in order to determine mistakes, overwriting, or other issues about user activity.

The various categories of user activities include:

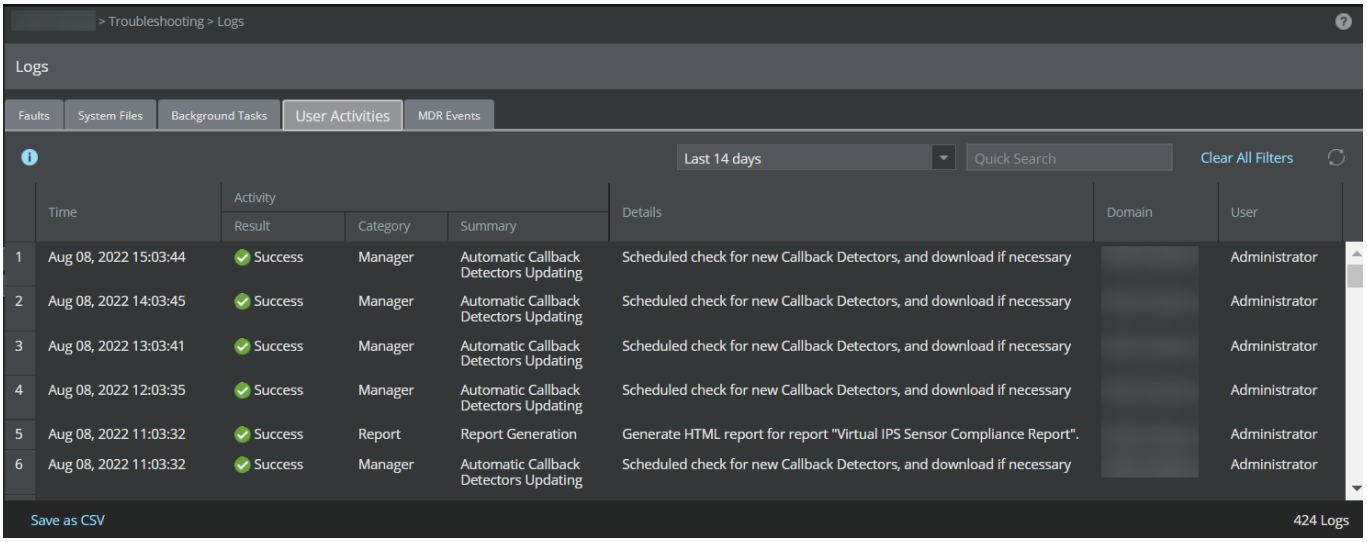
- Admin Domain
- User
- Manager

- Sensor
- IPS Policy
- Report
- Update Server
- Operational Status
- Threat Analyzer
- NTBA
- FIPS Self Test
- ePolicy Orchestrator
- Controller
- Unspecified

To view the user activities, follow the steps below.

Steps:

1. Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** and select **User Activities** tab to view the user activities table.



The data displayed in the table is based on the time frame of the core attribute in the user activities table. The data can be filtered for the time period of your preference using the **Custom Time Period** option. The default value is [last 7 days].

The following is table lists fields in the **User Activities** tab:

Options	Definition
Time	Displays date and time of activity occurrence.

Options	Definition
Activity	Displays the following information for a user activity: • **Result**: Displays result of the activity. The result of the activity will either be **Successful** or **Failed**. • **Category**: Displays category of the activity. • **Summary**: Displays brief summary of the activity.
Details	Displays brief report of the activity.
Domain	Displays name of the admin domain where the activity is performed.
User	Displays name of the user initiating the activity.

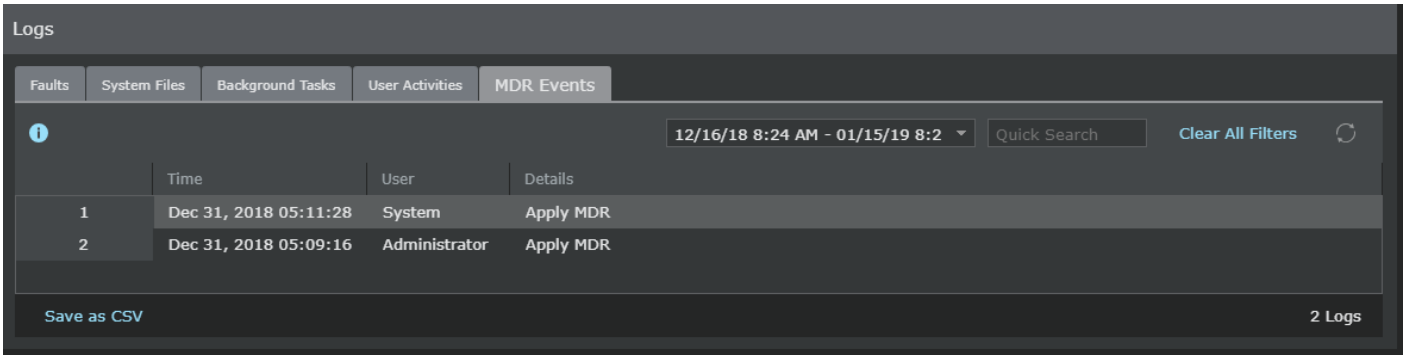
2. You can save a copy of user activities by clicking **Save as CSV**.

> **NOTE**
>
> The **Save as CSV** option saves only the copy of user activities based on the filters applied. To save a copy of all user activities, clear all filters before using saving it as CSV.

MDR Events

The **MDR Events** tab enables you to view previous MDR activities, including the date and time on which the activity occurred, the users performing the activity, and the nature of the activity.

Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** and select **MDR Events**.



The following table lists fields in the **MDR Events** tab:

Options	Definition
Time	Displays date and time of event occurrence.
User	Displays name of the user performing the activity.
Details	Displays brief description on nature of the activity.

Dashboard tab overview

The first page that you view after a successful logon to the Manager is the **Dashboard** tab.

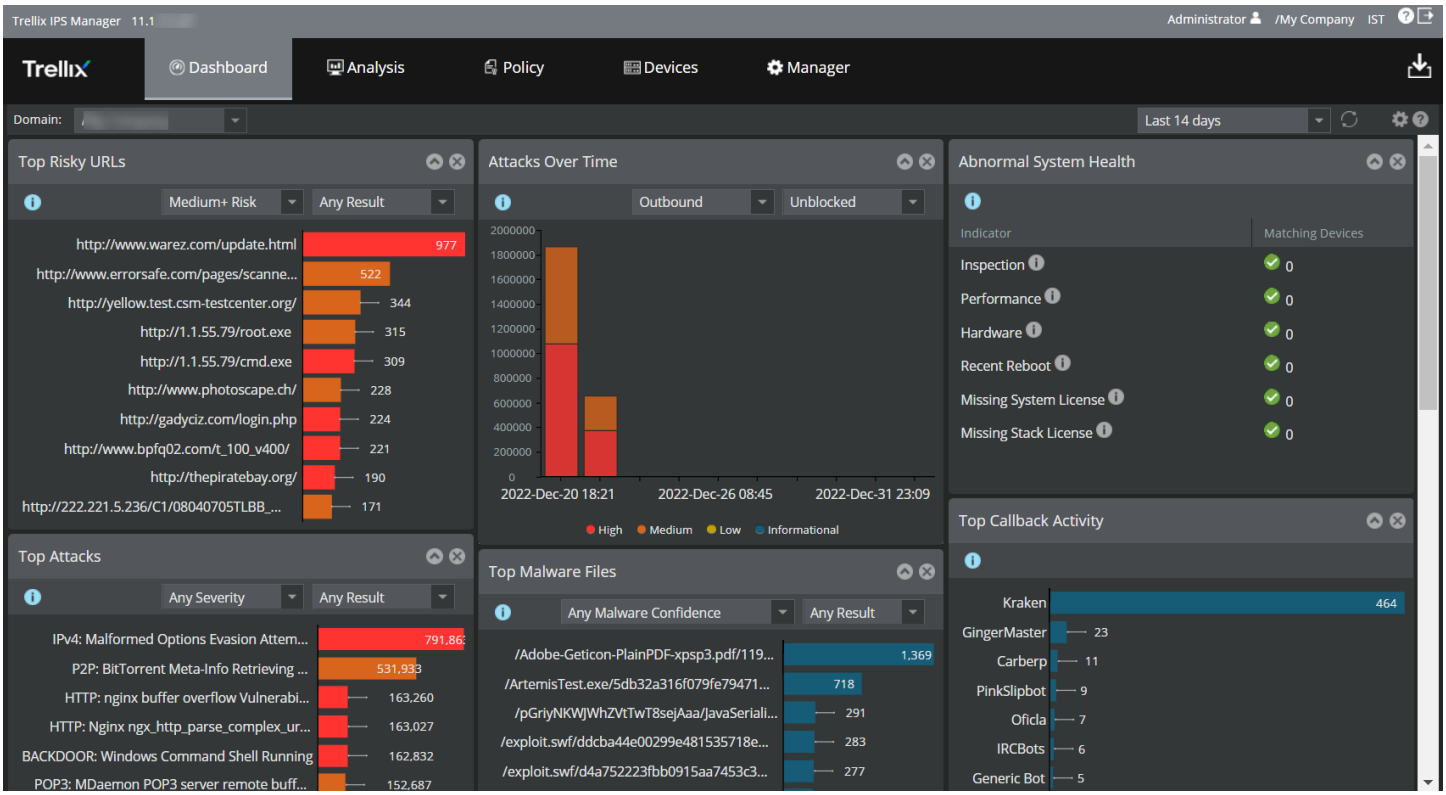
Dashboard tab

The **Dashboard** tab is the central interface from which all Manager interface components are available. The **Dashboard** tab is divided into two sections: the top menu bar and the lower monitors section.

By default, you can view the following security and operational monitors:

- Abnormal System Health
- Device Summary
- Manager Summary
- System Faults
- Top Applications
- Top Attacks
- Top Attackers
- Top Callback Activity
- Top High-Risk Endpoints
- Top Targets
- Top Malware Files
- Update Status

Figure 92. Dashboard tab



NOTE

The default time range is **Last 12 hours** and **Automatic Refresh** is set to 10 minutes.

Data viewed on the **Dashboard** can be customized according to your time preference using the **Custom Time Period** option from the refresh drop down. In addition, you can add monitors of your choice. You can also drag and drop these monitors on the **Dashboard** tab. The monitors display data based on the admin domain selected. Data from the child domains can also be included. In such cases, the data displayed in the monitors will also include data from the child domains. By default, the monitors display data for the root admin domain. **Include child domains** is selected by default.

NOTE

By default, all logons to the Manager display data in the dashboard for the root admin domain.

You can use the following options to customize your **Dashboard** tab view.

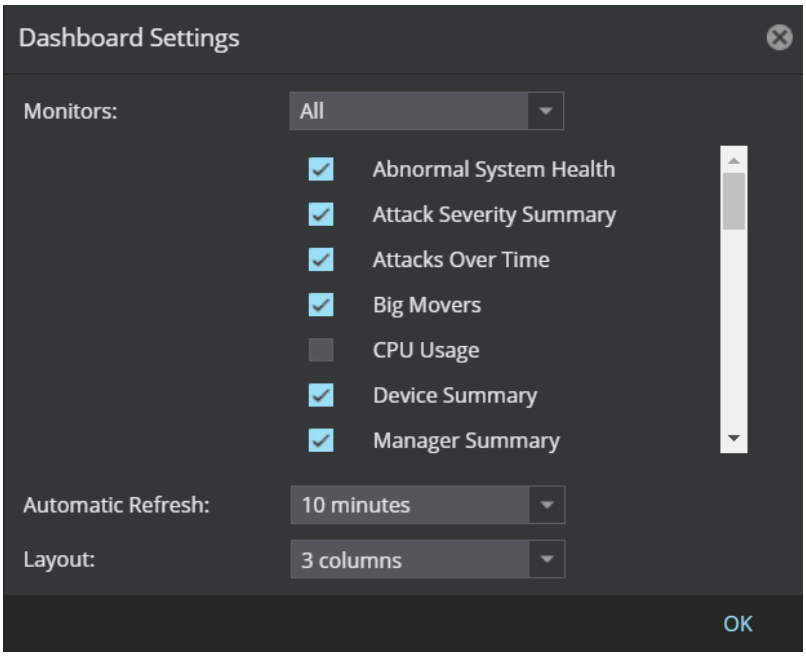
Name	Icon	Description
Hide		Minimize the monitor of your choice.
Expand		View the monitor of your choice.

Name	Icon	Description
Refresh		Manually refresh the page. Alternatively, set the automatic refresh time from the **Dashboard Settings** window. The default refresh time interval is 10 minutes.
Edit		View the **Dashboard Settings** dialog.

Dashboard Settings

Use the **Dashboard Settings** window to further customize your **Dashboard** tab view.

Figure 93. Dashboard Settings dialog



You can perform the following tasks here:

- **Monitors**— Use this option to select the monitors to view. The default category is **All**. Use the **Operational** or **Security** category to choose the monitors you want to view. You can also customize the data displayed in the monitors based on the admin domain and child domain. Monitors display data based on the admin domain selected from the **Domain** drop-down list.

  The following monitors are displayed under different categories:

Category	Monitors	Description
All		View both Operational and Security monitors.
Operational		
	Abnormal System Health	View the indicators of the health of Sensors.

Category	Monitors	Description
	CPU Usage	View the high CPU usage of the Sensor.
	Device Summary	View the current versions of the Sensor software and signature set of the logged in domain.
	Manager Summary	View the Manager details such as software version, signature set version, and others.
	Memory Usage	View the high memory usage of the Sensor.
	Release Announcements	View the latest updates and the current version of signature set applied to your Sensor.
	Running Tasks	View the status of all the Sensors configured in the Manager.
	System Faults	View the health of your device and the Manager.
	Throughput Usage	View the high throughput usage of the Sensor.
	NOTE Data remains unchanged for the **Manager summary**, **Release Announcements**, and **Running tasks** monitors irrespective of the admin domain selected. The **System Faults** and **Device Summary** monitors display the list of all the child domains linked to the admin domain selected.	
Security		
	Attack Severity Summary	View the unacknowledged alerts in the database, sorted by alert severity
	Attacks Over Time	View the attacks over a period of time in your network.
	Big Movers	View the attacks whose frequency has increased during a selected time period.
	Top Applications (IPS)	View the top applications based on attacks, bytes or connections.
	Top Applications (NTBA)	View the top applications in the NTBA device based on bytes or connections. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top Attack Subcategories	View the attack subcategories in your network.
	Top Attacker Countries	View the top attacker countries in your network.
	Top Attackers	View the top attackers in your network.
	Top Attacks	View the top attacks in your network.
	Top Callback Activity	View the callback activity.

Category	Monitors	Description
	Top Destinations (NTBA)	View the top destinations based on bytes or connections. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top Endpoint Executables (NTBA)	View the top executables based on number of endpoints using them or the number of attacks they have initiated. You can filter the executables based on the device, attacks (default) or endpoints, malware confidence, and classification. **NOTE** This monitor is populated only if you have enabled EIA integration.
	Top Endpoints Using Risky URLs	View the top endpoints using risky URLs in your network.
	Top Files (NTBA)	View the top files based on malware confidence level. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top High-Risk Endpoints	View the high-risk endpoints of your network.
	Top Malware Files	View the top malware downloads in your network. You can filter malware based on their confidence and detections (blocked, unblocked, and all).
	Top Risky URLs	View the top risky URLs of your network.
	Top Sources (NTBA)	View the top sources based on bytes or connections. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.
	Top Target Countries	View the top target countries in your network.
	Top Targets	View the top targets in your network.

Category	Monitors	Description
	Top URLs (NTBA)	View the top URLs at risk. **NOTE** At least 1 NTBA appliance is required to be configured to view this monitor.

NOTE

The Dashboard displays only the top 10 unacknowledged alerts under each Security Monitor. To view the acknowledged alerts, go to the **Attack Log** page and select **Acknowledged** from the drop-down list. You can also select **Any Alert State** from the drop-down list, and the Manager will display both acknowledged and unacknowledged alerts.

- **Automatic Refresh**— Use this option to set the automatic refresh time. The default time is 10 minutes. The minimum and maximum time for the automatic refresh are 1 minute and 10 minutes, respectively. For a manual refresh, select **Disabled** to disable the automatic refresh.
- **Layout**— Use this option to customize the number of columns to be displayed on the **Dashboard** tab.

NOTE

Data displayed in the **Top High-Risk Endpoints** monitor is automatically refreshed by the Manager on an hourly basis. This is not user configurable.

Security monitors

You can view and investigate the top threats in your network from the **Dashboard** page.

The Dashboard page displays the top threats as security monitors:

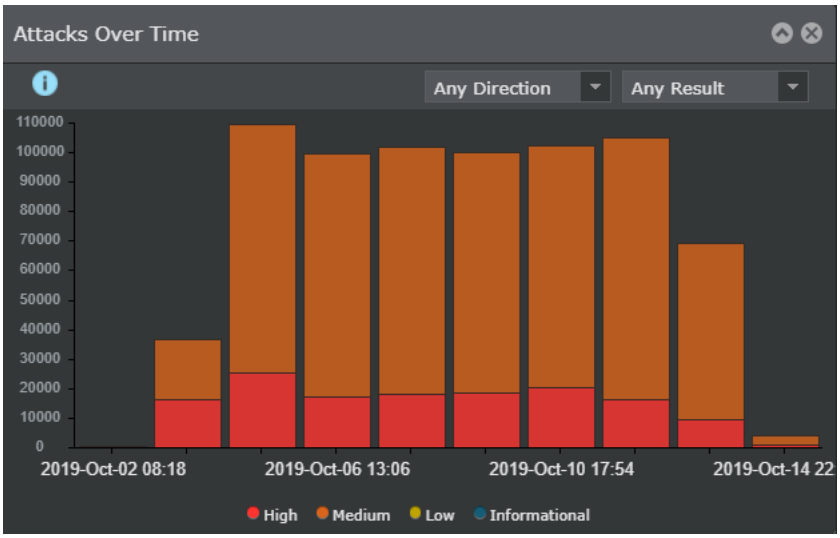
- Attack Severity Summary
- Attacks Over Time
- Big Movers
- Top Applications (IPS)
- Top Applications (NTBA)
- Top Attacker Subcategories
- Top Attacker Countries
- Top Attackers
- Top Attacks
- Top Callback Activity
- Top Destinations (NTBA)

- Top Endpoint Executables (NTBA)
- Top Endpoints Using Risky URLs
- Top Files (NTBA)
- Top High-Risk Endpoints
- Top Malware Files
- Top Risky URLs
- Top Sources (NTBA)
- Top Target Countries
- Top Targets
- Top URLs (NTBA)

Attacks Over Time

The **Attacks Over Time** monitor enables you to view the number of attacks that have been detected at different time intervals. Each bar contains information related to the number of attacks and the time in which the attacks were detected.

Figure 94. Attacks Over Time



The following options in the first drop-down list are available in the monitor to view the attacks based on direction.

- **Inbound** - Displays the attacks on inbound traffic
- **Outbound** - Displays the attacks on outbound traffic
- **Any Direction** - Displays attacks on both inbound and outbound traffic

The following options in the second drop-down list are available in the monitor to view the attacks based on result.

- **Blocked** - Displays blocked attacks over a period of time
- **Unblocked** - Displays unblocked attacks over a period of time

- **Any result** - Displays both blocked and unblocked attacks over a period of time

Each bar represents the attacks based on severity level for different time intervals. Clicking on a bar, you will be redirected to the **Attack Log** page where more details on the attack are displayed.

The legend at the bottom of the monitor indicates the color for each severity level of the attack displayed in the bar graph. The severity levels are as follows:

- **High**
- **Medium**
- **Low**
- **Informational**

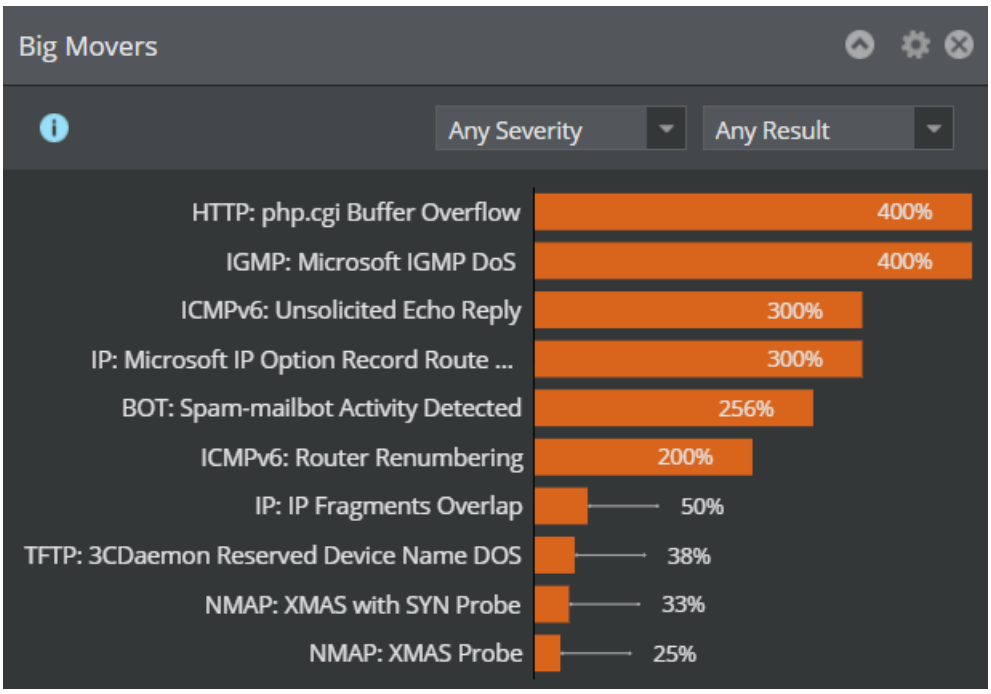
NOTE

To view or hide the display of attack data in the monitor for different severities, click on the color indicator that represents the severity.

Big Movers

The **Big Movers** monitor enables you to view the attacks whose frequency has increased during a selected time period. For example, if you select the time period as **Last 7 days** on the **Dashboard** tab and the current date is 27, the trend is calculated by comparing attacks in the last 7 days (dates 21 to 27) with attacks in the previous 7 days (dates 14 to 20).

Figure 95. Big Movers monitor



Each bar in the monitor represents the percentage increase in the attack count. Hovering over the bar for an attack, displays the following information:

- **Attack Name** - Name of the attack
- **Attack Severity** - Severity of the attack
- **Baseline Analysis Window Count** - Total count of the attack in the previous time window
- **Dashboard Analysis Window Attack Count** - Total count of the attack in the recent time window
- **Attack Count Increase** - Total increase in the attack count. This is the difference between the **Dashboard Analysis Window Attack Count** value and the **Baseline Analysis Window Count** value.

NOTE

Clicking on a bar in the monitor displays the corresponding attack details the Analysis → <Admin Domain Name> → **Threat Explorer** page.

For an attack to be displayed in the **Big Movers** monitor, the attack count should be greater than or equal to the minimum threshold value. The default minimum threshold value is 100. You can customize the value by clicking on the **Edit monitor settings** icon ( ) and set any value starting from 1 to 100000.

Figure 96. Big Movers monitor settings

The following options in the first drop-down list are available in the monitor to view the attacks based on severity.

- **Any Severity** - Displays attacks with any severity
- **High Severity** - Displays only high severity attacks
- **Medium Severity** - Displays only medium severity attacks
- **Low Severity** - Displays only low severity attacks

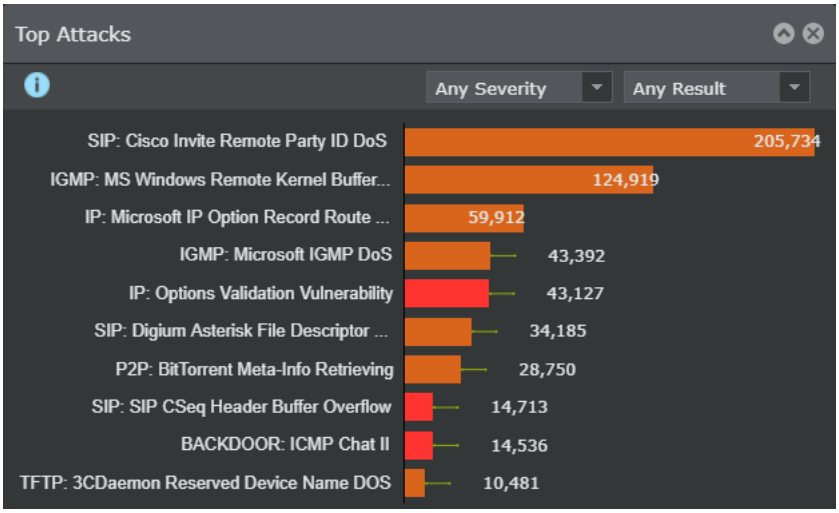
The following options in the second drop-down list are available in the monitor to view the attacks based on result:

- **Any result** - Displays both blocked and unblocked attacks over a period of time
- **Blocked** - Displays blocked attacks over a period of time
- **Unblocked** - Displays unblocked attacks over a period of time

Top Attacks

The **Top Attacks** monitor enables you to view the top attacks in the network for different levels of severity and results.

Figure 97. Top Attacks



The following options in the first drop-down list are available in the monitor to view the attacks based on severity:

- **Any Severity** - Displays the attacks on any severity
- **High Severity** - Displays the details of only high severity attacks
- **Medium+Severity** - Displays the details of only medium and high severity attacks
- **Low+Severity** - Displays the details of attacks with severity as low and above

The following options in the second drop-down list are available in the monitor to view the attacks based on result:

- **Blocked** - Displays the top attacks that are blocked by the Sensor
- **Unblocked** - Displays the top attacks that are unblocked by the Sensor
- **Any result** - Displays top attacks that are either blocked or unblocked by the Sensor

Each bar represents an attacks based on the selected severity and results. Clicking on a bar will redirect you to the **Threat Explorer** page where you can view more details about the attack.

Attack Severity Summary

The **Attack Severity Summary** monitor of the Dashboard page displays statistics for the unacknowledged alerts in the logged-in domain. Alerts are categorized by system impact severity level: High, Medium, Low and Informational.

Each time the Manager starts on the Manager server, the last 100,000 High, Medium, Low, and Informational alerts are retrieved from the database. After the Manager starts, any unacknowledged alerts are added to that initial 100,000. The alert count is calculated across all admin domains, so the total count of 100,000 alerts is based on time and not on admin domain. For example, out of 100,000 unacknowledged alerts, admin domain A may have 80,000, while admin domain B may have 20,000. If

you login with a Super User role, you will see alerts across all admin domains, where as users logged in with other user roles will see alerts specific to their domain.

Operational monitors

The **Dashboard** page displays operational monitors as follows:

- **Abnormal System Health** — Displays indicators that help you to gauge the health of the system
- **CPU Usage** — Displays the device CPU utilization
- **Device Summary** — Displays the current versions of the Sensor software and signature set of the logged-in domain
- **Manager Summary** — Displays the Manager details such as software version, signature set version, and others
- **Memory Usage** — Displays the memory utilization
- **Release Announcements** — Enables you to view any product or security-related messages. The messages can be related to operating system patches, signature set release, Manager software update, Sensor software update, and so on
- **Running Tasks** — Displays the status of currently In-Progress activities on your Manager that Trellix IPS identifies as long running processes
- **System Faults** — Displays the current health of the Manager and installed Sensors in Trellix IPS. Based on the severity of issues, the **System Faults** monitor displays messages like whether Manager/Sensor is up or down.
- **Throughput Usage** — Displays the Sensor throughput utilization

Abnormal System Health

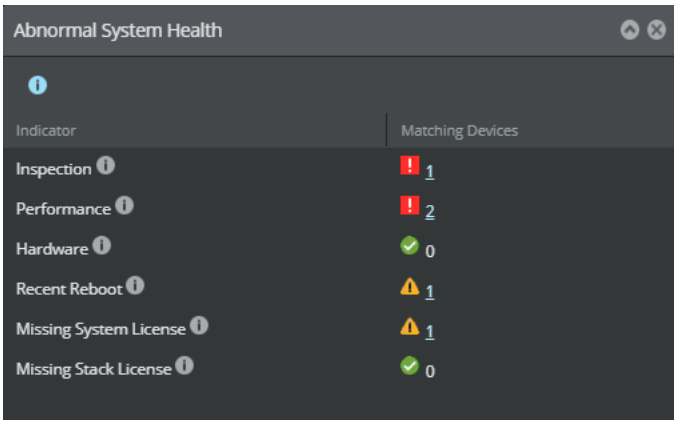
The **Abnormal System Health** monitor of the **Dashboard** page displays indicators that help you to gauge the health of the system. You can use this information to decide if your Sensors require new upgrade or regular maintenance will suffice. For example, if there are frequent performance related faults reported by a Sensor, you might want to consider buying new licences for increasing the capacity or upgrade the Sensor to a newer software version.

This monitor displays the following indicators :

- **Inspection** — Total number of devices in layer 2 bypass mode.
- **Performance** — Total number of devices with one or more performance faults.
- **Hardware** — Total number of devices with one or more hardware faults.
- **Recent Reboot** — Total number of devices that rebooted recently.
- **Missing System License** — Total number of devices that do not have a license but require one.
- **Missing Stack License** — Total number of stacks that does not have a license.

> **NOTE**
>
> The **Performance** and **Hardware** indicators display the historical data because all faults available in the Manager database are considered for calculating the count. Remaining indicators show real time data.

Figure 98. Abnormal System Health monitor



When you click on the number in the **Matching Devices** column, the **Device Manager** page opens with the relevant information for the indicator.

The description of color codes next to the values are as follows:

	Indicates no risk
	Indicates medium risk
	Indicates high risk

NOTE

The **Abnormal System Health** monitor is not available in the Central Manager.

Background Tasks

The **Running Tasks** monitor of the **Dashboard** page displays the status of currently In-Progress activities on your system that Trellix IPS identifies as long running processes.

When a long running process is taking place in your Manager, the status is displayed as "In progress" in the **Running Tasks** monitor. You can also go to **Logs** page and select **Background Tasks** tab to view long running processes. Once the activity is completed, the entry for that activity is removed from the **Running Tasks** monitor and displayed only under **Background Tasks** tab in the **Logs** page.

Device Summary

The **Device Summary** monitor of the Dashboard page displays the current versions of the signature set, Callback Detectors, Gateway Anti-Malware and Gateway Anti-Virus, and Sensor software of the logged-on domain. It displays the following information:

- **Device** — The name that you entered for the Sensor in the **Devices** page. You have the ability to click this device to be routed directly to device **Summary** page at Devices → <Admin Domain Name> → Devices → <Device Name> → **Summary**.

- **Model** — The model number of the Sensor which will be the same as that displayed in the **Devices** page.
- **Versions**
  - **Signature Set** — The current version of the signature set applied to your Sensors.
  - **Callback Detectors** — The current version of the callback detectors applied.
  - **GAM** (Gateway Anti-Malware) — The current version of Gateway Anti-Malware DAT that is running on that Sensor. You will notice that the corresponding engine version displayed in parentheses.
  - **Anti-Malware** — The current version of Anti-Malware DAT that is running on that Sensor. You will notice that the corresponding engine version displayed in parentheses.
  - **Software** — The current version of the device software.
- **Status** — Indicates whether any of the software versions need to be updated. The text displayed will either read **Changes pending** or **Up to date**.

CPU Usage

The **CPU Usage** monitor enables you to view the following details:

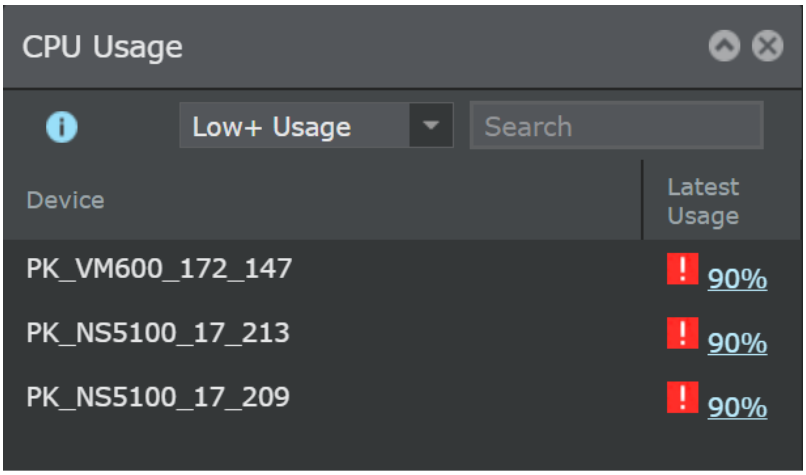
- **Device** — The name of the Sensor as mentioned in the **Devices** page.
- **Latest Usage** — The percentage of CPU utilized by the Sensor.

> **NOTE**
>
> By clicking the hyperlink in the **Latest Usage** column, you will be redirected to the **Performance Charts** page.

To view the details of both medium and high CPU usage, select the option **Medium+ Usage** from the drop-down list. To view the details of only the high CPU usage, select the option **High Usage** and from the drop-down list. To view the details of low, medium and high CPU usage, select **Low+ Usage**.

> **NOTE**
>
> To filter the display of CPU usage based on a device name, use the **Search device** text field option.

Figure 99. CPU Usage



Throughput Usage

The **Throughput Usage** monitor enables you to view the high usage of Sensor throughput.

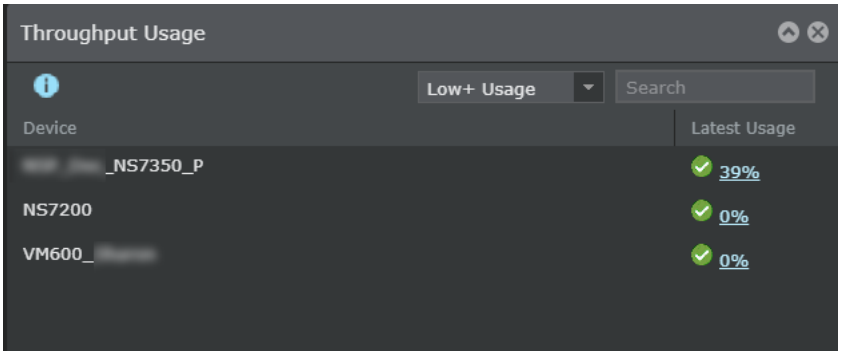
- **Device**—The name of the Sensor as mentioned in the **Devices** page.
- **Latest Usage**—The percentage of throughput utilization by the Sensor.

> **NOTE**
> By clicking the hyperlink in the **Lastest Usage** column, you will be redirected to the **Performance Charts** page.

To view the details of both medium and high throughput usage, select the option **Medium+ Usage** from the drop-down list. To view the details of only the high throughput usage, select the option **High Usage** from the drop-down list. To view the details of low, medium and high throughput usage, select **Low+ Usage**.

> **NOTE**
> To filter the display of high throughput usage based on a device name, use the **Search device** text field option.

Figure 100. Throughput Usage

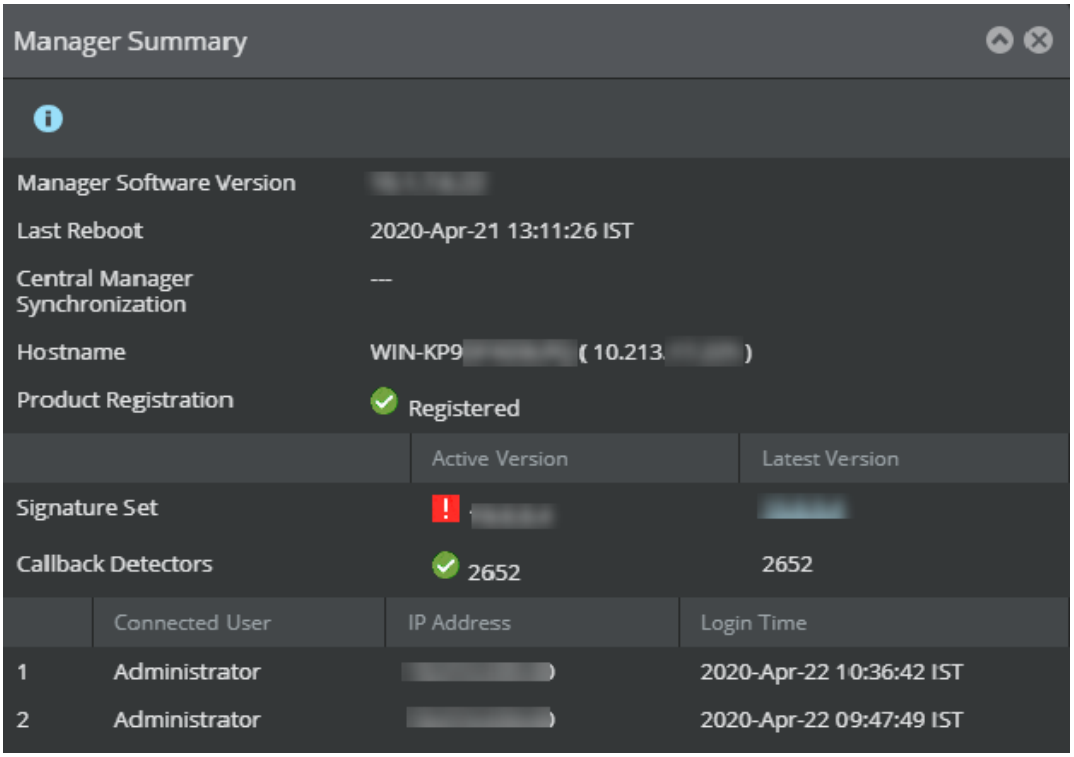


Manager summary

The **Summary** option (Dashboard → <Admin Domain Name> → <Manager Summary Monitor> → **Summary**) enables you to view the following details:

- **Manager Software Version**— Current Manager software version
- **Last Reboot**— The most recent time Manager service was started
- **Central Manager Synchronization**— Displays the synchronization status of the Central Manager with the Manager.
- **Host Name**— Host name and network identification of the Manager server (if host name is not available, only the IP is displayed)
- **Product Registration** — The registration status of the Manager
- **Signature Set**— Current active signature version available in Manager and the latest signature set version available for update
- **Callback Detectors**— Current active callback detector version available in Manager and the latest callback detector version available for update
- **Logged In Users**— All currently open user session information by:
  - Connected User
  - IP Address
  - Login Time

Figure 101. Manager Summary



Memory Usage

The **Memory usage** monitor enables you to view the memory utilization.

- **Device**—The name of the Sensor as mentioned in the **Devices** page.
  - **Flow Pool**—The percentage of the TCP and UDP flow used by the Sensor.
  - **Decrypted Flow Pool**—The percentage of SSL flows used by the Sensor.
  - **Packet Buffers**—The percentage of the packet buffer used by the Sensor.
  - **System Memory**—The percentage of the control path system memory used by the Sensor.

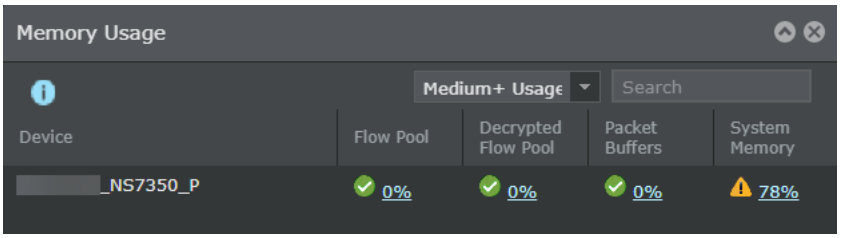
> **NOTE**
>
> By clicking the hyperlink in any of the categories, you will be redirected to the **Performance Charts** page.

Sometimes the hyperlinks may not be available for some options if the option is not applicable to the configured Sensor.

To view the details of both medium and high memory usage, select the option **Medium+ Usage** from the drop-down list. To view the details of only the high memory usage, select the option **High Usage** from the drop-down list. To view the details of low, medium and high memory usage, select **Low+ Usage**.

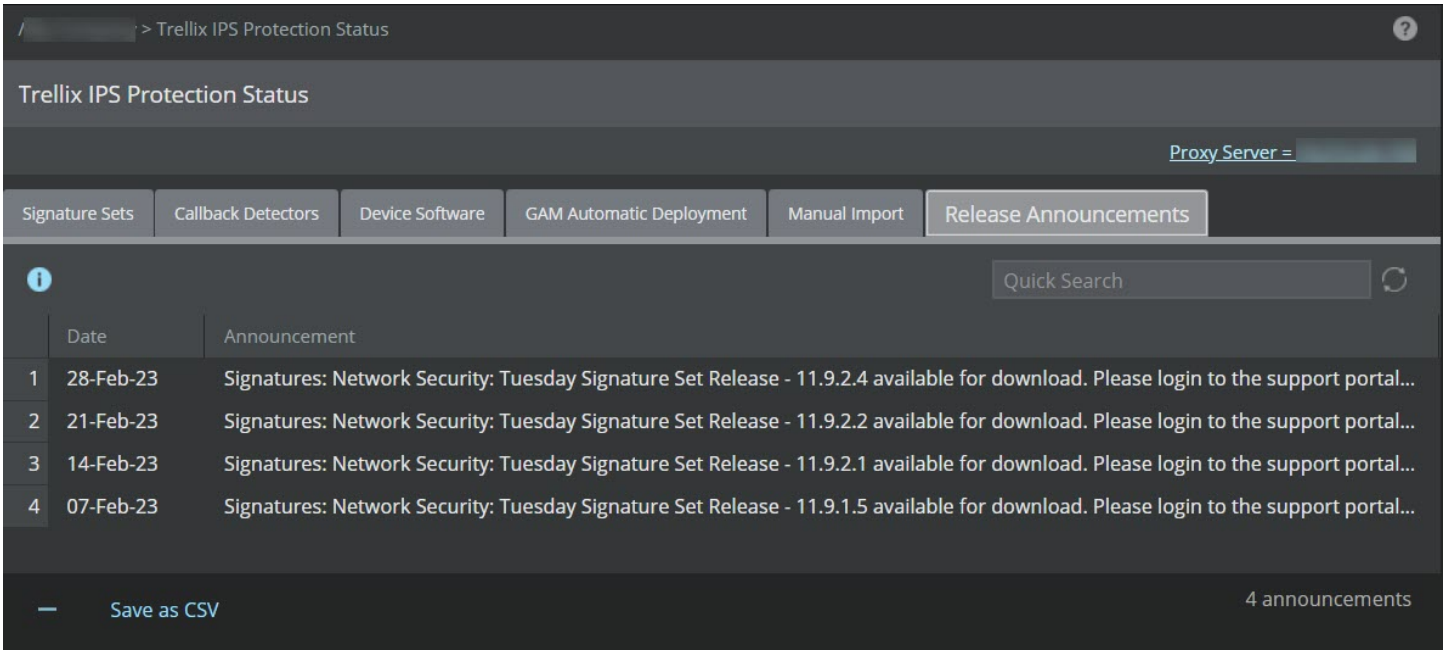
> **NOTE**
>
> To filter the display of memory usage based on a device name, use the **Search** text field option.

Figure 102. Memory usage



Release Announcements

The **Release Announcements** tab enables you to view any product or security-related messages. To view the messages, select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Release Announcements** tab. The **Release Announcements** tab is displayed.



The messages can be related to operating system updates, signature set release, Manager software update, and others. The Manager verifies the Trellix IPS Update Server for such messages every 15 minutes and it displays messages that are relevant to the version of Manager and signature set that you are using.

This feature makes sure that all relevant messages from the Trellix IPS support team reach you on time. Because the new messages are displayed on the homepage and **Release Announcements** tab, the chances of you missing any message are remote.

The Manager displays the release date and the message description of the relevant messages on the **Release Announcements** tab. The release date is the date on which the message was posted on the Update Server. You can delete the messages that you have already seen with – option and it is not listed again. To download these messages, select **Save as CSV**. You can also view the total available announcements.

The latest four unacknowledged messages are displayed on the Manager **Dashboard** page as well. Click **View All Messages** on the **Dashboard** page to navigate to the **Release Announcements** tab where all messages are displayed that are not deleted.

NOTE

Though all users can view the messages, only users with the role of Super User in the root admin domain can delete messages.

NOTE

In the Manager, child admin domain users can view only the last four messages displayed in the **Dashboard** page.

System Faults

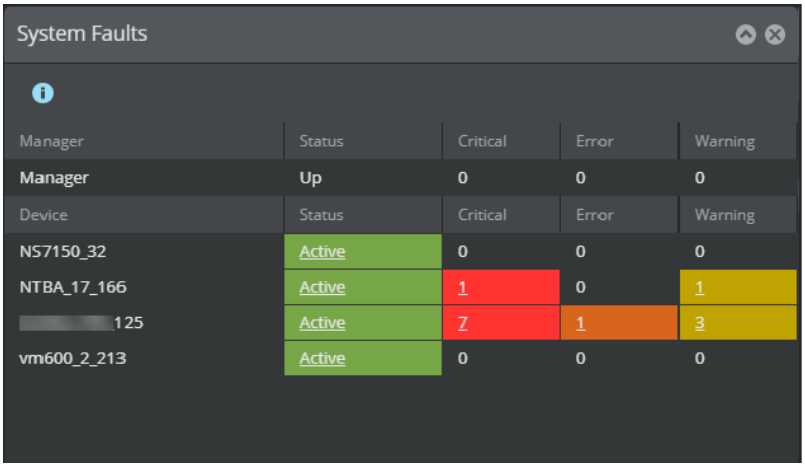
The **System Faults** monitor of the Dashboard page displays the current health of the Manager and installed Sensors in the system. Based on the severity of issues, the **System Faults** monitor displays messages like whether the Manager or Sensor is

up or down. Any messages sent by the Manager or Sensors are displayed in three categories, **Critical**, **Error**, or **Warning**. When you click on the values displayed under various columns, you are redirected to the page that displays information concerning the values.

System Faults page

The **System Faults** page displays the current health of the Manager and installed Sensors.

Figure 103. System Faults

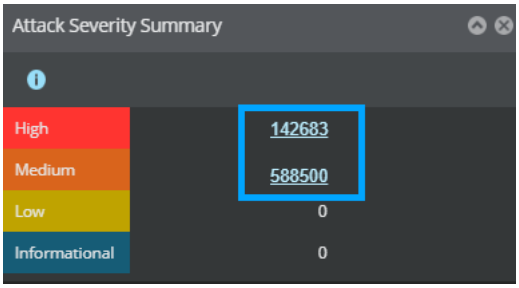


To open the **System Faults** page:

From the Manager **Dashboard** page, click any link in the **System Faults** link to open the **Faults** tab in the **Logs** page. The **Faults** tab displays system faults information.

The alert counts greater than zero are hyperlinked in the Manager. You can click on the hyperlink to drill down to individual alert details.

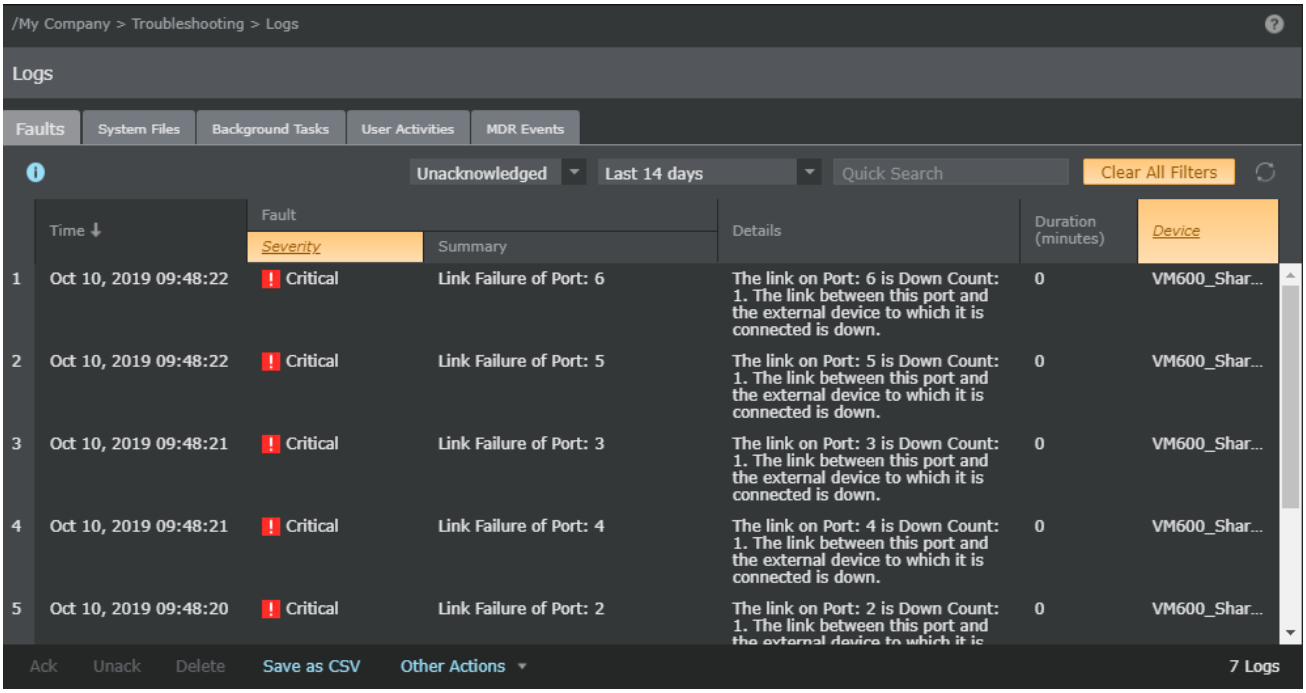
Figure 104. Hyperlinked alert count in Manager



System Faults interface

The System Faults interface main screen displays a quick view of each of your installed Trellix IPS components. There are two tables: one for the Manager and one for all installed devices. Manager and Device tables each reflect the current status of component connection and the number of fault messages. You can click any of the categories, Critical, Error, or Warning links to view the **Faults** tab in the **Logs** page for details.

Figure 105. System Faults view



System Faults color scheme

The color scheme of the **System Faults** cells reflect the number of current unacknowledged alerts.

- **Green** — If all cells are green, there are no unacknowledged alerts for that component.
- **Blue** — If cells for a component are blue, there are one or more unacknowledged Informational alerts for that component.
- **Yellow** — If cells for a component are yellow, there are one or more unacknowledged Warning alerts for that component.
- **Orange** — If cells for a component are orange, there are one or more unacknowledged Error alerts for that component.
- **Red** — If cells for a component are red, there are one or more Critical alerts that are unacknowledged for that component.

> **NOTE**
>
> Acknowledging a fault means that you are aware of the problem and plan to take appropriate action.

Here is another scenario: You log on to Manager. The **System Faults** status in the **Dashboard** page reads **Critical** (red). Click the fault link that opens the details page for the fault. After examining the fault, you manually **Acknowledge** it. After 30 seconds, the **Dashboard** page refreshes and the **System Faults** displays **Up/Active**. The problem may still exist, but since you acknowledged the fault, Manager determines all other system issues are good, and you are taking the steps to fix the fault issue. Thus, you are not constantly reminded of the fault.

Some faults clear on their own, and disappear from view. For example, if someone removes one of the power supplies from an NS7100 Sensor, a **Critical** (red) fault appears, describing the situation. When the power supply is reinserted, another fault appears describing the new situation, along with a third indicating that there is no power. When power is detected on the supply, the power supply is considered operational again, and Manager clears all three fault messages.

System Faults' fields

The fields in the **System Faults** table are as follows:

- **Manager**— Manager controlling the system.
- **Failover Mode**— Specifies if the Manager is primary or secondary.
- **Failover Status**— Specifies if the Manager is active or on standby.
- **Device (Failover/Device Cluster)**— The user-given name of the Sensor or HA pair.
- **Status**— Operational status of component.

  For Manager, **Up** indicates proper functioning; **Down** indicates the component is not functioning.
- **Fault Level**— The Critical, Error, and Warning fields relate to the impact of a system fault. You can click any of the faults and view details on the **Faults** tab.
  - **Critical**— Major faults, such as component failure.
  - **Error**— Medium faults, such as a stopped process, incorrect port speed configuration, or a session time-out (automatic logout).
  - **Warning**— Minor faults, such as multiple bad logons or an attempt to delete a resource in System Configuration without properly clearing fields.

Sensor Status details

The **Status** column against the Sensor listed in the **System Faults** monitor displays one of the following status for the listed Sensors:

- **Active**— All channels are up.
- **Attention**— One or two communication channels are down.
- **Disconnected**— All three communication channels are down.
- **Standby**— The Command Channel is still being set up.
- **Uninitialized**— There is a failure in the initial setup.
- **Unknown**— Displayed when a Sensor has been added to the Trellix IPS user interface, but the actual Sensor has not been set up yet to communicate with the Manager.

Clicking the link in the **Status** cell for a Sensor opens the **Summary** page.

For Sensors, status is determined by the state of three communication channel parameters: Command Channel, Alert Channel, and Packet Log Channel. The **Summary** page displays information on Sensor health and the three communication channel parameters.

Monitoring System Faults

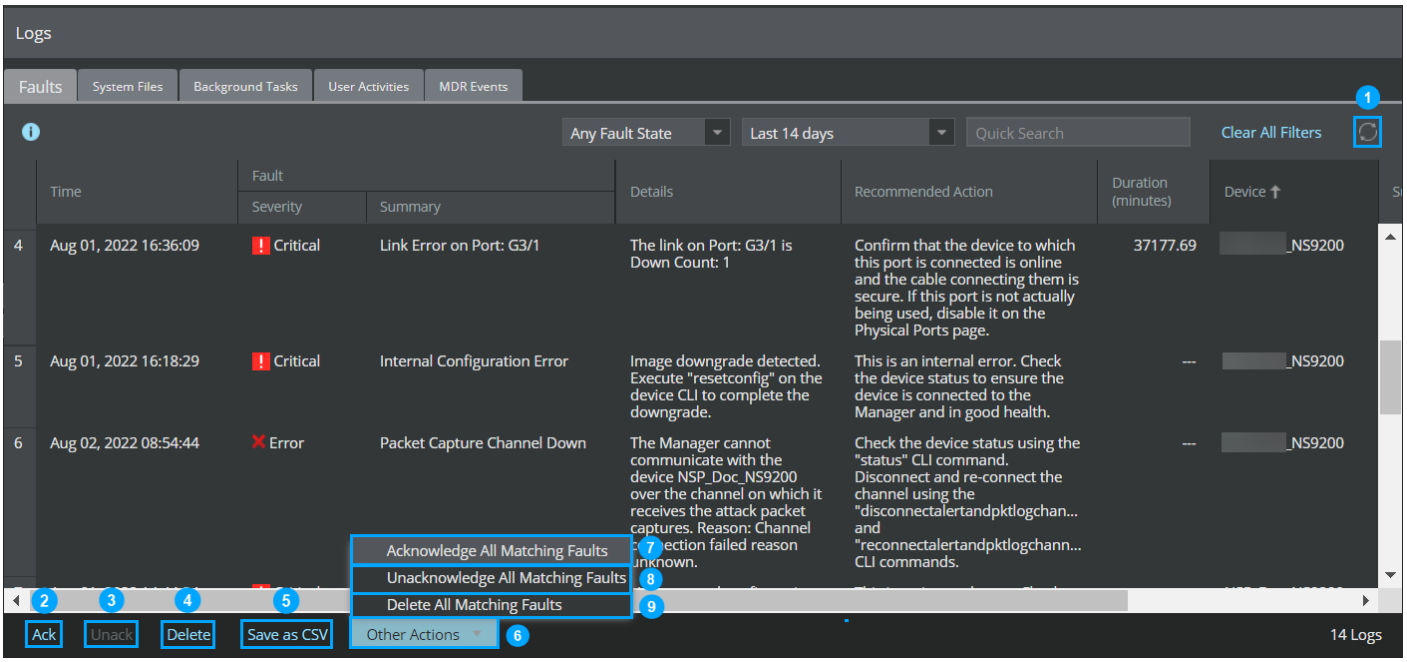
System Faults provide the functional status for all of your installed Trellix IPS components. Messages are generated to detail the system faults experienced by Trellix IPS.

Summary of selected fault messages

The **Faults** tab in the **Logs** page, displays the summary of the selected fault messages. For more information see Faults (page 343).

Faults tab action buttons

The following action buttons are available in the **Faults** tab:



Callout	Action button
1	**Refresh**—Updates the Manager faults log with new faults from the database.
2	**Acknowledge**— Marks the fault as acknowledged/read. Acknowledging a fault means that you are aware of its existence and plan to take appropriate action. The **Ack.** field displays a checkmark on manual acknowledgment. When you acknowledge a fault, the fault will still be available in the Manager which can be used for analysis later.
3	**Unacknowledge**— Marks the faults as unrecognized and the **Ack.** field is blank. By default, all logs are unacknowledged. You can unacknowledge an acknowledged log.
4	**Delete**— Deletes the selected faults from the Manager.
5	**Save as CSV**— Saves a copy of the faults displayed with filters applied.

Callout	Action button
6	**Other Actions**— You can perform further actions on the faults using the option available under **Other Actions**. The **Other Actions** has the following options: • Acknowledge All Matching Faults • Unacknowledge All Matching Faults • Delete All Matching Faults
7	**Acknowledge All Matching Faults**— Acknowledges all faults of the same type for the selected filter range.
8	**Unacknowledge All Matching Faults**— Unacknowledges all faults of the same type for the selected filter range.
9	**Delete All Matching Faults**— Deletes all faults of the same type for the selected filter range.

For a complete listing of system fault messages and their interpretation, see the [Troubleshooting] section.

System fault messages

For a complete listing of system fault messages and their interpretation, see the [Troubleshooting] section.

Overview

The **Analysis** tab on the Menu bar enables you to perform network and events analysis.

When you want to analyze a situation in your network - you want to view an issue, check on the issue, drill down to the root cause, and resolve. These stages can be furnished in the Manager as follows:

- **Monitoring** — The **Dashboard** page enables you to view any system health or network issues. Your goal is to understand the overall posture and identify anomalies.
- **Initial Investigation** — The **Analysis** tab options enable you to research anomalies and establish the context via the security monitors, callback activity, malware downloads, high-risk endpoints and network forensics.
- **Detailed Investigation** — **Attack Log** enables you to determine the root cause of the network issue. It allows you to isolate, correlate and validate events and provides you the grass root details like raw logs, Mitre attack details, and packet captures. This in turn helps you to resolve the issue.

Attack Log

The **Attack Log** lists attacks with most recent being listed first. It contains alerts that are raised whenever there is a discrepancy in the traffic flowing through the network. The Sensors parsing the traffic detects any attack and raises an alert. Attack details are presented using multiple columns known as attributes. The attributes represent packet fields, such as source and destination IP address, as well as Sensor analysis fields such as attack severity. The **Attack Log** contains both acknowledged and unacknowledged alerts. You can acknowledge alerts and also update rules, quarantine hosts, tag endpoints, configure auto-acknowledgment rules, etc. You can also perform forensics on alerts for further analysis.

NOTE

Features that are not applicable to the Central Manager are explicitly mentioned in the relevant sections. All other features are applicable to both the Manager and the Central Manager.

What are alerts?

Alerts are asynchronous notifications sent when a system event or attack triggers the IPS. When a packet violating your enforced security policies is detected, the Sensor compiles information about the offending packet and sends the information to the Manager in the form of an alert. An alert contains a variety of information on the incident that triggered it—such as the type of attack, its source and destination IP addresses, its source and destination ports, as well as security analysis information (performed by the Sensor) such as attack severity and type. You can use this information to perform forensic analysis on the alert—that is, careful investigation to determine its cause and how to prevent others of its kind.

An attack is a violation of set policy parameters. An alert is one or more attack instances. In many cases, an alert represents a single detected attack. A multi-attack alert is generated when multiple instances of identical attacks (same attacker IP, target IP, and specific attack) are detected within a two minute period; data for all attacks is throttled into one alert instance, however, you can also choose to configure for how many of each throttled attacks you want to see an individual alert.

Trellix IPS stores alerts in the Manager server database until you delete them. You can view your alerts in the Manager using the Analysis → <Admin Domain Name> → **Attack Log** page.

For more information, refer to [Configure alert suppression with packet log response] topic in [IPS Administration] section.

Alert Summary

Alerts exist in one of the following states:

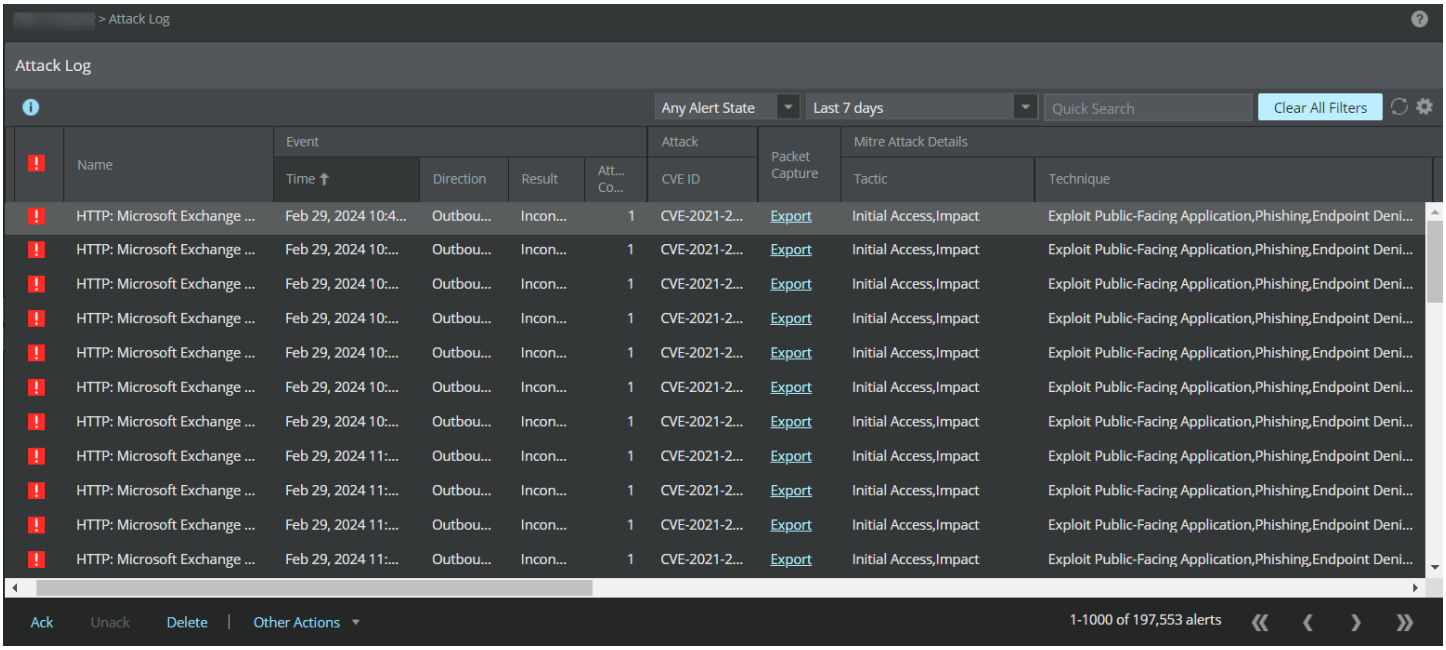
- Unacknowledged
- Acknowledged

When an alert is raised, it appears in the Manager in an unacknowledged state. *Unacknowledged* means that you have not officially recognized its presence by marking it *acknowledged*. An alert remains in an unacknowledged state until you either acknowledge it or delete it.

Unacknowledged alerts display in the **Attack Severity Summary** monitor of the **Dashboard** page. Acknowledging alerts dismisses them from the **Dashboard**. Acknowledged alerts display only in the **Attack Log** and in reports.

Alerts are backed up to the database and archived in order of occurrence. Deleted alerts are removed from the database. Hence, proper care should be exercised before deleting an alert.

Figure 106. Attack log

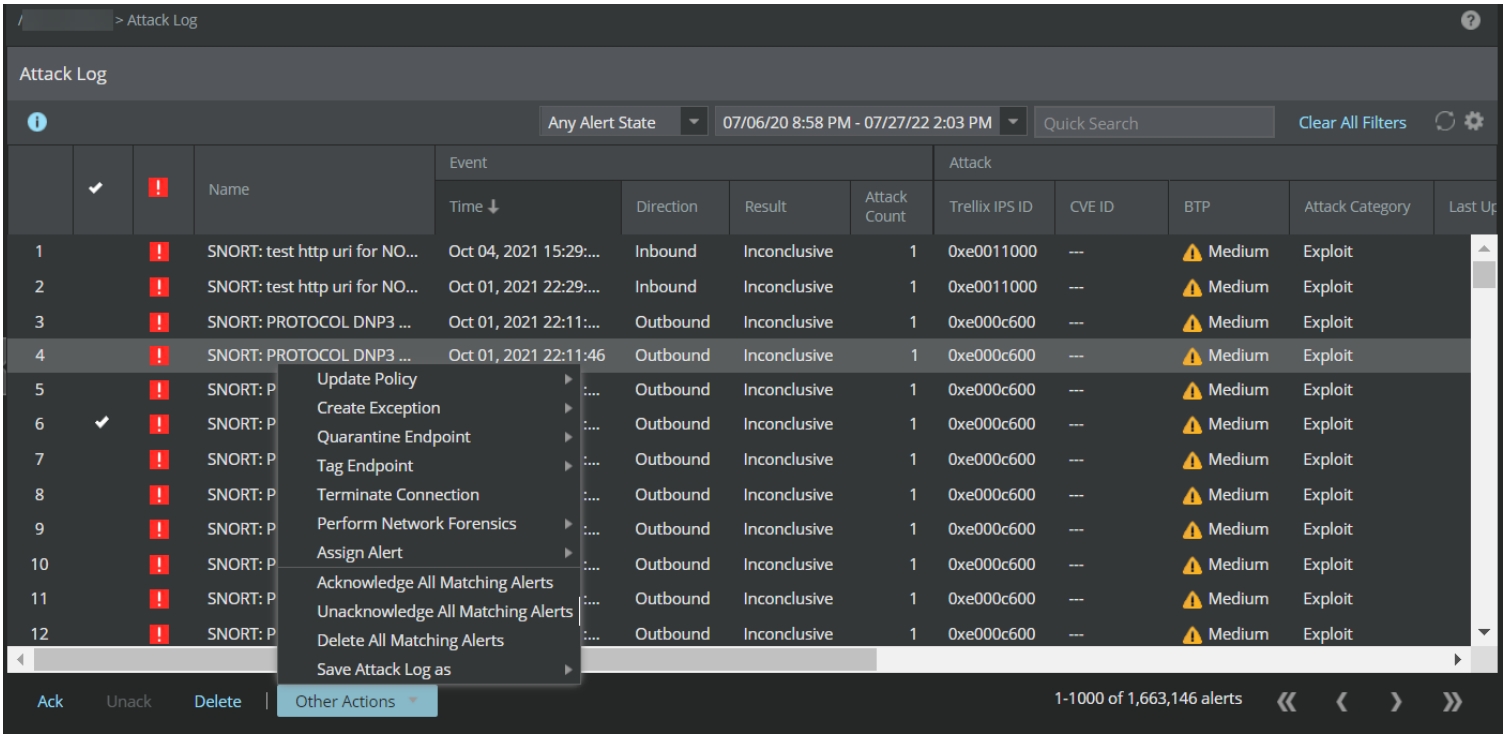


Acknowledged and unacknowledged alerts

When you have examined an alert and have determined a course of action, acknowledging the alert is the next step. The acknowledge option provides a simplistic visual checklist to help you differentiate between the alerts you have examined and those you have yet to review. You can view the acknowledged and unacknowledged alerts in the **Attack Log** of the Manager. To view the acknowledged and unacknowledged alerts, hover over a column, click the drop-down arrow that appears and select the *tick* mark to view the acknowledged and unacknowledged alert column. Acknowledged alerts are displayed with a *tick* mark against that alert. When you acknowledge an alert, the alert is removed from the statistical values of the **Attack Severity Summary** monitor in the **Dashboard**.

An acknowledged alert can be reverted back to unacknowledged state. To acknowledge/unacknowledge an alert, select the alert and click **Ack**/**Unack**. You can also acknowledge or unacknowledge all the alerts that appears in the **Attack Log**. To acknowledge/unacknowledge all the alerts, click the **Other Actions** button, and then select **Acknowledge All Matching Alerts**/ **Unacknowledge All Matching Alerts**.

Figure 107. Acknowledge/Unacknowledge alerts



Suppressing alerts

Over the course of time, you will become very familiar with your Trellix IPS alert data as you perform forensic analysis using the Attack Log. At some point, you may even become tired of seeing some of the same alerts time and again. Trellix IPS provides multiple options for suppressing alerts, that is, reducing the number of alerts in either the Attack Log and/or database, so that you can work on your higher priority issues.

The following alert suppression options are available using various actions within the Manager interface:

- **Disable alerting** — During policy creation/modification, you can disable the alert for one or more attacks. This is not attack detection disabling, just alert disabling. The Sensor still detects the attack and can send an automatic response, if configured. (If no response is configured, nothing is done when the attack is detected.)
- **Auto Acknowledge** — Also during policy creation, you have the option of automatically acknowledging a detected attack. The **Auto-Acknowledge** feature suppresses the alert from the Attack Log by marking the alert as acknowledged. You can also create new auto acknowledgement rules for the alerts.
- **Alert throttling** — Alert throttling (seen as **Alerting Options** in the Manager interface) enables you to set a suppression limit for a singular Exploit attack, which originates from one attacker, targets a single destination IP, and is detected by the same VIPS (interface or sub-interface) multiple times within a limited time frame. Exploit throttling limits the number of duplicate alerts that are sent to the Manager from a Sensor. Throttling is very effective against repetitive Exploit attacks where a attacker IP address is spoofed and generates a high number of alerts.

  For more details, refer to [Configure alert suppression with packet log response] topic in[IPS Administration] section.

	Send alert to Manager	Send Sensor response action	Display alert in Attack Log
Normal behavior	Yes	Yes	Yes
Detection on, disable alerting	No	Yes	No
Auto acknowledge	Yes	Yes	Yes/No (depending on the column view in Attack Log)
Alert throttling	Yes	Yes	Yes

Filter, sort, and refresh alerts

The volume of alerts generated in the **Attack Log** makes it difficult for the analysis of alerts. The different sorting and filtering options provided in the **Attack Log** helps drill-down only the necessary alerts for further analysis. Use the arrow keys at the bottom of the page to navigate back and forth between the alert pages.

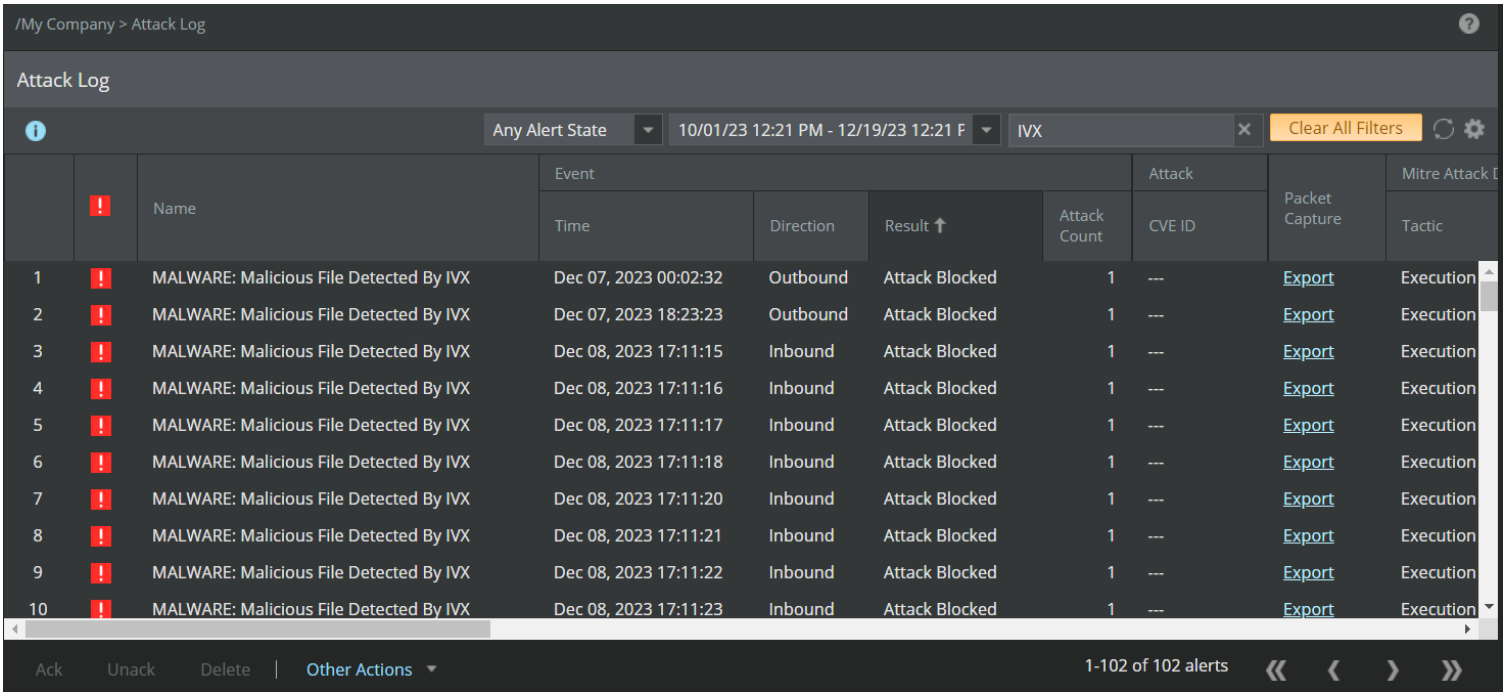
Sort alerts

Alerts when generated are in unacknowledged state. Once an alert is acknowledged, a *tick* mark appears next to the alert in the acknowledged and unacknowledged column. You can sort the alerts by selecting any one of the three options, **Unacknowledged**, **Acknowledged** and **Any Alert State**. You can also sort the alerts based on the period in which the alerts were generated. The **Custom Time Period** option lets you customize the time period.

When the *time period* option is selected, the display shows the alert, attack counts, and other parameters for the chosen time period. The alert count displays the number of times each attack has been reported within the parameters. For example, for a query, there are two reported alerts (number of alerts = 2) and two reported attacks (attack count = 2) for the "ARP: ARP Spoofing Detected" attack. Thus, the "ARP: ARP Spoofing Detected" attack was detected and reported exactly twice during the queried period. Also, the number of alerts and attack count for the "Samba Trans2Open Buffer Overflow" attack: 74 alerts have been generated for this attack; however, there were 2133 attack instances. One or more attack instances was suppressed according to the configuration set.

When looking for a particular alert, you can enter the keyword for the alert in the **Quick Search** field and the results are automatically displayed in the log. Click **Clear All Filters** to undo all the filters applied.

The **Clear All Filters** button color changes to orange which indicates that a filter is active, and that the attack log is not displaying all the alerts. For example, if you want to filter the alerts detected by IVX engine, type **`ivx`** or **`IVX`** in the **Quick Search** field. The **Clear All Filters** button color changes to orange and the Manager filters IVX specific alerts.



Filter alerts

You can customize the columns in the **Attack Log** to view only the necessary details about the alert. You can rearrange/resize the columns to view the details according to your preference. Following are the column options for the alerts:

Column header	Description
Acknowledged/ unacknowledged alerts	The *tick* mark indicates that the alert is acknowledged.
Attack Severity	Indicates different colors based on the attack severity, high/medium/low/informational
Name	Name of the attack

Column header	Description
Event	Displays various information about the attack • **Time** — Time at which the attack occurred • **Direction** — Transmission destination with regard to internal network (inbound or outbound) • **Result** — Result of the alerted attack The Result categories for alerted attacks are as follows: • **Attack Successful** — The attack was successful. • **Inconclusive** — The result of the attack is not known. This is most likely due to a generic policy, such as the Default or All-Inclusive policy where the policy rules are not environment specific. For example, this may be the result if an attack occurs against an irrelevant node. • **Attack Failed** — The attack had no impact. • **n/a** — The alert was raised for suspicious, but not necessarily malicious, traffic. This result is common for Reconnaissance attacks due to the nature of port scanning and endpoint sweeping. • **Attack Blocked** — Attacks blocked by a "Drop packets" Sensor response • **Attack SmartBlocked** — Attacks blocked by a "Drop packets" Sensor response as per GTI reputation response • **DoS Blocking Activated** — Applies to DoS traffic and indicates that the Sensor has identified traffic that is suspicious in nature that is exceeding its learned threshold or is not recognized based on its profile. The Sensor has started blocking unknown traffic, while attempting (on a packet-by-packet basis) to block only DoS traffic from a trusted source. The Sensor attempts to allow legitimate traffic to flow from the trusted source. Because of the nature of DoS attacks, one cannot be certain that 100% of bad traffic was blocked nor that 100% of 'good' traffic was permitted. For more in-depth description of Trellix IPS's DoS handling, see Denial-of-Service attacks (page 1038). The following is the alert result status when Simulated Blocking is enabled. • **Blocking Simulated (Attack Failed)** — The attack had no impact. • **Blocking Simulated (Attack Blocked)** — An alert is raised for the attack that had potential impact. • **Blocking Simulated (Attack Successful)** — The attack was successful. • **Blocking Simulated (Inconclusive)** — The result of the attack is not known. This is most likely due to a generic policy, such as the Default or All-Inclusive policy where the policy rules are not environment specific. For example, this may be the result if an attack occurs against an irrelevant node. • **Blocking Simulated (n/a)** — The alert was raised for suspicious, but not necessarily malicious, traffic. This result is common for Reconnaissance attacks due to the nature of port scanning and endpoint sweeping. • **Blocking Simulated (Attack SmartBlocked)** — An alert is raised for the attack that had potential impact as per GTI reputation response.

<table>
<tr><th>Column header</th><th>Description</th></tr>
<tr><td></td><td>

Attack Count — Number of instances of the same attack
Relevance — Indicates if the endpoint is vulnerable to this particular attack
Alert ID — ID assigned to the alert
Assigned to — Displays the name of the user if the attack is assigned

</td></tr>
<tr><td>Attack</td><td>Displays specific information about the attack

Trellix IPS ID — ID of the Sensor from where the alert was generated
CVE ID — CVE ID of an attack that has been identified in the network and captured by the Sensor

NOTE
The CVE ID is displayed only for those attacks present in the signature set that have a valid CVE ID assigned to them.

NOTE

In case you are performing a fresh installation of Trellix IPS Manager, the CVE ID column in the Attack Log page displays CVE IDs for all the alerts that have valid CVE IDs assigned to them in the signature set.
In case you are upgrading the Manager to version 10.1.7.44 from versions prior to 10.1.7.29, the CVE ID column in the Attack Log page displays CVE IDs for all the alerts that have valid CVE IDs assigned to them in the signature set.
In case you are upgrading the Manager to version 10.1.7.44 from version 10.1.7.29, 10.1.7.35, or 10.1.7.40, the CVE ID column in the Attack Log page displays CVE IDs only for the alerts (that have valid CVE IDs assigned to them in the signature set) generated post upgrade. You will not be able to view the CVE IDs for old alerts. In order to view CVE IDs for such alerts:

Double-click on the old alert for which you want to view the details.
The <Attack Name> panel opens on the right hand side.
Click on the Description tab in the panel and scroll down to the Reference section.
You can view the CVE ID in this section, provided the alert has a valid CVE ID assigned to it in the signature set.

BTP — Displays the BTP level as either High, Medium or Low
Attack Category — General attack type
Last Updated — Recent version of the signature set in which the attack was updated

</td></tr>
<tr><td>Packet Capture</td><td>You can export the packet capture for that alert.</td></tr>
</table>

Column header	Description
Mitre Attack Details	Displays key components of the Mitre matrix table for an attack or alert: • **Tactic** — Name of the adversarial tactic matching with the attack or alert • **Technique** — Name of the corresponding adversarial technique matching with the attack or alert • **Sub-Technique** — Name of the corresponding adversarial sub-technique matching with the attack or alert • **Technique/Sub-Technique ID** — ID of the specific technique/sub-technique in the <*techniqueID.sub-techniqueID*> format. For example, in the ID T1595.001, T1595 represents the technique Active Scanning and 001 represents the corresponding sub-technique named Scanning IP Blocks. **NOTE** **Mitre Attack Details** column option is available in both Trellix IPS Manager and Central Manager. **NOTE** If an attack matches with multiple tactics, techniques, and/or sub-techniques, their names along with applicable technique/sub-technique IDs are shown in the respective fields under the **Mitre Attack Details** column. When an attack is mapped to multiple tactics, techniques, and/or sub-techniques, there is one-to-one correspondence among the tactics, techniques, sub-techniques, and technique/sub-technique IDs. For example, the first tactic corresponds to the first technique, sub-technique, technique/sub-technique ID, and so on. **NOTE** If the **Tactic**, **Technique**, **Sub-Technique**, or **Technique/Sub-Technique ID** is not available for any alert or attack, that particular field is displayed as **---**. **NOTE** Mitre attack related details in the **Attack Log** are not shown for older alerts.
Attacker	Displays details about the attacker endpoint • **IP Address** — IP address of the attacker endpoint • **Port** — Port on which the attack was detected • **Risk** — Displays the risk level as **High Risk**, **Medium Risk** or **Low Risk** • **Hostname** — Name of the host from where the attack was generated • **Country** — Country of the attacker host • **Proxy IP** — IP address of the proxy server

Column header	Description
Target	Displays details about the target endpoint • **IP Address** — IP address of the target endpoint • **Port** — Port to which the attack is directed • **Risk** — Displays the risk level as **High Risk**, **Medium Risk** or **Low Risk** • **Hostname** — Name of the host to which the attack is directed • **Country** — Country of the target host • **Proxy IP** — IP address of the proxy server

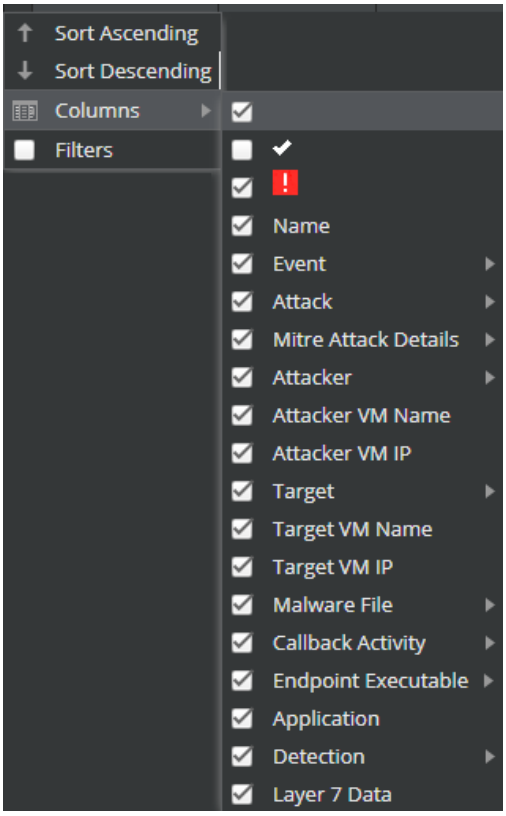
Malware File	Displays details about the attack in case of malware attacks
	• **File Name** — Name of the malware file
	• **File Hash**
	  • **MD5** — Displays the MD5 hash of the file
	  • **SHA1** — Displays the SHA1 hash of the file
	  • **SHA256** — Displays the SHA256 hash of the file
	• **Malware Name** — Name of the malware
	• **Malware Confidence** — Malware confidence level returned by the configured malware scanning engines
	• **Engine** — The configured scanning engine that detected the malware

Callback Activity	Displays details about the callback activity for BOT attacks • **Activity Name** — Name of the callback activity for the BOT attacks • **C&C Domain** — Displays the C&C Domain of the callback activity
Endpoint Executable	Displays details about the endpoints running the executables • **Manager** — Name of the Manager. This field is applicable for Central Manager only. • **Name** — Binary name of the executable • **Hash** — File hash of the executable • **Malware Confidence** — Displays the malware confidence level returned by the configured McAfee EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.
Application	Displays the Layer7 applications involved
Detection	Displays details about the Sensor that detected the attack • **Domain** — Name of the domain to which the Sensor belongs • **Device** — Name of the device that detected the attack • **Interface** — Interface at which the attack was detected

Column header	Description
Layer 7 Data	Displays the following layer 7 data field details: • **FTP Action** • **FTP Banner** • **FTP File Name** • **FTP Return Code** • **FTP User Name** • **HTTP CLSID** • **HTTP Host** • **HTTP Request Content Type** • **HTTP Request Filename** • **HTTP Request Method** • **HTTP Request Referer** • **HTTP Request URL** • **HTTP Response Content Type** • **HTTP Return Code** • **HTTP Server Type** • **HTTP URI** • **HTTP User-Agent** • **HTTP2 STREAM ID** • **HTTP2 Settings Enable Push (Client)** • **HTTP2/3 HTTP VERSION** • **NetBIOS Action** • **NetBIOS File Name** • **SMTP Attachments** • **SMTP Banner** • **SMTP Recipients** • **SMTP Sender** • **SSL Certificate Common Name** • **SSL Server Name Indication** • **TELNET User Name** You can view the protocols/fields that are enabled in the **L7 Data Collection** page under Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Advanced**. You can also customize the settings for the protocols/fields in the **L7 Data Collection** page.

Column header	Description
	The default Percentage (%) value of flow memory re-allocated to collect layer 7 data is 20%.

Figure 108. Filtering alerts



In addition to the column filters, there are specific sub-filters for each column. These sub-filters are based on specific values for that column. For example, the **Direction** column will have **Inbound**, **Outbound**, **Unknown**, and **Bi-directional** as the sub-filters. The alerts are filtered based on the selected option. Further, the **Sort Ascending** and **Sort Descending** options for each column toggles the alerts either in ascending order or descending order.

NOTE

Alerts cannot sorted using the **Mitre Attack Details** column.

Automatic refresh of alerts

Alerts in the **Attack Log** page can be refreshed automatically. Refer the following steps to enable or disable automatic refresh:

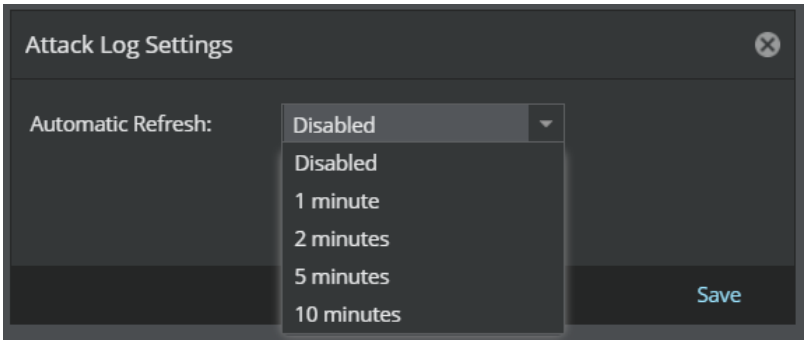
NOTE

Alerts can be refreshed manually by clicking .

1. Click .

   The **Attack Log Settings** dialog box is displayed.

   Figure 109. Attack Log Settings



   NOTE

   Make sure that the set time period to fetch alerts is greater than the automatic refresh interval to not lose any alert data.

2. From the **Automatic Refresh** drop-down, select the refresh interval based on your requirement.

   NOTE

   To disable automatic refresh select **Disabled** from the drop-down.

3. Click **Save**.

NOTE

The **Attack Log** page refreshes automatically every time you visit the page from the **Dashboard** tab, **Threat Explorer**, **Network Forensics**, etc. when the **Automatic Refresh** is enabled.

NOTE

When you select an alert in the **Attack Log** page, with auto refresh enabled, the alert remains selected with the details panel still displaying the alert data though new alerts are added to the page.

Consolidate group alerts

The **Attack Log** page displays thousands of alerts that run into multiple pages and it consumes more time to search for specific type of alerts. To enable you to find alerts in less time, the grouping feature is available in the **Attack Log** page. Using this feature you can group the alerts based on specific fields, and view a consolidated list of alerts.

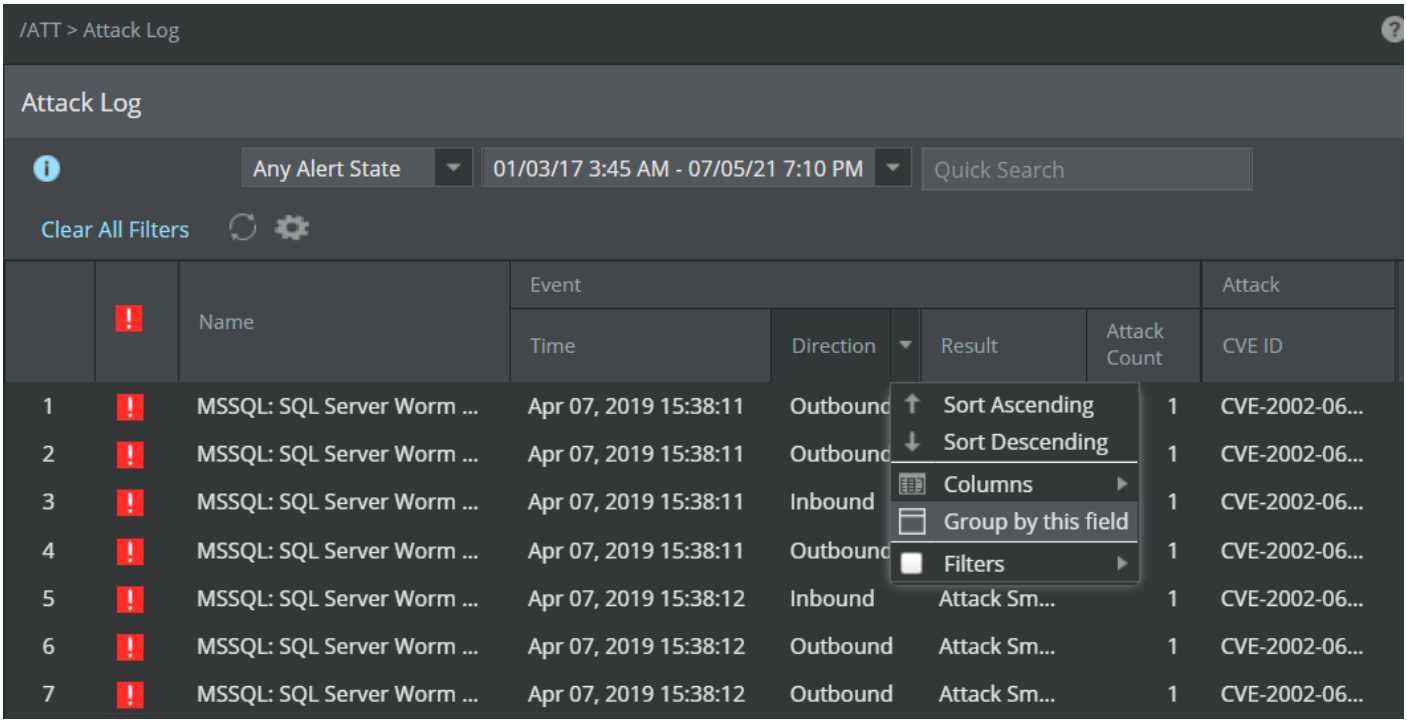
View grouped alerts

You can consolidate and view a group of alerts based on specific fields in the **Attack Log** page. To view a consolidated group of alerts perform the following steps:

Steps:

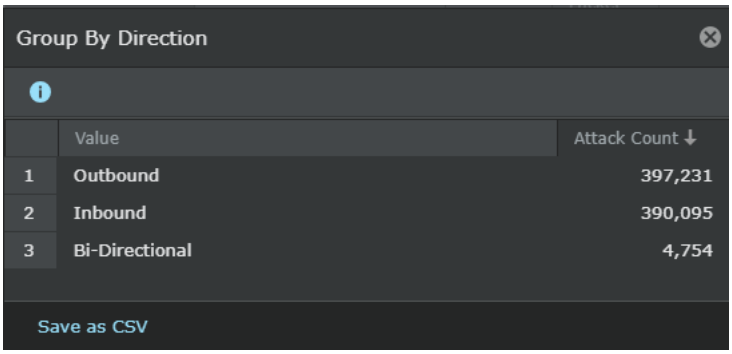
1. Select Analysis → <Admin Domain Name> → **Attack Log**.
2. On **Attack Log** page, click the arrow in the triangular icon in the column header of the field by which you wish to group the alert and select **Group by this field**.

Figure 110. Grouping alerts



A window is displayed for the selected field. For example, if you select the **Group by this field** option for the **Direction** field, the **Group By Direction** window is displayed.

Figure 111. Select a Value to group alerts

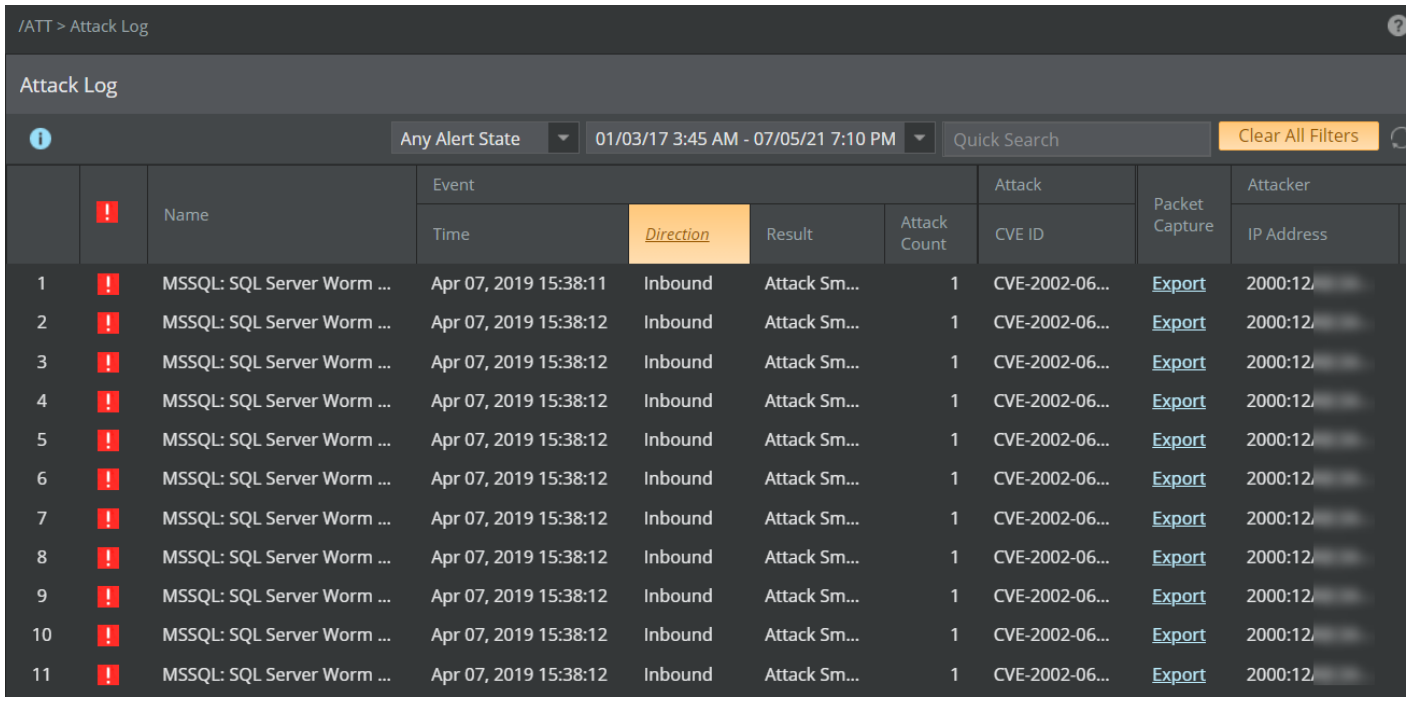


The following display options are available in the column header.

Option	Definition
Group By <field name>	Displays the list of items available for the selected field. For example, the **Group By Direction** window displays the following items: • **Inbound** • **Outbound** • **Unknown**
Attack Count	Displays the total count of the attacks for each group.

3. In the window, double click the row of the item you want to view the grouped alerts for. The window closes and the grouped alerts are displayed on the **Attack Log** page.

Figure 112. Alerts grouped in Inbound direction



NOTE

The column header color changes to orange, which indicates that the alerts are grouped by that option and only those alerts are displayed in this page.

In this example, after grouping the alerts, you can further group them to the next level of grouping by selecting the **Group by this field** option on any other column header where this option is available. For example, after grouping the alerts based on **Inbound** transmission from the **Direction** field, you can further filter the group based on **Medium** BTP level from the **BTP** field in the **Attack** column. As a result, the **Attack Log** page displays only those alerts having both inbound direction and medium level BTP.

Alerts can be grouped by all the fields in the **Attack Log** page, except the following:

- **Time**,**Attack Count** and **Alert ID** under **Event** column
- **Trellix IPS ID** under **Attack** column
- **Packet Capture**
- **Layer 7 Data**

> **NOTE**
>
> In a Central Manager setup, you can group the display of alerts by the **Manager** column in the **Attack Log** page.

To remove the filtering of grouped alerts, click **Clear All Filters**.

Alert details

You can view the details of a specific attack for a clearer picture of the key information related to the attack. The information can then be used to augment your policy settings and/or to initiate a response action, such as a TCP reset or endpoint quarantine rule.

To view the details of a specific attack, do the following:

Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Double-click on the alert for which you want to view the details.

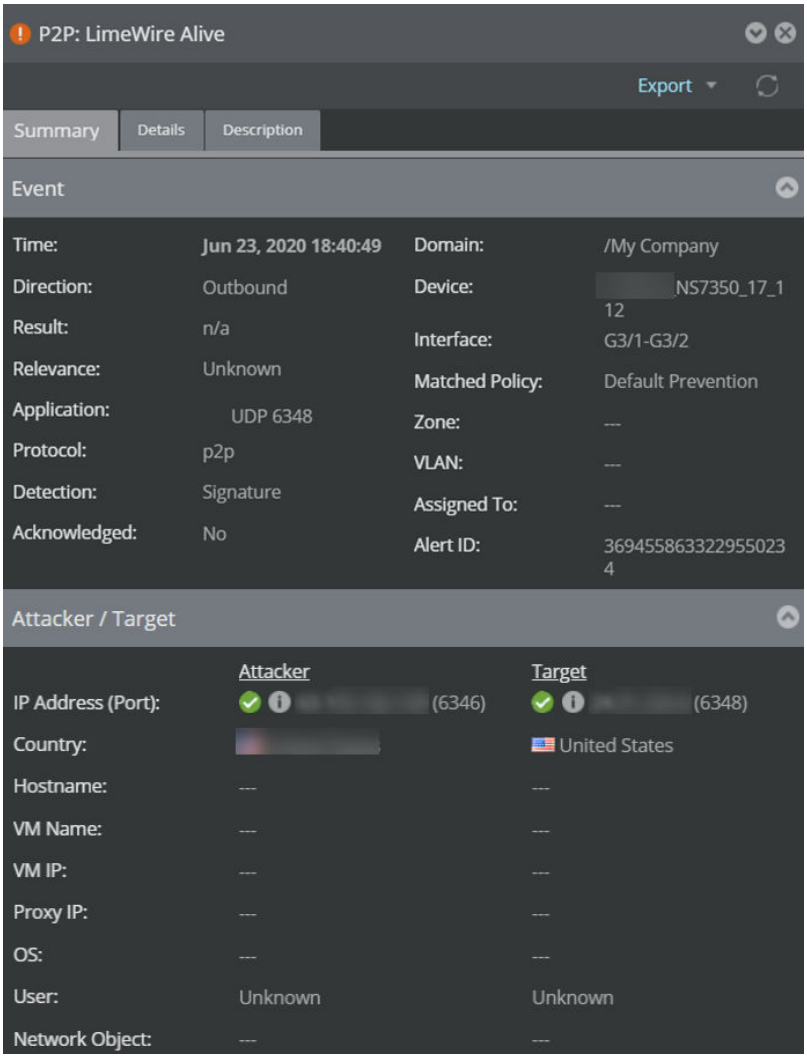
   The **<Attack Name>** panel opens on the right hand side.

   The details of the alert are displayed as follows:

Option	Definition
Summary	• **Event** — Displays the general alert details like the time, direction, device, etc. • **Attacker/Target** — Displays the IP address, hostname and other details of the attacker and the target. In case of mobile related alerts, the relevant fields related to mobile traffic are displayed.
Details	• **Matched Signature** — Displays information about the configured signature conditions that matches with the attack. • **Malware File** — Displays the malware attack information such as the file name, file hash (MD5, SHA1, and SHA256), malware name, malware confidence, engine, size, description, and CVE ID. **NOTE** **Malware File** option is displayed only for malware attacks. • **Layer 7** — Displays the layer 7 information for protocols like HTTP, SMTP, etc.

Option	Definition
Description	Displays further details about the alert like the BTP score, RfSB, protection category, etc. • **Reference** — Displays the different IDs created for the alert and attack, such as Trellix IPS ID, CVE ID etc. It also contains a collapsible subsection named **Mitre Attack Details** which displays the matching **Tactic**, **Technique**, **Sub-Technique**, and **Technique/Sub-Technique ID** for the attack or alert. The **Technique/Sub-technique ID** is hyperlinked that connects to the specific technique/sub-technique web page on the MITRE ATT&CK website. **NOTE** **Mitre Attack Details** subsection is available in both Trellix IPS Manager and Central Manager. **NOTE** If an attack matches with multiple tactics, techniques, and/or sub-techniques, their names along with applicable technique/sub-technique IDs are displayed in the **Mitre Attack Details** subsection. When an attack is mapped to multiple tactics, techniques, and/or sub-techniques, there is one-to-one correspondence among the tactics, techniques, sub-techniques, and technique/sub-technique IDs. For example, the first tactic corresponds to the first technique, sub-technique, technique/sub-technique ID, and so on. **NOTE** If the **Tactic**, **Technique**, **Sub-Technique**, or **Technique/Sub-Technique ID** is not available for any alert or attack, that particular field is displayed as **---** within the subsection. **NOTE** Mitre attack related details are not shown for older alerts. • **Component Attacks** — Displays the component attacks in case of reconnaissance attacks only. • **Signatures** — Displays the signature associated with the attack. • **Comments** — You can add any comments for the alert if any.

Figure 113. Alert Details panel



Attack type display

All alerts have a tab that relates to the attack type/category. For an exploit attack, the region is named **Exploit**; for a policy violation, the region is named **Policy Violation**; and so forth. Each attack type has unique fields, but all (except Statistical) include source and target IP of the attack.

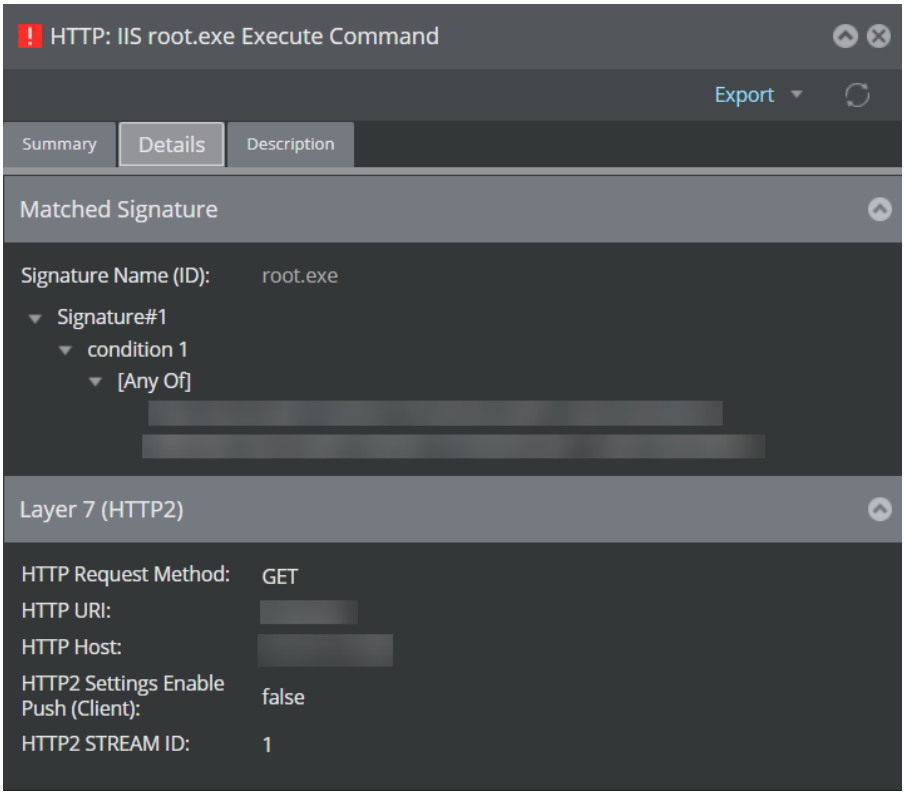
- Exploit
- Volume DoS
- Malware
- Policy Violation
- Reconnaissance

Layer 7 data alert

The Sensor raises an alert when it detects attacks targeting your protected Layer 7 data for all the major protocols like HTTP, SMTP, etc.

The **Details** tab in the **<Attack Name>** panel displays the application protocol, the attack category as well as the matched signature based on which the attack was detected.

Figure 114. Layer 7 - Alert Details



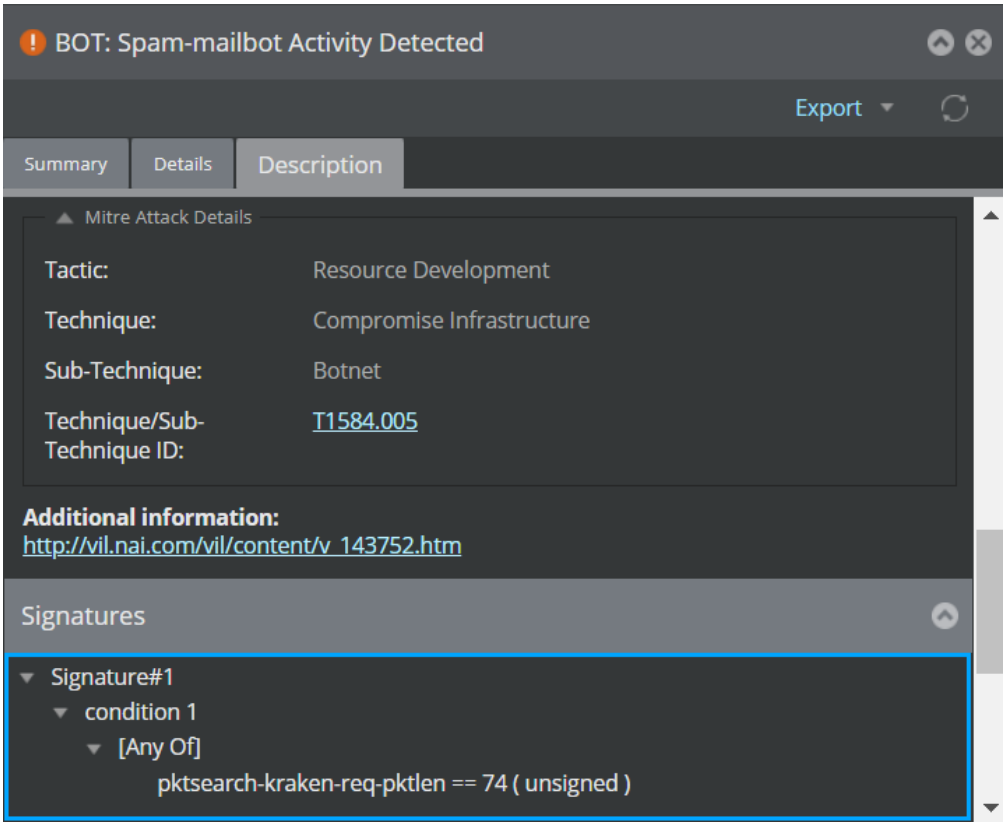
Signature descriptions

The Manager displays attacks categorized as:

- Signature-based attacks
- Correlated attacks
- Non-signature-based attacks (Reconnaissance and DDoS)

Signature-based attacks are the only attacks that contain signatures and so the only attacks that provide signature descriptions. These descriptions will be provided directly in the **<Attack name>** panel.

Figure 115. Alert details panel



The following data is displayed depending on the attack:

- String patterns used in attack detection
- Logical relationship of the condition such as AND, OR and AND THEN based on which the attack was identified.
- Comparison fields used to match the signature
- String match pattern and value matched
- Information after the signature, if applicable

Signature descriptions can be viewed from the **Attack Log**. Selecting an appropriate alert and viewing its details displays the description of the signature that matched the attack signature. All other signature descriptions in that attack signature will be hidden.

Signature descriptions for each signature type

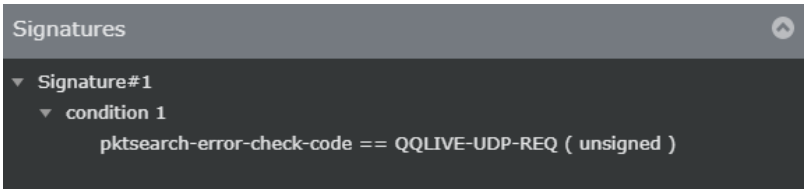
When identifying a signature-based attack, various components distinguish each attack's contents from another. Each variation consists distinct information that is specific to the attack characteristics. The information comprises one or more conditions (which vary for each attack) that need to be satisfied in order to obtain a match. If the signature is defined by more than one condition, matching is always carried out in an order set by a logical relationship. The logical relationship is regulated by AND, OR, and AND THEN elements.

- String-match signatures will display information such as the string match patterns, name of the string fields, and logical relation of the condition.

Figure 116. Example of a string-matched signature with its short description

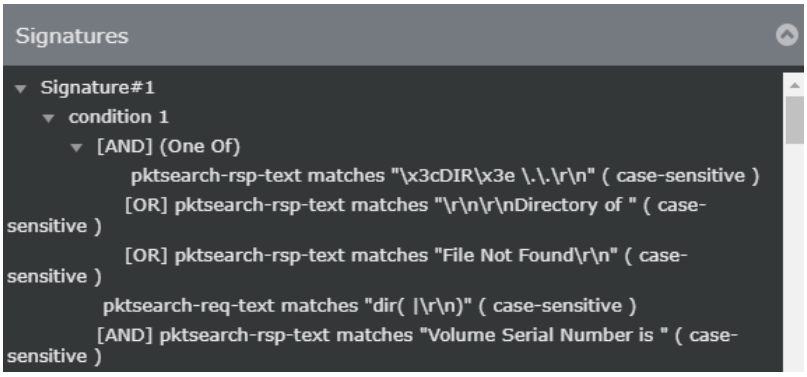
- Non-string match signatures will display information such as comparison field name, attack description and logical relation of the condition.

Figure 117. Example of a non-string matched signature



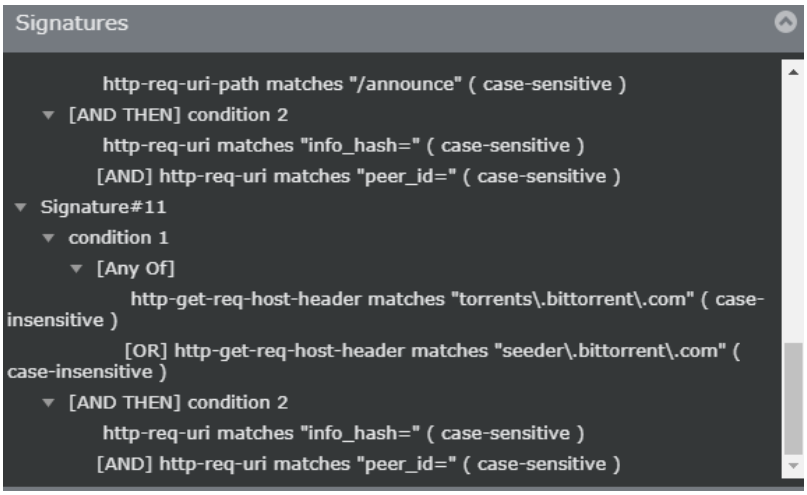
- System event (or sysevent) signatures display information such as the name of the system event and logical relation of the condition.

Figure 118. Example of a system event signature with an AND and OR condition



- Signatures with an AND or OR condition will provide you with exact details of the condition.
- Signatures with an AND or OR and an AND THEN condition will provide all the constituent conditions.

Figure 119. Example of a signature with AND, OR, and AND THEN conditions



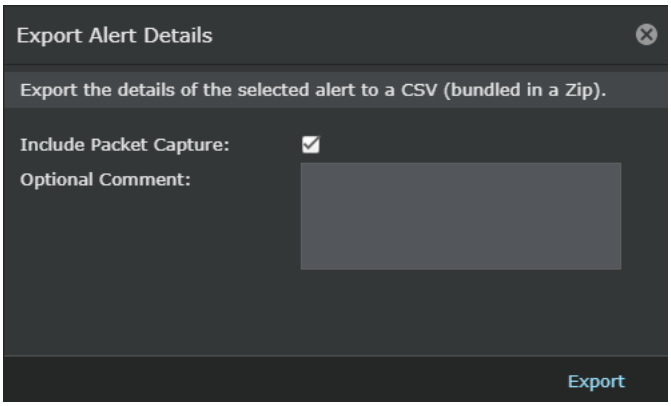
Export

You can export the files in instances where further analysis of the attack is required. Alert details and packet capture of an alert can be exported.

Alert details

The alert details are exported as a .csv file. You can also include to export the packet capture for that alert.

Figure 120. Export alert details



Packet capture

You can export only the packet capture for the selected alert. This helps analyze the specific attack details. You can export the packet capture only if you have the permission enabled by your system administrator for your user.

NOTE

The **Packet Capture Unavailable** message is displayed when there is no packet capture available for an alert.

To export alert details or packet capture for an alert:

1. Go to Analysis → <Admin Domain Name> → **Attack Log**.
2. Double-click on the alert for which you want to export the details.

   The **<Attack Name>** panel opens on the right hand side.
3. Under the **Summary** tab, click **Export** on top, and select either **Alert Details** or **Packet Capture**.

Alert Actions

The alerts generated can be further analyzed in case of critical alerts or used to perform actions that helps organize the alerts. Different options for alert actions are available on clicking the **Other Actions** button at the bottom of the page. The various alert actions are as follows:

Update Policy

Alerts are generated whenever there is an attack that violates a policy. When certain attacks are regularly detected, you can add them to the policy to take actions against the attack, which avoids repetitive alert generation for that attack.

Global IPS

You can add an attack to the **Master Attack Repository** policy set. This is a default generic policy which is applied across multiple Sensors. Hence, all the Sensors are updated with the attack. To add the attack to the policy:

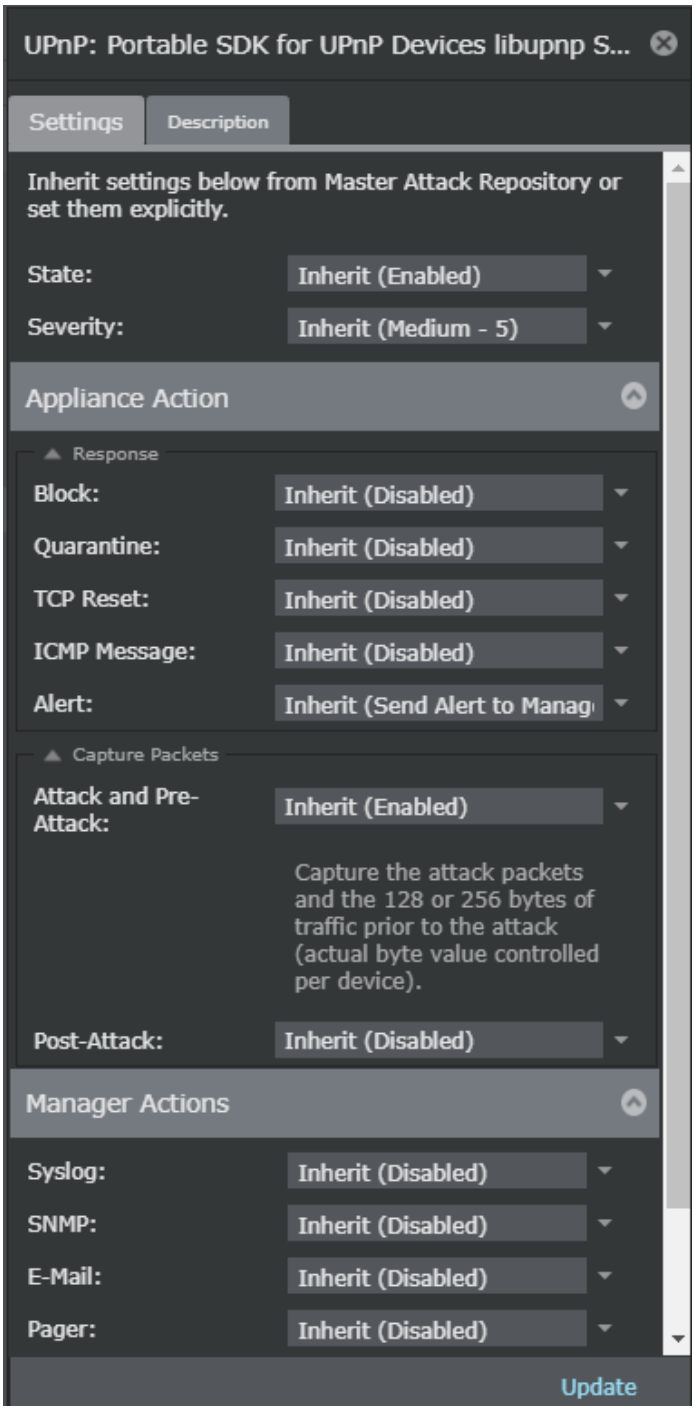
Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert, click **Other Actions** at the bottom of the page.
3. Select **Update Policy**, and click **(Global IPS) Master Attack Repository** for IPS devices or **Master NTBA** for NTBA appliances.

   The **<Attack Name>** panel opens.
4. Make the required changes to the policy settings and click **Update**.

   The attack is added to the **Master Attack Repository** policy set.

Figure 121. Global policy update



To view or edit the attack added to the **Master Attack Repository** policy set:

1. Navigate to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.
2. Double-click the **Master Attack Repository** policy.

   You can view the attack added to the list under **Attack Definitions** tab.

Domain IPS

You can add an attack to the policy of an admin domain. This depends on the admin domain from where the alert was generated. When an attack is added to the policy, the policy specific to that admin domain is updated. The attack is added to the selected policy set. To add the attack to the policy:

Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert, click **Other Actions** at the bottom of the page.
3. Select **Update Policy**, and click **(Domain IPS) /<Admin Domain Name>/<Policy Name>**.

   The **<Attack Name>** panel opens.
4. Make the required changes to the policy settings and click **Update**.

   The attack is added to the selected policy set.

   To view/edit the attack added to the policy:

   1. Navigate to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.
   2. Double-click the policy.

      You can view the attack added to the list under the **Attack Definitions** tab.

Interface IPS

An attack can be added to a specific interface which updates the existing policy of that interface. This depends on the interface from where the alert was generated. When an attack is added to the policy, the policy for that interface is updated. The attack is added to the selected policy set of that interface.

> **NOTE**
>
> This option is not visible for NTBA appliances.

To add the attack to the policy:

Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert, click **Other Actions** at the bottom of the page.
3. Select **Update Policy**, and click **(Interface IPS) /<Admin Domain Name>/<Device Name>/<Interface>**.

   The **<Attack Name>** panel opens.
4. Make the required changes to the policy settings and click **Update**.

   The attack is added to the selected policy set of that interface only.

   To view/edit the attack added to the policy of that interface:

   1. Navigate to Policy → <Admin Domain Name> → Intrusion Prevention → **Policy Manager**.
   2. Double-click the interface for which the policy is updated.

      The **<Device Name>/<Interface>** panels opens on the right side. You can view the attack added under **Customized Attacks** in the **IPS** section.

Malware

You can add malware attacks to the malware policy generated from an admin domain. This policy will be updated for that admin domain only.

Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert, click **Other Actions** at the bottom of the page.
3. Select **Update Policy**, and click **(Malware) /<Admin Domain Name>/<Malware Policy>**.

   The **<Attack Name>** panel opens.
4. Make the required changes to the policy settings and click **Update**.

   The attack is added to the malware policy of that admin domain.

   To view/edit the attack added to the malware policy:

   1. Navigate to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **Advanced Malware**.
   2. Double-click on the policy.

      The **Advanced Malware** page opens.

   NOTE

   The attacks added to the policies do not come into effect immediately. You have to update the Sensor for a policy update from **Deploy Pending Changes**.

   For more information on malware policies, see the section Advanced Malware Policies (page 930).

Create exceptions

As a network security administrator, you may sometimes notice a spike in alerts in the **Attack Log** from one host. Such high incidence of alerts can be caused by several factors which the IPS considers suspicious. You can either choose to act on every alert or provide a time frame during which the host issue can be resolved. During this period, you can choose to stop receiving alerts in the **Attack Log** and focus on other alerts.

In order to stop receiving such alerts temporarily, the Manager enables you with an option to create an alert exception that prevents such alerts from appearing in the **Attack Log**. An alert exception is a rule in the Manager that prevents specific alerts from showing up in the **Attack Log**, by automatically acknowledging similar alerts. Note that since you are only choosing to acknowledge the alerts automatically, the IPS process packets continues to generate alerts. IPS also continues to carry out response actions such as blocking, sending a TCP reset, etc. if any of these are enabled.

NOTE

Before you create an exception for any alert, it is important you make sure that the host in consideration will not be a potential threat. In most real-world situations, the host is usually an infected internal server or client which will not launch a full-scale attack. It is imperative to determine all factors that necessitate creation of an alert exception.

Add Ignore Rules

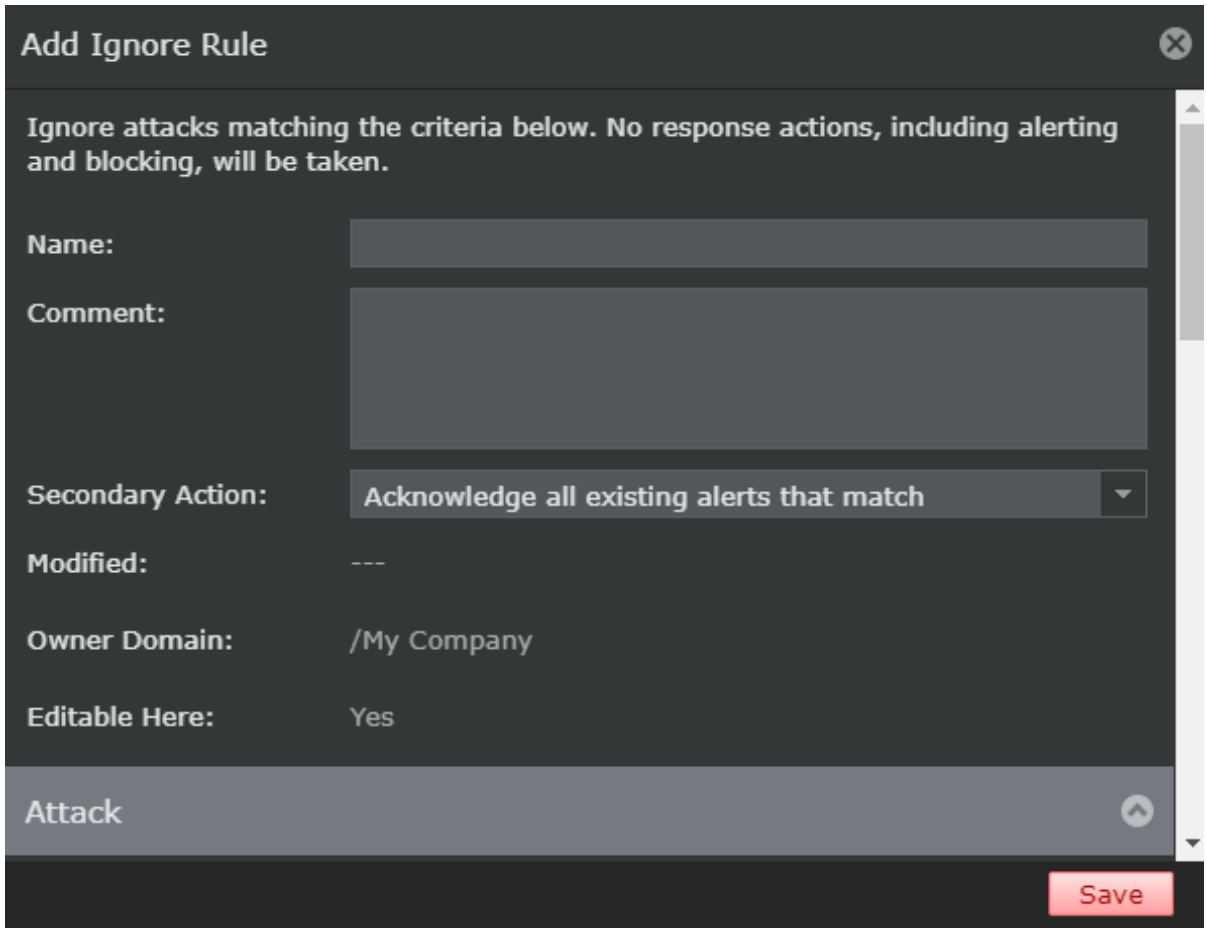
You can select a particular alert and configure an ignore rule. If necessary, you can create a new ignore rule and apply it to the selected alert. You apply an ignore rule to the resource for which the attack is raised and the direction of the attack.

To create Ignore Rules for the alerts generated, complete the following steps:

1. Select Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert for which you want to create the Ignore Rule, and click **Other Actions**.
3. Select **Create Exception** and click the **Add Ignore Rule** option.

   The **Add Ignore Rule** panel appears.

Figure 122. Add ignore rule panel



4. Specify your options in the corresponding fields.

Field	Description
Name	Type the name for the Ignore Rule.
Com-ment	Type additional comments if required.

Field	Description
Secondary Action	The secondary/additional action to be performed on the alert other than ignoring the alert. • **None** — No action taken other than ignoring the alert. • **Acknowledge all existing alerts that match** — Acknowledges all the alerts that match the criteria. You can later view these alerts as acknowledged alerts in the **Attack Log**. • **Delete all exisitng alerts that match** — Deletes all the alerts that match the ignore rule criteria. These alerts will not be available in the database also.
Modified	Displays the last modified user, date and time for the Ignore Rule. The field is blank when creating the rule for the first time.
Owner Domain	The name of the admin domain under which the Ignore Rules are added
Editable here	The status **Yes** indicates that the Ignore Rule is owned by the current admin domain. The status **No** indicates that the Ignore Rule is not owned by the current admin domain.
Attack	Select the attack to match the criteria. 1. Type the first few letters of the attack name in the **Search attack name** field, select the attack from the list. 2. Click the **Add** button to add the attack name to the list. 3. Select the **Direction** from the drop-down list. The options are **Inbound**, **Outbound**, and **Any**. Click ✕ to remove the attack from the list.
Scope	Select one or more device or interface to match the criteria. 1. Select the device or interface from the **Resource** drop-down-list. 2. Click the **Add** button to add the device or interface to the list. Click ✕ to remove the item from the list.

Field	Description
Attacker	1. Select the rule object from the **Endpoint** drop-down-list. 2. Click on the **Add** button to add the rule object to the list. Click the **Add** icon to add a new rule object. The supported network objects are: • **IPv4 Address Range** • **IPv4 Endpoint** • **IPv4 Network** • **IPv6 Address Range** • **IPv6 Endpoint** • **IPv6 Network** • **Network Group for Exception Object** Click to edit or view a rule object. Click to remove the rule object from the list. 3. Select the type of port from the **Port** drop-down list. The available options are: • **Any** • **TCP** • **UDP** • **TCP or UDP** 4. Type the port values for TCP and UDP protocols in the field provided. The supported port values are 1 to 65535. To specify multiple ports used in the same protocol, provide the values separated by commas. Example: 15,25.

Field	Description
Target	Select one or more rule objects. 1. Select the rule object from the **Endpoint** drop-down-list. 2. Click on the **Add** button to add the rule object to the list. Click to add a new rule object. The supported network objects are: • **IPv4 Address Range** • **IPv4 Endpoint** • **IPv4 Network** • **IPv6 Address Range** • **IPv6 Endpoint** • **IPv6 Network** • **Network Group for Exception Object** Click to edit or view a rule object. Click to remove the rule object from the list. 3. Select the type of port from the **Port** drop-down list. The available options are: • **Any** • **TCP** • **UDP** • **TCP or UDP** 4. Type the port values for TCP and UDP protocols in the field provided. The supported port values are 1 to 65535. To specify multiple ports used in the same protocol, provide the values separated by commas. Example: 15,25.

5. Click **Save** to save the Ignore Rule.

   For more information on Ignore Rules, refer to [Manage Ignore Rules] in [IPS Administration] section.

Add Auto-Acknowledgement Rule

To create auto-acknowledgement rules for alerts, complete the following tasks:

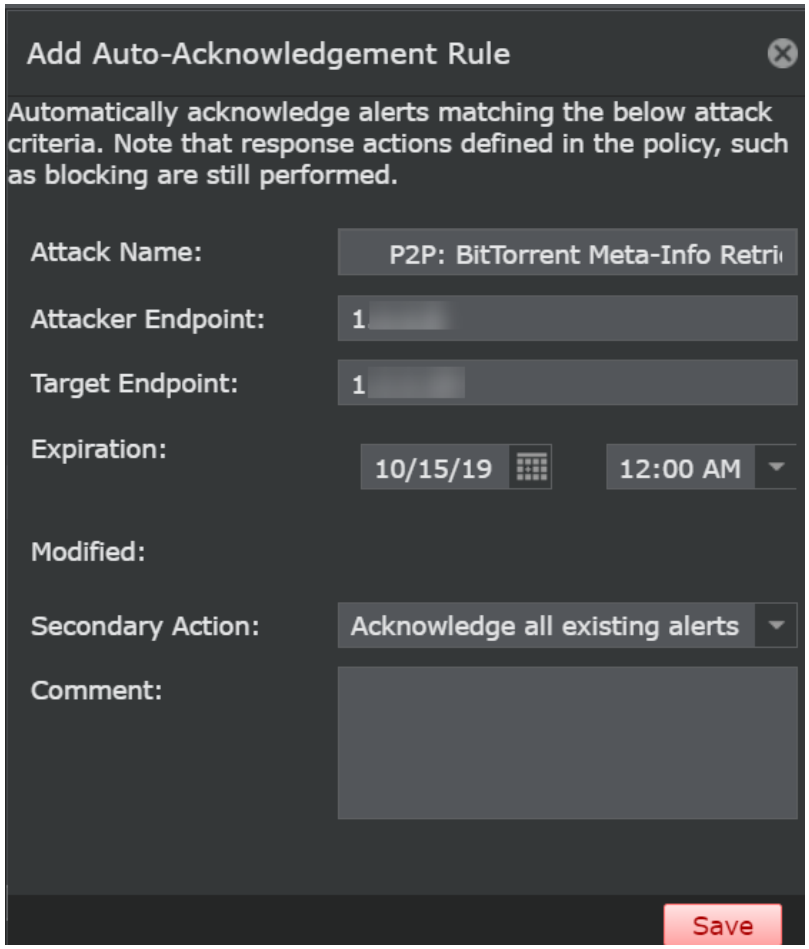
> **NOTE**
>
> Adding auto-acknowledgement rules for alerts is not applicable for the Central Manager.

Steps:

1. Select Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert for which you want to create an auto-acknowledgement rule, and click **Other Actions**.
3. Select **Create Exception** and click the **Add Auto-Acknowledgement Rule** option.

   The **Add Auto-Acknowledgement Rule** panel appears.

Figure 123. Auto acknowledgement rule



4. The following fields are auto filled based on the alert selected. You can modify the details if required.

Option	Definition
Attack Name	Name of the attack for which the alert was generated.
Attacker Endpoint	IP address of the attacker.
Target Endpoint	IP address to which the attack was targeted.
Expiration	Date and time at which the rule expires.
Modified	Displays the last modified user name, date and time. The field is blank when creating the rule for the first time.
Secondary Action	The secondary/additional action to be performed on the alert other than auto acknowledging the alert. • **None** — No action taken other than auto acknowledging that particular alert. • **Acknowledge all existing alerts that match** — Acknowledges all the alerts that match the criteria. You can later view these alerts as acknowledged alerts in the **Attack Log**.
Comment	Type additional comments if required.

5. Click **Save** to save the Ignore Rule.

   For more information on auto-acknowledgement, see the [Auto-Acknowledgement] section in the [Trellix Intrusion Prevention System Product Guide].

Add domains to Exclusion list

Domains which are excluded are first checked when the Sensor is analyzing the attacks. To exclude a domain, complete the following tasks:

Steps:

1. Select Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose domain you want to exclude, and click **Other Actions**.
3. Select **Create Exception** and click the **Exclusion List Domain: <domain name>** option.

   A confirmation message is displayed.

   In case of callback activity alerts you can exclude the C&C domain by selecting **Exclude the C&C Domain**.
4. Click **Yes**.

   The successfully excluded message is displayed.

   You can view/edit the excluded domain under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Domain Name Exceptions**.

   For more information on exclusion list domains, see Add hash values to the allow list (page 976).

Add file hash to Allow/Block list

The MD5 hash value of a malware file added to the allow list is exempted from analysis as it is safe. On the other hand, the MD5 hash value of a malware file added to the block list is immediately blocked as it is malicious. You can add the file hash of a malware alert from the Attack Log.

> **NOTE**
>
> In case MD5 entries limit has reached, the Manager adds SHA256 hash value(s) of the malware file(s) to its allow/block list and sends the same hash value(s) to the Sensor through incremental or full update.

There are multiple ways a file hash can be added to the Allow/Block list.

Adding a hash from the <Attack Name> panel:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Double-click the malware alert whose file hash you want to allow or block.

   The **<Attack Name>** panel opens on the right hand side of the browser window.
3. Click the **Details** tab.
4. The file hashes are listed within the **File Hash** section under the **File Name** field. Click **Allow** or **Block** to add the hash to Allow or Block list.

Adding a hash from Other Actions menu:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the malware alert whose file hash you want to allow or block.
3. Click **Other Actions**, select **Create Exception**, and click **Allow File Hash: <hash file>**/**Block File Hash: <hash file>**.
4. Click **Yes**.

   A successfully allowed/blocked message is displayed.

   You can view/edit the allowed/blocked file hashes under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **File Hashes**.

Adding a hash from Malware Files page:

1. Navigate to Analysis → <Admin Domain Name> → **Malware Files**.
2. Click **Take action** for a specific entry and select **Allow** or **Block** to automatically add the file to the Manager's allow/block list. In the next 5 minutes, the Manager sends the hash value to the allow/block list of all the Sensors, depending on the action taken.

Enabling "Add to Block List" through the Advanced Malware Policy Page:

1. Navigate to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **Advanced Malware**.

   The Advanced Malware policies are listed.
2. Double click a policy to edit.
3. In the policy configuration page, for a specific **File Type**, choose the severity under **Add to Block List** column and click **Save**.

   For a file to be added to the block list, the file's severity must be the same or more than the severity you specify. For example, if you specify high as the criteria, then files of severity high and very high are added to the block list. Within the next 5 minutes, the Manager adds this file to the local block list of all the Sensors that it manages.

Reclassify Endpoint Executable

You can separately classify alerts with executables hash files. You can either allow or block it. When an executable hash file is seen for the first time in the network, you have the option to unclassify it and send it for further analysis. You can later perform forensics for these hash files.

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose file hash you want to allow or block or unclassify.
3. Click **Other Actions**, select **Create Exception**, and click **Reclassify Endpoint Executable: <hash file>**.

   A confirmation message is displayed.
4. Click **Yes**.

   A successfully allowed/blocked/unclassified message is displayed.

   You can view/edit the endpoint executable file hash under Analysis → <Admin Domain Name> → **Endpoint Executables**.

   For more information on endpoint executable file hash, see Analyze Endpoint Executables (page 476).

Quarantine an Endpoint

When an endpoint is infected, that endpoint can be quarantined so that the traffic is blocked. This will prevent further infection of endpoints in the network. Trellix IPS provides the option to quarantine an endpoint for specific time periods. This provides time to fix the endpoint. You can either quarantine the source IP or the destination IP which blocks the traffic.

NOTE

If the source IP is behind a proxy server, the proxy server IP is quarantined. Consequently, all traffic through the proxy server gets quarantined.

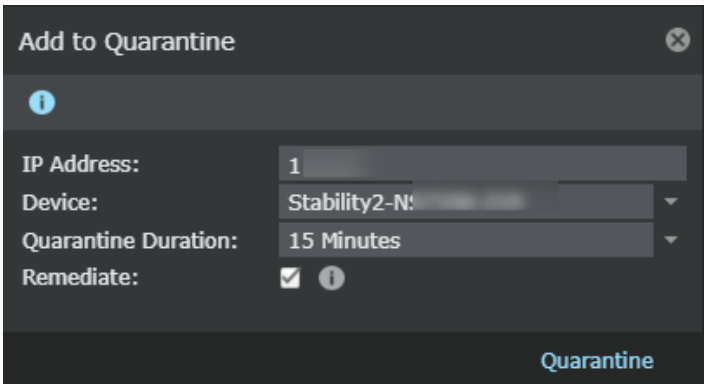
NOTE

Quarantine endpoint is not applicable for the Central Manager.

Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose IP has to be quarantined.
3. Click **Other Actions**, and select **Quarantine Endpoint**. Click the endpoint IP address you want to quarantine.

Figure 124. Add to quarantine



If the endpoint is added to the list of quarantined endpoints, a message is displayed that quarantine is successful. If the endpoint is already quarantined, a message displays that the endpoint IP is already present in the **Quarantine** list.

The **Add to Quarantine** pop-up opens.

4. Update the following fields:

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.

Option	Definition
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal**. Remediation cannot be configured for IPv6 address. The checkbox and the information icon for remediation is not displayed if you enter an IPv6 address in the **IP Address** field.

5. Click **Quarantine**.

Quarantine options for NTBA alerts

You can choose to quarantine policy violation, callback attacks, recon and threshold-based attacks, endpoint-based anomaly attacks, and behavioral NTBA alerts.

The quarantine response action needs to be enabled at the policy level per zone.

If the attack was detected by Cisco router, the NTBA Appliance quarantines that endpoint by setting an ACL at the router for 5 minutes by default.

If the attack was detected at a Sensor, the NTBA Appliance sends the quarantine details as part of the alert to the Manager. In response to this, the Manager sends the corresponding source endpoint as part of endpoint quarantine to the Sensor.

The quarantine details sent in the alert are exporter id, response action, and source interface.

The period for which quarantine is effective is 5 minutes by default. If you want to change this value, contact Trellix Technical Support.

Tag an Endpoint

A tagging endpoint is quarantined which helps in the analysis of the source endpoint or the destination endpoint. Trellix ePO - On-prem and ISC enables tagging of endpoints and provides analysis information in case of suspicious activities. In case of ePO tagging, only managed endpoints can be tagged. The tagged endpoint is quarantined and a response action can be configured for the endpoint from the ePO server. In case of ISC, the tagged VMs are quarantined. Response action for the tagged endpoint can be configured, which either allows the traffic to flow through the VM or completely blocks the traffic.

NOTE

Tagging an endpoint to ePO is not applicable for the Central Manager.

ePO

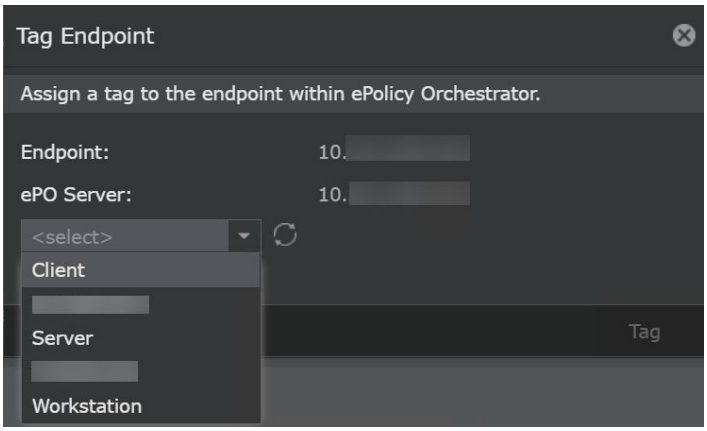
To tag an endpoint to the ePO server, complete the following steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.

2. Select the alert whose endpoint you wish to tag. It can either be the source IP or the destination IP.
3. Select Other Actions → Tag Endpoint → **in ePO**, and click the source or destination IP to be tagged.

   The **Tag Endpoint** pop-up opens.

Figure 125. Tag an endpoint



   The ePO server is selected by default depending on the admin domain from which the endpoint is being tagged.
4. Select the tag from the **Tag to Assign** drop-down list.
5. Click **Tag**.

   A successfully tagged message is displayed.

> **NOTE**
>
> You can create your own tags in ePO other than the default tags that exist. To retrieve the latest set of tags, click the refresh icon. To avoid errors, make sure that the endpoint being tagged is a managed endpoint and the tags exists in the ePO server.

For more details, refer to the chapter [Integration with Trellix ePolicy Orchestrator - On-prem] in [Trellix Intrusion Prevention System Integration Guide].

ISC

To tag an endpoint to ISC, complete the following steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose endpoint you wish to tag.
3. Select Other Actions → Tag Endpoint → **via ISC**, and click the source or destination IP to be tagged.

   The **Tag Virtual Endpoint via ISC** pop-up opens.

   The endpoint and VSS server are detected by default.
4. Select the tag from the **Tag to Assign** drop-down list.
5. Click **Tag**.

   A successfully tagged message is displayed.

NOTE

Only the default tags are available for tagging the endpoint.

For more details, refer to the chapter [IPS for virtual networks using Intel® Security Controller] in [Trellix Virtual Intrusion Prevention System Product Guide].

Terminate Connection

A TCP reset is a network response that disconnects an established TCP transmission. The **Terminate Connection** option shuts down an attack from a malicious source, ends a transmission to a vulnerable destination, or drops both ends of a source-to-destination transmission.

NOTE

Sending a TCP reset applies only to TCP protocol-based attacks. If a Sensor is in inline mode, it will drop all further packets instead of sending TCP resets.

NOTE

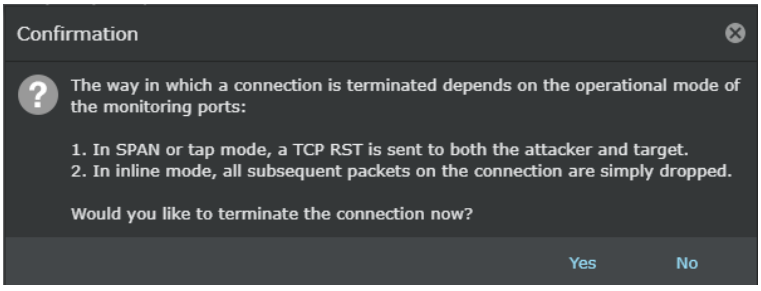
Terminate Connection is not applicable for the Central Manager.

Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the TCP-based attack instance.
3. Click **Other Actions**, and select **Terminate Connection**.

   A confirmation window opens.

Figure 126. Terminate connection



4. Select **Yes** to terminate the connection.

   The connection is terminated by sending a message to the device.

Perform Network Forensics

You can perform the Network Forensics for either the source endpoint or the destination endpoint. This analyzes and provides information about the endpoints.

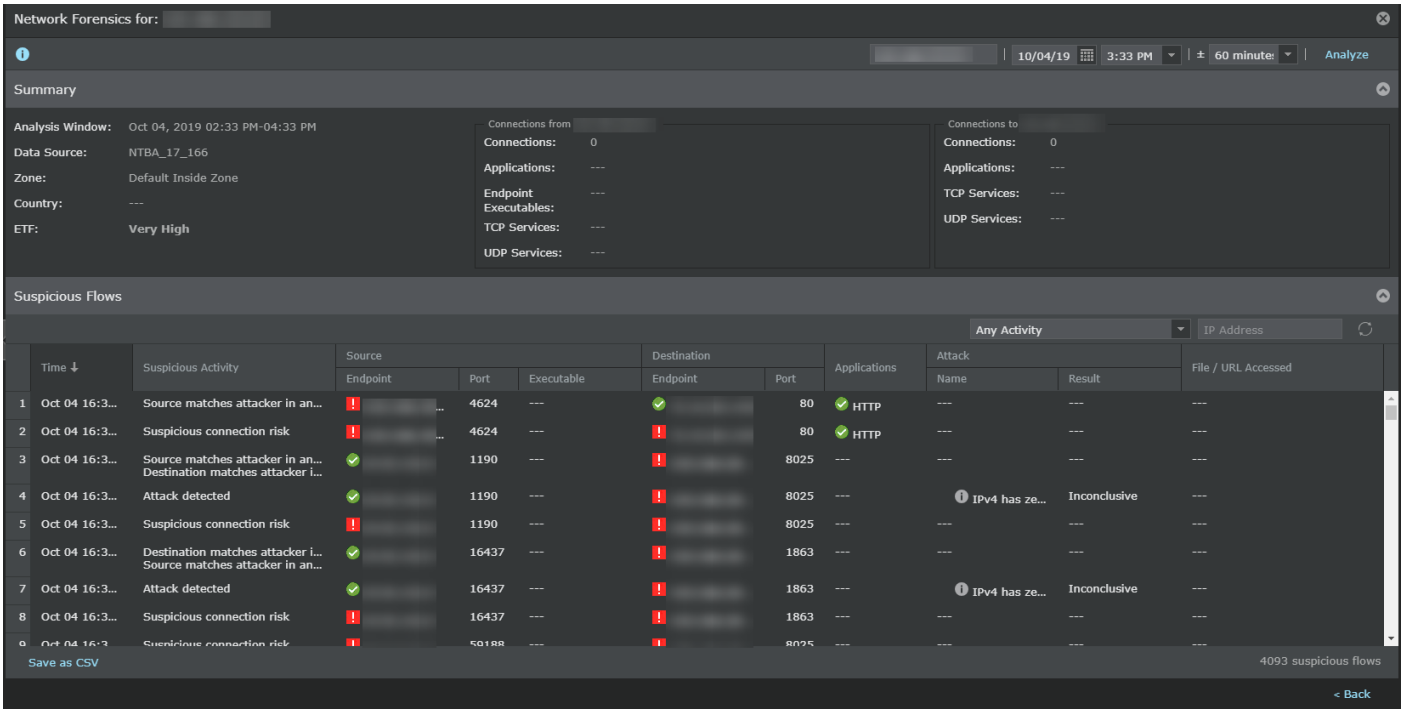
NOTE

Network Forensics is not applicable for the Central Manager.

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose IP to which you want to perform forensics.
3. Click **Other Actions**, and select **Perform Network Forensics**. Click the endpoint IP for which you want to perform forensics.

   The **Network Forensics** page opens. The IP address is populated based on the endpoint selected to perform forensics.

Figure 127. Network Forensics



4. Select the date and time. Use the ± time to view endpoint behavior before and after an attack.
5. Click **Analyze**.

   Detailed information about the endpoint is displayed.

   Click the icon to close the network forensics page.

   For more information on network forensics, see the [Network Threat Behavior Analysis Product Guide].

Perform GTI Forensics

GTI forensics connects to the GTI cloud and extracts the forensics information for the endpoint. It displays the threat details for the endpoint.

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose IP address to which you want to perform forensics.

3. Click **Other Actions**, and select **Perform GTI Forensics**. Click the endpoint IP for which you want to perform forensics.

   The **Threat Intelligence** forensics page opens in your browser with information about the endpoint.

Assignment of alert

Users with read-write (RW) permission can manipulate the assignment of an alert, including assigning it to oneself, removing current assignment (making it unassigned again) irrespective of who the current assignee is, and assigning the alert to a specific user.

Assign alerts to users

You can assign a new alert to a specific administrative user account.

To assign new alerts to users:

Steps:

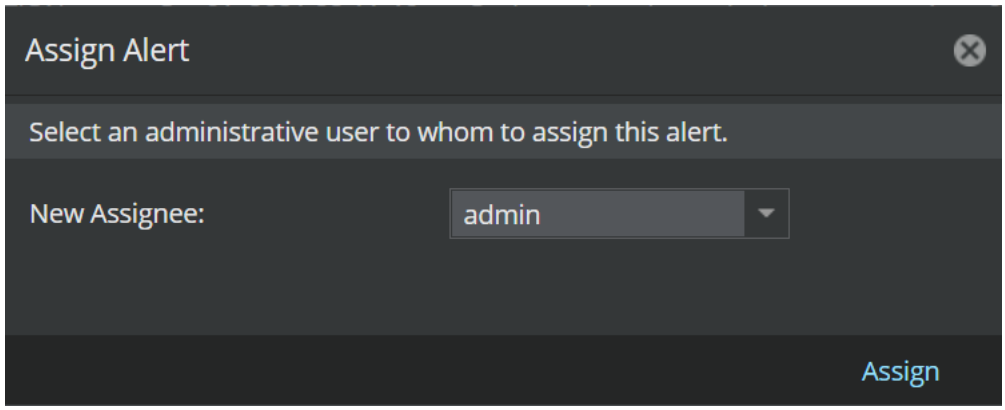
1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert you want to assign.

   By default, a new alert is unassigned.
3. Click **Other Actions**, select **Assign Alert** and either click **Assign to me** or **Assign to Someone Else**.

   If you selected **Assign to me**, the alert is assigned to you. The **Assigned** message flashes once the alert is assigned.

   If you selected **Assign to Someone Else**, the **Assign Alert** pop-up opens. Proceed to step 4.

Figure 128. Assign alert to someone else



4. Select the user from the **New Assignee** drop-down list.
5. Click **Assign**.

   The **Assigned** message flashes once the alert is assigned to the user.

Remove assignments from alerts

Prerequisites:

- You have the appropriate read/write permissions.
- The alert is in your name.

Steps:

You can remove the alerts that are assigned to you by performing the following steps:

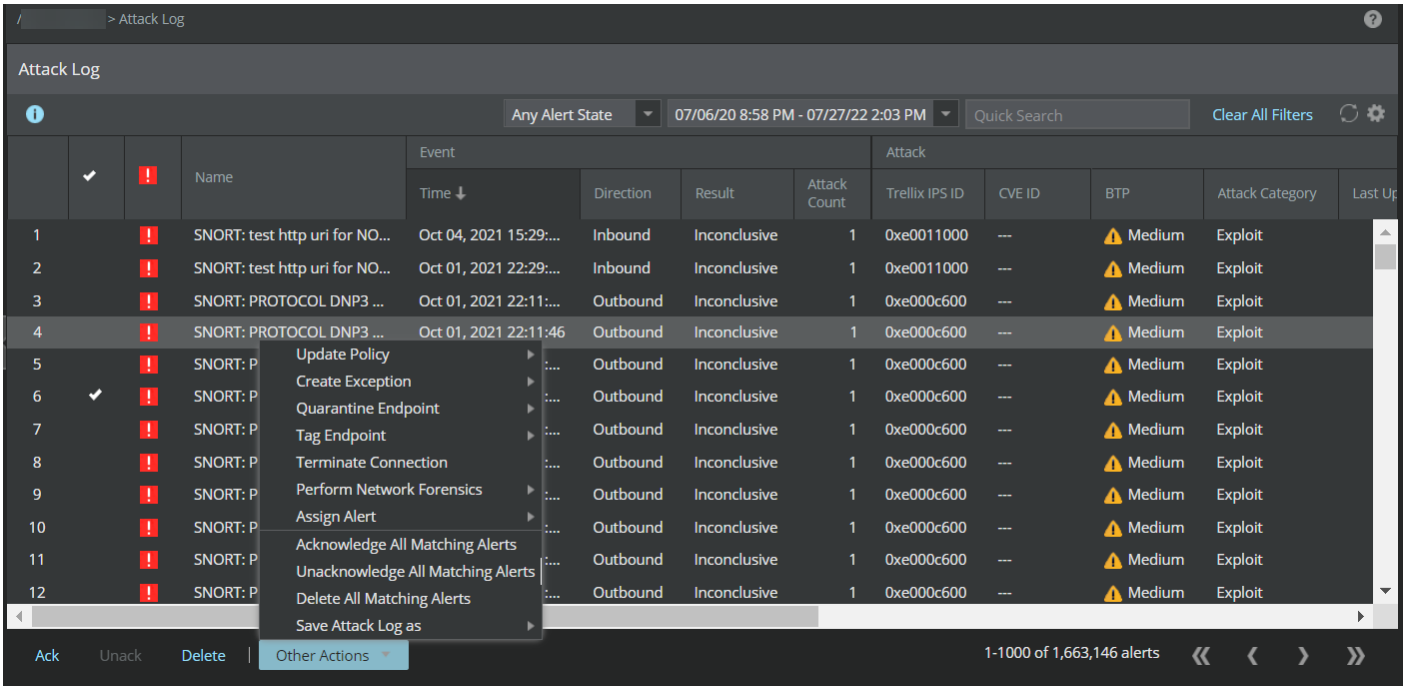
1. In the Attack log, select the alert you want to unassign.
2. Click **Other Actions**, select **Assign Alert** and click **Remove Current Assignment**.

   The **Assignment Removed** message flashes once the assignment is removed.

Delete Alerts

Any alert deleted from the **Attack Log** is also deleted from the database. To delete an alert, select the alert and click **Delete**. To delete all the alerts that are displayed in the **Attack Log**, click the **Other Actions** button, and then select **Delete All Matching Alerts**. When you click the **Delete All Matching Alerts**, all alerts in the **Attack Log** are deleted.

Figure 129. Delete alerts



Save Attack Log

You can save the list of alerts from the Attack Log for further analysis or future reference. The Attack Log can be exported as a PDF file or CSV file. To export the list of alerts, click **Other Actions**, select **Save Attack Log as**, and click the format in which you want to the Attack Log to be exported.

Alert rate

The alert rate of a Manager/Central Manager is the number of alerts processed by the Manager per second. The alert rate mainly depends on the event rate in the Manager. The event rate of a Manager/Central Manager is the number of events processed by the Manager per second. An event can be defined as an action performed in the Sensor like an alert, packet log, ACL event, IPS event, performance monitoring, application identification, etc. The total number of events generated by the Sensors attached to a Manager depends on various parameters like type of traffic, amount of traffic, policies used, Sensor capacity, etc.

The following table details the test conditions when the Manager alert rate is 300 per second at an event rate of 375 per second:

Server Details	Sensor models	Composition of Traffic
Windows 2022 based Manager server virtual machine 32GB RAM 8 x 2.2GHz CPU cores 500GB Hard Disk Drive 16GB allocated for JVM (by default)	NS-series Sensors Virtual IPS Sensors	Malware alert ranging between 20% to 80% and Signature ranging between 80% to 20% with Packet logging enabled
		Signature alert ranging between 40% to 60%, Malware alert ranging between 20% to 40%, Alert with GTI and DNS Lookup upto 20% with Packet logging enabled
Linux based Manager server virtual machine 32GB RAM 8 x 2.4GHz CPU cores 500GB Hard Disk Drive 24GB allocated for JVM (by default)		Signature set attack only traffic with Packet logging enabled
		Malware only traffic with Manager Block list, Trellix IPS Analysis, GTI File Reputation, and Gateway Anti-Malware engines enabled

NOTE

The IPS alerts comprises up to 80% of the total events in the Trellix IPS.

NOTE

The alert rate and the event rate are higher in a Linux based Manager appliance when compared to a Windows or Linux based Manager virtual machines.

For example, consider an organization using the Trellix IPS solution. The network has four different subnets as follows:

Subnet	Policies used	Amount of traffic inspected	Average number of alerts generated per second
Engineering	Default Testing	300 Gbps	200
Finance	Default Testing with Default Malware	40 Gbps	50
Sales	Default Prevention	80 Gbps	100
Human Resource	Default Detection	30 Gbps	75

Each of the above subnets is managed by a separate Manager.

In the above network, Finance, Sales, and Human Resource subnets have lower alert rate. So, the alerts are seen in the **Attack Log** page of the Manager in real time. But in the Engineering subnet, the alert is higher. These additional alerts are placed in a queue to be processed by the Manager and result in delays. When such delays accumulate over time, the Manager fails to fetch alerts in real time, and consequently, the **Attack Log** does not show up-to-date alerts. To achieve a higher alert rate in the Manager, you can upgrade to the Manager version 10.1.7.65 or higher, where the alert rate is 300 per second when the event rate is up to 375 per second.

If you observer higher alert rate in your environment regularly, do the following:

1. The Manager must be upgraded to software version 10.1.7.65 or higher.
2. Fine tune the IPS policies used.

   NOTE

   Trellix recommends you to avoid using the **Default Testing** policy. This policy includes all types of attacks and some of these attacks may not be relevant to your network. Instead, you can identify and disable such irrelevant attacks or use the **Default Prevention** policy.

3. Configure **Alert Filters** or **Ignore Rules** to avoid known traffic like the traffic from vulnerability scanners, testing servers, etc.
4. Configure **Firewall Rules** to skip scanning traffic from known source or destination IP addresses and vulnerability scanners.
5. Configure **Auto Acknowledgment** for low and informational severity attacks. This will save the Manager CPU cycles consumed for alert processing of source or destination IP addresses like DNS queries, GTI calls, etc.
6. Configure scheduled DB pruning to maintain only around 10 million alerts or 90 days of alerts as recommended in your enterprise network policy.
7. Install another Manager server and divide the Sensors between these Managers such that the alerts are not overloaded in an individual Manager.

If you are using a Central Manager to manage the Managers running version 10.1.7.65 or higher, the value of **`iv.core.nscm.alertSize`** attribute in the **`ems.properties`** file of the local Manager should be updated.

To edit the **`ems.properties`** file in the Manager, do the following:

Windows based Manager server

1. RDP to the Manager server.
2. Go to **`<Manager_Install_Dir>\config\ems.properties`**

   NOTE

   The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

3. In the **`ems.properties`** file, locate the following:

   ```
   iv.core.nscm.alertSize=50
   ```

4. Edit the above line as follows:

   ```
   iv.core.nscm.alertSize=500
   ```

   NOTE

   If you are having high alert rate in your Manager, set the **`iv.core.nscm.alertSize`** attribute value to 1500 for high alert synchronization between the Central Manager and the Manager.

5. Save the changes.
6. Reboot the Manager server.

Linux based Manager server

1. Log in to the Manager shell.
2. Execute the **`edit ems.properties`** command.

   > **NOTE**
   >
   > The **`edit`** command will edit the file using **vi-editor**. Trellix recommends you to use **vi_editor** command to perform editing operations on the files.

3. In the **`ems.properties`** file, locate the following:

   ```
   iv.core.nscm.alertSize=50
   ```

4. Edit the above line as follows:

   ```
   iv.core.nscm.alertSize=500
   ```

   > **NOTE**
   >
   > If you are having high alert rate in your Manager, set the **`iv.core.nscm.alertSize`** attribute value to 1500 for high alert synchronization between the Central Manager and the Manager.

5. Save the changes.
6. Execute the **`reboot`** command to restart the Manager server.

Threat Explorer

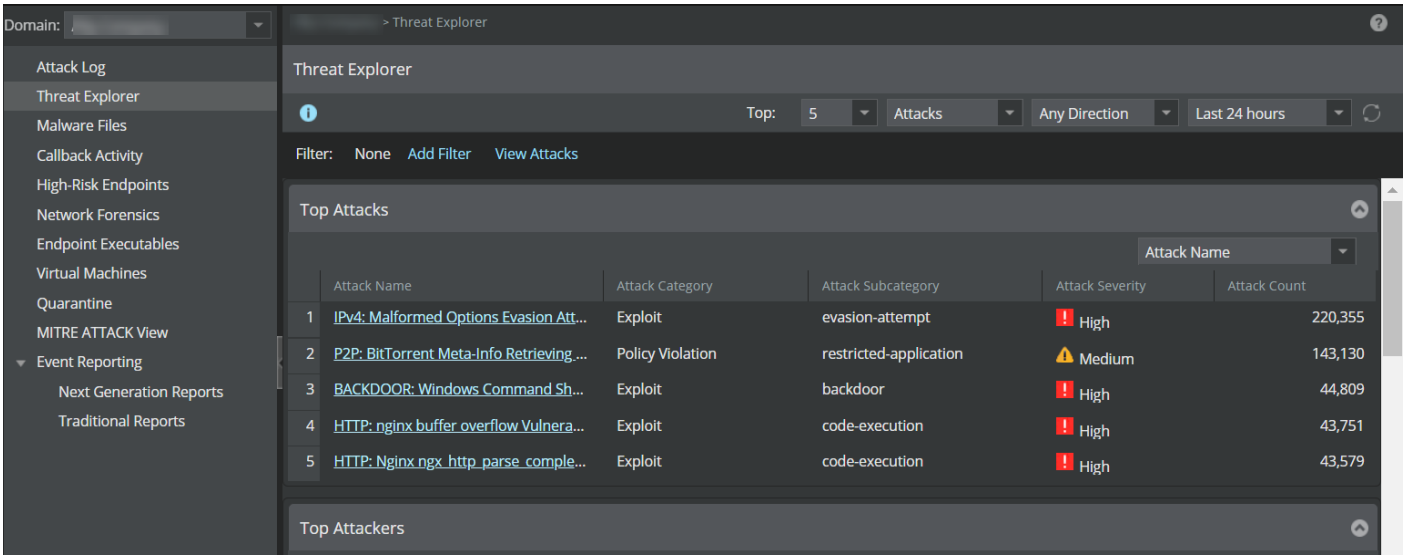
The Manager helps you easily view the top attacks, attackers, targets, and malware within a given period of time and a direction (optional) using the Threat Explorer. The Threat Explorer shows the attacks that have happened the most, the IP addresses responsible for most of the attacks, the IP addresses that are mostly attacked, the applications used to perform most of these attacks, and the most commonly downloaded or uploaded malware to perform these attacks.

To view the **Threat Explorer** page, perform any one of the following actions:

- On the **Analysis** tab, click <Domain Name> → **Threat Explorer**.
- On the **Dashborad** tab, click on any of the attack statistics. It will open the **Threat Explorer** page.

Also, for a given IP address, the integration with other Trellix point products helps you to view the host name, operating system, open ports, and known vulnerabilities, thus making the information readily available.

Figure 130. Threat Explorer page



The **Top** option helps you to filter the data displayed in the tables on the basis of the following components:

- The number of top N core attributes you want to view. The minimum and maximum values of N are 5 and 25, respectively. The default value of N is 5.
- The **Attacks** filters the top attacks, attacker, target, and so on.
- The inbound or outbound direction of the attack. The default is **Any direction**.
- The time frame of the core attributes in the top N tables. The minimum time is last 5 minutes. The data can be filtered for the time period of your preference using the **Custom Time Period** option. The default value is last 12 hours.

Figure 131. Top option

In case of NTBA appliances, there are two more filter options available:

- **Bytes** and **Connections** — Filters the top options based on bytes or connections for source IPs, destinations IPs, and so on
- **<Device Name>** — You can select the NTBA appliance for which you would like to view the core attributes.

Figure 132. Top option for NTBA appliances

You can use the following options to customize your **Threat Explorer** page view.

Name	Icon	Description
Hide		Hide the top N table of your choice.

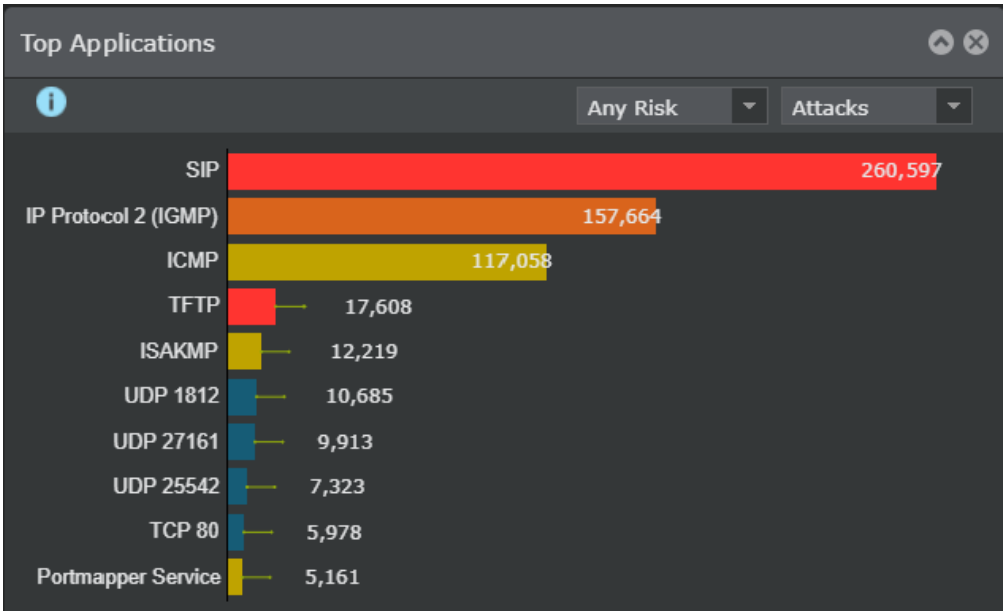
Name	Icon	Description
Expand		Expand the top N table of your choice.
Add filter	Add Filter	Add filter of your choice.
Launch Attack Log	View Attacks	Go to Attack Log to view the alerts.

Scenario: Ease of drill down from the Dashboard page

With a task-based design, the Manager user interface enables you to easily drill-down to locate root cause for an issue. Let us see an example here.

The **Dashboard** page allows you to investigate on the top applications under the **Top Applications** graph.

Figure 133. Top Application monitor in the Dashboard



You can view the top applications bar chart based on the risk type. The available options in the drop-down list are **Any Risk**, **High Risk** and **Medium+ Risk**. The default option is **Any Risk**.

You can further categorize the view of top applications based on the following options:

- **Attacks**
- **Bytes**
- **Connections**

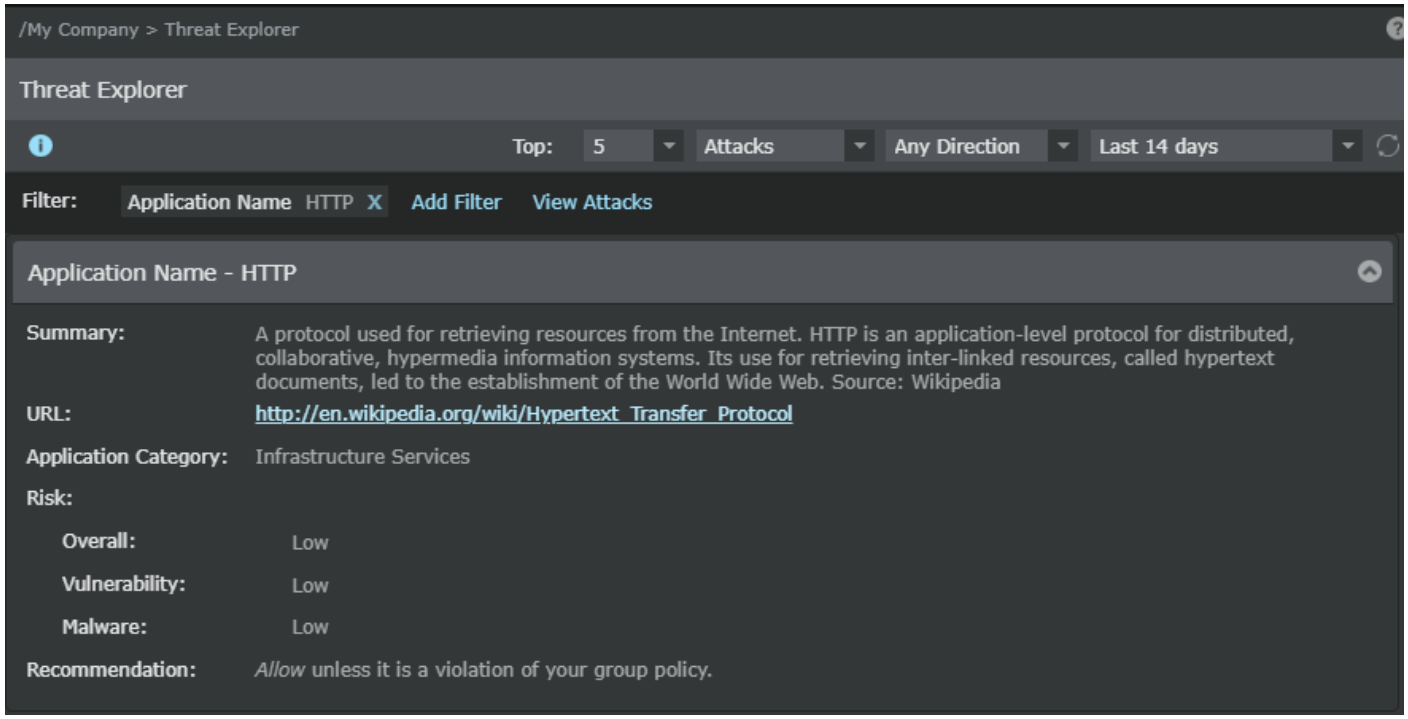
The default option is **Attacks**.

To further investigate on a top application:

1. Hover over the top application bar chart. You can view details like the application name, connection count, risk and category.

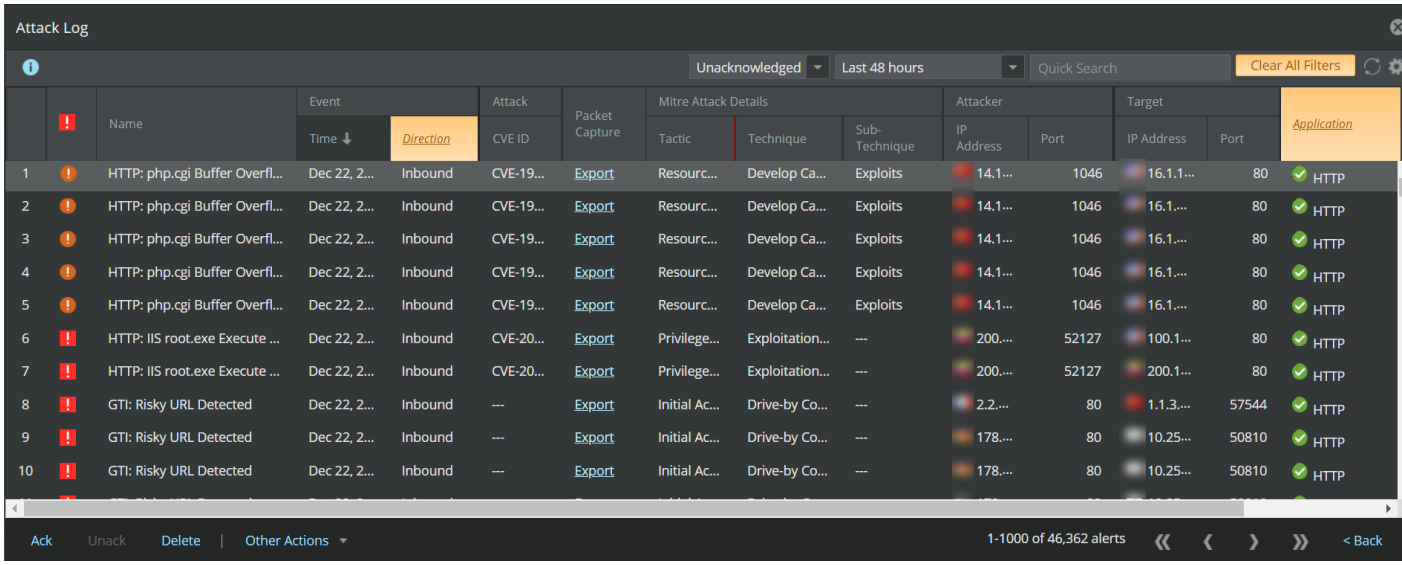
2. Click on an application bar in the **Top Applications** monitor. This navigates to **Threat Explorer** page with the filter created for the corresponding application and the top N tables populated accordingly with the data.

Figure 134. Top applications in Threat Explorer



3. You can perform these actions based on your investigation needs.
   - Add multiple level filter criteria to view more specific details.
   - Click **View Attacks** to navigate to **Attack Log** and view all alerts pertaining to this application.

Figure 135. Attack log with filters



NOTE

The filter criteria is already applied when you are on **Threat Explorer** via the **Dashboard** page. If you navigate directly from **Analysis** tab, the **Threat Explorer** page does not have any filters.

For more details on filters, refer to section Add a filter (page 436).

Top N security tables based on alert data

Use this section to view and manage the most common top security tables based on alert data from the **Threat Explorer** page.

The following tables are shown by default:

- Top Attacks
- Top Attackers
- Top Targets
- Top Attack Applications
- Top Attack Executables
- Top Malware

Core attributes

Each of the top N security tables has one core attribute that helps you to start a filter. Select the required admin domain from the **Domain** drop-down list. The **Threat Explorer** page displays data applicable to that admin domain only. The **Include child**

domain is selected by default. This can be deselected when data for the admin domain need not include data from the child domain. Click the core attribute to view the details of the selected attribute.

The core attributes of the top N security tables are explained in the following table.

Top N Table Name	Core Attribute
Top Attacks	Attack Name
Top Attackers	Attacker IP Address
Top Targets	Target IP Address
Top Attack Applications	Application Name
Top Executables	Executable Hash
Top Malware	Malware File Hash

Sort options

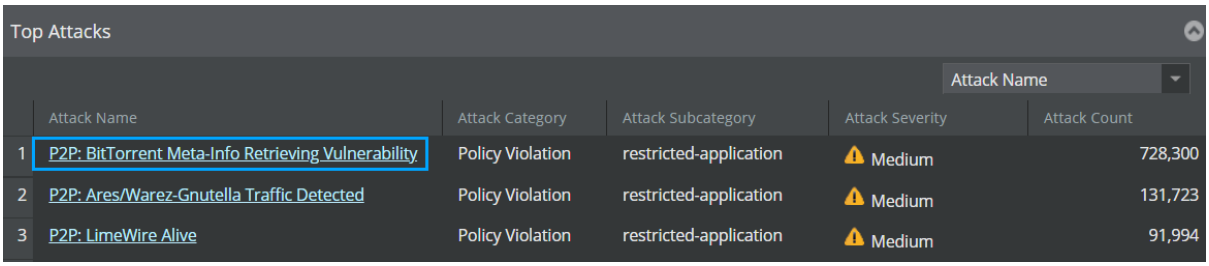
To sort the tables by specific attributes, select from the sort options at the top right corner of each top table. Use these options to select the attribute of your choice from the drop-down list.

Figure 136. Sort drop-down list

Scenario

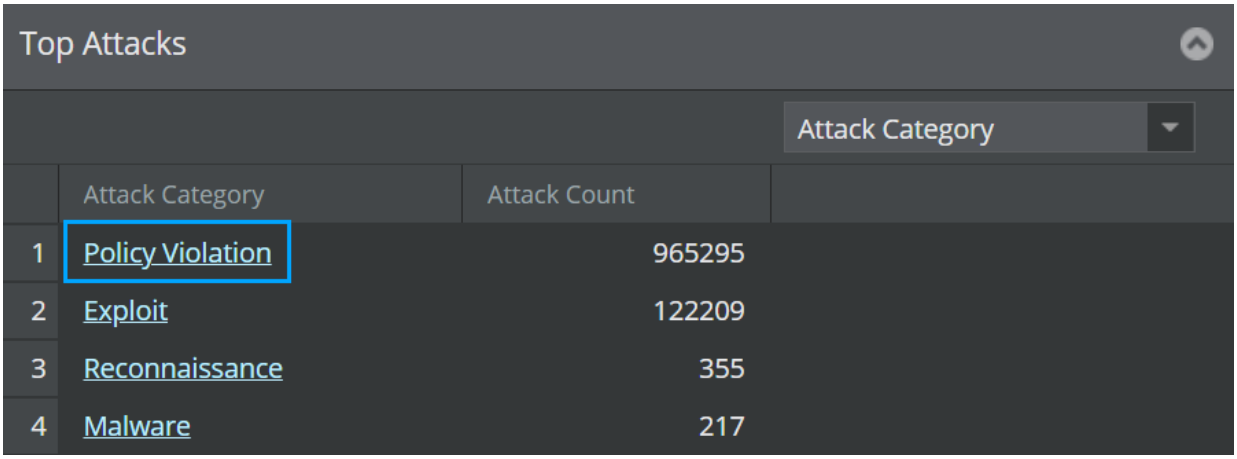
The core attributes are hyperlinked in the respective tables in the default view. For example, in the default view, the core attribute, **Attack Name**, of the **Top Attacks** is hyperlinked.

Figure 137. Hyperlinked core attribute



But, if you want to sort the tables by specific attributes, then the non-core attribute can also appear as a hyperlink. For example, if you want to sort the **Top Attacks** table by the **Attack Category** attribute, then the selected attribute, **Attack Category**, will be hyperlinked.

Figure 138. Hyperlinked non-core attribute



When you click a core attribute and start the filter:

- The page is refreshed and a new table is added along with the existing top N tables, which shows the specific details of the selected core attribute.
- The same top N security tables are displayed; but the data in each table is displayed according to the selected core attribute and admin domain.

IMPORTANT

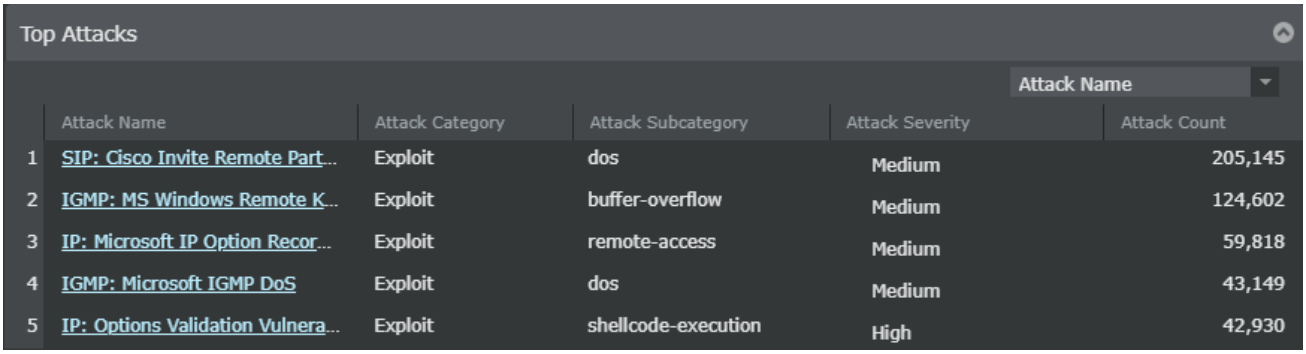
You can never view more than one attack, attacker, target, application, malware and admin domain combination at the same time.

Top Attacks security table

The **Top Attacks** security table displays the following information.

Option	Definition
Attack Name	Name of the attack. Click this hyperlink to view the attack details. This is the core attribute of the **Top Attacks** table.
Attack Category	General attack type.
Attack Subcategory	Specific classification within attack type (for example, virus, Trojan Horse).
Attack Severity	Malicious impact potential of the attack. This can be high, medium, or low.
Attack Count	Number of times a particular attack was detected for a single alert instance.

Figure 139. Top Attacks table

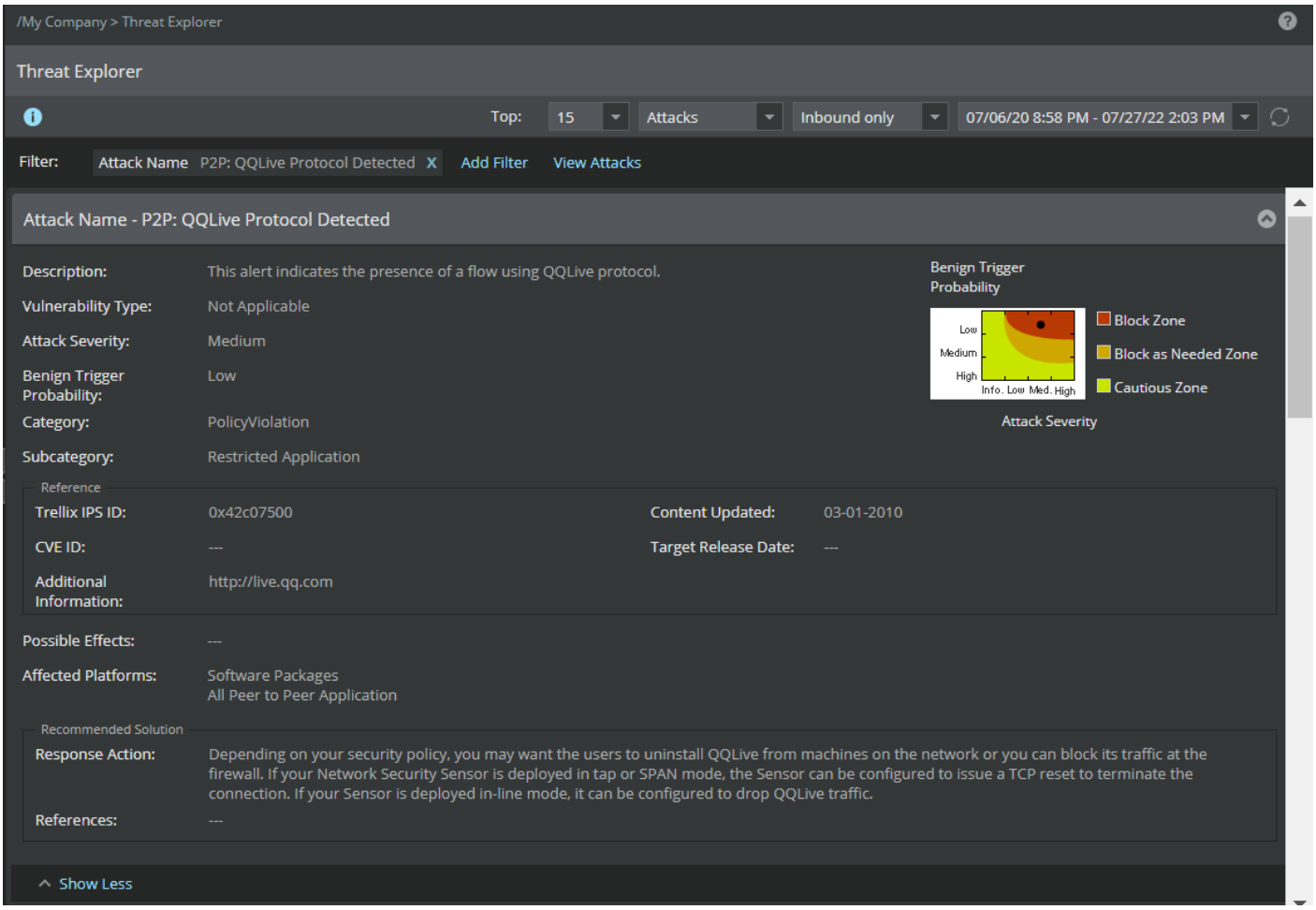


Core attribute

Select the core attribute as **Attack Name** and click the hyperlink to view the following details:

- **Description**— Shows the description of the specific attack including the attack definition and conditions.
- **Vulnerability Type**— Shows the type of the inherent system flaw that can be exploited by attackers.
- **Attack Severity**— Shows the malicious impact potential of the attack. This can be high, medium, or low.
- **Benign Trigger Probability (BTP)**— Shows the probability of a false alert.
- **Category**— Shows the general attack type.
- **Subcategory**— Shows the specific classification within attack type (for example, virus, Trojan Horse).
- **Reference**— Shows the following standards and sources for finding information on known attacks.
  - **Trellix IPS ID**— Shows the globally unique attack ID within the Trellix IPS.
  - **Content Updated**— Shows the last date when the attack information was updated.
  - **CVE ID**— Shows The Common Vulnerabilities and Exposures (CVE) name related to an attack.
  - **Target Release Date**— Shows the target release date of the attack.
  - **Additional Information**— Shows the additional information of the particular attack.
- **Possible Effects**— Shows the results of a successful attack.
- **Affected Platforms**— Shows the systems or software directly impacted by the attack.
- **Recommended Solution**— This section shows the solution recommended by Trellix.
  - **Response Action**— Shows the Sensor's response action to this attack.
  - **References**— Shows the references for this attack.

Figure 140. Attacks — core attribute



Select View Attacks to go to **Attack Log** and view the alerts related to the attack.

Use the following icons to customize your attack details view.

Name	Icon	Description
Expand	Show More	Expand your view.
Hide	Show Less	Hide your view.

IMPORTANT

All the other top N security table are populated with the data related to the selected core attribute and admin domain.

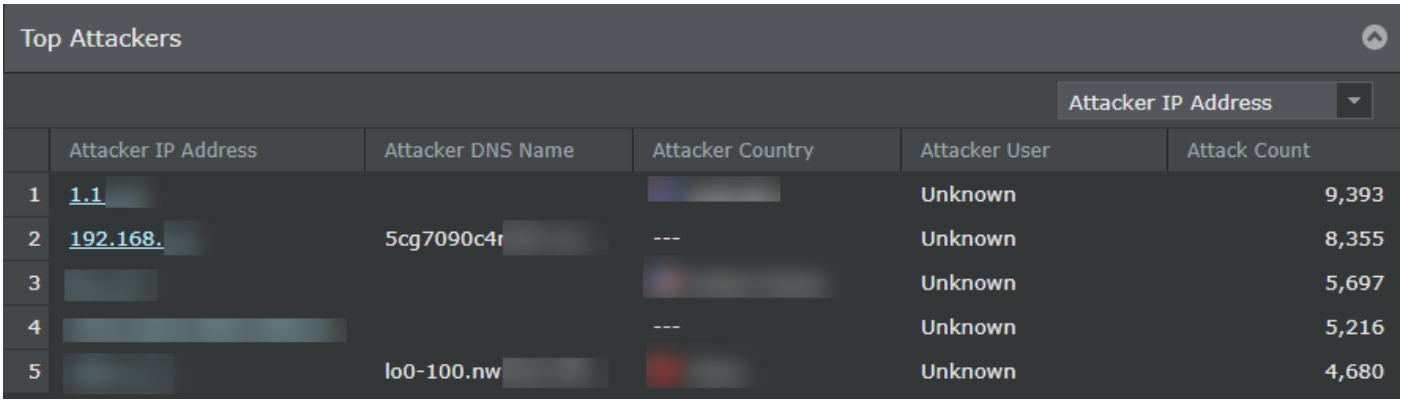
At any time, you can click X to leave the selected core attribute and return to the main **Threat Explorer** page.

Top Attackers security table

The **Top Attackers** security table displays the following information.

Attribute	Description
Attacker IP Address	IP address of the attacker. This is the core attribute of the **Top Attackers** table.
Attacker DNS Name	DNS name of the attacker to resolve these names to IP addresses.
Attacker Country	Name of the country of the attacker.
Attacker User	Username of the attacker.
Attack Count	Number of times a particular attack was detected for a single alert instance.

Figure 141. Top Attackers table



Core attribute

Select the core attribute as **Attacker IP Address** and click the hyperlink to view the following details:

- Endpoint Information
- ePO Threat Events

> **NOTE**
>
> The ePO Threat Events tab appears by clicking the **Optional Tabs** drop-down and selecting **ePO Threat Events** check-box.

Endpoint Information

The additional information displayed in the Endpoint Information section is shown in the following table.

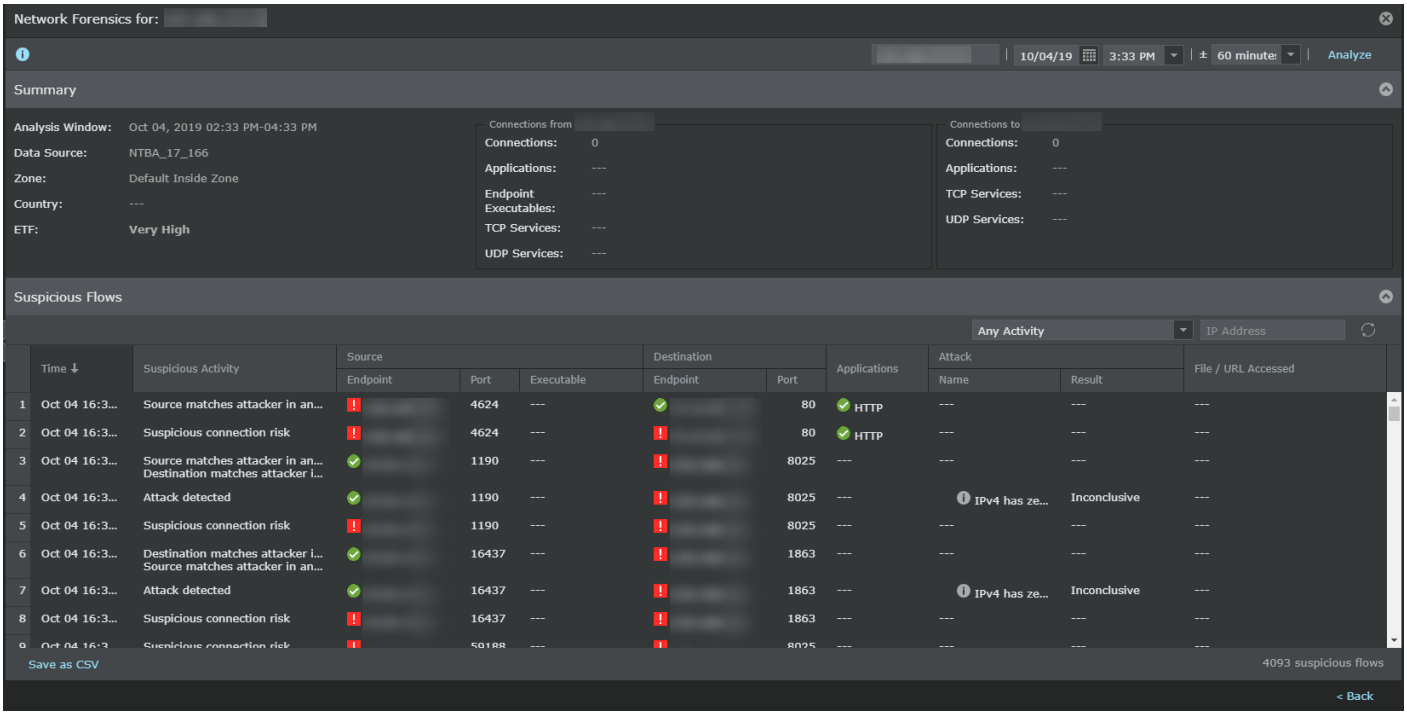
Item	Description
Country	Country of the endpoint
DNS Name	DNS name of the endpoint to resolve the names to IP addresses
NetBIOS Name	NetBIOS name of the endpoint to access the host machines
Operating system	Operating system platform of the endpoint

Item	Description
Device Type	Type of the Sensor (for example, IPS Sensor)
MAC Address	MAC address of the endpoint
Domain/Workgroup	Domain or workgroup of the endpoint
User	Operating system user name of the endpoint
Data Source	Database tables from where information is retrieved
Trellix Agent Check-In Time	Check-in time of the Trellix Agent that communicates with the same ePO server integrated with the admin domain
Endpoint Type	Type of endpoint: • UNMANAGED (No Agent) — This indicates that there is no Trellix Agent installed on the endpoint. • UNMANAGED (MANAGED) — This indicates that the endpoint has a Trellix Agent but there is no active communication channel between the Agent and ePO server integrated with the admin domain. • MANAGED — This indicates that the endpoint has a Trellix Agent and there is active communication channel between the Agent and Trellix ePO - On-prem server integrated with the admin domain. The endpoint is managed by the agent.
Installed products	List of the installed products

The **Endpoint Information** sub-tab shows the following details specific to the endpoint.

- **Network Forensics** — Click this tab to analyze the network behavior of the endpoint when NTBA is configured.

Figure 142. Network Forensics page

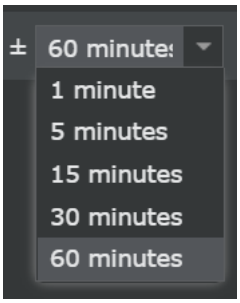


You can filter your view by choosing the time and date of your choice.

Figure 143. Date and time options in Network Forensics page

You can view the data according to your time preference by selecting the time period from the drop-down list. You can use the ± icon to view the details before and after any event/attack.

Figure 144. Show option



The following table shows the information displayed in the **Network Forensics** section.

Item	Description
Summary	Endpoint summary that includes IP address, country of the endpoint, etc. View the client connections from this endpoint that include the TCP services, UDP services, etc. View the server connections to this endpoint that include the TCP services, UDP services, etc.
Suspicious Flows	
Suspicious activity indicator	View indicators that map to an event like an alert or attack.
IP Address	Specify an IP address and use Search to view flows for this address.
Time	Displays the date and time when the suspicious flow for an event occurred **TIP** You can sort the flows view based on time.
Suspicious Activity	Displays the indicator that specifies the suspicious activity performed like an URL accessed that was involved in another attack, blocked executable accessed and others

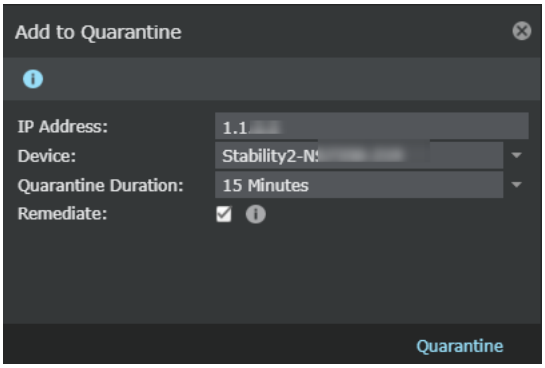
Item	Description
Source	Specifies the source from which the flow was initiated for an endpoint. Details include endpoint and ports used.
Destination	Specifies the destination details like endpoint involved and port
Applications	Displays the applications accessed from the endpoint
Attack	Attacks for a specific endpoint that include attack name and result
File / URL Accessed	Specifies file or URL access details for a specific endpoint

To close the network forensics page, click the icon.

For more information, see the section Using context-aware data for network forensics (page 468).

- **Quarantine** — Use this option to block all the traffic originating from the specified IP address seen on the selected device for the selected time.

Figure 145. Quarantine Endpoint dialog



To quarantine endpoints to block all the traffic originating from the specified IP address:

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal** Remediation cannot be configured for IPv6 address. The checkbox and the information icon for remediation is not displayed if you enter an IPv6 address in the **IP Address** field.

Click **Quarantine**. The endpoint is added and displayed in the **Quarantine** page.

- **Tag (in ePO)**— Use this option to assign a tag to the selected endpoint in Trellix ePO - On-prem.

  You are able to assign tags only to endpoints whose **Endpoint Type** denotes MANAGED. This means that the endpoint runs a suitable version of Trellix Agent and is managed by Trellix ePO - On-prem.

  To assign a tag:

  1. Select a tag from the drop-down list. If the tag you looking for does not appear in the list, click the refresh button.
  2. Click **Tag**.

     If the tagging is successful you receive a message stating its success. If not, you receive a failure notification.

ePO Threat Events

The **ePO Threat Events** sub-tab displays the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for a selected endpoint. The information displayed under this sub-tab includes the date and time at which the threat event was generated, the ID associated with the event, the event description, event category, action taken on the event, and the type of the threat that triggered the event.

You can click the  icon to refresh the list and view the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for the selected endpoint. The **Search** text field allows you to search for a specific event based on the **Event Received Time**, **Event ID**, **Event Category** and **Threat Type**. For example, to view all events associated with the Event ID 1095, type **`1095`** in the **Search** field.

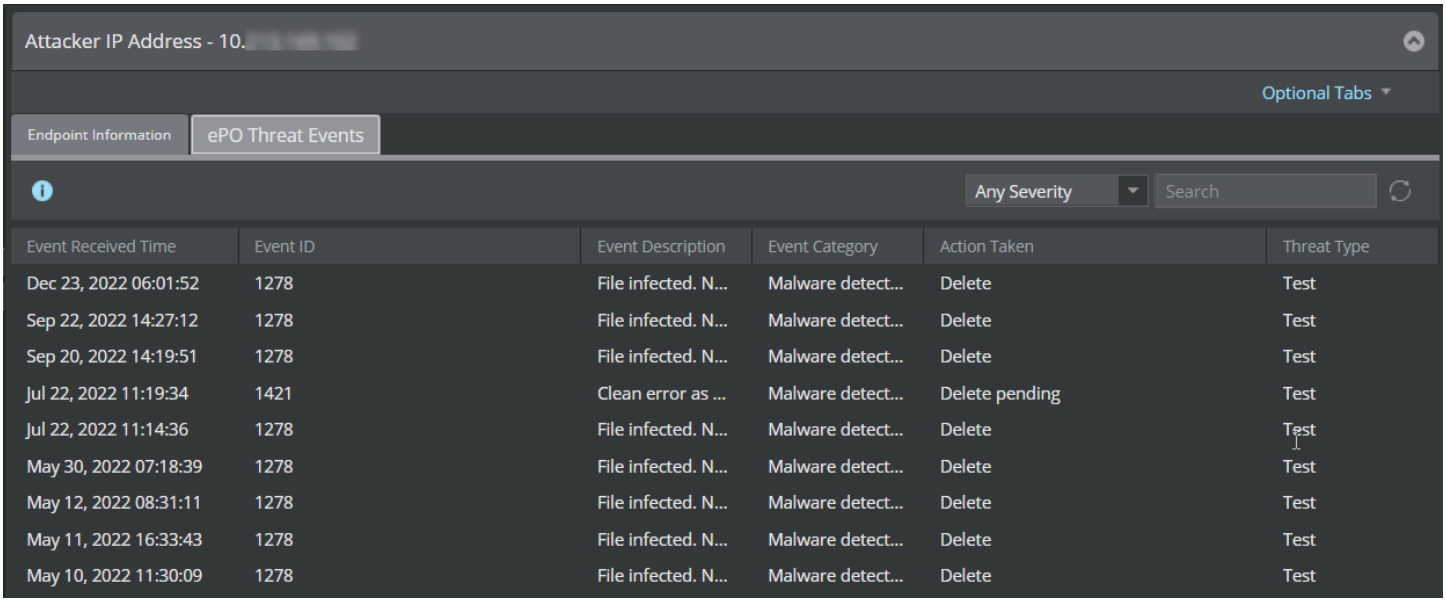
NOTE

The sub-tab has **Any Severity** filter selected by default. With this filter selected, the sub-tab displays all types of events including those which are informational and/or of low-severity. Such events act as noise and impede one's ability to find true threats. To exclude these events, select the **Warning+ Severity Only** filter from the drop-down menu. This displays only those events with Critical, Alert and Warning severity.

NOTE

Ensure that the ePO server has the latest Trellix IPS Extension file installed. For information on how to download and install the Trellix IPS Extension, see the section [Install Trellix IPS extension file in Trellix ePO - On-prem] in [Trellix Intrusion Prevention System Integration Guide].

Figure 146. ePO Threat Events sub-tab



Top Targets security table

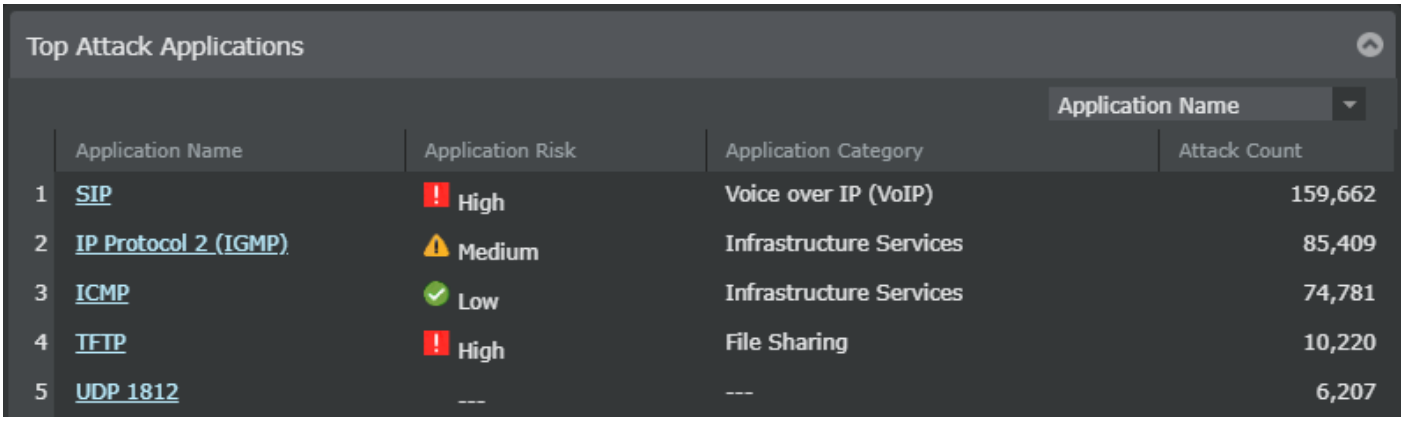
The **Top Targets** security table displays the information about the target like the target IP address, target DNS name, target country, etc. Refer to the **Top Attackers** security table section for the details. The only difference lies in the fact that the **Top Attackers** table displays the information about the attackers, while the **Top Targets** table shows the information about the targets.

Top Attack Applications security table

The **Top Attack Applications** security table displays the following information.

Attribute	Description
Application Name	Name of the application. This is the core attribute.
Application Risk	Risk level of the application. The risk level may be high, medium, or low.
Application Category	Category consists of applications that you would want to handle in a similar manner. An application can belong to multiple categories based on its functions and features (for example, Skype can belong to InstantMessaging, File Sharing, and Voice Over categories).
Attack Count	Number of times a particular attack was detected for a single alert instance.

Figure 147. Top Attack Applications table

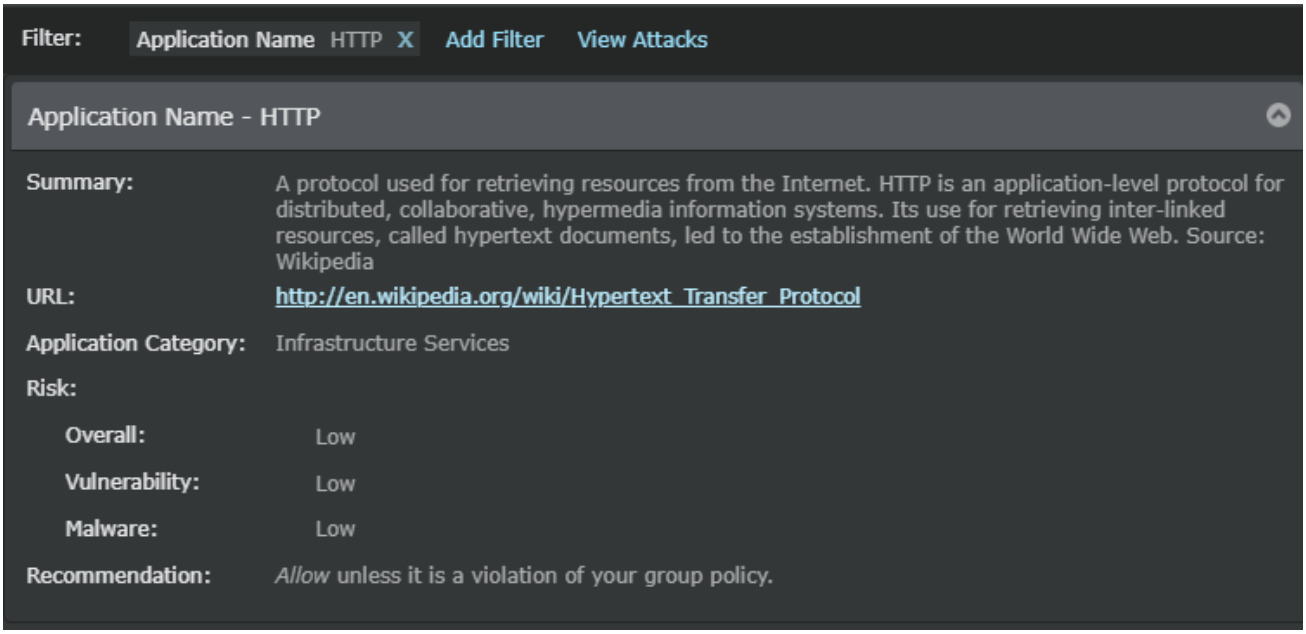


Core attribute

Select the core attribute as **Application Name** and click the hyperlink to view the following details:

Item	Description
Summary	Details of the application.
URL	URL of the application.
Application Category	Category consists of applications that you would want to handle in a similar manner. An application can belong to multiple categories based on its functions and features (for example, Skype can belong to InstantMessaging, File Sharing, and Voice Over categories).
Risk	Risk level associated with the application. The risk level can be high, medium, or low. Trellix ARC categorizes an application based on its vulnerability and the probability for it to deliver malware.
Recommendation	Recommendation by Trellix about the application.

Figure 148. Core attribute of Top Attack Applications table



Select View Attacks to navigate to **Attack Log** and view the alerts matching this application.

IMPORTANT

All the other top N security tables are populated with the data related to the selected core attribute and admin domain.

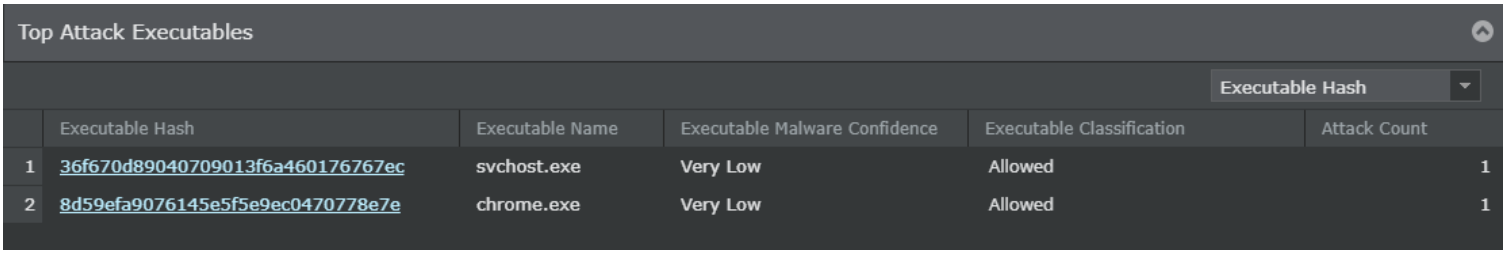
At any time, you can click X to leave the selected core attribute and return to the main **Threat Explorer** page.

Top Attack Executables security table

The **Top Attack Executables** security table displays the following information.

Attribute	Description
Executable Hash	Name of the executable hash. This is the core attribute.
Executable Name	Name of the executable. The name will be displayed if it is from a signed/trusted CA.
Executable Malware Confidence	Malware confidence of the executable. The malware confidence may be very high, high, medium, low, very low, and unknown.
Executable Classification	Classification of the executable. It may be allowed, blocked, or unclassified.
Attack Count	Number of times a particular attack was detected for a single alert instance.

Figure 149. Top Attack Executables table



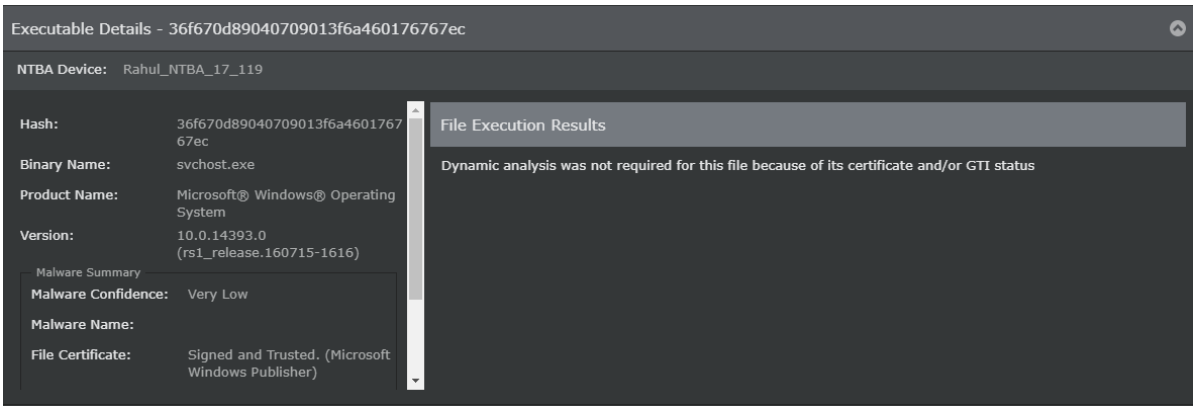
Core attribute

Select the core attribute as **Executable Hash** and click the hyperlink to view the following details:

Field	Description
View Detections	Takes you to the **Malware Files** page to view the malware confidence computed by individual engines and the overall malware confidence for the executable
Hash	Displays the file hash. This link takes you to the **Threat Explorer** with a filter on the hash and the selected time.
Binary Name (type)	Displays the binary name and the type, whether process or library
Product Name	Displays the product name for the executable
Version	Displays the product version number
Malware Confidence	Displays the malware confidence level returned by the configured EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.
Classification	Displays the executable classification whether blocked, allowed, or unclassified
Classified	Displays the method of classification (*Auto* if the executable has been auto-classified by the NTBA Appliance or *Manual* if it has been manually classified) and the timestamp, only for classified executables
Certificate Status	Displays if the certificate is from a trusted CA or not. Valid values for executables are **Signed** and **Signed and Trusted**. If the executables are unsigned, the status displays blank.
Certificate Signer	Displays the certificate signer name.
GTI Reputation	Displays the file reputation received from GTI. Valid values are **Very Low**, **Low**, **Medium**, **High**, **Very High**, and **Unknown**.
Malware Indicators	Shows some of the methods that were used to compute the executable reputation.

Field	Description
Invoked Libraries	Lists all libraries (DLLs) invoked by the executable. The DLLs are displayed only if EIA finds the corresponding malware confidence to be greater than or equal to the Trellix ePO - On-prem Reputation Threshold value. By default, the Trellix ePO - On-prem Reputation Threshold value is Medium. **NOTE** Invoked libraries are displayed when the executable is a process.
Name	Displays names of the library files invoked by the executable
Hash	Displays the file hash. This link takes you to the **Threat Explorer** with a filter on the hash and the selected time.
Malware Confidence	Displays the malware confidence level returned by the configured EIA

Figure 150. Core attribute of Top Executables table



Select View Attacks to navigate to **Attack Log** and view the alerts that matches the selected endpoint executable.

IMPORTANT

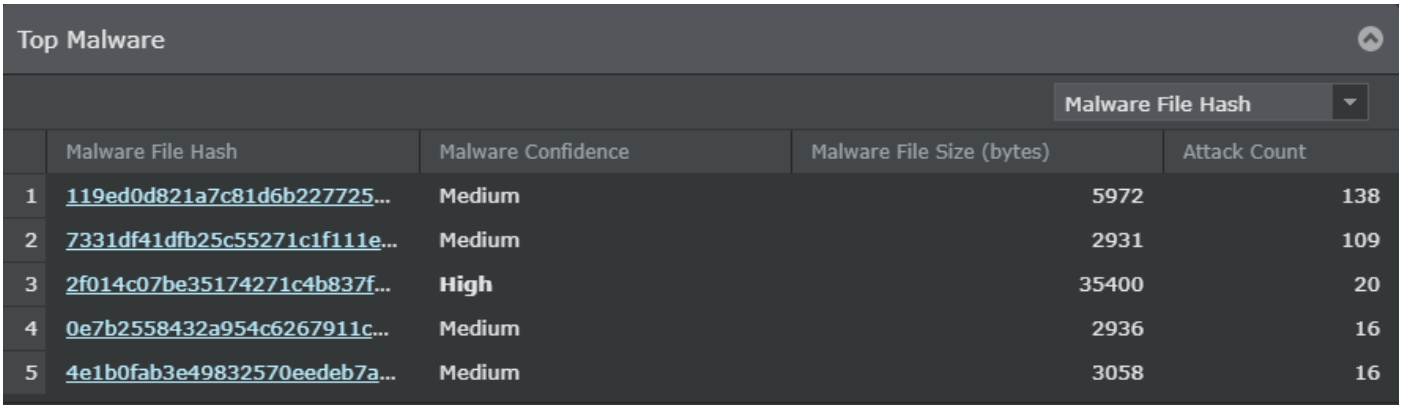
All the other top N security tables are populated with the data related to the selected core attribute and admin domain.

At any time, you can click X to leave the selected core attribute and return to the main **Threat Explorer** page.

Top Malware security table

The **Top Malware** security table displays the following information.

Figure 151. Top Malware table

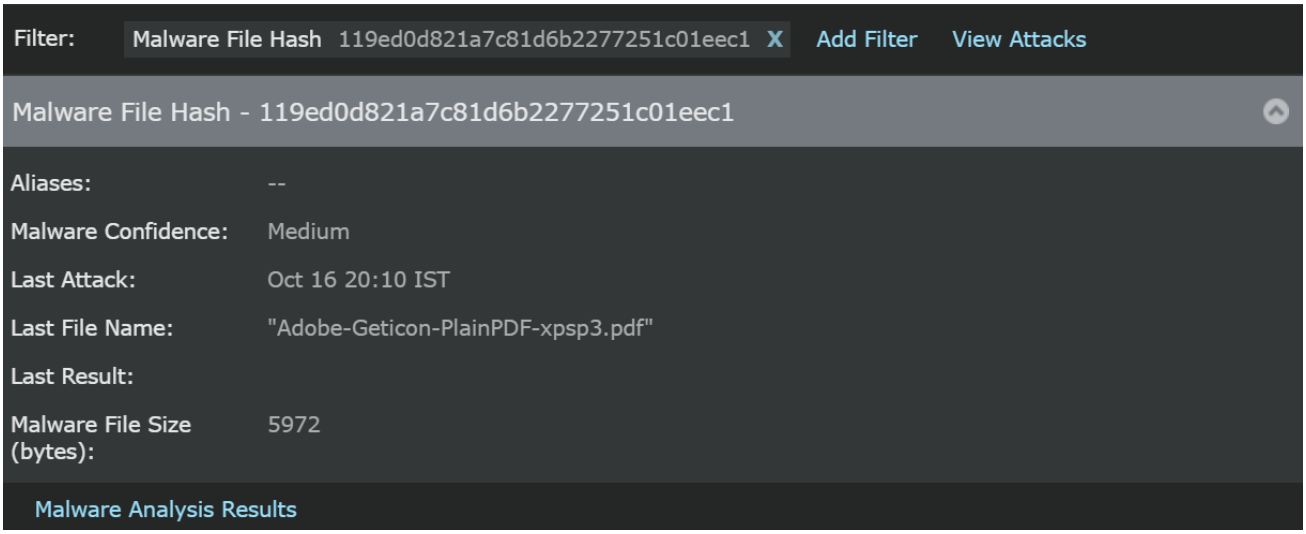


Attribute	Description
Malware File Hash	Details of the downloaded hash file.
Malware Confidence	Confidence level of the downloaded malware based on its specificity and severity.
Malware File Size (bytes)	Size of the downloaded malware file.
Attack Count	Number of times a particular attack was detected for a single alert instance.

Core attribute

Select the core attribute as **Malware** and click the hyperlink to view the details like the file size of the downloaded malware and the malware confidence.

Figure 152. Core attribute of Top Malware table



Select View Attacks to navigate to **Attack Log** and view alerts that match the malware file hash selected.

IMPORTANT

All the other top N security tables are populated with the data related to the selected core attribute and admin domain.

At any time, you can click X to leave the selected core attribute and return to the main **Threat Explorer** page.

Filtering options

There are two ways to get to Threat Explorer. First, when you click a hyperlink in any of the **Dashboard** security monitors, you will be directed to the Threat Explorer page with the core attribute and admin domain already set. The second way is to navigate to Analysis → <Admin Domain Name> → **Threat Explorer**.

Dashboard workflow

See section Threat Explorer (page 416) to understand the dashboard workflow to Threat Explorer.

Threat Explorer workflow

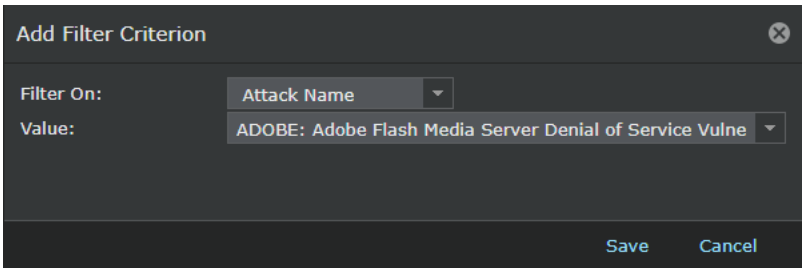
When you navigate to Analysis → <Admin Domain Name> → **Threat Explorer**, you can set the filter based on your needs. The page displays the default top N security tables and root admin domain, which includes data from the child domains also. No filter criteria is set at this point of time.

Add a filter

You can add a filter of your choice. This is specially useful if you are unable to find a specific attribute in the security tables. To add a filter of your choice:

1. From the **Domain** drop-down list in the left pane, select the root admin domain.
2. Click Add Filter.
3. Enter the values in the following fields:
   - **Filter On** — Select a core attribute from the drop-down list.
   - **Value** — Choose the specific value from the drop-down list. You need to enter the specific values for the Attacker IP, target IP, and Malware.

Figure 153. Add Filter Criterion dialog



NOTE

- On the **Dashboard** page, if you click a hyperlink on any security monitor, you are directed to the **Threat Explorer** page with the core attribute and admin domain already set. You can then choose to add more filter criteria. Example: A click in the **Top Attackers** security monitor displays the TE page with the core attribute **Attacker IP address**, for example, 10.1.1.15 and **My Company** already set.
- If you click on the attack details in the **Top Attacker Countries** and the **Top Target Countries** monitors, you are redirected to the **Attack Log** page with the filter attribute for the **Country** already set.

4. Click **Save**. The refreshed page provides details for further analysis. For the preceding example, you can view the Attacker IP details like endpoint information.

NOTE

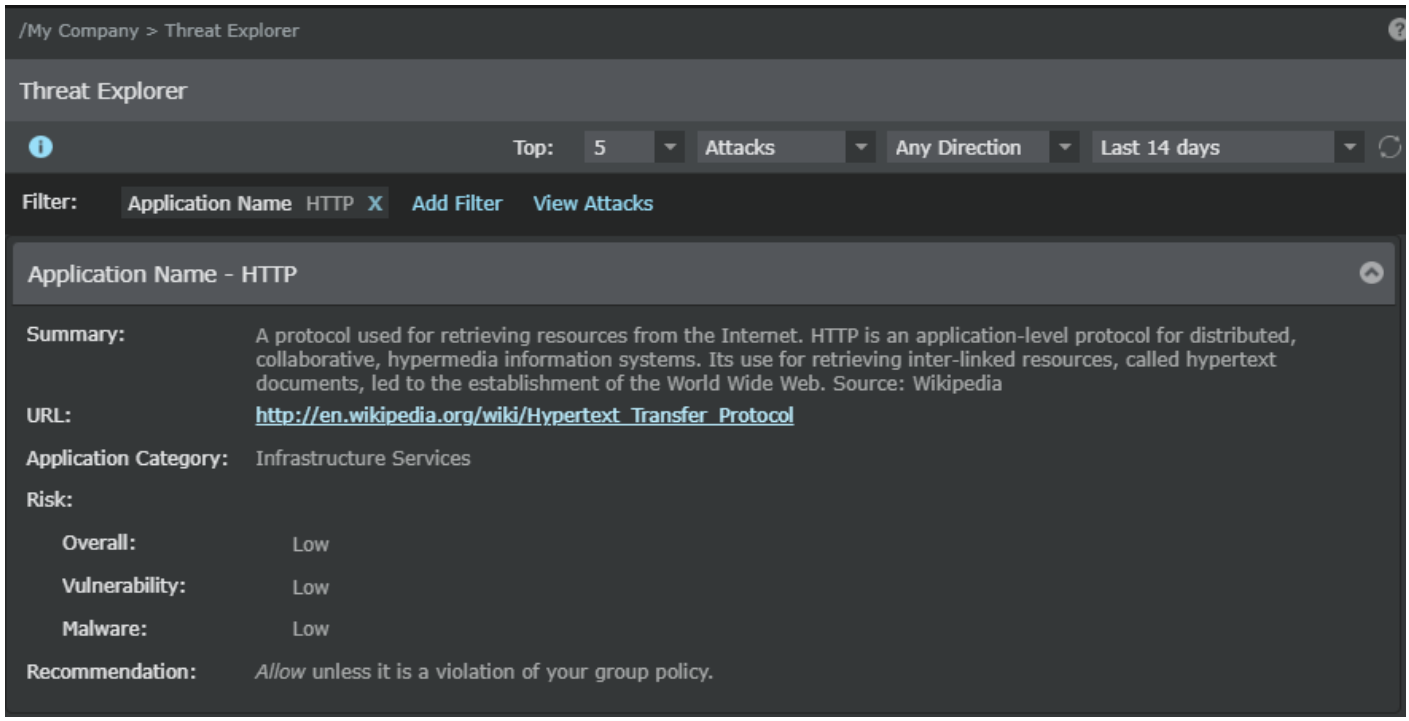
You can select the time duration and network flow from the options in the right hand corner.

5. View the details. Now you want to investigate details from a data source, for example, 10.1.1.12 and **My Company** as the admin domain. Set a secondary filter. To do this, click **Add Filter** and select this IP. The refreshed page displays details based on both primary and secondary filters applied.

CAUTION

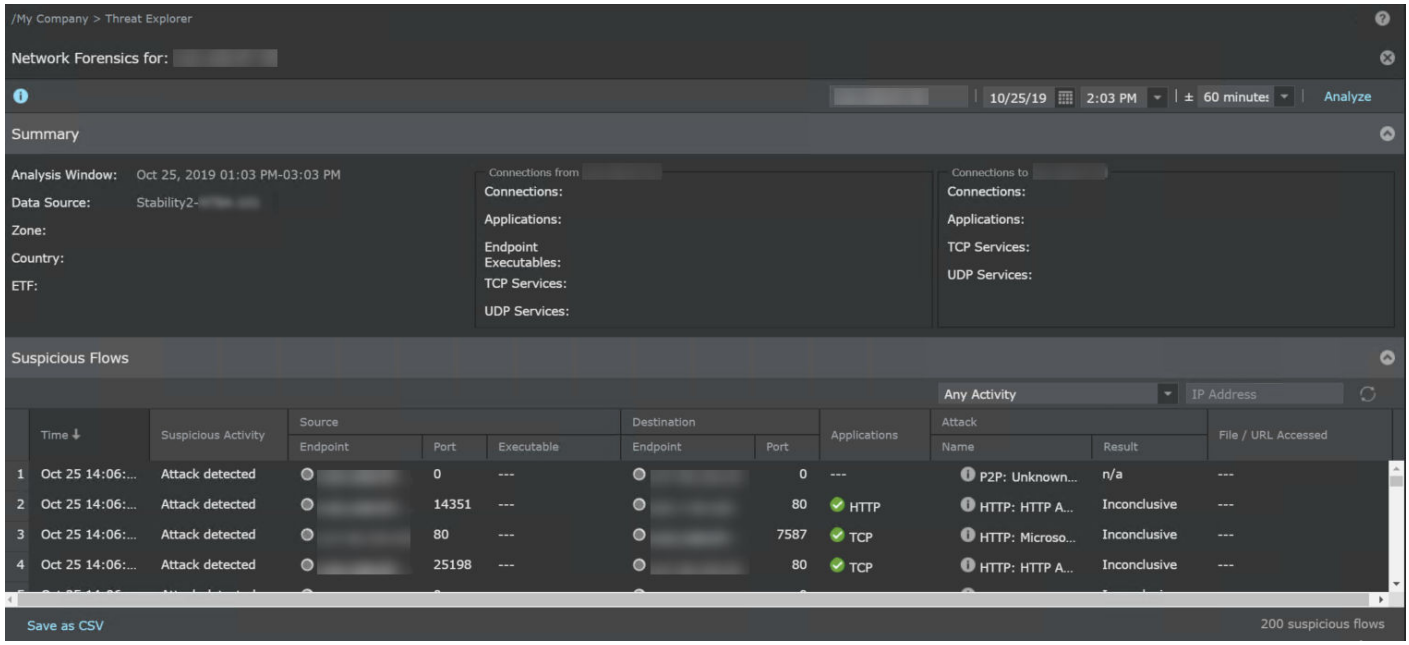
If you remove the primary filter, the secondary filter becomes the primary criterion and vice-versa.

Figure 154. Data source details



6. Click Network Forensics → **Analyze** to analyze this endpoint's recent behavior in the network. You can view details like ETF, client and server connections to this endpoint, and data source.

Figure 155. Network forensics



7. Click **View Attacks** and select the option to investigate this IP address as an attacker or target. The **Attack Log** page displays details about this IP address.

NOTE

(Optional) You can view the endpoint threat events (ePO Threat Events) if the Manager is integrated with Trellix ePolicy Orchestrator - On-prem.

Navigate to Attack Log

On the **Analysis** tab, click <Domain Name> → **Threat Explorer**. Select View Attacks to go to Attack Log to analyze and view the alerts.

When you click **View Attacks**, it opens the **Attack Log** page. This page shows the specific details of the selected attribute in the specific top N table. This page shows the alerts of the selected attribute according to the time duration set in Threat Explorer.

When no attribute is selected, clicking opens up a filter that loads all alerts generated within the time duration and direction set in Threat Explorer.

Figure 156. Threat explorer with time and direction filter

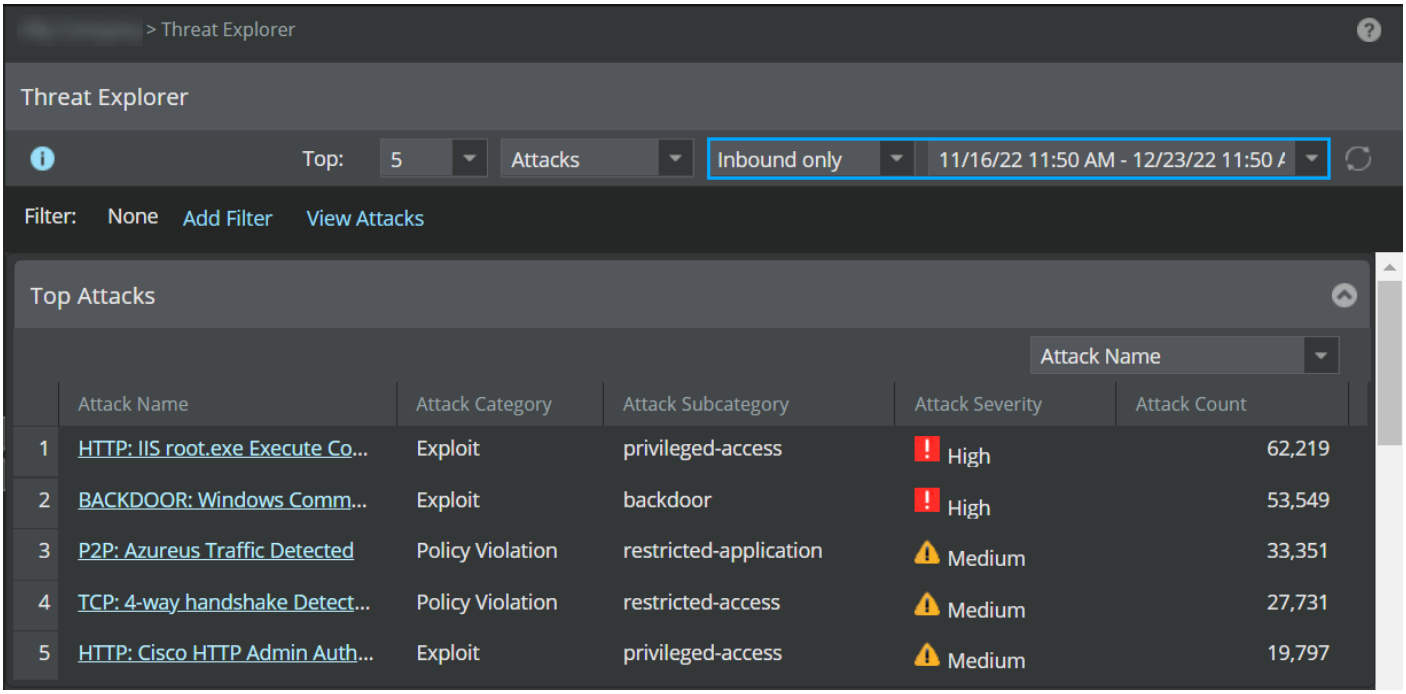
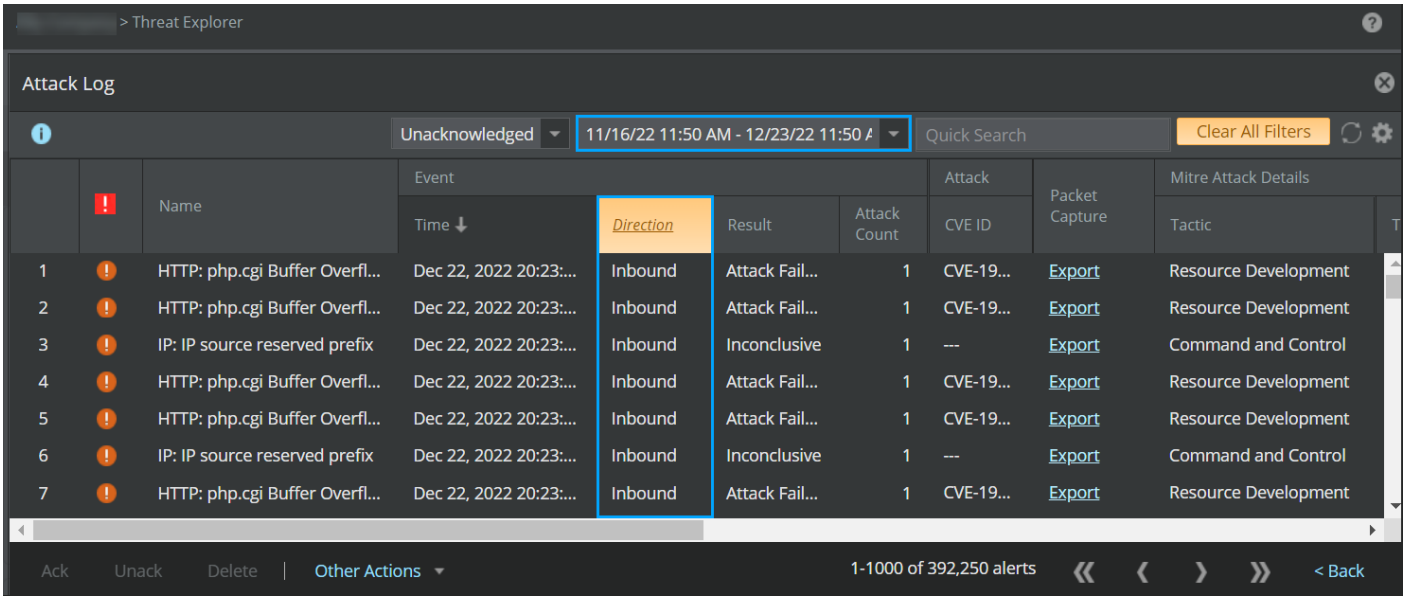


Figure 157. Attack log with Threat Explorer filter



You can also apply multiple filters in threat explorer and view attacks in attack log.

Click **Back** or icon to close the **Attack Log** page.

Top N security tables based on flow data

Use this section to view and manage the most common top security tables based on bytes and connections from the **Threat Explorer** page.

NOTE

A minimum of 1 NTBA appliance is required to be configured to explore threats based on bytes or connections.

The following tables are shown by selecting the option **Bytes** from the drop-down list:

- Top Sources
- Top Destinations
- Top Applications
- Top Executables

The following tables are shown by selecting the option **Connections** from the drop-down list:

- Top Sources
- Top Destinations
- Top Applications
- Top Executables
- Top URLs
- Top Files

Core attributes

The core attributes of the top N security tables based on flow data are explained in the following table.

Top N Table Name	Core Attribute
Top Sources	Source IP Address
Top Destinations	Destination IP Address
Top Applications	Application Name
Top Executables	Executable Hash
Top URLs	URL Name
Top Files	File Hash

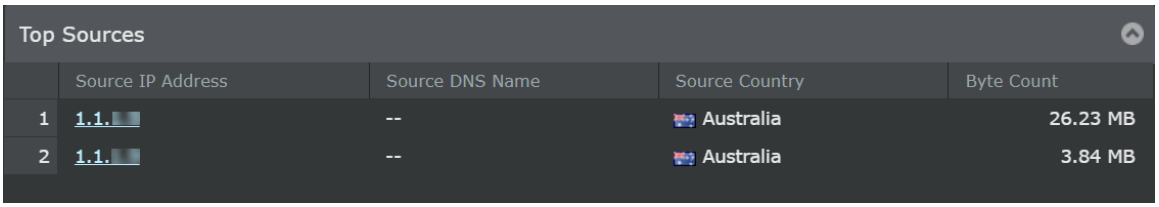
NOTE

The **Top URLs** and **Top Files** are displayed only when you select the **Connections** option.

Scenario

The core attributes are hyperlinked in the respective tables in the default view. For example, in the default view, the core attribute, **Source IP Address**, of the **Top Sources** is hyperlinked.

Figure 158. Hyperlinked core attribute



NOTE

The sort options at the top right corner of each top table are applicable only for **Attacks** option and not for **Bytes** and **Connections**.

Top Sources Security table

The **Top Sources** security table displays the following information.

Attribute	Description
Source IP Address	IP address of the source. This is the core attribute of the **Top Sources** table.
Source DNS Name	DNS name of the source IP addresses
Source Country	Name of the country of the source IP address.
Byte/Connection Count	Total number of connection count for the source IP address.

Top Destinations security table

The **Top Destinations** security table displays the following information.

Attribute	Description
Destination IP Address	IP address of the destination. This is the core attribute of the **Top Destination** table.
Destination DNS Name	DNS name of the destination IP addresses
Destination Country	Name of the country of the destination IP address.
Byte/Connection Count	Total number of connection count for the destination IP address.

Top Applications security table

The **Top Applications** security table displays the following information.

Attribute	Description
Application Name	The name of the application. This is the core attribute of the **Top Applications** table.
Application Risk	The risk severity of the application.
Application Category	The category of the application.
Byte/Connection Count	Total number of connection count for the application.

Top Executables security table

The **Top Executables** security table displays the following information:

Attribute	Description
Executable hash	Malware executable hash number. This is the core attribute of the **Top Executables** table.
Executable Name	Name of the executable. Example: outlook.exe.
Executable Malware Confidence	Confidence level of the malware
Executable Classifiication	Classification of the executable
Attack Count	The total number of connections for the executable

Top URLs security table

The **Top URLs** security table displays the following information.

Attribute	Description
URL Name	Name of the URL. This is the core attribute of the **Top URLs** table.
URL Risk	Risk level of the URL. Example: High.
URL Category	Category of the URL. Example: Gambling.
Connection Count	The total number of connection count for the URL.

Top Files security table

The **Top Files** security table displays the following information.

Attribute	Description
File Hash	File hash number. This is the core attribute of the **Top Files** table.
Malware Confidence	Confidence level of the malware.
File Name	Name of the malware file
Connection Count	The total number of connection count for the file.

Filtering options

You can add a filter of your choice. This is specially useful if you are unable to find a specific attribute in the security tables. To add a filter of your choice:

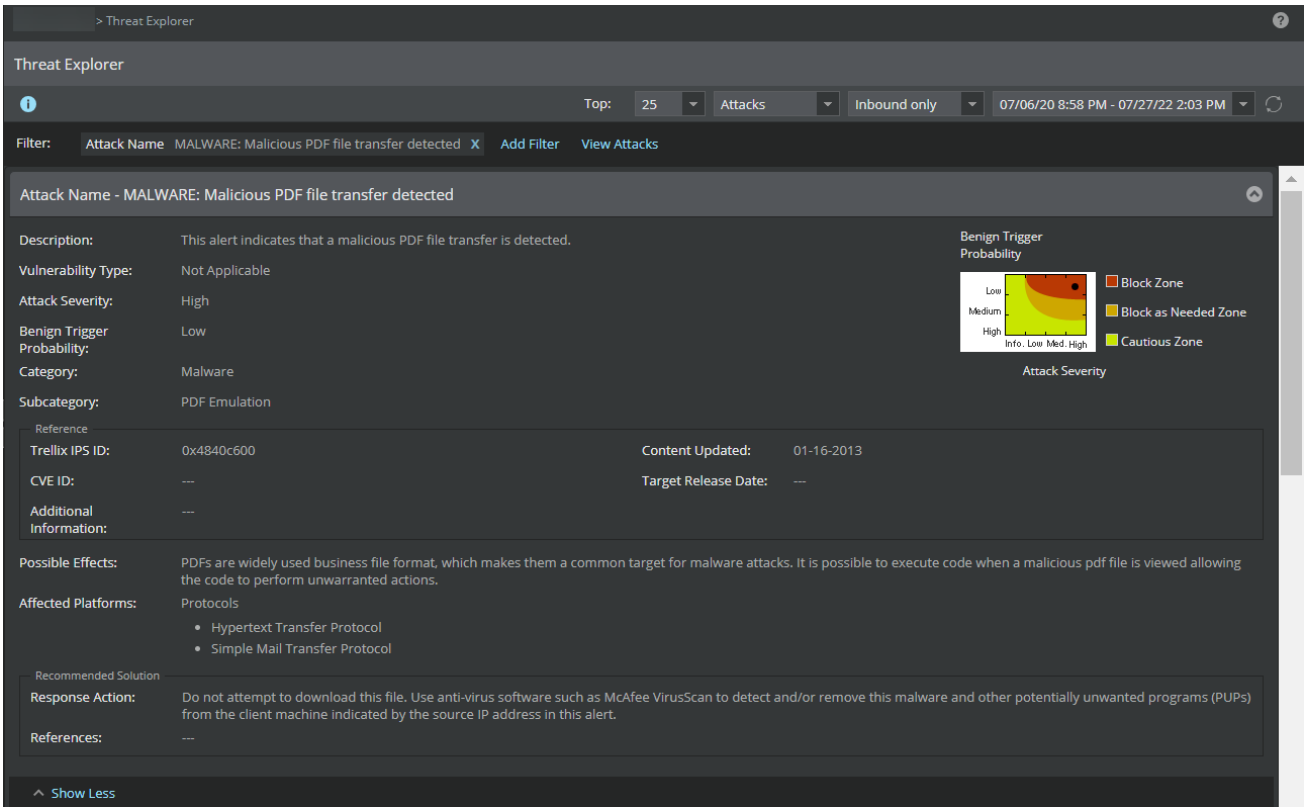
1. From the **Domain** drop-down list in the left pane, select the root admin domain.
2. Click **Add Filter**.
3. Enter the values in the following fields:
   - **Filter On** — Select a core attribute from the drop-down list.
   - **Value** — Choose the specific value from the drop-down list.

NOTE

- In the **Dashboard** page, if you directly click a hyperlink on any security monitor, you are directed to the **Threat Explorer** page with the core attribute and admin domain already set. You can then choose to add more filter criteria. Example: A click in the **Top Applications(NTBA)** security monitor displays the **Threat Explorer** page with the core attribute **Application Name**, for example, HTTP. You can select the time duration and network flow from the options in the right hand corner.
- If you click on the attack details in the **Top Attack Countries** and the **Top Target Countries** monitors, you are redirected to the **Attack Log** page with the filter attribute for the **Country** already set.

4. To investigate details on an attack name, for example, *MALWARE: Malicious PDF File transfer Detected*, click **Add Filter**, select this attack name and click **Save**. The refreshed page displays details based on both primary and secondary filters applied.

Figure 159. Add Filters



CAUTION

If you remove the primary filter, the secondary filter becomes the primary criterion and vice-versa.

5. Click **View Attacks** to navigate to the **Attack Log** page and investigate based on filtered criteria.

NOTE

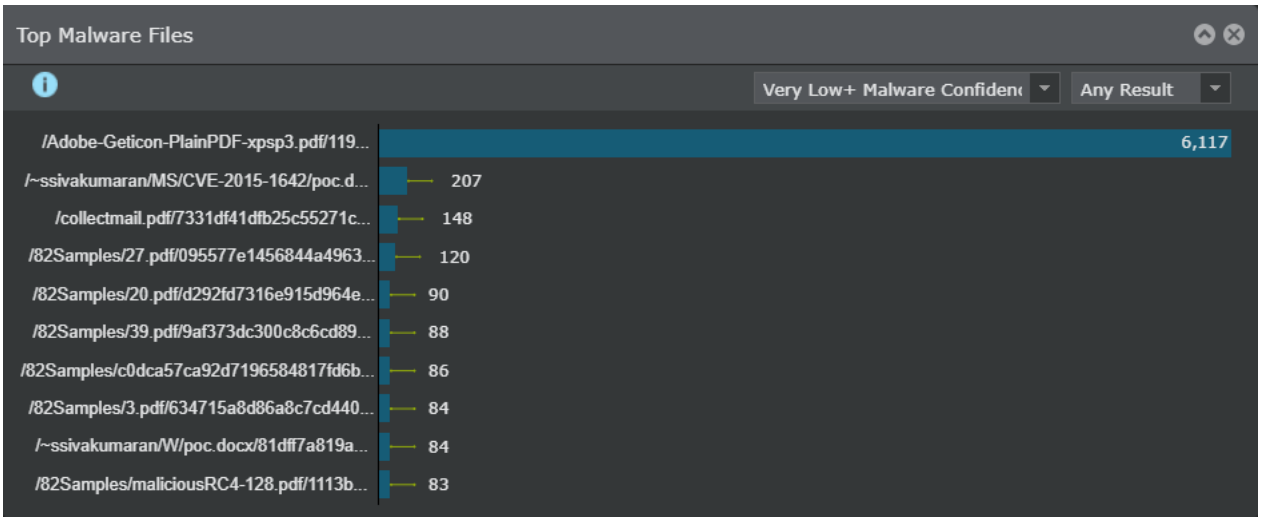
When **Connections** or **Bytes** are selected, you can view the attacks only when a single filter is applied. If secondary filter is also applied, the option to view attack is disabled.

Analyze Malware Files

You can leverage the analysis technique provided by Trellix IPS to perform an in-depth analysis of the malware detected in your network. The Manager provides you with a complete view of the malware and threats on your network for further analysis and actions, thus providing a comprehensive view of the threat landscape in your network. You can view the **Top Malware Files**. This dashboard is populated because a malicious file has been detected. In addition to viewing the threats to your network, the Manager also provides you the option to archive malware files.

To view malware detected by Trellix IPS, use the **Top Malware Files** monitor. The dashboard displays the **Malware File Hash** and the **Attack Count** of the detected malware. Security monitors are displayed as bar charts in the **Dashboard** page.

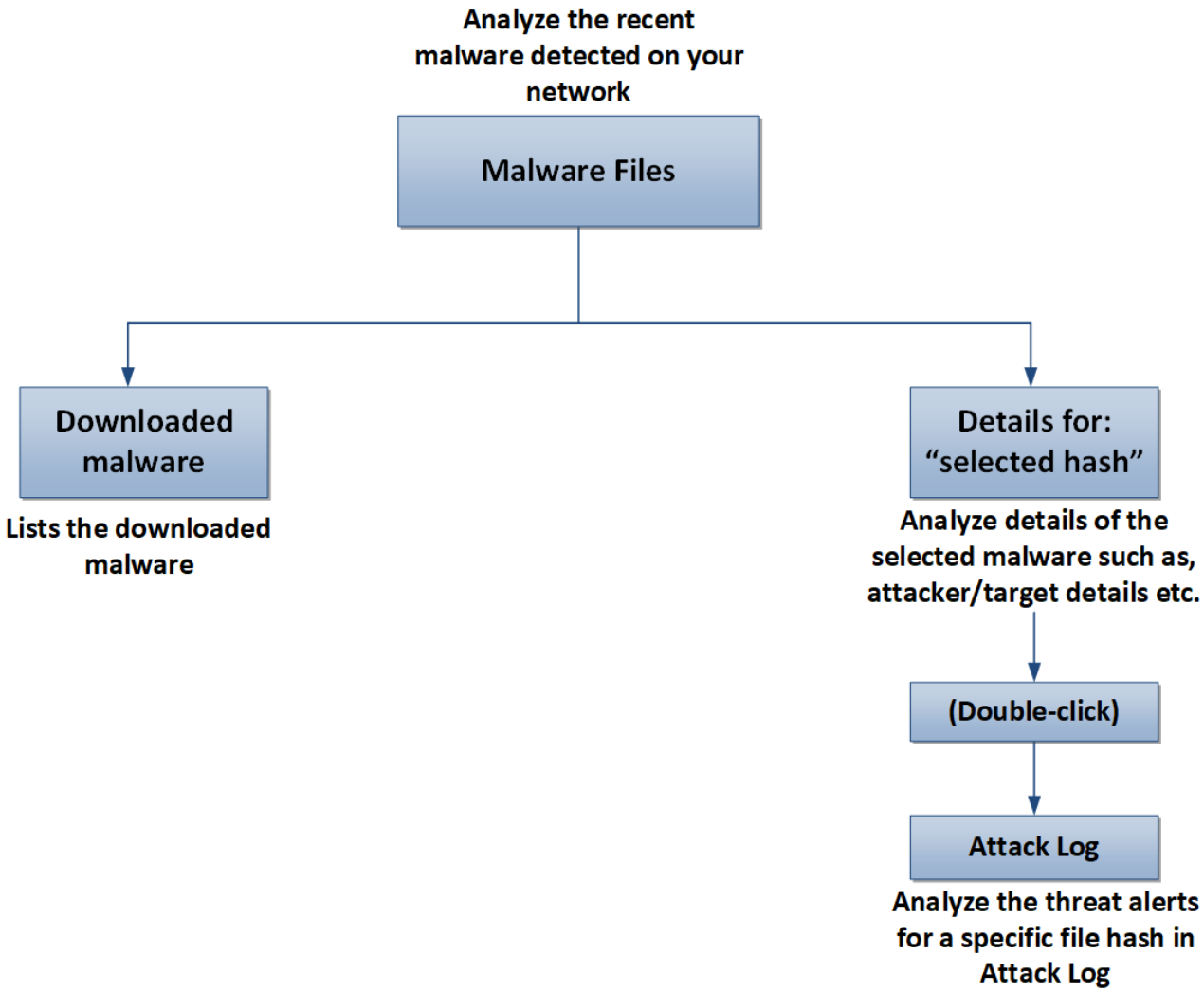
Figure 160. Top Malware Files



If you want to drill down further on a specific malware, click on a bar, and you will be redirected to the Analysis → **Malware Files** page, which displays additional details on that malware. This page provides you with the flexibility of filtering and sorting the information displayed based on your choice. In addition to these filtering/sorting options, you can also view the alerts that match the filter criteria by opening the **Attack Log** page directly from the **Threat Explorer**. You can view the malware files specific to admin domains by selecting the required admin domain from the **Domain** drop-down list. Summarized data for malware files, which includes data from the child domains, also can be viewed. If you have integrated the Manager with ePolicy Orchestrator - On-prem or Logon Collector, you can view the host type, host name, user name, operating system details, top10 anti-virus events, and the details of system security products installed on the host.

The following chart gives you the comprehensive analysis options provided by the **Malware Files** page. These tabs are explained in the subsequent sections.

Figure 161. Malware analysis



The following filter options are provided.

Figure 162. View data specific to admin domain

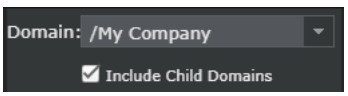


Figure 163. Analyze detected malware within a specific time

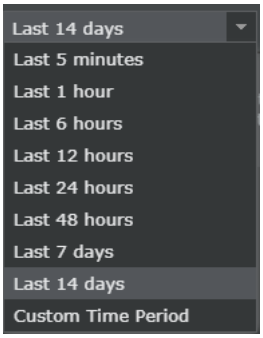


Figure 164. Analyze the type of malware, whether blocked, unblocked, or all

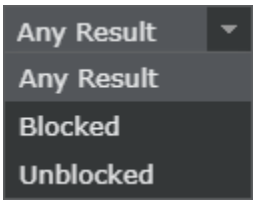


Figure 165. Analyze the malware based on malware confidence returned by engines

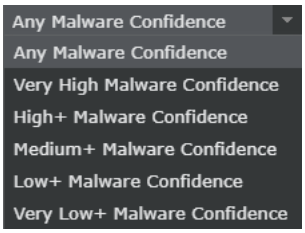
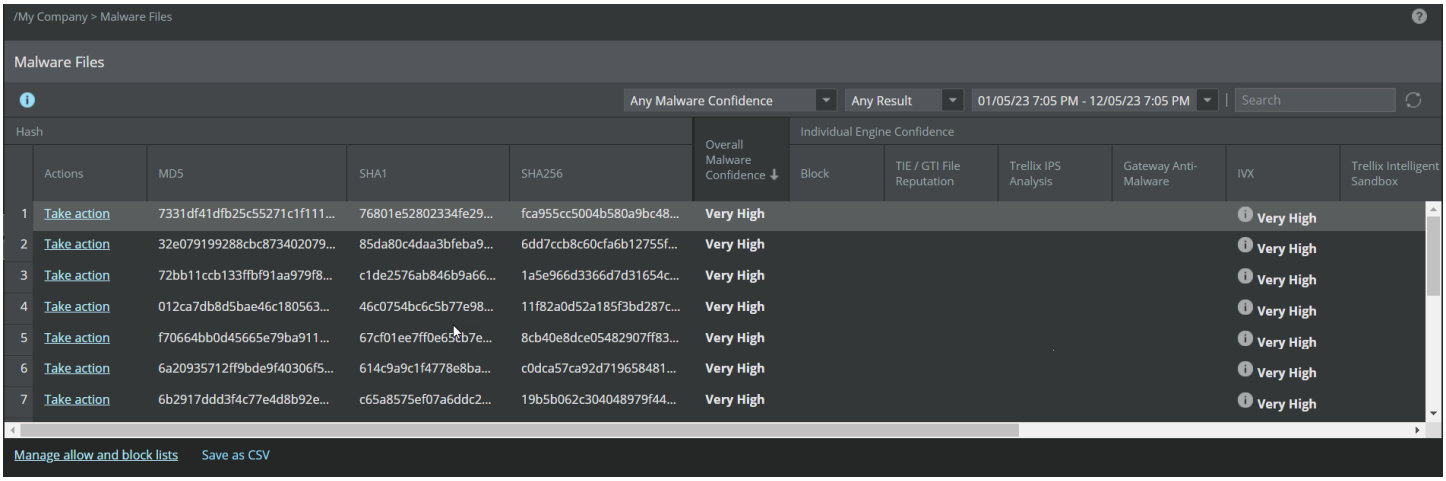


Figure 166. Details of the detected malware



Option	Definitions

Hash	Displays the hash value of the file and the actions that you can take.
	• **Actions**— Click **Take action** to take the following actions:
	  • **Export**— Click to download the malware file from the Manager server to a network location. The file is saved with an extension .trellix. This prevents you from even accidentally opening the malicious file. The file is available for download only if you enable the **Save File** option for the corresponding file type in the Advanced Malware policy that detected this malware.
	NOTE
	The antivirus program on your computer might prevent you from downloading the file.
	  • **Allow**— Click to automatically add the file to the Manager's allow list. In the next 5 minutes, the Manager sends the MD5 hash value to the allow list of all the Sensors.
	NOTE
	In case MD5 entries limit has reached, the Manager adds SHA256 hash value(s) of the malware file(s) to its allow list and sends the same hash value(s) to the Sensor through incremental or full update.
	  • **Block**— Click to automatically add the file to the Manager's block list. In the next 5 minutes, the Manager sends the MD5 hash value to the block list of all the Sensors.
	NOTE
	In case MD5 entries limit has reached, the Manager adds SHA256 hash value(s) of the malware file(s) to its block list and sends the same hash value(s) to the Sensor through incremental or full update.
	• **MD5** — Displays the MD5 hash of the file
	• **SHA1** — Displays the SHA1 hash of the file
	• **SHA256** — Displays the SHA256 hash of the file

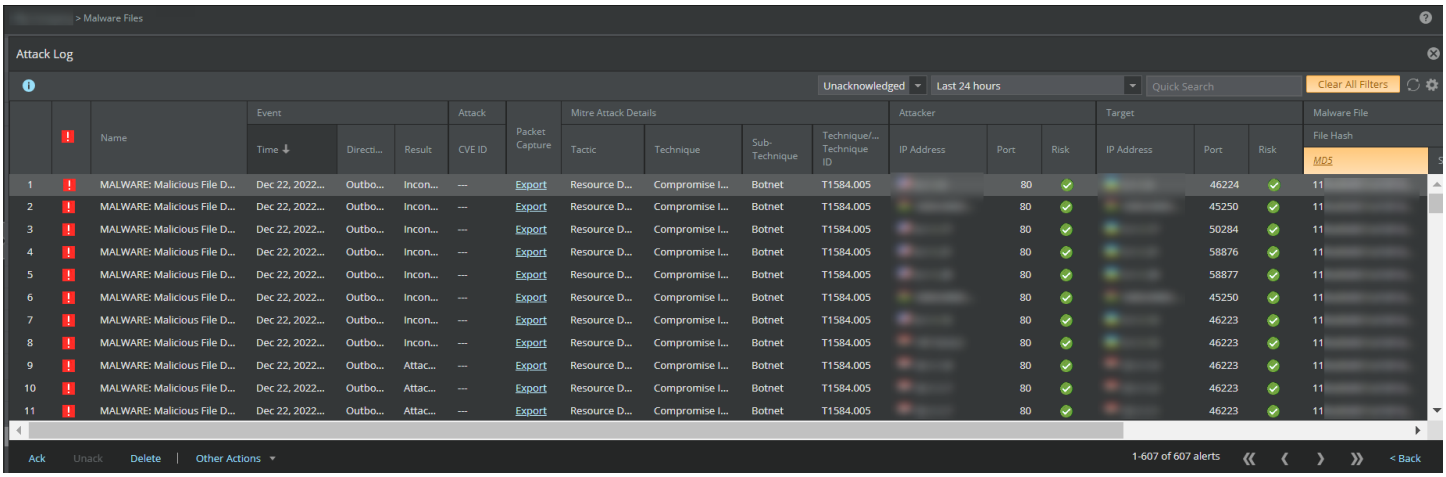
Overall Malware Confidence	The overall malware confidence level returned by the configured malware scanning engines
Individual Engine Confidence	The confidence level returned by each configured malware scanning engine, individually. Click to view the engine-specific details.
Last Attack	The date and time the last malware was detected.
Total Attacks	The number of times the malware was detected.
Last File Name	The name of the last saved malware file. In case of HTTP downloads it will be the URL.
File Size (bytes)	The size of the malware file saved

Option	Definitions
Comment	Additional comments on the detected malware

Attack Log

Upon double-clicking on the malware file hash, the **Attack Log** opens where you can view and analyze alerts related to the selected hash.

Figure 167. Attack log alerts for the hash selected



To close the attack log, click **Back** or icon.

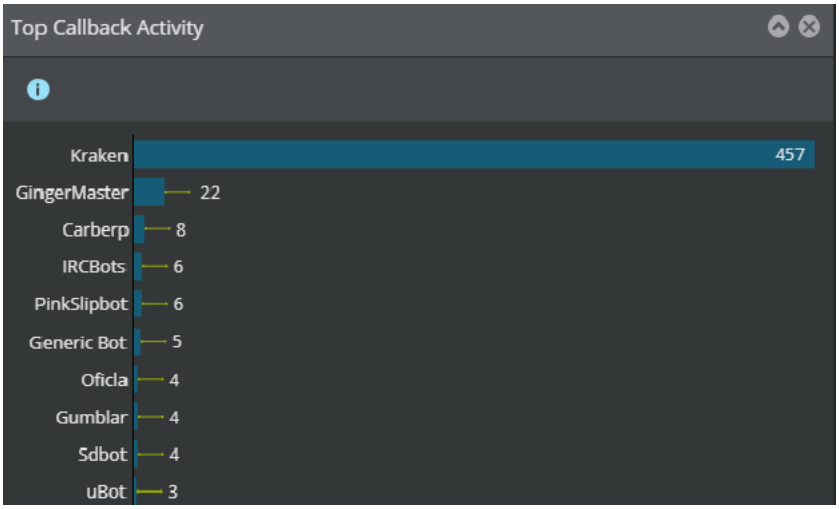
Manage allow and block lists

The **Manage allow and block lists** is a link to the **File Hashes** page. For more information, see the [Trellix Intrusion Prevention System Product Guide].

Analyze Callback Activities

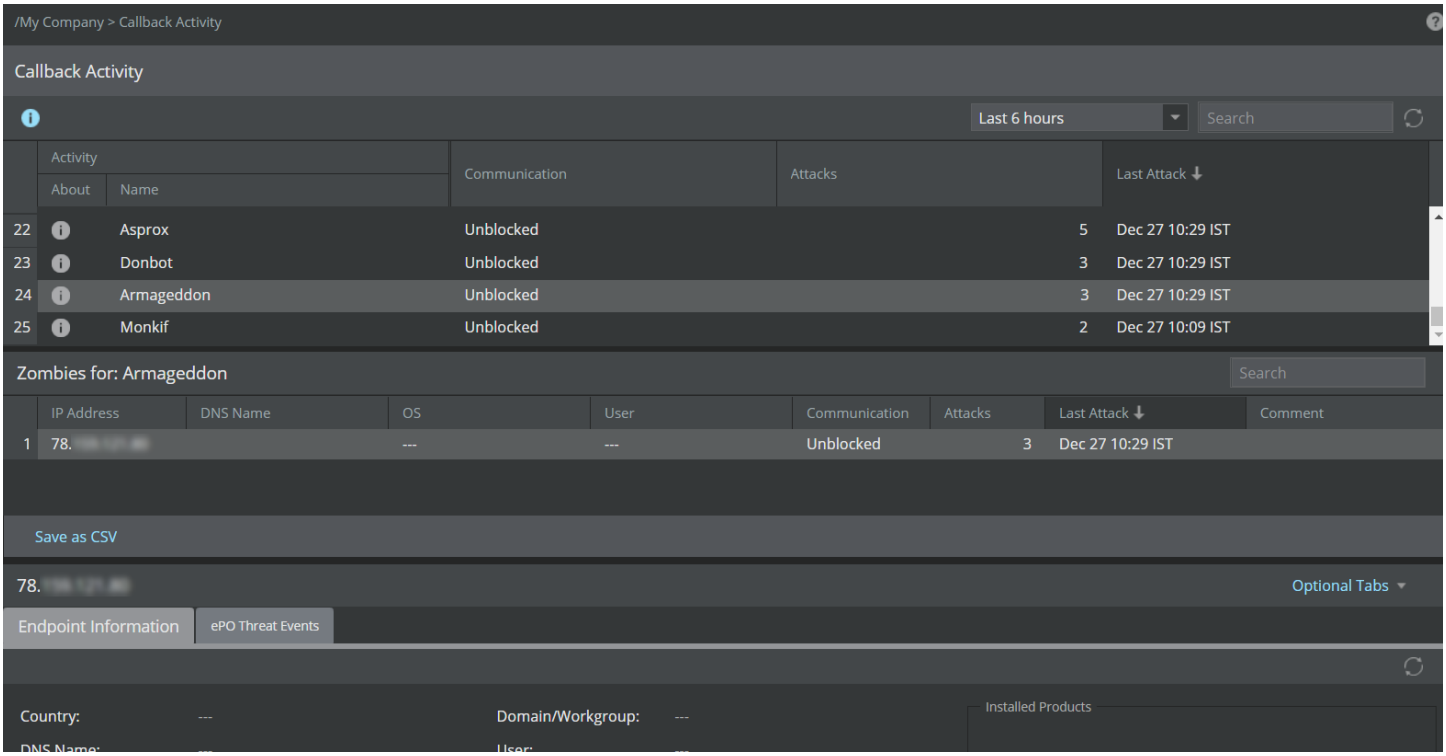
You can leverage the analysis technique provided by the Trellix IPS to perform an in-depth analysis of the callback activity in your network. The Manager provides you with a complete view of the bot events and threats on your network for further analysis and actions, thus providing a comprehensive view of the threat landscape in your network. You can view the **Top Callback Activity** dashboard. This dashboard is populated when bot activity is detected in your network. The dashboards display the callback activity name and the number of bots (zombies) in your network for the corresponding callback activity. The **Dashboard** page security monitors are displayed as bar charts.

Figure 168. Dashboard-Top Callback Activity



If you want to drill down further on a specific bot activity, click the bar, and you'll be redirected to the Analysis → **Callback Activity** page, which displays additional details on that activity. This page provides you with the flexibility of filtering and sorting the information displayed based on your choices. In addition to these filtering/sorting options, you can also view the alerts that match the filter criteria by opening the **Attack Log** page. You can view the callback activities specific to admin domains by selecting the required admin domain from the **Domain** drop-down list. Summarized data for callback activities, which includes data from the child domains, also can be viewed. If you have integrated the Manager with products like ePolicy Orchestrator - On-prem, Intelligent Sandbox, or Trellix Virtual Execution, you can view the host name, operating system, open ports, known vulnerabilities.

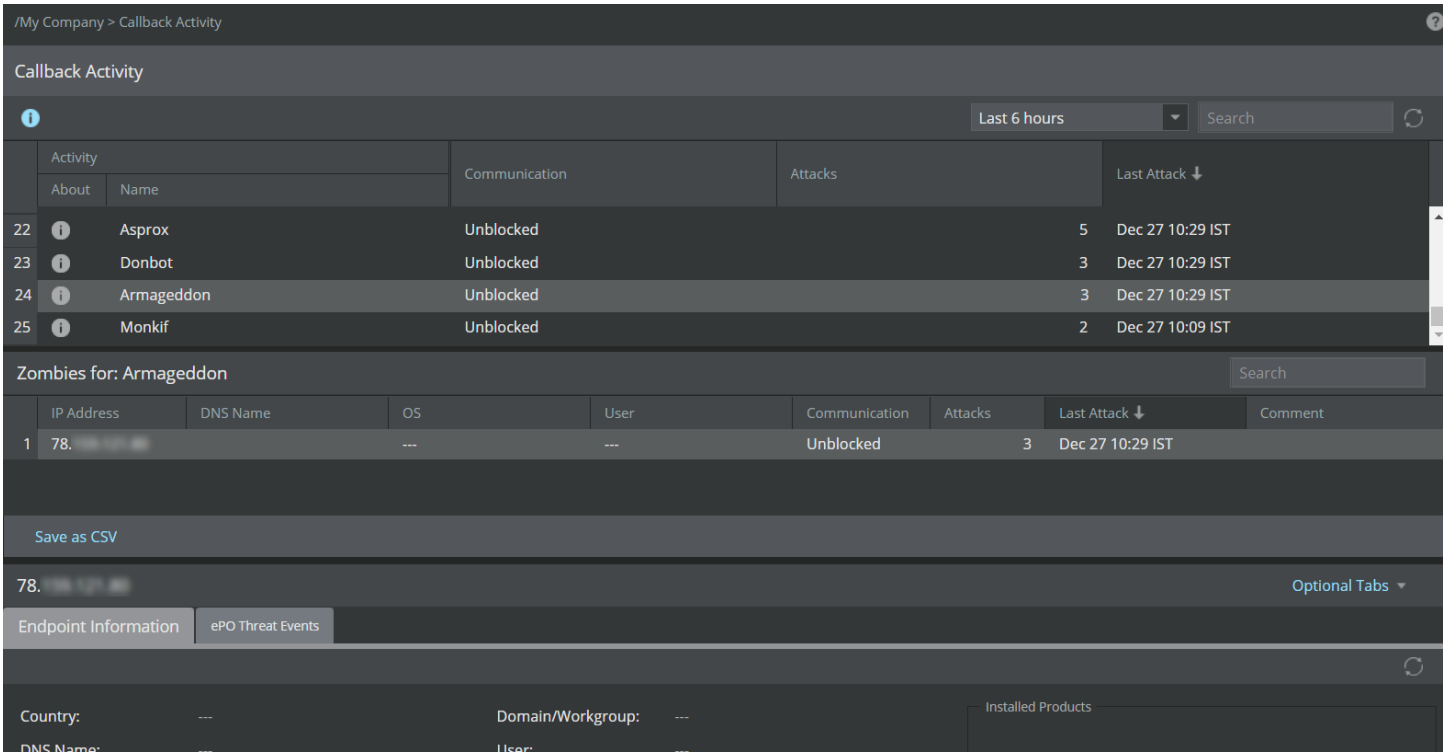
Figure 169. Callback activity analysis



You can analyze details of the callback activities, such as the callback activity name, status of the Command and Control Server communication, number of events and the details of the last event occurrence.

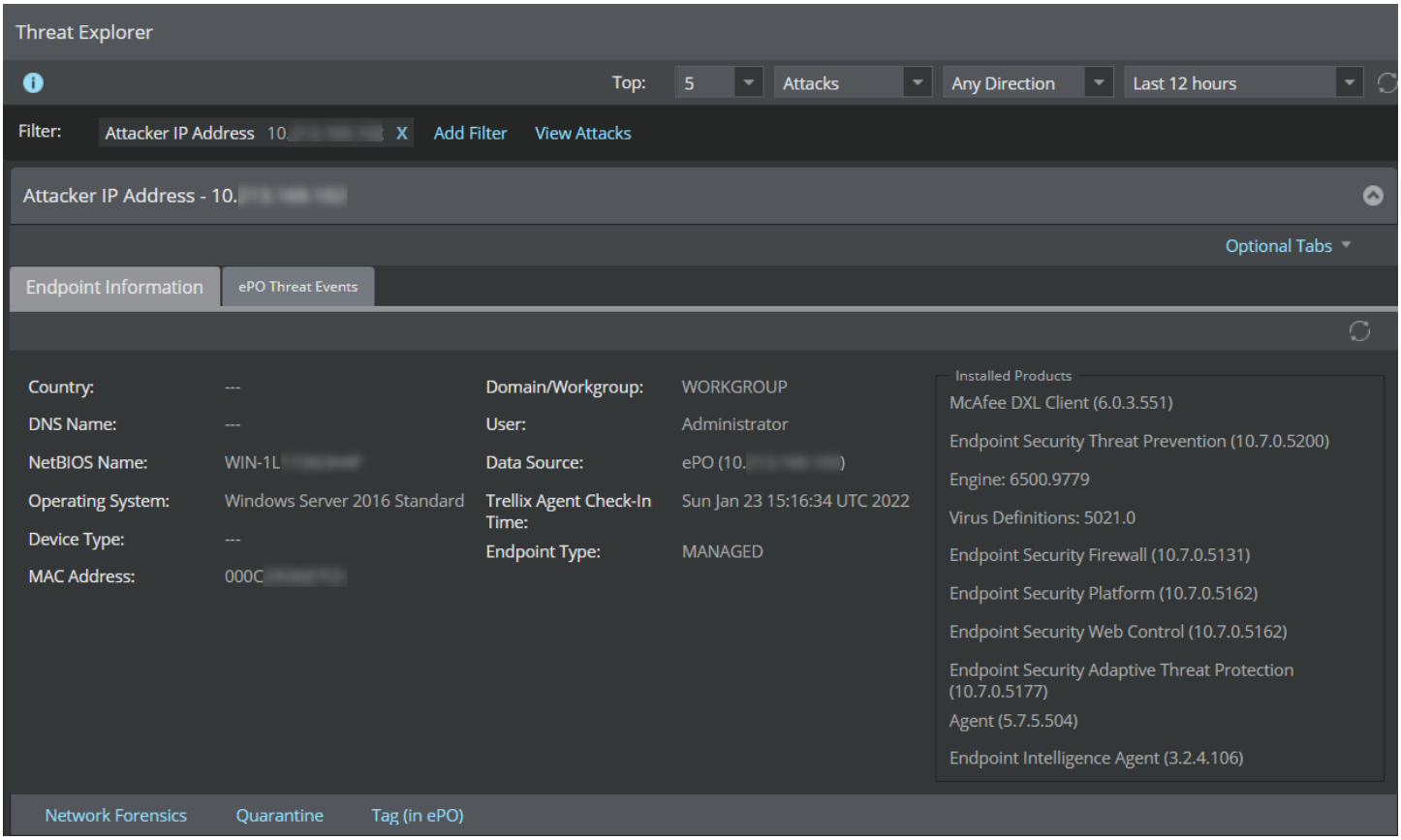
You can further analyze the details of all the zombies in the activity. For each zombie you can view its IP address, DNS name, operating system, user details, status of the Command and Control Server communication, number of events and the details of the last event occurrence.

Figure 170. Analyze callback activities



Filters can be applied at the admin domain levels which provide bot data for the selected admin domains. Data from the child domains are included in the data provided. The **Include child domains** checkbox is selected by default. Deselect the checkbox to view data only for the selected admin domain.

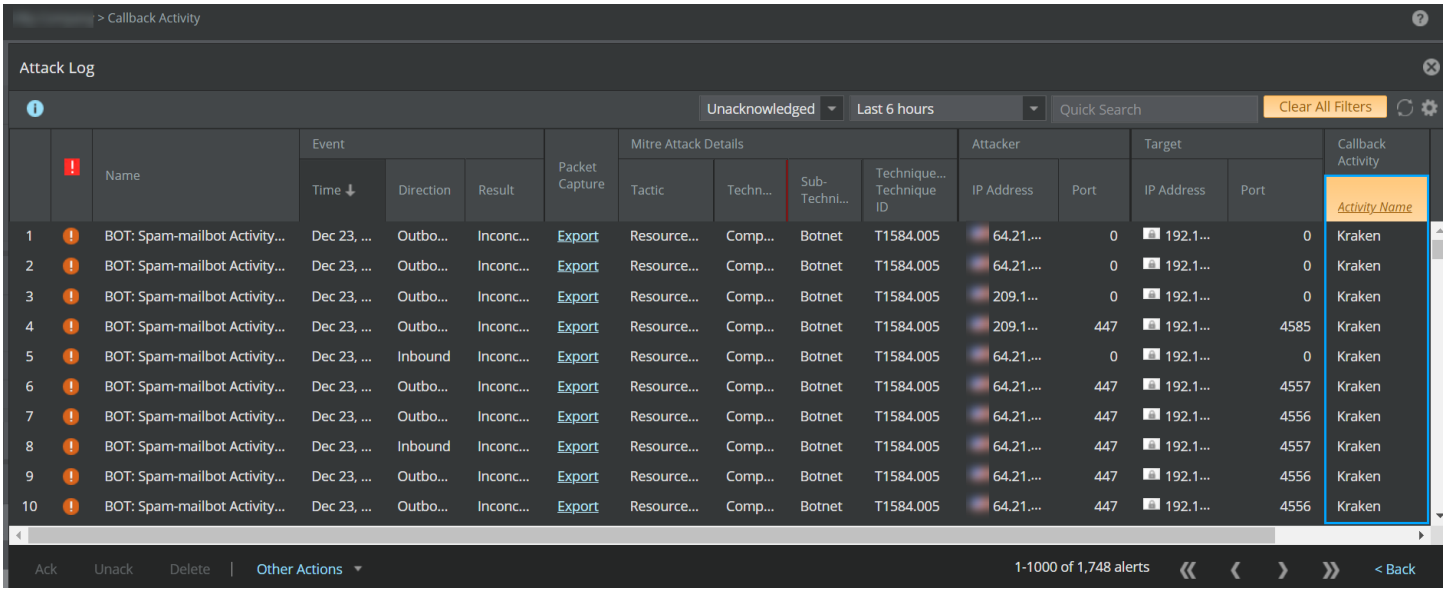
Figure 171. View data specific to admin domain



Attack Log

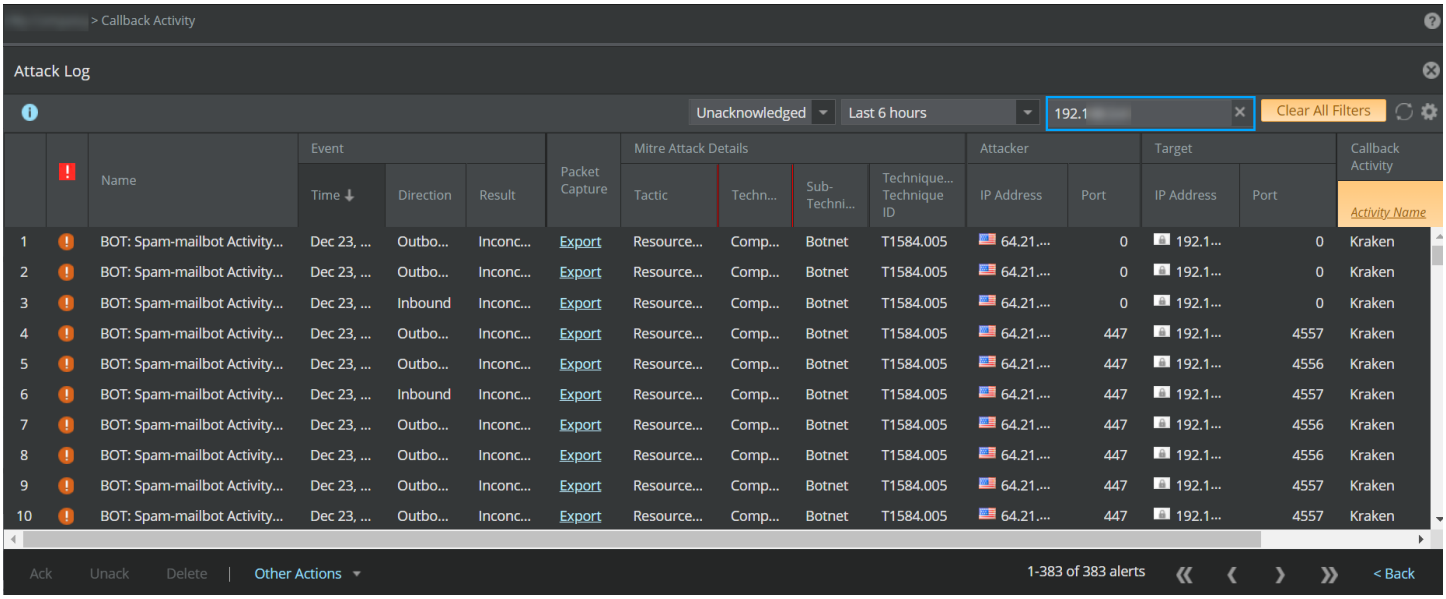
Upon double-clicking any callback activity under the **Activity** section, the **Attack Log** opens where you can view and analyze the alerts related to the callback activity.

Figure 172. Callback Activity related alerts in Attack Log



Double-click the IP address under the **Zombies for: <Activity>** section to view alerts related to the IP address and callback activity.

Figure 173. IP address related alerts in Attack Log



To close the attack log, click **Back** or icon.

Activity

This tab displays the following details of the selected activity.

Option	Definitions
About	Click to view the detailed **Activity Description**. This comprehensive activity report provides information, such as the activity description, symptoms of the bot, bot prevention methods, and bot removal tips.
Name	The name of the callback activity family
Communication	The status of the bot's communication with the Command and Control server, whether blocked or unblocked
Attacks	The number of attacks executed by all the bots listed under the callback activity family
Last Attack	The date and time of occurrence of the last attack

Zombies for: <activity>

This tab displays the details of the selected zombie for a particular activity.

Option	Definitions
IP address	IP address of the attacker
DNS name	DNS name of the endpoint to resolve the names to IP addresses
OS	Operating system platform of the endpoint
User	Operating system user name of the endpoint.
Communication	The status of the bot's communication with the Command and Control server, whether blocked or unblocked
Attacks	The number of attacks executed by a selected bot/IP address
Last Attack	The date and time of occurrence of the last attack
Comment	Additional comments on the activity can be added

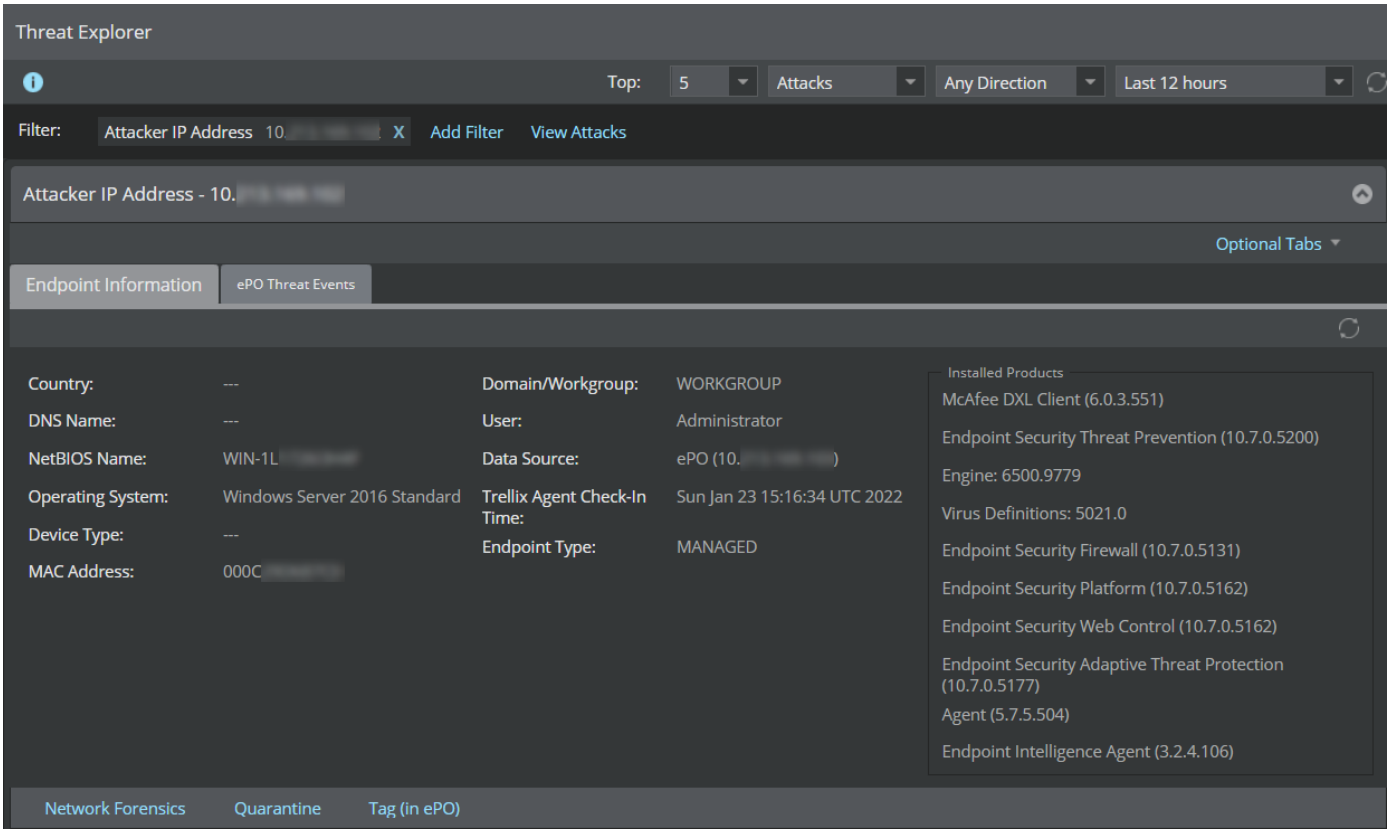
'Zombie IP address'

This tab displays various events related to a specific zombie.

- **Endpoint Information**

  The **Endpoint Information** sub-tab shows the following details specific to the endpoint.

Figure 174. Analyze Endpoint Information



Option	Definitions
Country	Country of the endpoint
DNS Name	DNS name of the endpoint to resolve the names to IP addresses
NetBIOS Name	NetBIOS name of the endpoint to access the endpoint machines
Operating System	Operating system platform of the endpoint
Device Type	Device type of the attacker/target
MAC Address	MAC address of the endpoint
Domain/Work-group	Domain or workgroup of the endpoint
User	Operating system user name of the endpoint
Data Source	Point product (Trellix ePO - On-prem) from where information is retrieved
Trellix Agent Check-In Time	Check-in time of the Trellix Agent that communicates with the same Trellix ePO - On-prem server integrated with the admin domain

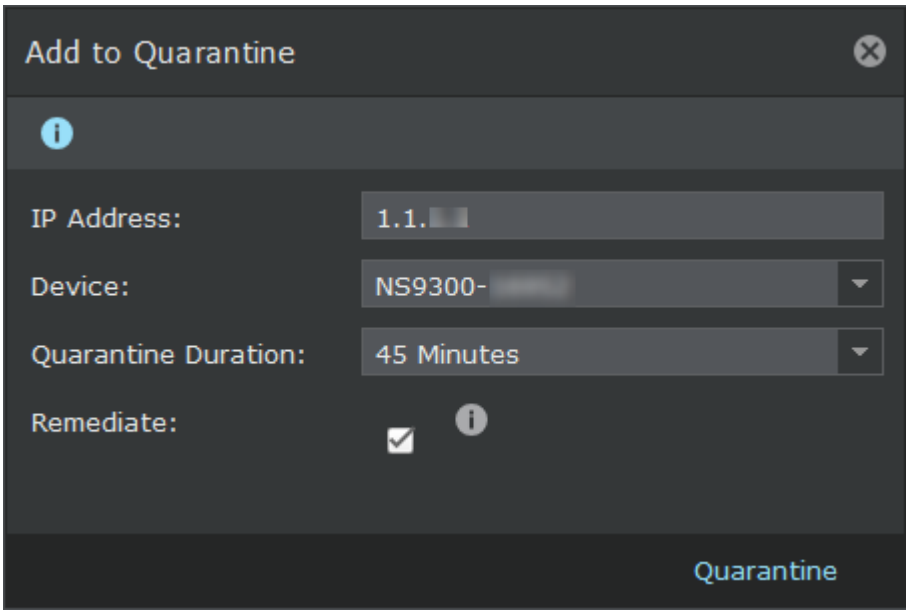
Option	Definitions
Endpoint Type	Type of the endpoints: • UNMANAGED (No Agent) — This indicates that there is no Trellix Agent installed on the endpoint. • UNMANAGED (MANAGED) — This indicates that the endpoint has a Trellix Agent but there is no active communication channel between the Agent and Trellix ePO - On-prem server integrated with the admin domain. • MANAGED — This indicates that the endpoint has a Trellix Agent and there is active communication channel between the Agent and Trellix ePO - On-prem server integrated with the admin domain. The endpoint is managed by the agent.
Installed products	List of the installed products

- **Threat Explorer**
  - **Explore as attacker IP** — Explore the threats where the endpoint is the source IP address.
  - **Explore as target IP** — Explore the threats where the endpoint is the destination IP address.
- **Network Forensics** — Click this tab to analyze the network behavior of the endpoint when NTBA is configured.

  You can filter your view by choosing the time and date of your choice.

  You can view the data according to your time preference by selecting the time period from the drop-down list. You can use the ± icon to view the details before and after any event/attack.
- **Quarantine** — Use this option to block all the traffic originating from the specified IP address seen on the selected device for the selected time.

Figure 175. Quarantine Endpoint dialog



To quarantine endpoints to block all the traffic originating from the specified IP address:

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal**. Remediation cannot be configured for IPv6 address. The checkbox and the information icon for remediation are not displayed if you enter an IPv6 address in the **IP Address** field.

Click **Quarantine**. The endpoint is added and displayed in the **Quarantine** page.

- **Tag (in ePO)** — Use this option to assign a tag to the selected endpoint in Trellix ePO - On-prem.

  You are able to assign tags only to endpoints whose **Endpoint Type** denotes MANAGED. This means that the endpoint runs a suitable version of Trellix Agent and is managed by Trellix ePO - On-prem.

  To assign a tag:

  1. Select a tag from the drop-down list. If the tag you are looking for does not appear in the list, click the refresh button.
  2. Click **Tag**.

     If the tagging is successful, you receive a message stating its success. If not, you receive a failure notification.

- **ePO Threat Events**

  The **ePO Threat Events** sub-tab displays the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for a selected endpoint. The information displayed under this sub-tab includes the date and time at which the threat event was generated, the ID associated with the event, the event description, event category, action taken on the event, and the type of the threat that triggered the event.

  You can click the  icon to refresh the list and view the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for the selected endpoint. The **Search** text field allows you to search for a specific event based on the **Event Received Time**, **Event ID**, **Event Category** and **Threat Type**. For example, to view all events associated with the Event ID 1095, type **`1095`** in the **Search** field.

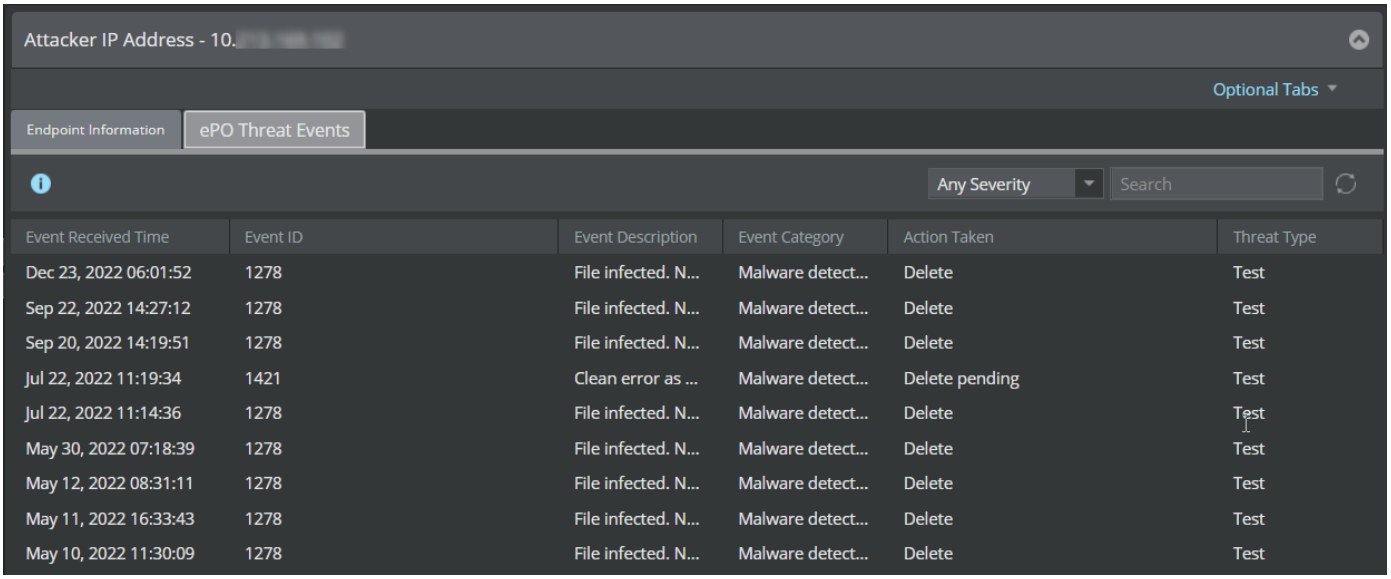
  NOTE

  The sub-tab has **Any Severity** filter selected by default. With this filter selected, the sub-tab displays all types of events including those which are informational and/or of low-severity. Such events act as noise and impede one's ability to find true threats. To exclude these events, select the **Warning+ Severity Only** filter from the drop-down menu. This displays only those events with Critical, Alert and Warning severity.

NOTE

Ensure that the ePO server has the latest Trellix IPS Extension file installed. For information on how to download and install the Trellix IPS Extension, see section [Install Trellix IPS extension file in Trellix ePO - On-prem] in [Trellix Intrusion Prevention System Integration Guide].

Figure 176. ePO Threat Events sub-tab



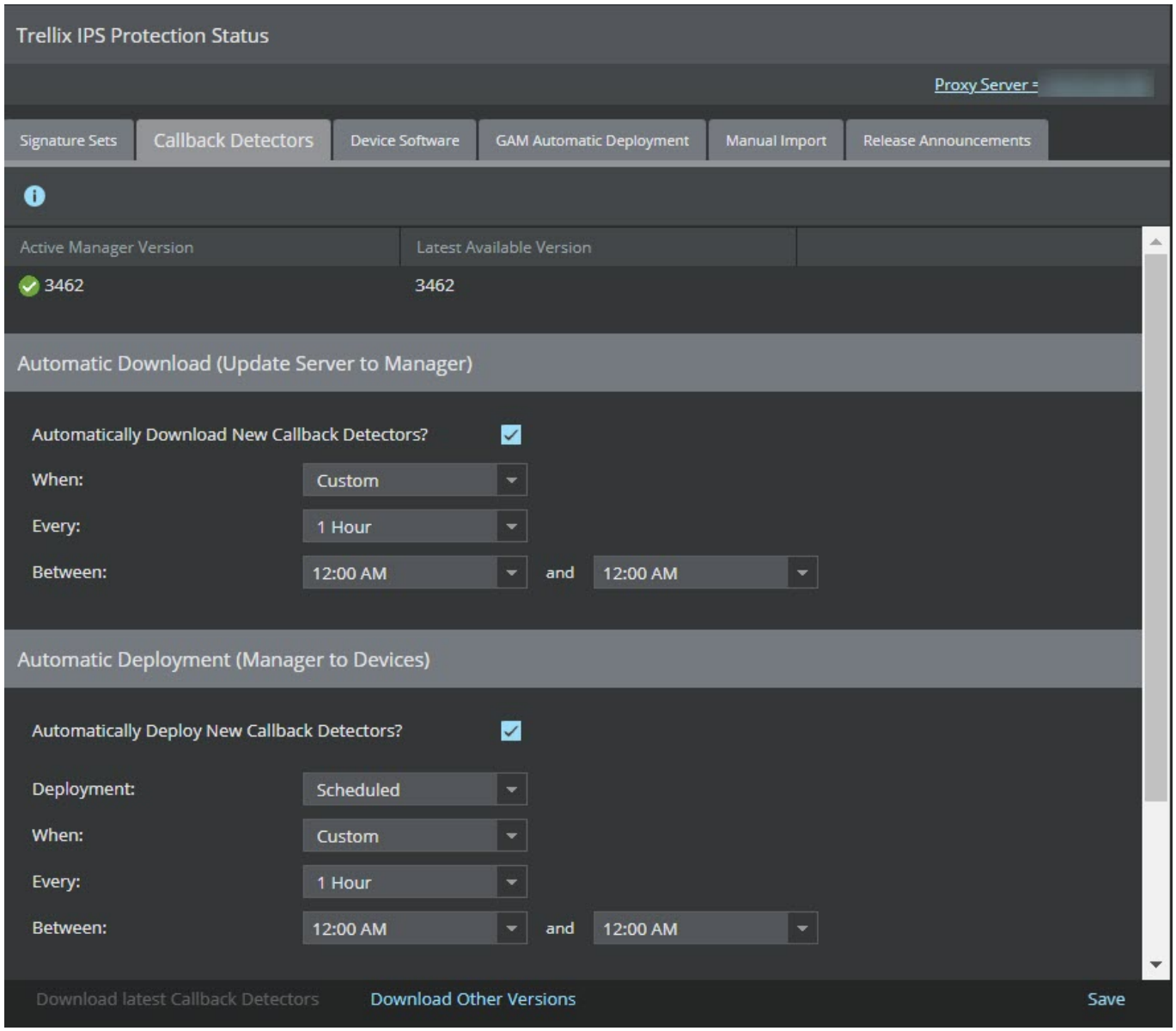
Callback detectors

You can download callback detectors and push it to the Sensor.

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Callback Detectors** tab. The **Callback Detectors** tab is displayed.
   - The **Active Manager Version** displays currently available version.
   - The **Latest Available Version** displays the latest available version for you to download.

NOTE

You can also change the display settings to meet your requirements from the filter option.



2. To download the latest callback detectors, select **Download Latest Callback Detectors**.

   A **Confirmation** dialog box appears, select **OK**. A status window opens to process the signature download.

3. To download other versions of callback detectors, select **Download Other Versions**.

   The latest 10 versions are available for you to download. It displays the update details such as the **Release Date** and **Size (MB)** for that particular **Version**.

4. Select the version required and click **Download**.

   The selected callback detectors become the active callback detectors on the Manager.

   To automatically download the callback detectors, refer to Automatic download of callback detectors (page 76).

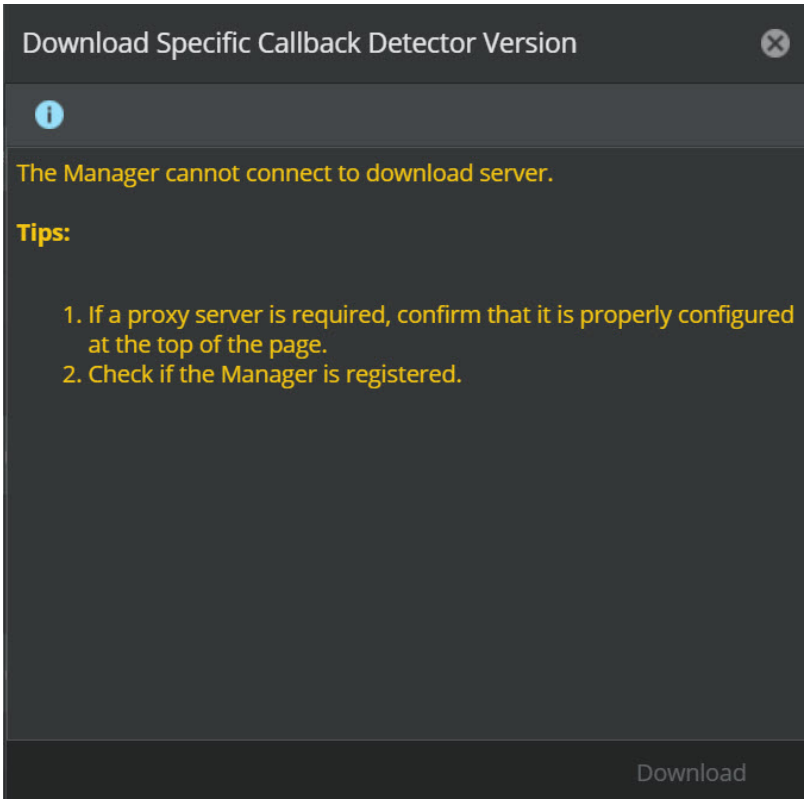
   You can also view the active and latest callback detectors version in the **Manager Summary** monitor of the Manager Dashboard. In the **Device Summary** monitor, you can view the callback detectors version on specific devices.

- If the active manager version is the latest available version, **Download Latest Callback Detectors** is disabled.
- A icon is displayed beside the **Active Manager Version** if the active callback detector version matches the latest callback detector version.
- A icon is displayed beside the **Active Manager Version** if the active callback detector version is older than the latest callback detector version.

NOTE

In an air-gap network, unregistered, or proxy server disabled Manager:

- The **Latest Available Version** is displayed as **---**.
- A icon is displayed beside the **Active Manager Version**.
- When you select **Download Other Versions**, the **Download Specific Callback Detector Version** does not display available versions of callback detectors.



Automatically updating signature sets and callback detectors

The Manager allows you to schedule the download of the signature set and callback detectors. Once configured, the scheduler downloads the signature set and callback detectors from Trellix IPS Update Server to the Manager. For example, every one hour, the Manager verifies the Trellix IPS Update Server and downloads the new file uploads.

The success/failure of the import process is indicated through fault notifications, emails, and SNMP traps.

Once the new signature set and callback detectors are available on the Manager, they can be scheduled to be deployed on your devices.

A proxy server is provided for all internet communications. You can manage the proxy server and know the proxy details from the scheduler page.

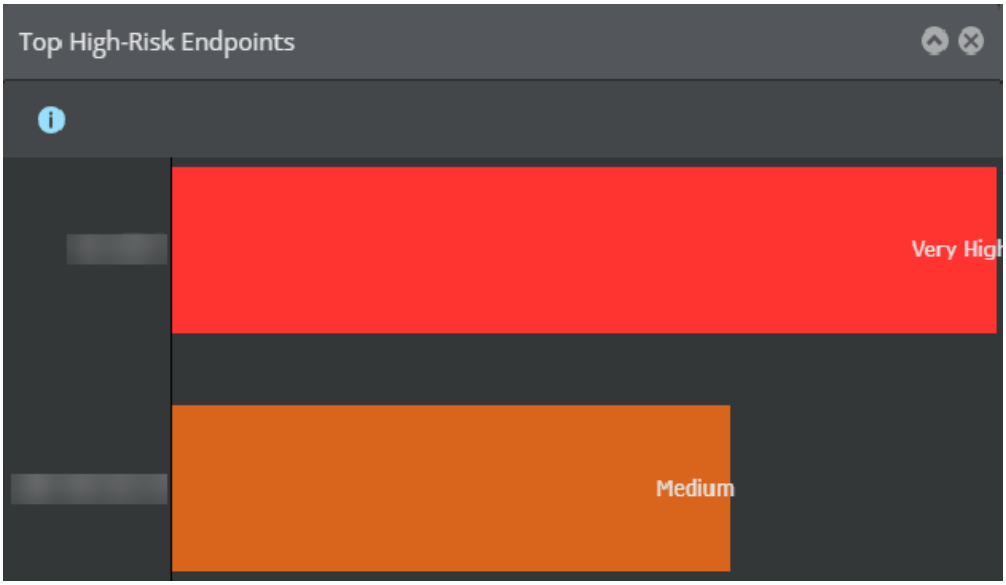
For more information on automatically updating signature sets, refer to Automatic download of signature sets (page 70).

For more information on automatically updating callback detectors, refer to Automatic download of callback detectors (page 76).

Analyze High-Risk Endpoints

You can view and analyze the endpoints whose behavior on the network is consistent with malware infection and callback activity. From the dashboard, view the **Top High-Risk Endpoints** that gives you details of endpoints whose behavior on the network is consistent with malware infection. On clicking an endpoint on the **Top High-Risk Endpoints** dashboard, you are directed to the Analysis → **High-Risk Endpoints** page. This page displays the details of the endpoints identified as risky to your network.

Figure 177. Top High-Risk Endpoints monitor



You can analyze the details of risky endpoints, such as IP address, DNS name, OS, the user details, the endpoint risk which is determined by the attacks, and certain behavioral indicators. You can view the count of the attacks per malware phase. These are classified as Exploits, Infections, and Callbacks.

You can further drill-down to view the details of these attacks, such as time of the attack, detailed attack description, name of the attack, and the result of the attack on your network. You can further download the packet log to analyze the affected data packets, obtain the attacker forensics and the target forensics, and view the direction of the traffic on which the attack is detected – whether inbound or outbound. The target and attacker details, such as, the IP address, country and the port can also be viewed. You can view these information specific to any admin domain by selecting the required admin domain from the **Domain** drop-down list. The data is calculated based on the admin domain selected and will change for each admin domain and the corresponding child domains selected.

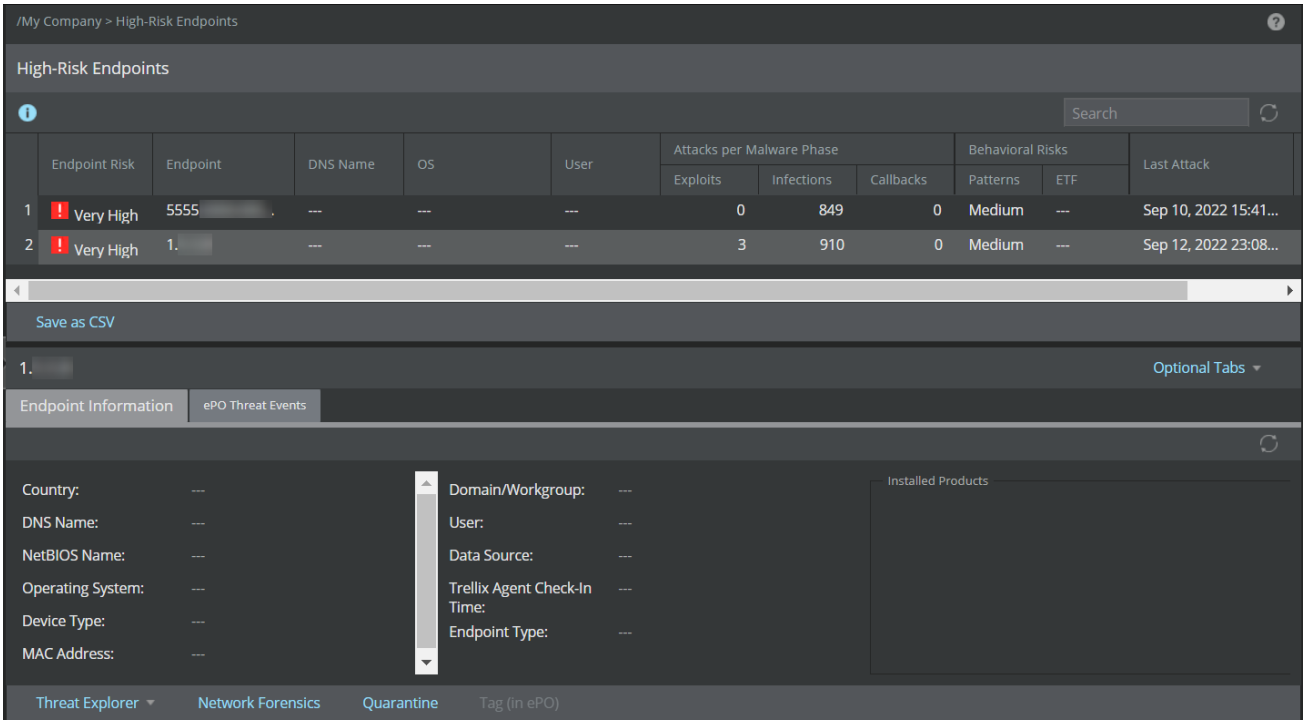
You can analyze the behavioral risks, such as patterns and Endpoint Threat Factor (ETF) and the occurrence of the last event. The patterns value indicates the risk of the endpoint based upon attack patterns. For example, a spike in certain attacks or groups of attacks to or from this endpoint over a given time period would increase its patterns value and therefore its overall endpoint risk. The ETF is a value assigned by Trellix IPS to internal endpoints to indicate their risk to the network. Multiple components

are considered to determine the value, including fluctuations in the number of connections/bytes to or from the endpoint, the reputation of endpoints with which it is communicating, and the number and severities of alerts it has generated. The ETF is in turn used to influence the overall endpoint risk.

NOTE

Data displayed in the **Top High-Risk Endpoints** monitor is automatically refreshed by the Manager on an hourly basis. This is not user configurable.

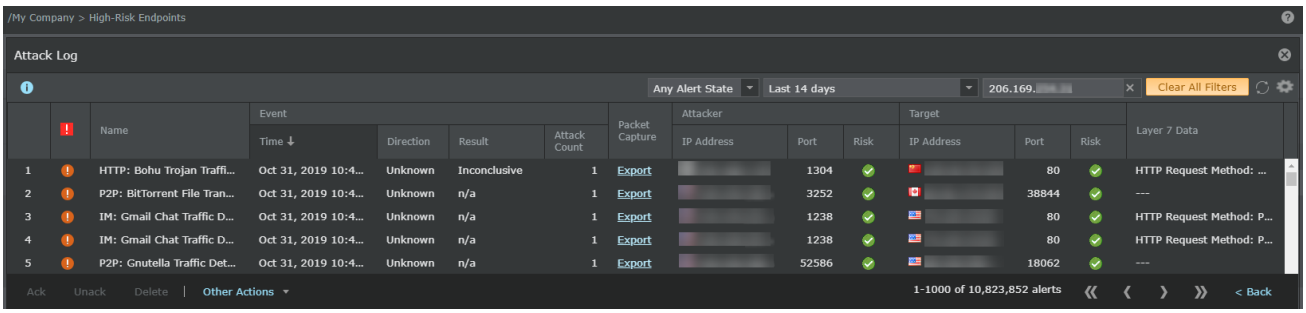
Figure 178. High-Risk Endpoints



Attack Log

Upon double-clicking on the endpoint IP address, the **Attack Log** page opens. You can analyze and view alerts related to the selected endpoint IP address.

Figure 179. High-Risk Endpoint related alerts in Attack Log



To close the attack log, click **Back** or ± icon.

The following table shows the information displayed in the **High-Risk Endpoints** section.

Option	Definitions
Endpoint Risk	Specifies the risk based on the attacks and certain behavioral indicators. The risk is displayed with an icon and a risk score. The icon and score details are as follows: • Dark red icon — Very high risk (Risk score above 180) • Red icon — High risk (Risk score ranges between 140 and 180) • Orange icon — Medium (Risk score ranges between 100 and 140) **NOTE** Low scores in the range of 20–100 are not displayed on the dashboard for a endpoint.
Endpoint	Specifies the endpoint IP address
DNS Name	DNS name of the endpoint to resolve the names to IP addresses
OS	Operating system platform of the endpoint
User	Operating system user name of the endpoint
Attacks per Malware Phase	Specifies the count of the attacks per malware phase • **Exploits** — Specifies the number of attacks which have compromised the system. These are detected by the signature set. • **Infections** — Specifies the number of attacks which are detected in the form of malware files being downloaded by the endpoint • **Callbacks** — Specifies the count of callback attacks where an infected endpoint tries to communicate with the C&C server
Behavioral Risks	• **Patterns** — Indicates the risk of the endpoint based upon attack patterns • **ETF** — A value assigned by Trellix IPS to internal executables to indicate their risk to the network
Last Attack	Specifies the date and time of the last event that affected the endpoint
Comment	Specifies any details or additional information about the endpoint activity

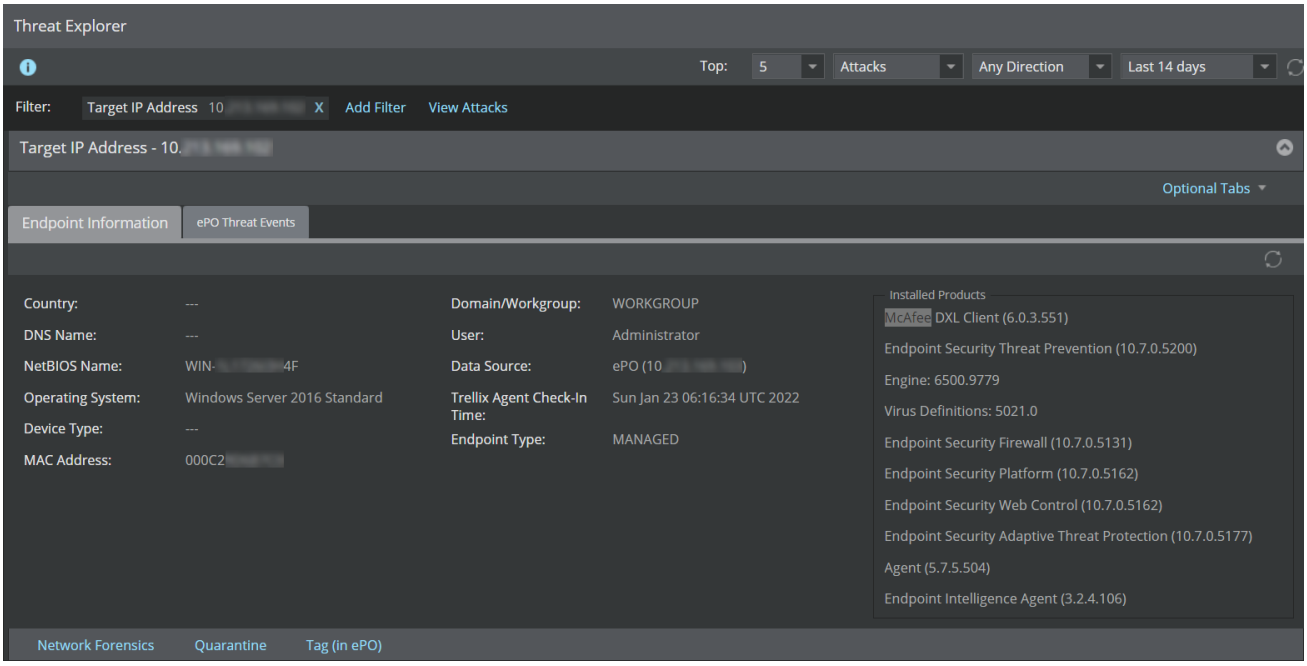
'Selected endpoint'

This tab displays various events related to a selected endpoint identified as risky to your network.

- **Endpoint Information**

  The **Endpoint Information** sub-tab shows the following details specific to the endpoint.

Figure 180. Endpoint Information sub-tab



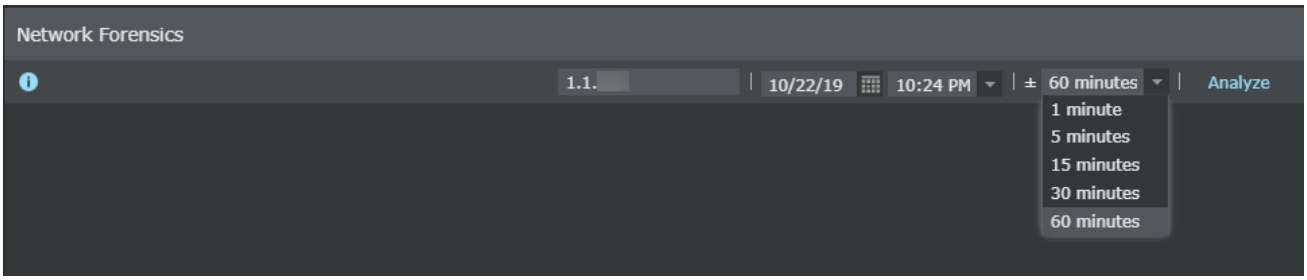
Option	Definitions
Country	Country of the endpoint
DNS Name	DNS name of the endpoint to resolve the names to IP addresses
NetBIOS Name	NetBIOS name of the endpoint to access the endpoint machines
Operating System	Operating system platform of the endpoint
Device Type	Device type of the attacker/target
MAC Address	MAC address of the endpoint
Domain/Workgroup	Domain or workgroup of the endpoint
User	Operating system user name of the endpoint
Data Source	Point product (ePO) from where information is retrieved
Trellix Agent Check-In Time	Check-in time of the Trellix Agent that communicates with the same ePO server integrated with the admin domain
Endpoint Type	Type of the endpoints: • UNMANAGED (No Agent)— This indicates that there is no Trellix Agent installed on the endpoint. • UNMANAGED (MANAGED)— This indicates that the endpoint has a Trellix Agent but there is no active communication channel between the Agent and ePO server integrated with the admin domain. • MANAGED — This indicates that the endpoint has a Trellix Agent and there is active communication channel between the Agent and Trellix ePO - On-prem server integrated with the admin domain. The endpoint is managed by the agent.

Option	Definitions
Installed products	List of the installed products

- **Threat Explorer**
  - **Explore as attacker IP** — Explore the threats where the endpoint is the source IP address.
  - **Explore as target IP** — Explore the threats where the endpoint is the destination IP address.

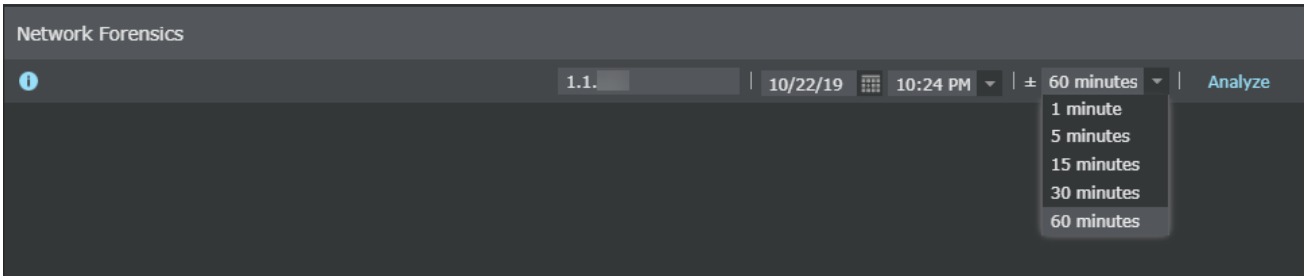
    For more information, see the section Threat Explorer (page 416).
- **Network Forensics** — Click this tab to analyze the network behavior of the endpoint when NTBA is configured.

Figure 181. Network Forensics page



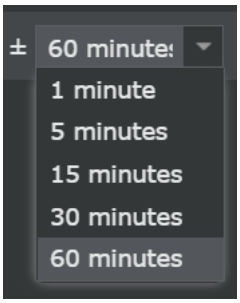
You can filter your view by choosing the time and date of your choice.

Figure 182. Date and time options in Network Forensics page



You can view the data according to your time preference by selecting the time period from the drop-down list. You can use the ± icon to view the details before and after any event/attack.

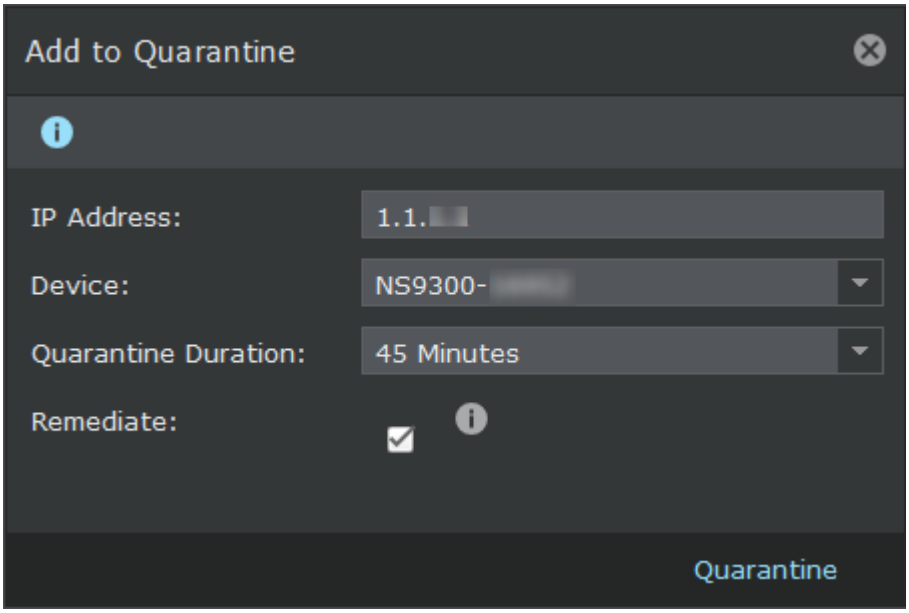
Figure 183. Show option



For more information, see the section Using context-aware data for network forensics (page 468).

- **Quarantine** — Use this option to block all the traffic originating from the specified IP address seen on the selected device for the selected time.

Figure 184. Quarantine Endpoint dialog



To quarantine endpoints to block all the traffic originating from the specified IP address:

Table 10. Properties option definitions

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal**. Remediation cannot be applied for IPv6 address. The checkbox and the information icon for remediation is not displayed if you enter an IPv6 address in the **IP Address** field.

Click **Quarantine**. The endpoint is added and displayed in the **Quarantine** page.

- **Tag (in ePO)**— Use this option to assign a tag to the selected endpoint in Trellix ePO - On-prem.

  You are able to assign tags only to endpoints whose **Endpoint Type** denotes MANAGED. This means that the endpoint runs a suitable version of Trellix Agent and is managed by Trellix ePO - On-prem.

To assign a tag:

1. Select a tag from the drop-down list. If the tag you looking for does not appear in the list, click the refresh button.
2. Click **Tag**.

   If the tagging is successful you receive a message stating its success. If not, you receive a failure notification.

- **ePO Threat Events**

The **ePO Threat Events** sub-tab displays the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for a selected endpoint. The information displayed under this sub-tab includes the date and time at which the threat event was generated, the ID associated with the event, the event description, event category, action taken on the event, and the type of the threat that triggered the event.

You can click the icon to refresh the list and view the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for the selected endpoint. The **Search** text field allows you to search for a specific event based on the **Event Received Time**, **Event ID**, **Event Category** and **Threat Type**. For example, to view all events associated with the Event ID 1095, type **`1095`** in the **Search** field.

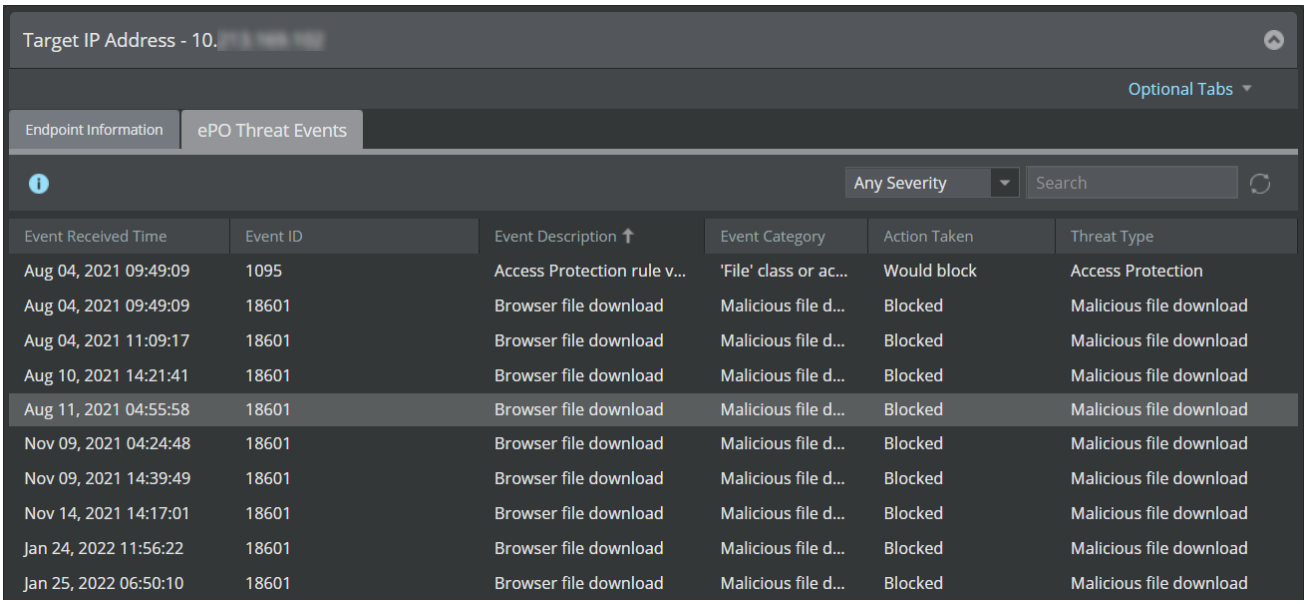
NOTE

The sub-tab has **Any Severity** filter selected by default. With this filter selected, the sub-tab displays all types of events including those which are informational and/or of low-severity. Such events act as noise and impede one's ability to find true threats. To exclude these events, select the **Warning+ Severity Only** filter from the drop-down menu. This displays only those events with Critical, Alert and Warning severity.

NOTE

Ensure that the ePO server has the latest Trellix IPS Extension file installed. For information on how to download and install the Trellix IPS Extension, see the section [Install Trellix IPS extension file in Trellix ePO - On-prem] in [Trellix Intrusion Prevention System Integration Guide].

Figure 185. ePO Threat Events sub-tab



Using context-aware data for network forensics

As a security administrator, you may want to analyze the root cause of a specific security event a few hours or days after an event has occurred. You may also want any supporting contextual data for an endpoint during that time interval.

NTBA performs context-aware network forensics to capture connections and layer 7 activity before and after a security event. This helps forensic analysis to be performed on the contextual data, against a set of predefined suspicious activity indicators.

NTBA collects forensic data for a target or attacker that is internal or external to the network. NTBA collects context-aware data as profile and forensic data. Profile data includes details like executables and services launched by an endpoint. Forensic data presents contextual data captured for specific minutes before and after a security event occurs like policy violation or an attack. By default, forensic data is collected for 10 minutes before and after an event.

The network forensics data collected by NTBA provides details such as connections made to a target and attacker, port information, network application, executables, URLs, and files. Metadata information like malware confidence, executable classification, reputation, and location are also shown if available. If a connection is suspicious, a Suspicious Activity indicator briefs the type of suspicious activity performed in the network.

How NTBA collects and stores context-aware data

When a security event like an attack occurs, NTBA performs the following high-level steps to collect context-aware data:

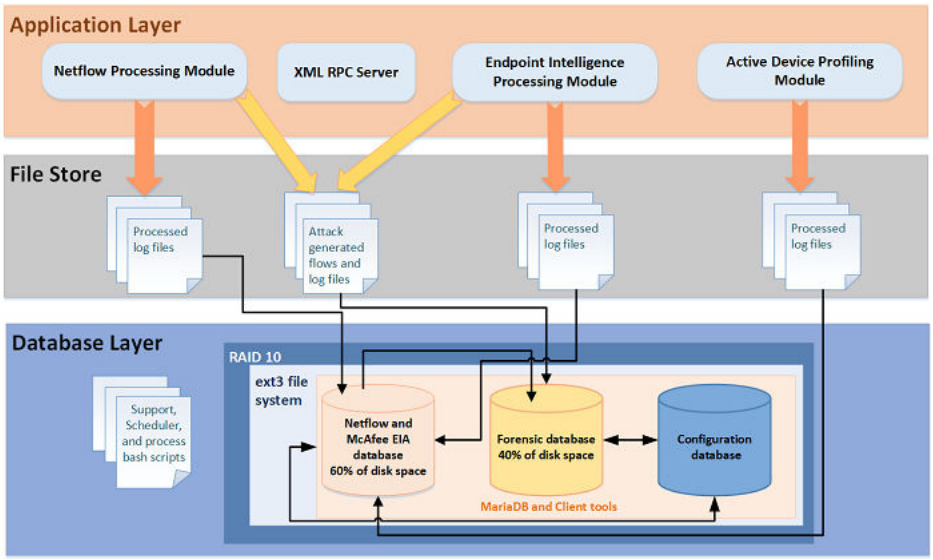
1. Consolidates conversations with attack information like 5-tuple, URLs, files, and programs involved in the connection for a target or attacker.
2. Collects the accessed URLs, files, executables, and connections for the specified time interval based on suspicious activity indicators. By default, these details are collected 60 minutes before and after an event occurred.
3. Checks if the endpoint is an attacker or target.
4. Collects data based on conditions that match the suspicious activity indicators.

Once the context-aware data is collected, NTBA stores this in the database for the configured period. By default, forensic data is stored for 30 days. You can configure the collection settings from Devices → Devices → <NTBA device> → Setup → **Collection Settings**.

The Manager enables you to configure the forensics collection settings, and retrieves the context-aware data from NTBA when you want to perform forensic analysis on a specific endpoint or attack.

The forensic data is stored as part of the virtual disk of NTBA. By default, the netflow data uses 60% and forensic data uses 40% of the disk space. By enabling export of Layer 7, the entire payload is not exported. Only fields related to HTTP, netbios, FTP, SMTP, file hash, and attack ID are exported. In HTTP application, specific fields of HTTP (like URI and host) are exported. Netflow monitoring is not made in real time as the statistics of the particular flow is sent every minute.

Figure 186. NTBA database architecture



The RAID 10 layer is the first layer, followed by ext3 file system, and database layer is the container for the netflow, forensic, and configuration databases.

You can modify the forensic database pruning settings from the Devices → Devices → <NTBA Device> → Maintenance → **Database Pruning** page. For more details, see [Maintenance of system data and files] in [Trellix Intrusion Prevention System Product Guide].

When you analyze an endpoint on the Network Forensics page, the Manager queries all the NTBAs and displays data from the NTBA that is mapped to the endpoint. On the Analysis → **Network Forensics** page, the displayed network forensic data is only from a single NTBA.

NOTE

If an IP address is mapped to more than one NTBA, the Network Forensics page has **Data Source** drop-down list to view network forensics data for NTBA mapped to an endpoint. The drop-down can be used to query the other NTBAs for forensic information.

NOTE

By default, if you directly navigate to the **Network Forensics** page to analyze an endpoint, the current date and time and analysis window of ± 60 minutes is displayed. If you perform forensics from other Manager UI paths for an endpoint, by default, the time of event occurrence and analysis window of ± 10 minutes is displayed.

Suspicious activity indicators

NTBA uses a set of predefined indicators to collect the forensic data. The indicators are triggered only when an attacker or target endpoint, flow, or executable makes a network connection in the configured analysis time window.

For example, on the **Network Forensics** page, you select an IP 1.1.1.6 that is involved in a policy violation. You select an analysis time of ±30 minutes to analyze the collected flows before and after the policy violation happened, and click **Analyze**. The suspicious flows and activity indicators are displayed based on connections made in the network in this defined time window of one hour.

NTBA collects forensic data based on the following rules:

Table 11. Suspicious activity indicators

Suspicious activity indicator	Description
Destination matches attacker in another attack	A target endpoint was involved in another attack or traffic from/to this endpoint.
Source matches attacker in another attack	An attacker endpoint was involved in another attack or traffic from/to this endpoint.
Suspicious endpoint risk	Endpoint made a connection to another endpoint with GTI risk level of **Medium Risk** or **High Risk**.
Unverified endpoint risk	Endpoint made a connection to another endpoint with GTI risk level of **Unverified**.
Executable used in another attack	Executable, for example, chrome.exe was involved in another attack or traffic from/to this endpoint.
Suspicious executable malware confidence	Endpoint accessed an executable that has malware confidence level above **Medium**.
Blocked executable	Endpoint accessed a blocked executable.
New executable	Endpoint accessed a new executable that has not been previously seen in the last x* days. *x refers to the number of days defined on the **Devices | NTBA Device Settings | Device Settings | Setup | Collection Settings** page.
URL used in another attack	Endpoint accessed a URL that was involved in another attack or traffic from/to this endpoint.
Suspicious URL risk	Endpoint accessed a URL with GTI risk level of **Medium Risk** or **High Risk**.
Unverified URL risk	Endpoint accessed a URL with GTI risk level of **Unverified Risk**.
File used in another attack	Endpoint accessed a file that is involved in another attack or traffic from/to this endpoint.

Suspicious activity indicator	Description
Suspicious file malware confidence	Endpoint accessed a file with suspicious malware confidence of **Medium** or **High**.
Unverified file malware confidence	Endpoint accessed a file with suspicious malware confidence of **Unknown**.
Attack detected	Specific suspicious flow generated an attack in the network.
New service detected	A new service was installed on an endpoint that has not been previously seen in the last x* days. *x refers to the number of days defined on the Devices → NTBA Device Settings → Device Settings → Setup → **Collection Settings** page.

On the Analysis → **Network Forensics** page, these are displayed in the **Suspicious Activity** column. You can also use these indicators as filters from the **Any Activity** drop-down list to view specific suspicious activity-based flows in the network.

NOTE

If EIA is disabled, executable-related indicators like executable used in another attack are not available. Similarly, if Trellix GTI is disabled, reputation-based indicators are not functional.

Enable Network Forensics

When network forensics is enabled, the Manager takes advantage of the NTBA Appliance to provide network activity for a given endpoint over a given time span. You can collect network forensic data for a time period for analysis.

Steps:

1. At the Global level, select Devices → Global → NTBA Device Settings → Device Settings → Setup → **Collection Settings**.

   TIP

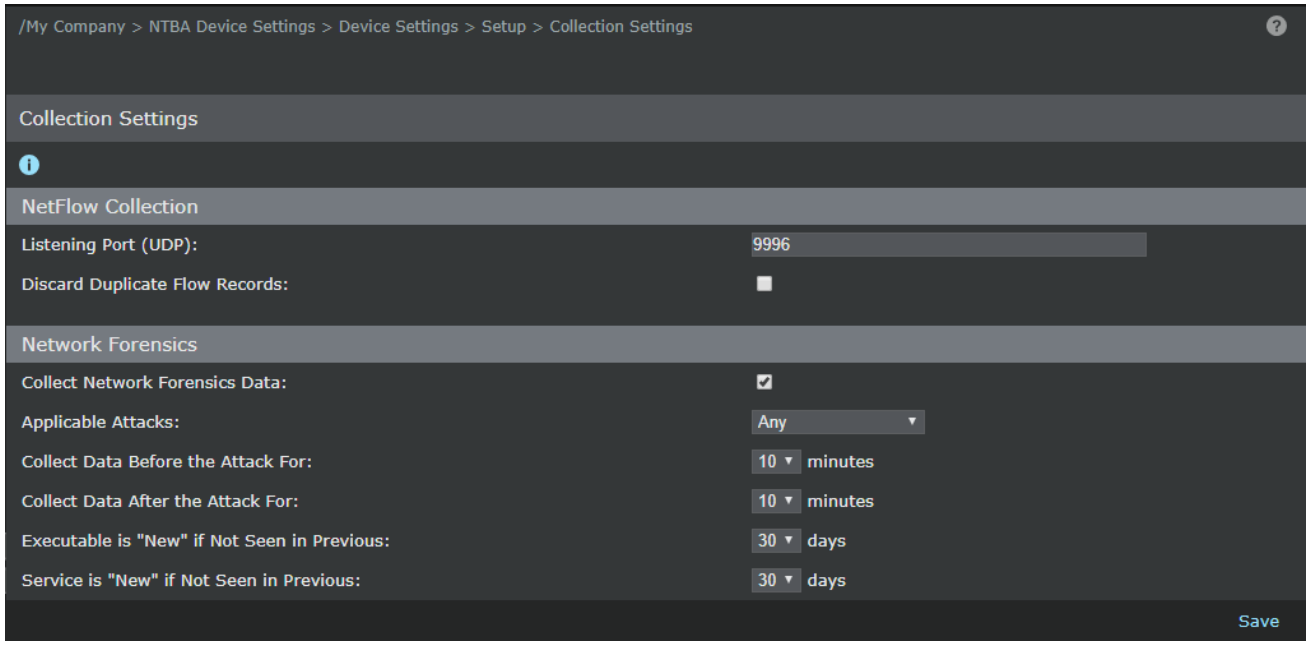
   At a device level, you can navigate to Devices → Devices → <NTBA Appliance> → Setup → **Collection Settings**. If you want to inherit the global level collection settings, select **Use Global Settings**.

2. Enter the listening port and select **Discard Duplicate Flow Records** if you do not wish duplicate records. By default, the UDP port is set to 9996.
3. In the **Network Forensics** area, specify the following:

Item	Description
Collect Network Forensics Data	Select this checkbox to collect network forensics data. By default, this checkbox is selected.
Applicable Attacks	Select **Any**, **IPS Attacks Only** or **NTBA Attacks Only**. By default, this is set to **Any**.
Collect Data Before the Attack For	Select the time for which you wish to collect data before a security event. By default, this is set to 10 minutes. The time range is 1-60 minutes.

Item	Description
Collect Data After the Attack For	Select the time for which you wish to collect data after a security event. By default, this is set to 10 minutes. The time range is 1-60 minutes.
Executable is 'New' if Not Seen in Previous	Collect executable details if the executable is new in the network. By default, this is set to 30 days. The day range is 3-90 days.
Service is 'New' if Not Seen in Previous	Collect service details if the service is new in the network. By default, this is set to 30 days. The day range is 3-90 days.

Figure 187. Forensic data collection



4. Click **Save**.

> **TIP**
>
> If no forensic data is displayed, execute the **`show forensic-db details`** command to check if the network forensics feature is enabled or not. By default, this feature is enabled. You can use the **`set dbdisksize`** and **`show l7dcapstats`** commands to set the percentage of disk size for the forensic data and view layer 7 captured data details.

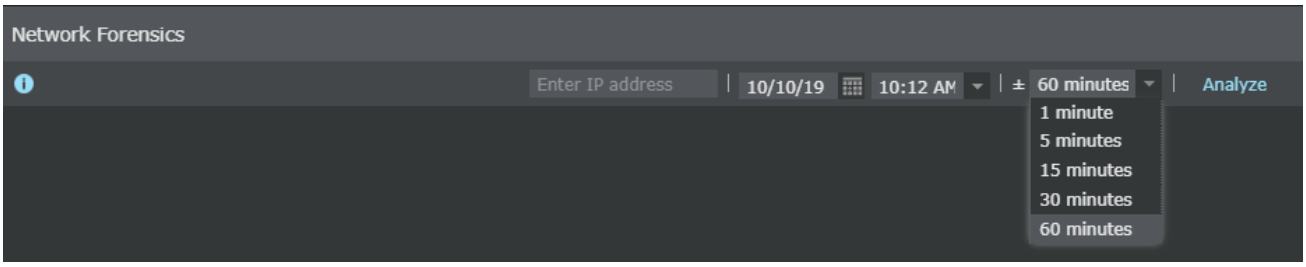
Perform network forensics on an endpoint from the Analysis tab

You can enter an IP address and track its network behavior for a specified time period.

Go to Analysis → **Network Forensics** to analyze the recent behavior of the specific endpoint in the network, including conversations and events in the specified time period.

Filter your view by choosing the time and date of your choice. Use the **±** option to view data before and after an attack. This enables to analyze context-aware data and see network behavior of an endpoint in the network.

Figure 188. Date and time options



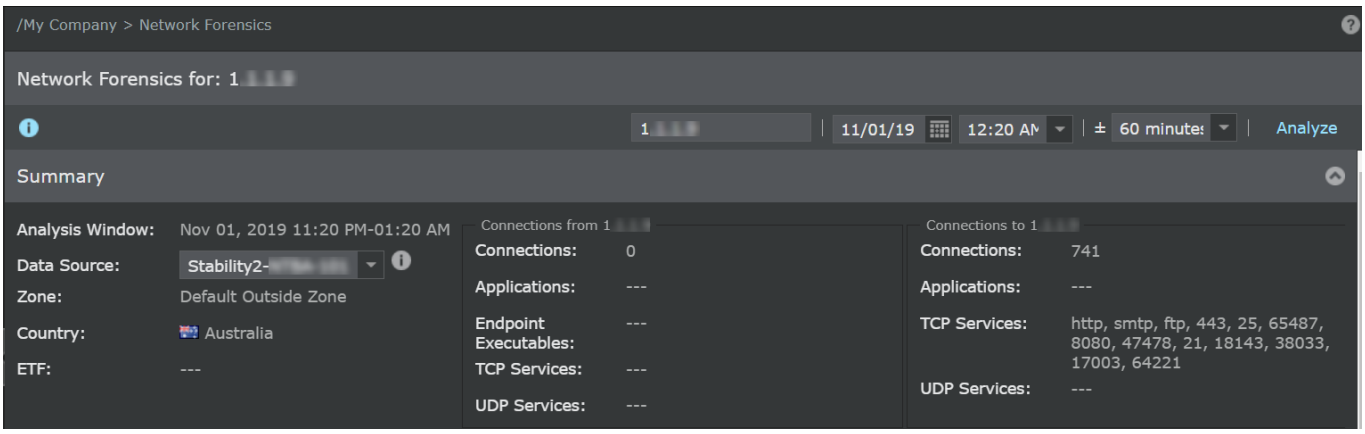
The following table shows the information displayed on the **Network Forensics** page.

Item	Description
Filter Criteria Panel	
Enter IP address	Enter the IP address of the endpoint whose network activities you wish to analyze.
Date	Select the date when the event occurred.
Event occurrence time	Select the time at which the event occurred. The event can be an attack, alert, or policy violation.
Analysis window	Select the time period in which you wish to track an endpoint's activities in the network. This includes activities performed by an endpoint before and after a security event.
Analyze	Retrieves suspicious flows, activities, and indicators for an event in the specified time period.

Steps:

1. In the **Enter IP address** field, enter an IP address for which you wish to view the suspicious flows and activity. Example: 1.1.1.9.
2. Select the date and time. Use the **±** time to view endpoint behavior before and after an attack.
3. Click **Analyze**.
4. In the top panel, view **Summary** for endpoint details and connections made to and from an endpoint.

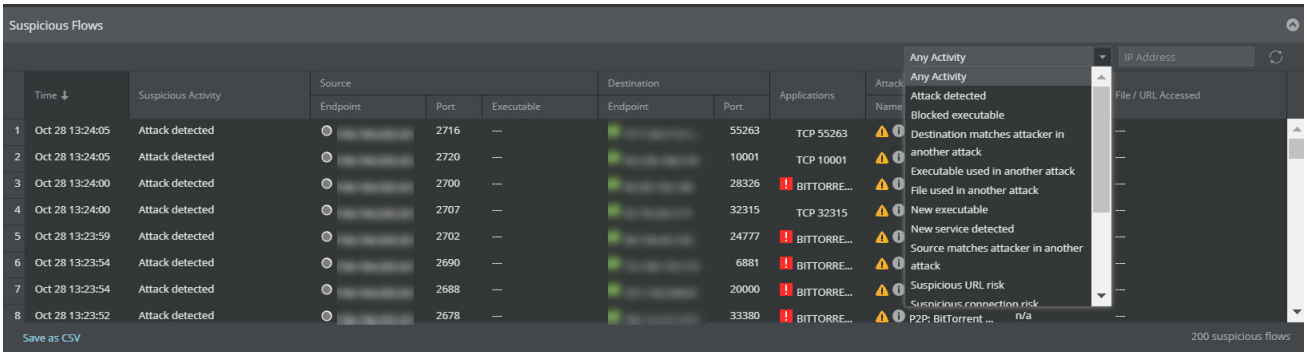
Figure 189. Summary Panel



Item	Description
Summary Panel	
Endpoint Summary	• **Analysis Window** — The period of analysis. • **Data Source** — The NTBA device that is mapped to an endpoint IP address. **NOTE** If one or more NTBAs have an endpoint IP address within the same time range, you can view these NTBA devices from this drop-down list. • **Zone** — The zone to which this endpoint belongs to. • **Country** — The country of the endpoint. • **ETF** — The ETF value assigned by NTBA to an endpoint.
Connections from endpoint	Specifies the client connections from an endpoint that include the TCP and UDP services and ports. • **Connections** — The number of connections made from an endpoint. • **Applications** — The applications accessed from an endpoint. • **Endpoint Executables** — The executables accessed. • **TCP Services** — The tcp services used by an endpoint. • **UDP Services** — The UDP services accessed by an endpoint.
Connections to endpoint	• **Connections** — The number of connections made to an endpoint. • **Applications** — The applications used on an endpoint. • **TCP Services** — The TCP services used on an endpoint. • **UDP Services** — The UDP services accessed on an endpoint.

5. In the lower panel, view **Suspicious Flows** for details like suspicious activity, applications, attack name, and files and URLs accessed.
   - From the flows, select the indicator to view specific activity-based flows. Example: Blocked executable.
   - View suspicious flows that have blocked executables involved in the attack.

Figure 190. Suspicious activity indicator filter



Item	Description
Suspicious Flows Panel	
Suspicious activity indicators	View indicators that map to an event like an alert or attack. • Destination matches attacker in another attack • Source matches attacker in another attack • Suspicious endpoint risk • Unverified endpoint risk • Executable used in another attack • Suspicious executable malware confidence • Blocked executable • New executable • URL used in another attack • Suspicious URL risk • Unverified URL risk • File used in another attack • Suspicious file malware confidence • Unverified file malware confidence • Attack detected • New service detected
IP Address	Specify an IP address and use **Search** to view flows for this address.
Time	Displays the date and time when the suspicious flow for an event occurred. **TIP** You can sort the flows view based on time.
Suspicious Activity	Displays the indicator that specifies the suspicious activity performed like an URL accessed that was involved in another attack, blocked executable accessed and others.
Source	Specifies the source from which the flow was initiated for an endpoint. Details include endpoint and ports used.
Destination	Specifies the destination details like endpoint involved and port.
Applications	Displays the applications accessed from the endpoint.
Attack	Attacks for a specific endpoint that includes attack name and result.
File/URL Accessed	Specifies file or URL access details for a specific endpoint.

6. Click **Save as CSV** to export suspicious flows for analysis.

Analyze Endpoint Executables

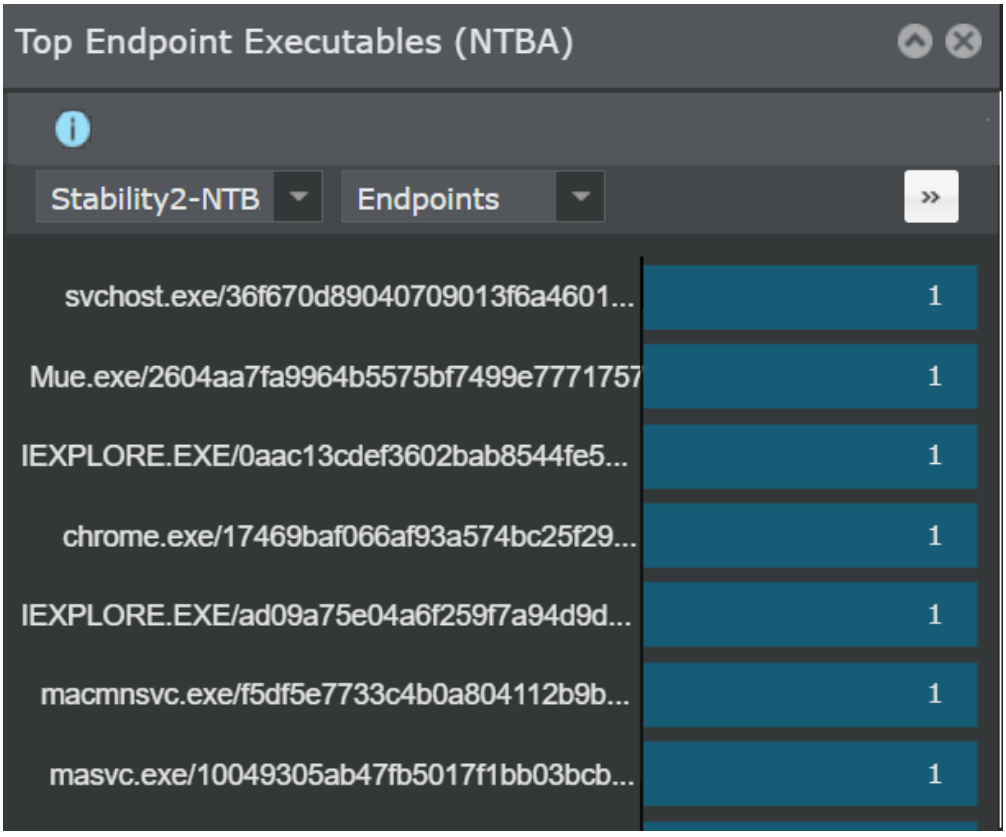
You can view the list of executables that have made outgoing connections using the Analysis → **Endpoint Executables** page, along with the classification and malware confidence computed for each executable. You can also view details, such as how many endpoints are running each executable, how many connections were made, etc. The Manager allows you to further drill down on each executable to view detailed information.

In an enterprise network, you can have hundred of thousands of executables making outgoing connections. To handle such a volume and yet quickly narrow down to a subset of endpoints or executables that exhibit malware like characteristics and require immediate attention, Trellix IPS supports the following options:

- You can enable auto-classification for executables based on file reputation provided by Trellix GTI. You can also enable auto-classification for executables signed by a trusted certificate authority.
- You can import a baseline computer profile for your organization under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **File Hashes**. This will help reduce the list of unclassified executables.
- You can also manually classify executables by monitoring their network behavior or based on the malware confidence computed by various engines. The manual classification will override the auto-classification as well as the classification imported using a baseline computer profile.

The **Top Endpoint Executables** is available in the Manager **Dashboard** page. You can filter the executables based on NTBA Appliance, attacks (default) or endpoints, or malware confidence. You can click on the graph to navigate to the **Threat Explorer** or the **Endpoint Executables** page for further investigation.

Figure 191. Endpoint Executables monitor



Viewing executables running on endpoint

The **Endpoint Executables** page on the **Analysis** tab provides a snapshot of all the executables running on your internal endpoints that have made network calls. It also provides network visibility on how many endpoints are running the executables, how many connections were made, and the events triggered by the executable during the selected timeframe.

> **NOTE**
>
> All NTBA Appliances that have EIA services running on them will be displayed in the **Devices** drop-down list. You can filter data based on the NTBA Appliance selection.

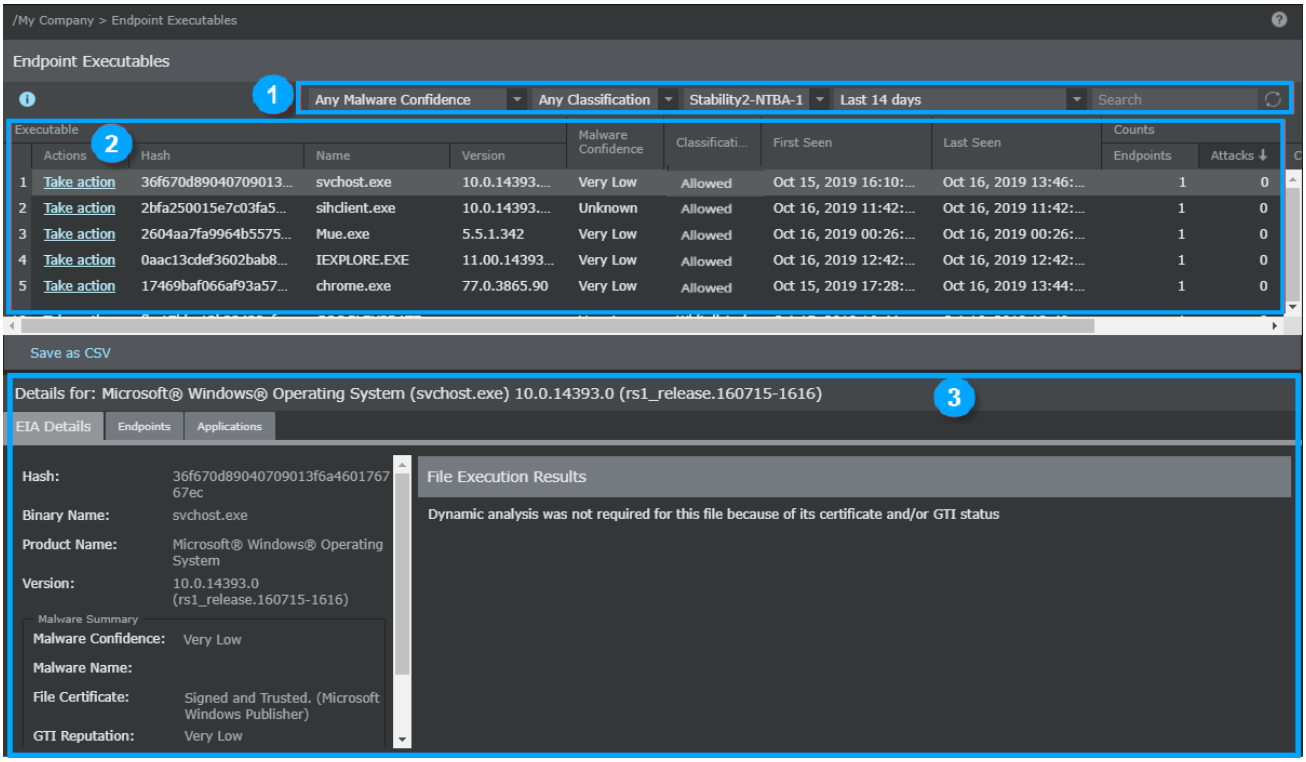
The executables listed here are processes and files. They can be allowed, blocked, and unclassified. You can use this page to investigate further on what factors led to the classification of the executable and manually change the classification.

By default, the order is sorted by the endpoints, so executables with most endpoint connections are displayed first.

> **NOTE**
>
> Maximum number of executables displayed on the **Endpoint Executables** page is 4096. Historical data and inactive executable data are kept for 30 days.

The page is divided into the **Executable** panel and the **Details** panel. Click a row in the **Executable** panel to view additional information about the executable hash in the **Details** panel.

Figure 192. Endpoint Executables page with default settings



Item	Description
1	Filters and Search options
2	Executable panel
3	Details panel

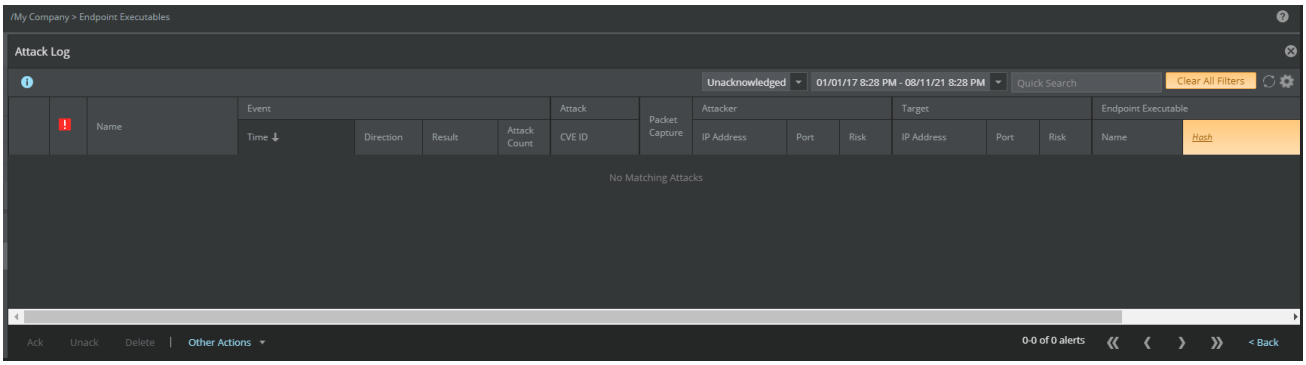
Following are the filters and search option available:

Field	Description	Default Value
Malware Confidence	• **Any Malware Confidence** — Displays all executables irrespective of their malware confidence • **High+ Malware Confidence** — Displays executables with high and very high malware confidence • **Medium+ Malware Confidence** — Displays executables with medium, high, and very high malware confidence • **Very High Malware Confidence** — Displays executables with very high malware confidence	High+ Malware Confidence
Classification	• **Any Classification** — Displays all executables, whether blocked, allowed, and unclassified • **Blocked** — Displays only blocked executables • **Unclassified** — Displays executables that are neither blocked nor allowed • **Allowed** — Displays only allowed executables	Any Classification
Devices	Displays the list of NTBA Appliances that have EIA services running on them	Displays device names in the alphabetical order
Time interval	• **Last 5 minutes** • **Last 1 hour** • **Last 6 hour** • **Last 12 hours** • **Last 24 hours** • **Last 48 hours** • **Last 7 days** • **Last 14 days** • **Custom Time Period**	Last 12 hours
Search	Allows you to search executable by the file hash or the binary name of the executable	Blank

Attack Log

Upon double-clicking on any executable hash, you navigate to the **Attack Log** page. You can analyze and view alerts related to the selected hash.

Figure 193. Selected hash alerts in Attack Log



The date and time filter used in the **Endpoint Executables** page is persisted upon navigating to attack log. To close the attack log, click **Back** or icon.

Manage Allow and Block lists

The **Manage allow and block lists** is a link to the **File Hashes** page.

For the selected NTBA Appliance, the **Executable** panel consists of the following:

Option	Definitions
Executable	• **Actions** — Click **Take Actions** to classify an executable as allowed, blocked, marked as, or unclassified • **Hash** — Displays the file hash of the executable • **Name** — Displays the binary name of the executable • **Version** — Displays the product version
Malware Confidence	Displays the malware confidence level returned by the configured EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.
Classification	Displays the executable classification whether blocked, allowed, or unclassified
First Seen	Displays when the executable was first reported by EIA to the NTBA Appliance for the selected timeframe
Last Seen	Displays when the executable was last reported by EIA to the NTBA Appliance
Counts	By default, the order is sorted by the endpoints, so executables with most endpoint connections are displayed first. • **Endpoints** — Displays the number of endpoints running the executable for the selected timeframe • **Attacks** — Displays the number of attacks triggered by the executable for the selected timeframe • **Connections** — Displays the number of connections made by the executable for the selected timeframe
Comment	Reason for changing the executable classification

Click any row to see additional information of the executable hash in the **Details** panel. The **Details** panel consists of the following:

EIA Details

This tab displays the executable or file information. This includes:

- **Properties** — Displays the malware confidence for the executable along with malware indicators that helped determine the reputation

Figure 194. Executable or file details

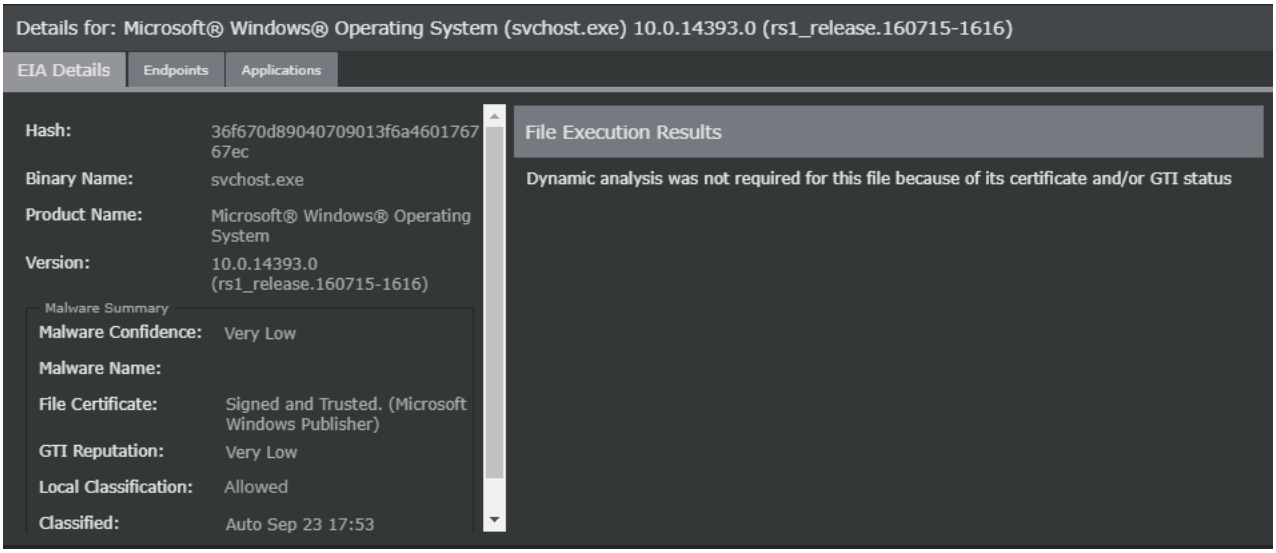


Table 12. Field descriptions of EIA Details tab

Field	Description
Hash	Displays the file hash
Binary Name	Displays the binary name and the type, whether process or library
Product Name	Displays the product name for the executable or file
Version	Displays the product version number
Malware Summary	
Malware Confidence	Displays the malware confidence level returned by the configured EIA. The malware confidence values are very high, high, medium, low, very low, and unknown.
Malware Name	Displays the malware name, for example, gtalk.exe
File Certificate	Displays the certificate signer and status for the file certificate, for example, Microsoft Corporation
GTI Reputation	Displays the file reputation received from GTI. Valid values are **Very Low**, **Low**, **Medium**, **High**, **Very High**, and **Unknown**.
Local Classification	Displays the executable classification whether **Blocked**, **Allowed**, or **Unclassified**
Classified	Displays the method of classification (*Auto* if the executable has been auto-classified by the NTBA Appliance or *Manual* if it has been manually classified) and the timestamp, only for classified executables.

Field	Description
File Execution Summary	Displays a summary of the tasks performed when a program was executed. Examples: connects to the internet, changes proxy settings, adds host file entries.
File Execution Details	Displays execution details as they happened • **Save as CSV** — Exports the list of executables in CSV format • **Executable** — Displays the executable name, example, gtalk.exe • **Action** — Displays action performed by the program, example, create_dir • **Target Object** — Specifies the path where this action was performed, example, `\Device\Harddisk\Users\Ellie\Local` • **Search** — Displays details based on search criteria

- **File Execution Results** — Shows some of the methods and engines that were used to compute the executable reputation

Endpoints

This tab displays the list of endpoints running the executable during the selected timeframe.

Figure 195. Endpoints information

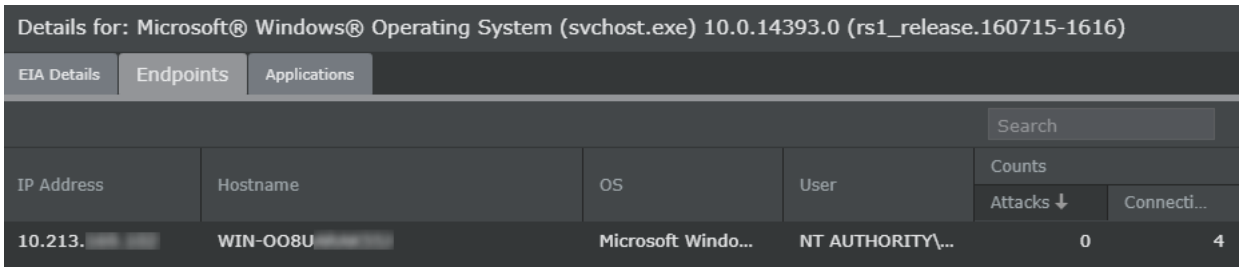


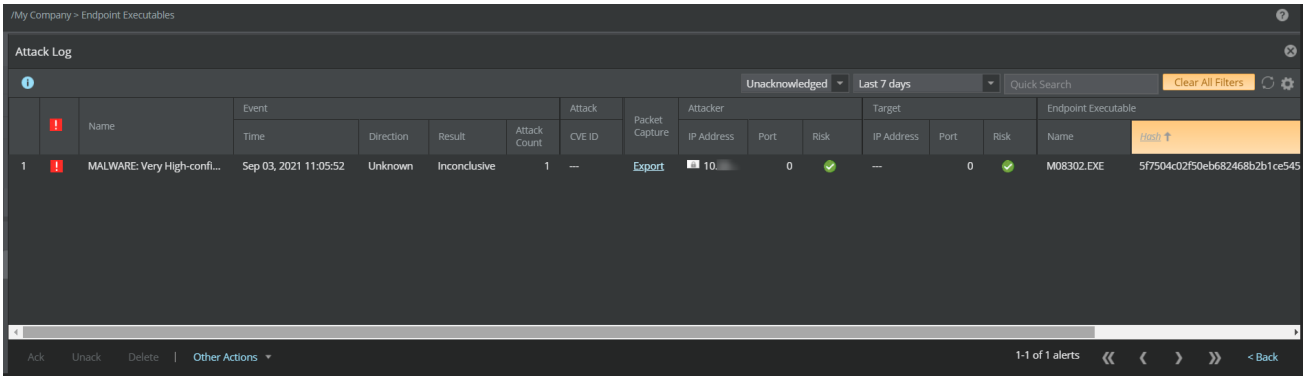
Table 13. Field descriptions of Endpoints tab

Field	Description
IP Address	Displays the IP address of the endpoint
Hostname	Displays the name of the managed host
OS	Displays the version of the operating system running on the endpoint. For example: Windows 10.
User	Displays the user name who invoked the executable or the DLL. The user name can include system users and local users.
Counts	• **Attacks** — Displays the number of attacks triggered by the executable during the selected timeframe • **Connections** — Displays the number of connections made by the executable during the selected timeframe

The **Search** field allows you to search by IP address, host name, operating system, or user columns.

Double-click the IP address to view alerts related to the IP address in the Attack Log. The alerts are filtered based on the IP address selected. To close Attack Log, click **Back** or icon.

Figure 196. Alerts based on the IP address selected



Applications

This tab displays the list of applications that have been invoked by the executable during the selected timeframe.

Figure 197. Applications invoked by the executable

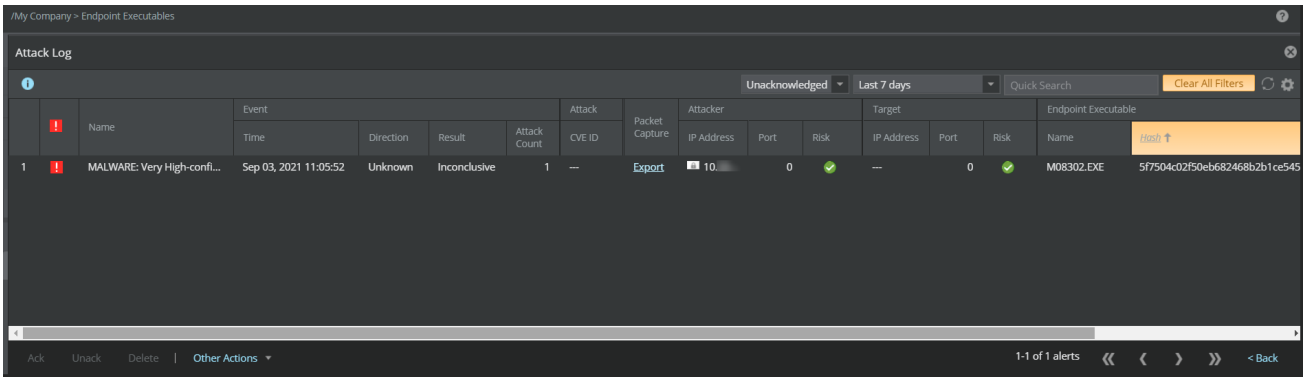
Table 14. Field descriptions of Applications tab

Field	Description
Application	Displays the name of the application
Risk	Displays whether the application is high, medium, or low risk. Trellix Advanced Research Center categorizes an application based on its vulnerability and the probability for it to deliver malware.
Category	Displays the category that the application falls under. For example, HTTP falls under the Infrastructure Services category.
Counts	• **Attacks** — Displays the number of attacks triggered by the executable during the selected timeframe • **Connections** — Displays the number of connections made by the executable during the selected timeframe

The **Search** field allows you to search by application name, risk, or category.

Double-click the application to view alerts related to the application in the Attack Log. The alerts are filtered based on the application selected. To close Attack Log, click **Back** or the icon.

Figure 198. Alerts based on the application selected



MITRE ATTACK view of attack details

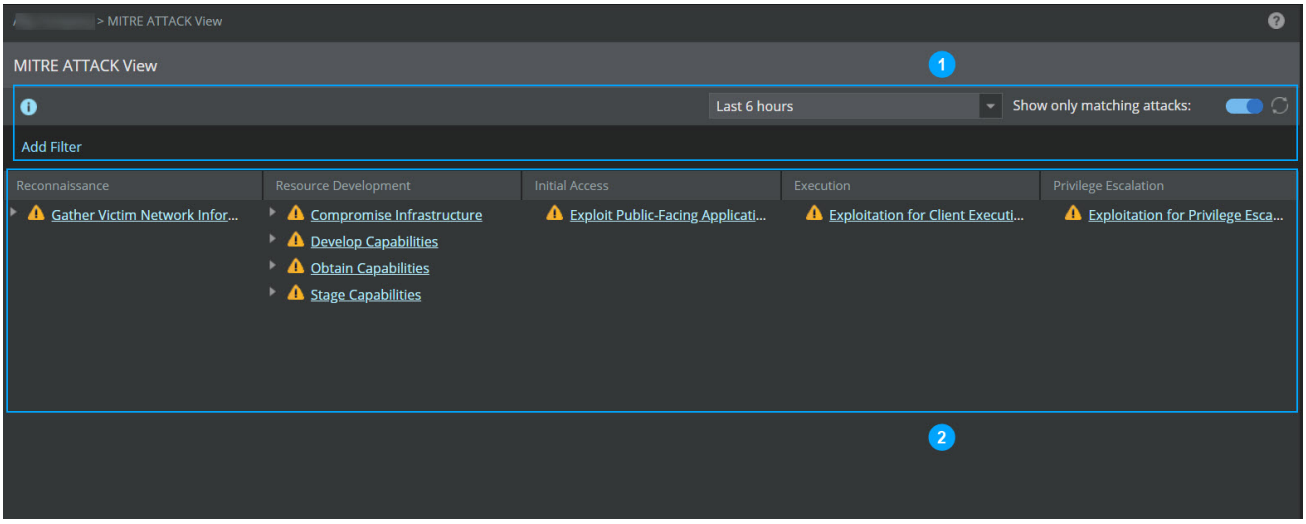
The Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) is a well-known and publicly available knowledge base developed by MITRE Corporation that highlights the tactics, techniques, and procedures (TTPs) used by cyber adversaries in different phases of attack lifecycle. These details are presented in the form of a matrix that showcases the tactics, techniques, and associated sub-techniques employed by cyber attackers in real-world scenarios.

The Analysis → <Admin Domain Name> → **MITRE ATTACK View** page in the Trellix IPS Manager provides a consolidated view of all adversarial tactics, techniques and sub-techniques in the MITRE ATT&CK matrix format for attacks detected on the network. It also provides users with further drill-down capabilities, such as applying filters based on the attack severity level or IP address, and delving into any specific technique/sub-technique to view only the attacks that fall under those categories. It thus can help in identifying security gaps, analyzing existing IPS policies, and strengthening network security for future.

NOTE

This page is not available in Trellix IPS Central Manager.

Figure 199. MITRE ATTACK View page



Callout	Description
1	Top menu
2	Grid view

The following options are available in the **MITRE ATTACK View** page:

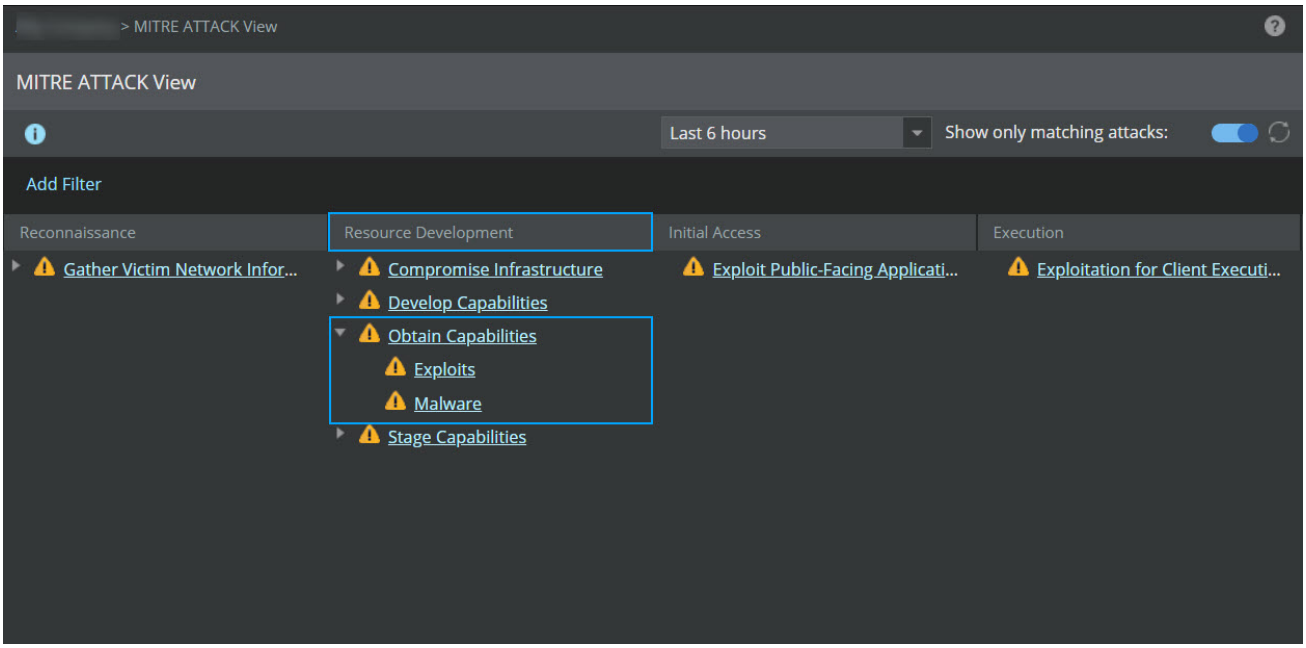
Options	Description
Top menu	
	This provides an overview of the **MITRE ATTACK View** page.
Time period	When this option is selected, it shows the tactics, techniques and/or sub-techniques associated with the attacks for the chosen time period. The minimum time is **Last 5 minutes**. The matrix data can be also filtered for any time period of your preference using the **Custom Time Period** option.
	Clicking this icon refreshes the page.
Show only matching attacks	This option comes with a toggle button with the following functionality: • When it is set to OFF, the page displays all tactics, techniques and sub-techniques available within the matrix including those for which matching attacks are found. Techniques and/or sub-techniques that are not associated with any alert are greyed out, whereas those mapped with any attack entries are hyperlinked and preceded with the  icon. Clicking on any hyperlink redirects you to the **Attack Log** page with that specific technique / sub-technique applied as filters. • When it is set to ON, the page displays the tactics and corresponding techniques and sub-techniques for only the matching attacks. Techniques and/or sub-techniques associated with any matching attacks are hyperlinked and preceded with the  icon. Clicking on any hyperlink redirects you to the **Attack Log** page with that specific technique / sub-technique applied as filters. **NOTE** This button is set to ON by default.
Add Filter	This option enables you to add a filter based on IP addresses and attack severity levels.

Grid view

The grid view of the **MITRE ATTACK View** page displays the MITRE ATT&CK matrix structure in which the adversarial tactics are organized as column headings. Cells appearing under each column are the techniques employed by cyber adversaries to achieve

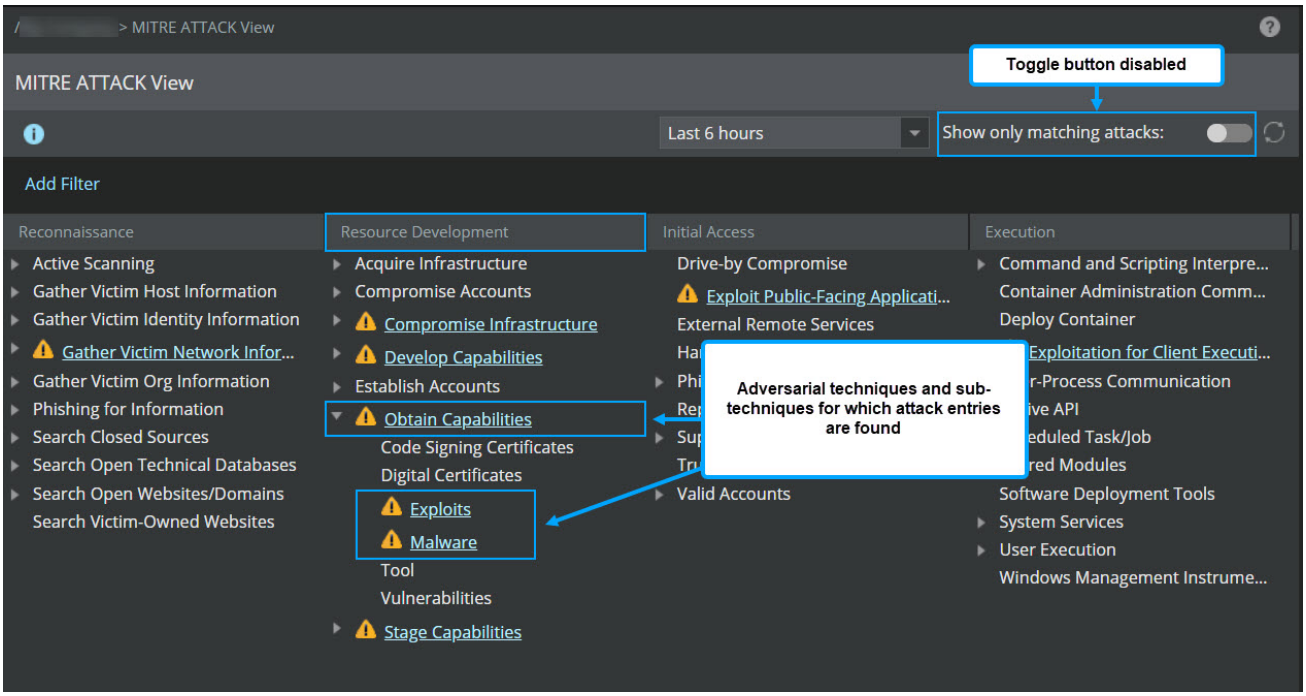
the tactical objectives. You can expand any technique to view the corresponding sub-technique(s), if any. The tactics, techniques and sub-techniques preceded with the ⚠ icon indicate the presence of attack entries. For example, the figure below shows the Mitre matrix view for all the matching attacks where we can see Obtain Capabilities as one of the adversarial techniques under the tactic column Resource Development. Expanding the technique reveal two corresponding sub-techniques - Exploits and Malware.

Figure 200. MITRE ATTACK View page showing techniques and sub-techniques for only matching attacks



When the **Show only matching attacks** toggle button is off, the page shows all the adversarial tactics, techniques and sub-techniques in which the hyperlinked entries for techniques and sub-techniques starting with ⚠ icon represent the matching attacks.

Figure 201. MITRE ATTACK View page showing all tactics, techniques and sub-techniques



The **MITRE ATTACK View** page can be customized by different options, such as sorting and filtering, which help drilling down into the attack details based on your requirement. The following options are available:

- **Sort Ascending**: You can sort all columns in the ascending order.
- **Sort Descending**: You can sort all columns in the descending order.

You can also apply filters based on IP address and/or attack severity levels. For more information, refer to the section Adding filters (page 486). For information on how to drill down on attacks in the **MITRE ATTACK View** page, refer to the section Analyzing attack details using matching tactic, technique, or sub-technique (page 487).

Adding filters

You can set filters based on your requirement in the **MITRE ATTACK View** page that provide you the capability to drill down into the attack details, learn more about the adversarial behavior, and nature of the cyber attack.

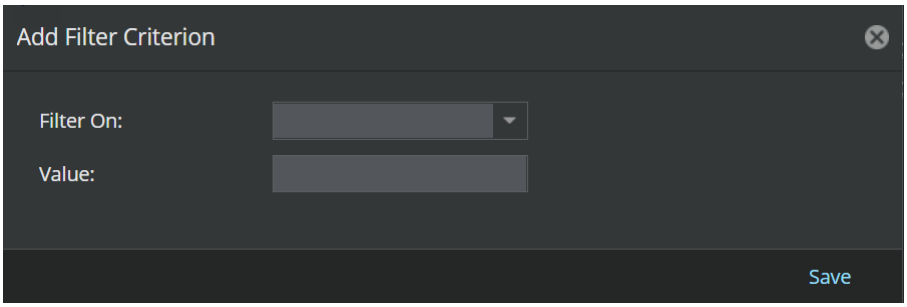
When you navigate to Analysis → <Admin Domain Name> → **MITRE ATTACK View**, it displays the matrix table and related data only for matching attacks for the time period set in the page. No filter criteria is set at this point of time. You can add one or more filters by performing the steps given below:

Steps:

1. On the **Analysis** tab, select the required domain from the **Domain** drop-down list in the left pane, and open the **MITRE ATTACK View** page.
2. Click Add Filter button.

   Add Filter Criterion dialog-box appears.

Figure 202. Add Filter Criterion dialog



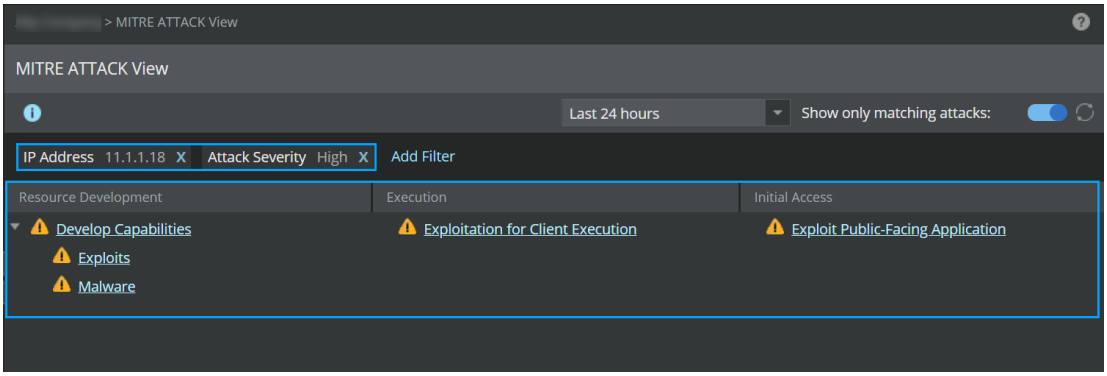
3. Enter the values in the following fields:
   - **Filter On** — Select **Attack Severity** or **IP Address** from the drop-down list.
   - **Value** — Enter the specific value as per the filter chosen. For **IP address** selected as the filter, you can manually enter any IPv4 or IPv6 IP address that you want to examine including attacker IP and target IP. For **Attack Severity** selected as the filter, you can choose **Informational**, **High**, **Medium** or **Low** from the **Value** drop-down list.

> **NOTE**
>
> You can apply one or more IP addresses or attack severity levels as filters.

4. Click **Save**.

   The page reloads and shows tactics, techniques, and sub-techniques in the Mitre matrix table format for the matching attacks based on the filter(s) applied. For example, the figure below shows the filtered data on the **MITRE ATTACK View** page after IP 11.1.1.18 and attack severity level **High** have been applied as filters.

Figure 203. The page view after applying IP and attack severity filters



Analyzing attack details using matching tactic, technique, or sub-technique

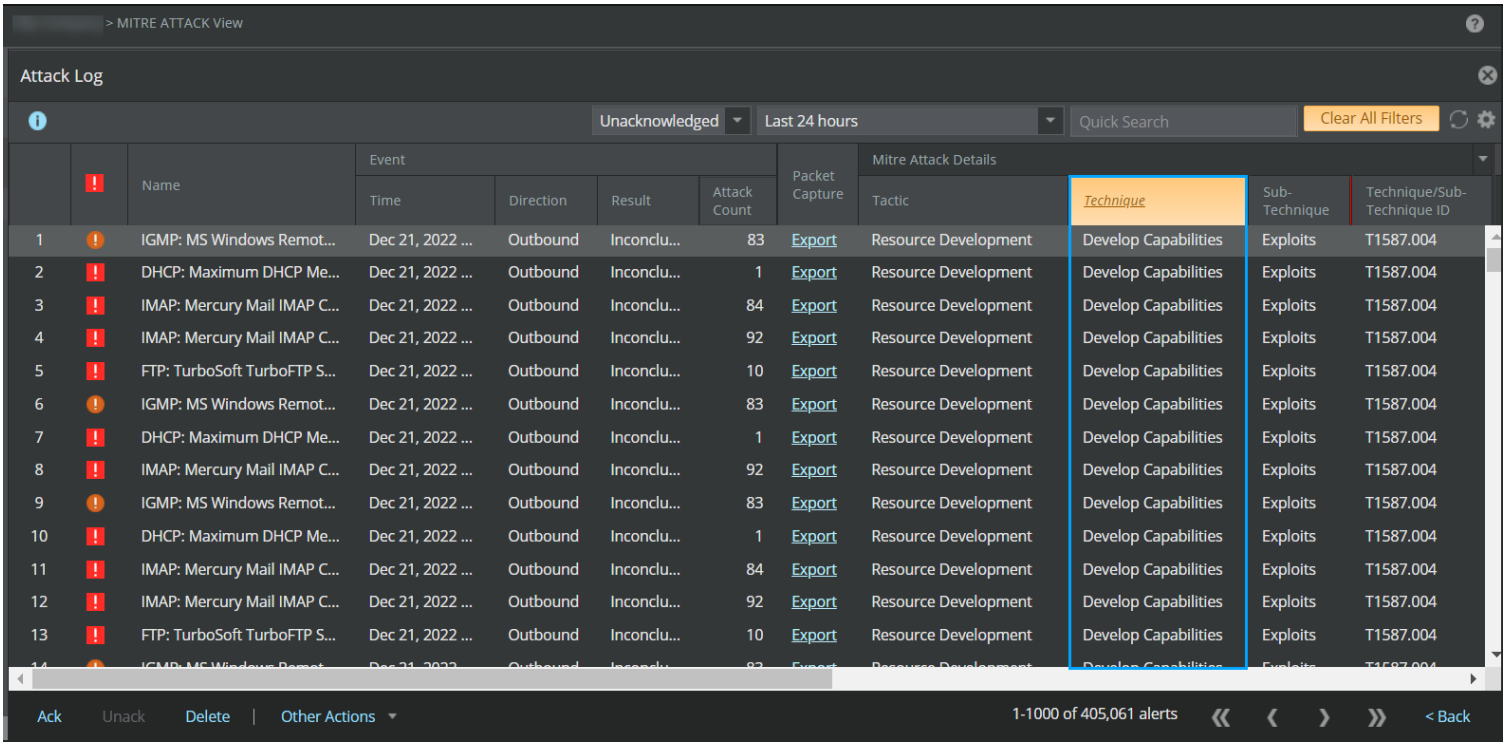
You can use any tactic, technique, and/or sub-technique displayed over the **MITRE ATTACK View** page to delve deeper into the attack data for further analysis. With the **Show only matching attacks** toggle button set to ON (default), the page displays all tactics as column headings within the grid view for which attack entries exist in the **Attack Log**. You can apply further filters (IP address and/or attack severity level) using the Add Filter button to get a more filtered and customized view of the adversarial tactics shown in the page.

Analyzing attack details using matching technique

Click any hyperlinked technique under a specific tactic column in the **MITRE ATTACK View** page for which you want to view the attack details. It will redirect you to the **Attack Log** page with the selected technique applied as the filter. The **Clear All Filters** button color in the **Attack Log** page changes to orange which indicates that the filter is active.

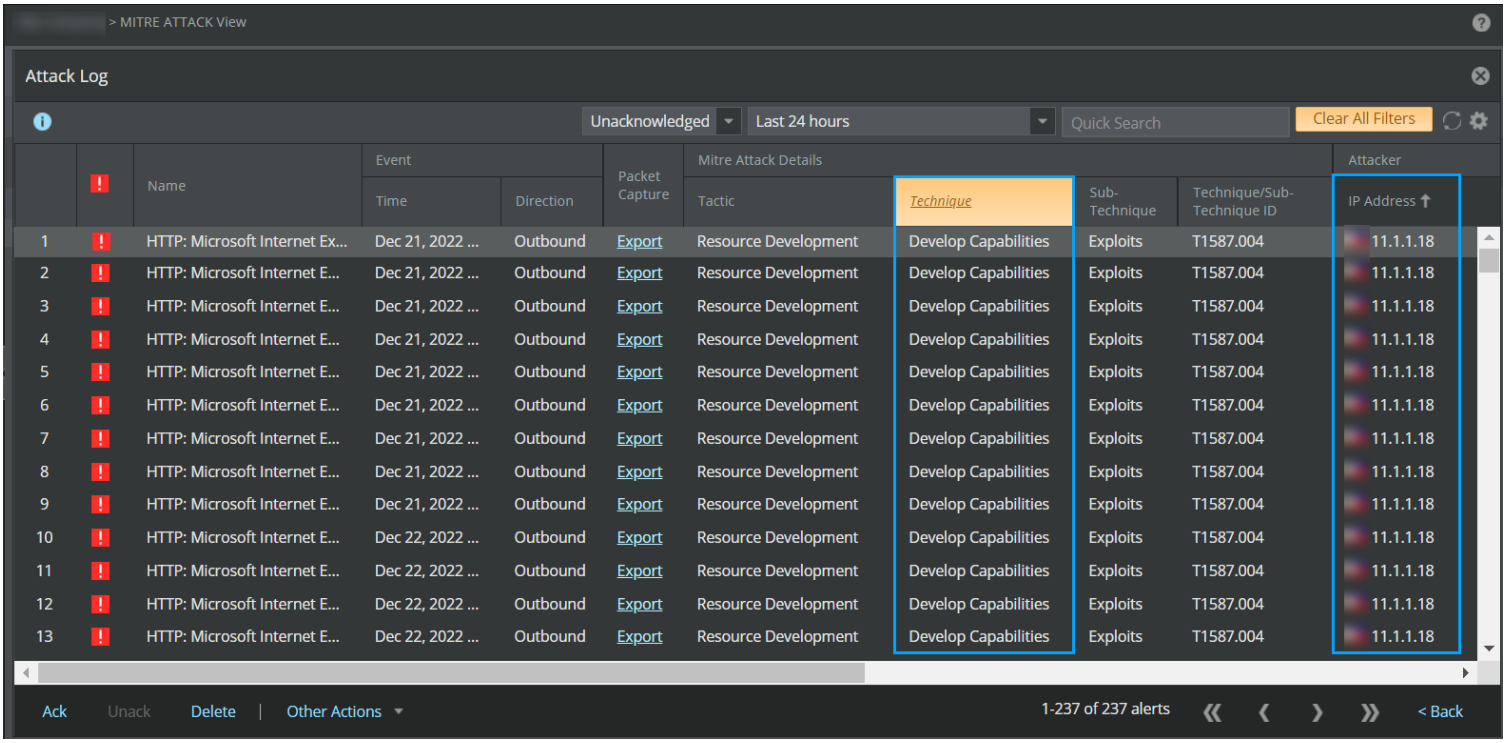
The figure below shows the **Attack Log** page view after clicking the hyperlinked technique Develop capabilities under the tactic Resource Development in the **MITRE ATTACK View** page.

Figure 204. Attack Log page view with technique filter



You can also apply the filters based on IP address and/or attack severity level in the **MITRE ATTACK View** page and then click any matching highlighted technique to view more filtered data in the **Attack Log** page. For example, the figure below shows the attack entries matching with technique Develop Capabilities and IP address 11.1.1.18 in the **Attack Log** page.

Figure 205. Attack Log page view with technique and IP filter

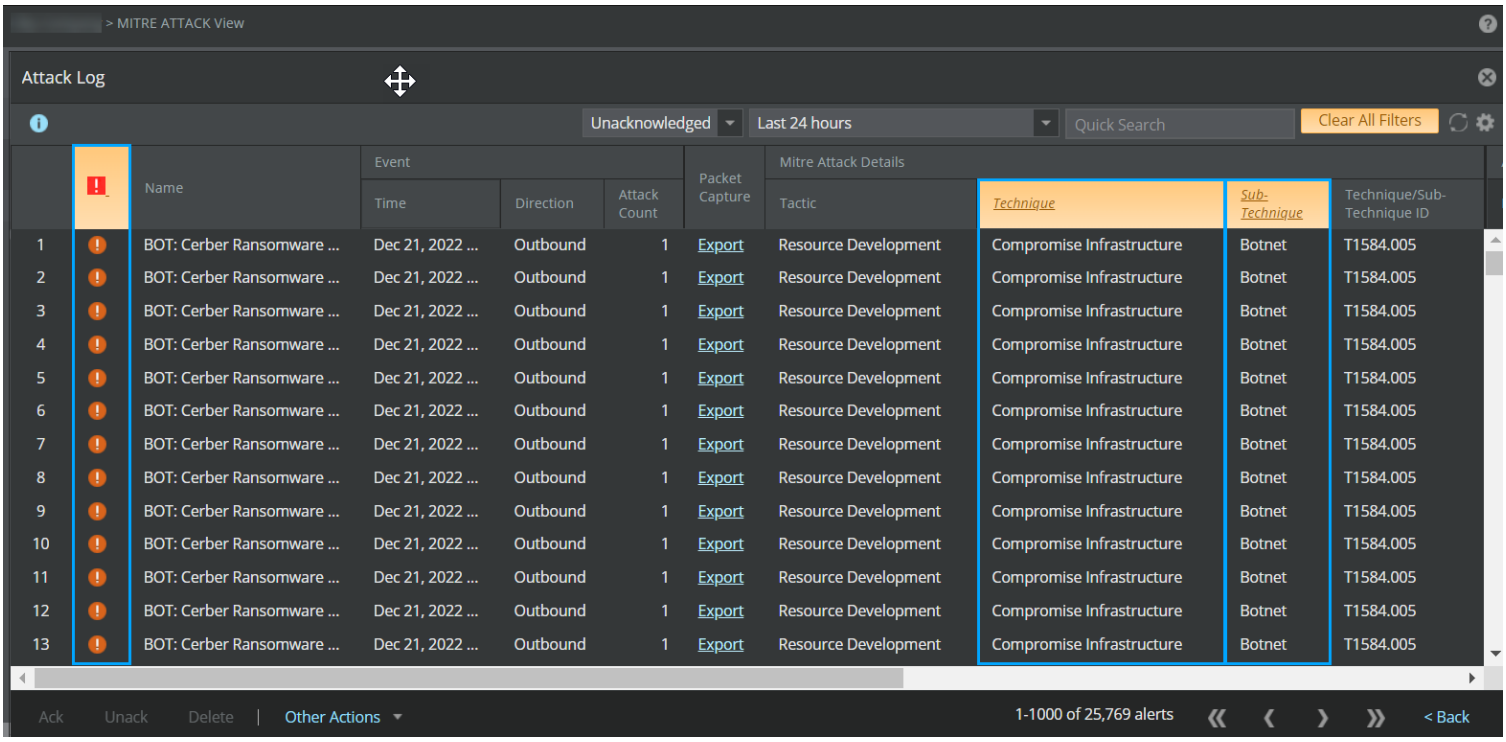


Analyzing attack details using matching sub-technique

Expand technique under a specific tactic column in the **MITRE ATTACK View** page to view the corresponding sub-technique(s) for which you want to view the attack details. You can then click any sub-technique of your preference. It will redirect you to the **Attack Log** page with the selected technique and sub-technique applied as filters.

You can also apply the filters based on IP address and/or attack severity level in the **MITRE ATTACK View** page to get more filtered attack entries in the **Attack Log** page. For example, when medium attack severity is chosen as filter in the **MITRE ATTACK View** page, clicking the hyperlink for sub-technique Botnet under the corresponding technique Compromise Infrastructure shows specific attack entries in the **Attack Log** page with the selected technique, sub-technique, and severity level applied as filters.

Figure 206. Attack Log page view with technique, sub-technique and attack severity filter



Note the following:

- You can further sort the filtered attack data by entering a keyword for any other applicable sub-technique, technique/sub-technique ID, IP address, or any other attributes in the **Quick Search** field. You can also apply filters for the same in the column level.
- You can select any specific entry in this page and perform same actions as you can perform in Analysis → <Admin Domain Name> → **Attack Log**.
- Mitre-based attack details are not shown for older alert data.

You can export and save the list of filtered data as a PDF file or CSV file from the **Attack Log** for future reference. To export, click **Other Actions**, select **Save Attack Log as**, and click the format in which you want the filtered data to be exported.

Click < Back or icon to close the **Attack Log** and go back to the **MITRE ATTACK View** page.

Event reporting

Next Generation reports

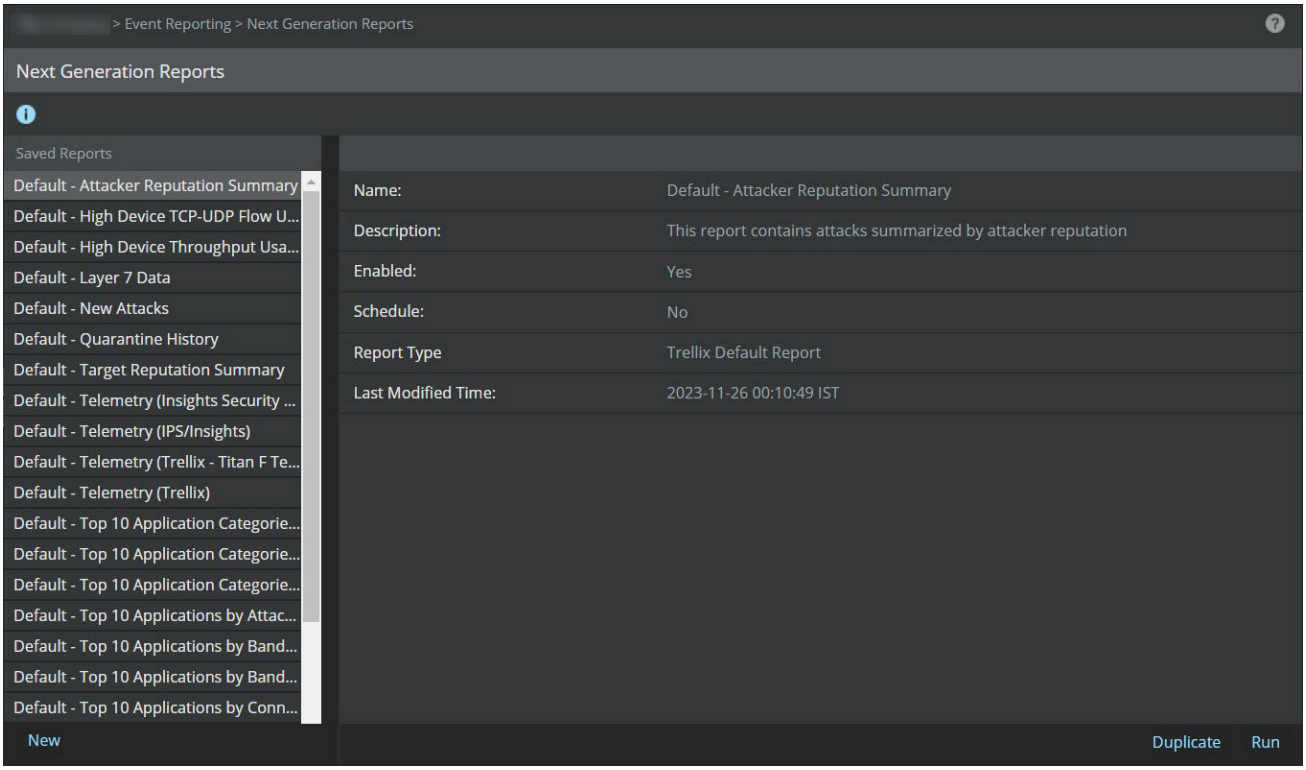
The Next Generation report option allows you to generate customized reports. You can make selections, such as the type of data to base the report on, and the format in which you want the data to be presented such as table, bar chart, and pie chart. From a list of fields that are applicable for a report, you can select the fields that you want to display; you can also specify the conditions that must be met to include the information for those fields in the report.

You can then save the query that you have just built for later use. You can also generate the report immediately or schedule it to run automatically by setting options like the period to be considered for displaying data, report output format etc.

Next Generation reports can be generated from the Analysis → Event Reporting → **Next Generation Reports** option in the Manager.

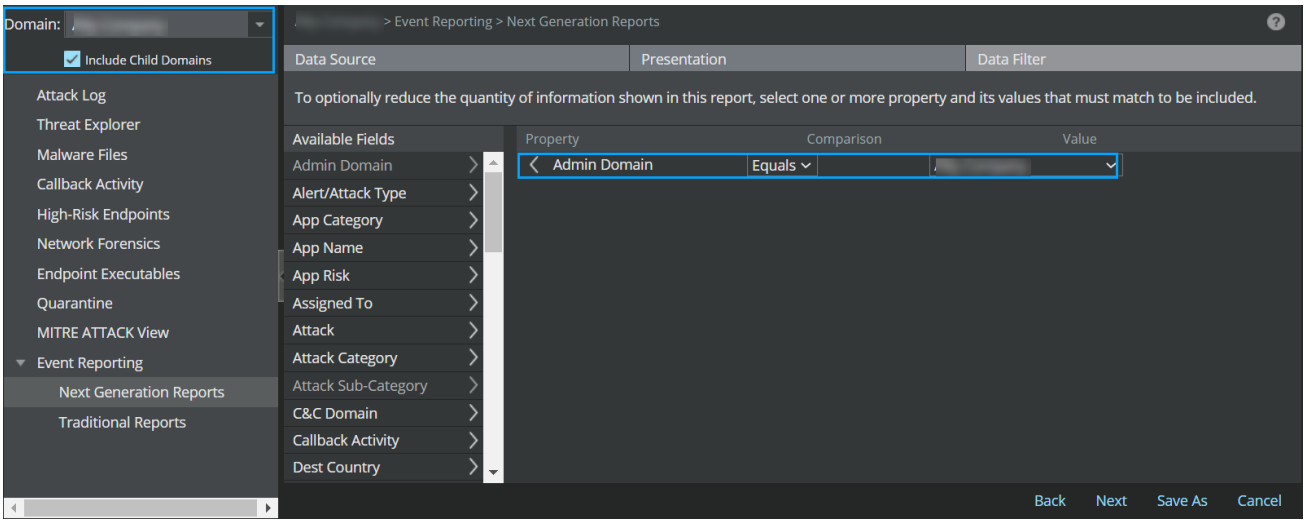
The **Next Generation** page displays the **Saved Reports** in the left pane by default.

Figure 207. Next Generation page



This figure shows the difference between the admin domain filter available in the left pane, and the admin domain filter available for some reports.

Figure 208. Admin domain filters



1 — This admin domain filter has no impact on the reports generated.

2 — This is the admin domain filter that you can use to generate the report based on the admin domain selected.

Next Generation saved reports

The **Saved Reports** panel lists three types of saved reports:

- **Trellix Default Report**— These are reports that are listed by default which can only be duplicated and run but cannot be edited or deleted.
- **Derived from Report "{report name of Trellix Default Report}"**— These are reports that are duplicates of Next Generation Default Reports. The duplicated reports can be edited as well as deleted. Note that editing is restricted to modifying the data filter options that is, you can edit the data filters but not the report presentation options.
- **User Defined Report**— These are reports, which are created when you click New from the main screen of Next Generation Report. In a User Defined report, you can define the data filter options as well as the report output display preferences (such as whether the report should be generated as a bar chart or a pie chart etc.)

Next Generation default reports

The Next Generation default report options are available as follows:

Table 15. Telemetry reports

Report Name	Description
Default - Telemetry (Insights Security Posture)	The telemetry information sent by the Manager to the Trellix Insights when Insights integration is enabled. **NOTE** This information is used to derive the security posture score on Trellix Insights.
Default - Telemetry (IPS/Insights)	The information sent by the Manager to the Trellix IPS product team and Trellix Insights team when telemetry is enabled
Default - Telemetry (Trellix)	The information sent by the Manager to the Trellix corporate team when telemetry is enabled
Default - Telemetry (Trellix - Titan F Telemetry Server)	The information sent by the Manager to the Titan F telemetry server when telemetry is enabled

Applications-related reports

For any Applications-related report to show data, you must enable Application Identification on the required Monitoring ports for the time period that you query. For example, if you want to run the Top 10 Application Categories by Attack Count report for the traffic monitored between 9 am and 10 am today, you must have enabled Application Identification on the corresponding monitoring ports between 9 am and 10 am today based on the Manager server's clock.

Table 16. Reports and Descriptions

Report Name	Description
Default - Top 10 Application Categories by Attack Count	Run this report to view the top 10 Categories based on the attacks generated per category. Like other Next Generation reports, this too displays information in graphical and tabular formats. The following are the information that you can find in this report: • For each of the top 10 categories, the bandwidth consumed, the number of flows, and the number of attacks generated per category. • The applications detected for each of the top 10 categories. For example, if web mail is one of the top 10 categories, it lists all the web mail applications that were detected. If an application belongs to multiple categories within the top 10, it is listed under each of those categories. • For each application, the bandwidth consumed, the number of flows, and the number of attacks generated.
Default - Top 10 Application Categories by Bandwidth Usage	This report is similar to the Top 10 Application Categories by attack count except that the details are based on the bandwidth consumed.
Default - Top 10 Application Categories by Connection Count	This report is similar to the Top 10 Application Categories by attack count except that the details are based on the number of connections or flows.
Default - Top 10 Applications by Attack Count	Run this report to view the top 10 Applications based on the number of attacks that each application was involved. The following are the information that you can find in this report: • Risk— Whether the application is high, medium, or low risk. Trellix ARC categorizes an application based on its vulnerability and the probability for it to deliver malware. • Bandwidth— The network bandwidth consumed by each application. • Connection count— The number of flows per application. • Attack count— The number of attacks that each application was involved. This report is sorted based on the attack count.
Default - Top 10 Applications by Bandwidth Usage for All Risk Levels	This report is similar to the Top 10 Applications by attack count except that it is based on the bandwidth consumed by each application.
Default - Top 10 Applications by Bandwidth Usage for Each Risk Level	This report provides the top 10 applications in each risk category based on the bandwidth consumed per application. That is, it lists the top 10 high-risk applications based on bandwidth consumed by each of those applications. Similarly, it lists the top 10 medium and low-risk applications in separate tables.
Default - Top 10 Applications by Connection Count	This report is similar to the Top 10 Applications by attack count except that it is based on the number of connections per application.

NOTE

For the applications-related reports to show data, you must enable Application Identification.

The Default Next Generation reports show information from all the Sensors for which you have enabled Application Identification. To view the details from specific Sensors, you can generate a Next Generation Duplicate report or a Next Generation User Defined Report.

Table 17. Device Performance - Hourly reports

Report Name	Description
Default - High Device TCP / UDP Flow Usage	Status of TCP/UDP flow utilization
Default - High Device Throughput Usage	Status of Sensor throughput utilization threshold

Table 18. NTBA Data Query reports

Report Name	Description
Default - Top Files Accessed	This report shows the most accessed files in the network during the selected period.
Default - Top Most Recently-Active Endpoints	This report shows the endpoints most recently active on the network.
Default - Top Endpoint Summary	This report shows the summary detail for endpoints in the network during the selected period.
Default - Top Endpoints by Bandwidth Usage	This report shows endpoints sending/receiving the most bytes in the network during the selected period.
Default - Top Endpoints by GTI Reputation	This report shows the endpoints with the Highest GTI Reputation in the network during the selected period.
Default - Top Endpoints by Threat Factor	This report shows the endpoints sorted by Threat Factor during the selected period.
Default - Top New Applications Seen	This report shows the applications that are new on the network during the selected period.
Default - Top New Services Seen	This report shows services that are new on the network during the selected period.
Default - Top New Endpoints Seen	This report shows the endpoints that are new on the network during the selected period.
Default - Top Services by Bandwidth Usage	This report shows services consuming the most bandwidth (bytes) in the network during the selected period.
Default - Top Applications by Bandwidth Usage	This report shows applications consuming the most bandwidth (bytes) in the network during the selected period.
Default - Top Most Recent Connections	This report shows connection summary in the network during the selected period.
Default - Top 10 Exporter Interfaces	This report lists the Exporter interfaces that were high on traffic during the selected period.

Report Name	Description
Default - Top 10 Conversations	This report lists conversations that were high on traffic during the selected time period. The report displays the following fields: • **Source IP Address** - IP address of the source host • **Destination IP Address** - IP address of the destination host • **Service Name** - Name of the service used by the conversation • **In Bytes** - Inbound traffic in bytes • **Out Bytes** - Outbound traffic in bytes • **Total Bytes** - Total traffic in bytes • **Utilization %** - Bandwidth utilization percentage
Default - Top 10 Endpoint Executables	This report lists conversations that were high on traffic during the selected time period.
Default - Endpoint Executable Details	This report shows the details of all the executables on the network during the selected time period.

Run Next Generation default report

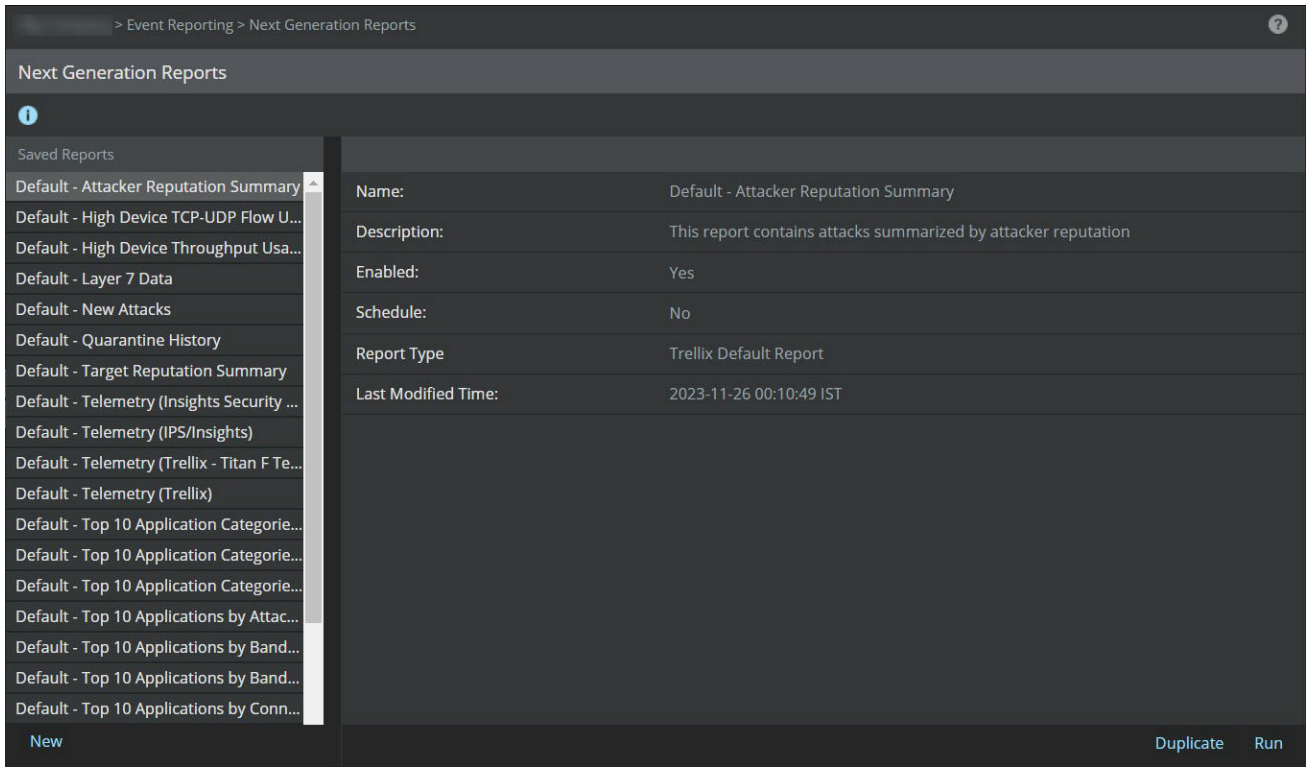
1. Select Analysis → Event Reporting → Next Generation Reports.

   The **Next Generation Reports** page is displayed. The available reports are listed in the left pane.

2. Select the report that you want to run among those listed in the **Saved Reports** pane.

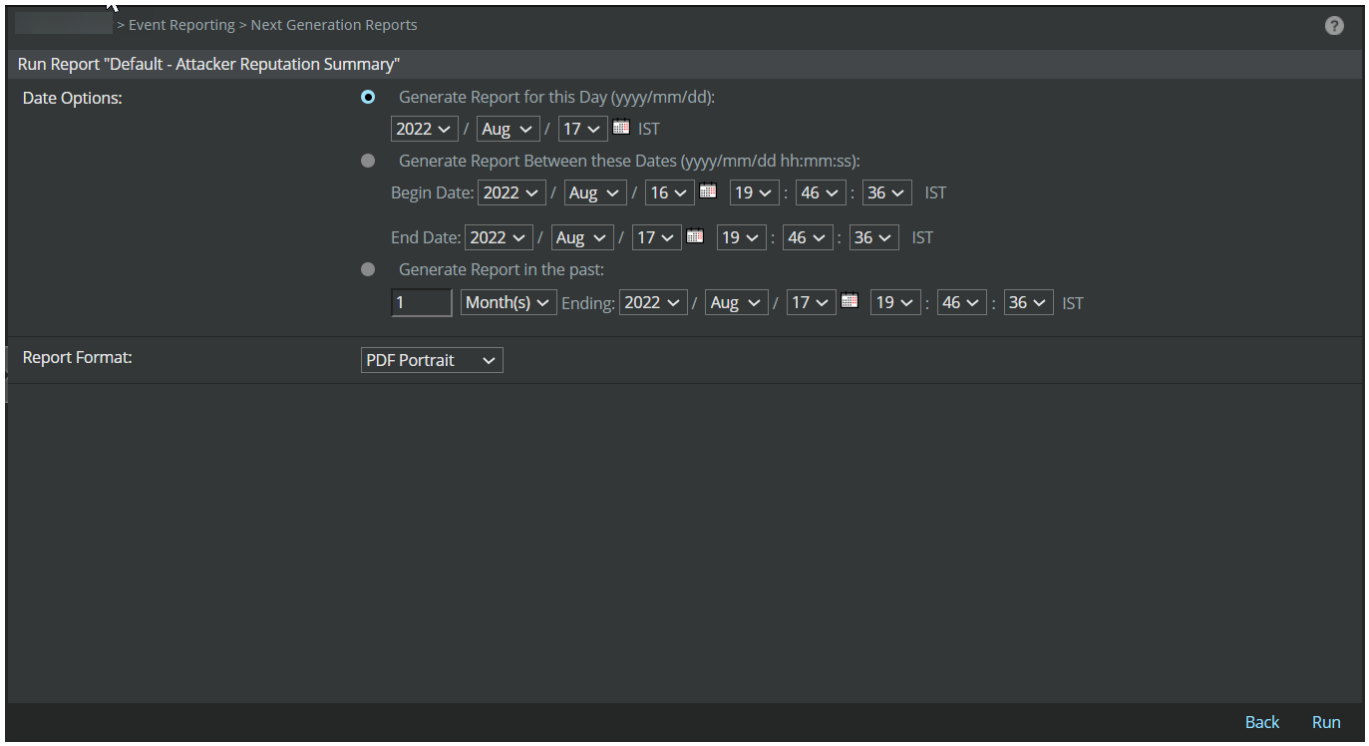
   For example, select **Default - Attacker Reputation Summary** report in the left pane. The details of the report are listed in the right pane.

Figure 209. Next Generation Saved reports



3. Click **Run**. The Run Report page is displayed.

Figure 210. Run Reports page



4. Select the **Date Options**. [Query for the day or between two dates, or for the specified period (number of months or weeks or days or hours.)]
5. Select the **Report Format**. (**HTML** or **PDF Portrait** or **PDF Landscape**, **Save as CSV** or **Save as HTML**.)
6. Click **Run**. For HTML and PDF options, the report is displayed in the Manager. For Save as CSV and Save as HTML, use the File Download option to save the report.

Create Next Generation duplicate reports

The Manager allows you to create duplicate reports of the Default Next Generation reports. The parameters for the duplicated report can then be edited to suit your requirements.

To create a duplicate report, do the following:

1. Select a Next Generation default report and click **Duplicate**.
2. Enter the Name and Description (mandatory fields) and click **OK**.
3. The duplicate report is displayed under Next Generation **Saved Reports** section.
4. Click Edit to change the parameters.
5. Select a row in the left panel to view the Data Fields options.

> **NOTE**
>
> The admin domain selected in the left pane has no impact on the reports generated. The admin domain data filter selected is explicitly to filter the reports that are generated.

6. Click Save As to save the change made.
7. In the Save Report page, you need to enter a Name and Description for the Query. You can also select the following options in the Save Report:
   - Automate Report Generation
   - Report Frequency
   - Select events to display
   - Report Format
8. Select Next.

   Select Recipients page is displayed.
9. Click New to add a recipient through the Add Recipient dialog.
10. Click Finish to complete the process and Next Generation Reports main page is displayed.

Generate Next Generation user defined reports

You can create a new report with a choice of data source, presentation and filter.

1. Navigate to Analysis → Event Reporting → **Next Generation Reports**. Click **New**.

   You need to select the data sources for the report. Data source represent the database tables from where information is retrieved to generate the report. The following are the options for data source: **Alert Data, Application Data, Endpoint Data,** and **Performance data**.

2. Click **Next** to set the display options for the report. Report can be displayed as a Table, Bar Chart, or Pie Chart.
3. Click **Next**.
4. Select the columns of choice that you want to include in the report output by selecting rows in the left panel.
5. Click **Next**.
6. Select a row in the left panel to view the Data Filter options.

   You can enhance the filter options for the fields selected in step 4 from the **Available Fields** options. Use the > and < options to add or remove conditions.

   NOTE

   The admin domain selected in the left pane has no impact on the reports generated. The admin domain data filter selected is explicitly to filter the reports that are generated.

   When you finish the selections, you can save your report query using **Save As**.
7. In the **Save Report** page, you need to enter a **Name** and **Description** for the Query.

   You can also select the following options in the Save Query:

   - Automate Report Generation
   - Report Frequency
   - Select events to display
   - Report Format
8. Click **Finish** to save the query.
9. The report is saved and displayed in the **Saved Reports** section of the **Next Generation Reports** page.
10. Select the report, and then click **Run** to view the **Run Query**.
11. In the **Run Query**, enter the **Data Options** and the **Report Format**.

    Click **Run**, to run the report query. The generated report is displayed in the selected report format.

    When the Bar Chart display option is selected, the output contains both the bar chart and table. If you select the Pie Chart option, the Pie Chart and the table are displayed. If there are no alerts, only the table is displayed.

    Data Display Order:

Table Type	Bar Chart	Pie Chart	Table Only
Alert information table	Data is displayed in descending order	Data is displayed in descending order	Data is displayed in ascending order

    Once the User Defined Report is saved, you cannot change its data source.

    NOTE

    In the case of Host Event Table all table information (only table/table with bar chart/ table with pie chart) is displayed in an ascending order.

NOTE

The **New** option is not supported for NTBA Generated Reports. User can either run it or duplicate and modify some of the conditions in the query.

Generate period-specific reports on device performance

Follow this procedure to generate a period specific Next Generation report on device performance.

Steps:

1. Navigate to Analysis → <Admin Domain Name> → Event Reporting → **Next Generation Reports**.
2. .Click New at the bottom of the left pane.
3. Select Application Data and select the option Hourly in the Data Source page.

   Daily, weekly and monthly period specific reports can be generated by selecting the option Daily, Weekly or Monthly.
4. Click Next.
5. Click the Table option under Display Options and click Next.

   Click the desired fields in the Available Fields pane to move it to the Selected Fields pane (You can click the left / right arrow on each columns to change the position of the column. You can click X on each column to remove the column). Click Next.
6. Click the properties listed on the left pane and move them to the right pane to reduce the quantity of information shown in the report. Click Next to select the date option in the next page, click Save As to save the report.
7. Select one of the Date Options (either query for the day or between two dates or for a selected period in the past). Select the report format (HTML, PDF Portrait, PDF Landscape, Save as CSV or Save as HTML) and click Finish.
8. To generate the report, select the report created in the left pane and click Run. The hourly report is generated.

Generate Applications Next Generation user-defined reports

Prerequisites:

This section assumes that you are familiar with terms related to Application Identification and how this feature works.

Make sure you have enabled Application Identification on the required Monitoring ports for the time period that you want to run the report.

Follow this procedure to generate Applications Next Generation user-defined report.

Steps:

1. In the Manager, select Analysis → Event Reporting → **Next Generation Reports**.
2. Click New and select Application Data.
3. Specify how you want the data to be consolidated in the report (Hourly |Daily | Weekly | Monthly).

   Consider that you select weekly, and generate the report for a two weeks' time period, and FTP is one of the applications detected. Then, the details for FTP is shown separately for each of those two weeks. Similarly, the details are shown for all the detected applications during those two weeks.

4. To view the report in a tabular format, select Table as the Display Option and click Next.
   a. Select Application Name, Category Name, or Risk as the first column.
   b. Select Attack Count, Bandwidth Usage, or Connection Count as the second column.
   c. If required select Start Time as the third column.
   d. Click Next and go to step 7.
5. To view the details in a bar chart and a tabular format, Select Bar Chart as the Display Option and click Next.
   a. Select Application Name, Category Name, or Risk as the Bar label.
   b. Select Attack Count, Bandwidth Usage, or Connection Count as the Bar value.
   c. Click Next and go to step 7.
6. To view the details in a pie chart and a tabular format, Select Pie Chart as the Display Option and click Next.
   a. Select Application Name, Category Name, or Risk as the Pie slice label.
   b. Select Attack Count, Bandwidth Usage, or Connection Count as the Pie slice value.
   c. Click Next.
7. In the Data Filter section, click on the right arrow next to the Admin Domain and select the required Admin Domain name from the Value drop-down.

   The Value drop-down for Admin Domain lists only those domains that have Sensors assigned to them. Admin domains that have no Sensors but only dedicated Monitoring ports are not listed.
8. To include data only from specific Sensors of the selected Admin Domain, click on the right arrow next to Sensor. To include data from all the Sensors of the selected Admin Domains, you do not need to add the Sensor row.

   NOTE

   The admin domain selected in the left pane has no impact on the reports generated. The admin domain data filter selected is explicitly to filter the reports that are generated.
9. Select the comparison value (equals or does not equal) and the Sensor name.
10. Add another row for Sensor, if required.
11. Click Next.
12. Select one of the Date Options (either query for the day or between two dates or for a selected period in the past). Select the report format (HTML, PDF Portrait, PDF Landscape, Save as CSV or Save as HTML).
13. Run the report immediately or save it for later use.

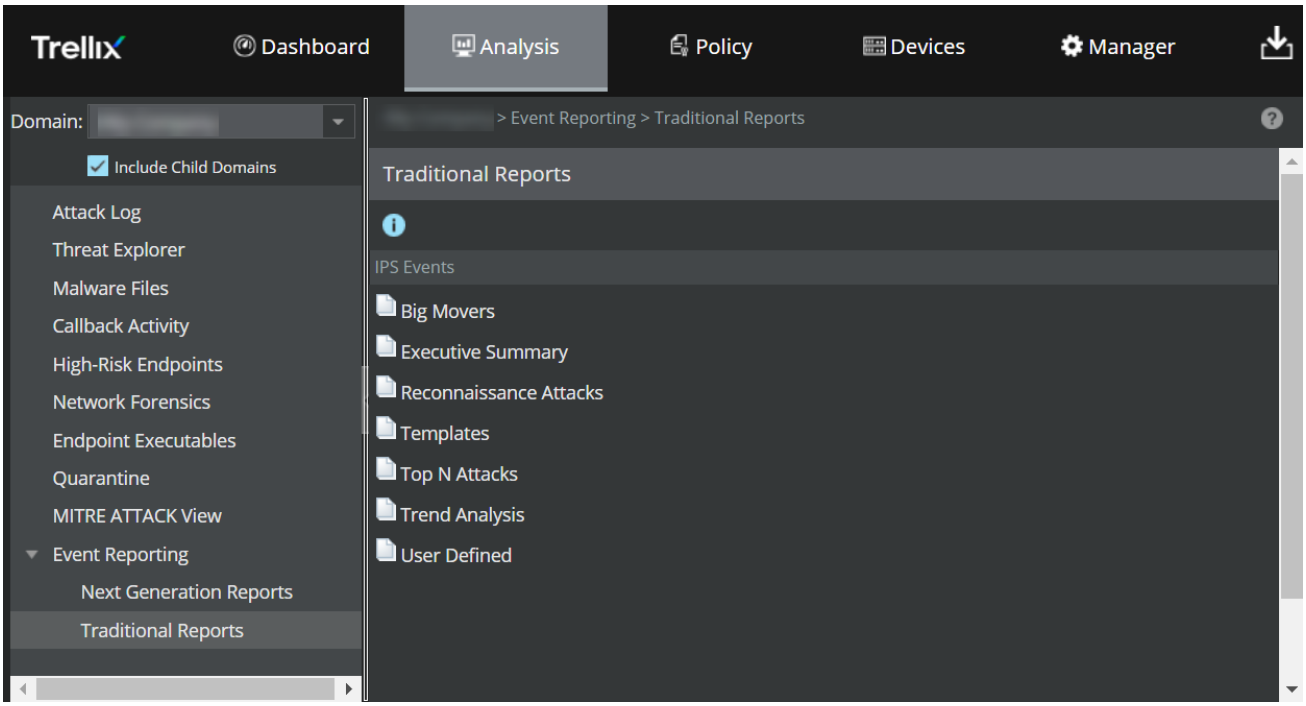
    If you save the report, it is listed along with the other saved Next Generation reports. You can run it like how you would run any of the Next Generation reports.

Traditional Reports

Traditional Reports are based on pre-defined conditions and provide information on the alerts generated by your Sensor. The generated alert information can include source and destination IP of the attack, time when the attack occurred, Sensor that detected the attack, and so forth. The various IPS Reports provide concentrated views according to the specific parameters of each report. Each report lists alerts from most to least common detected. All IPS Reports can be viewed in either HTML or PDF or CSV format. The **Executive Summary** and **Top N** reports can also be viewed in bar graph or pie chart format.

You can also schedule the IPS Reports and the Audit report so that they are automatically generated at the specified times.

Figure 211. IPS Events in Traditional Reports home

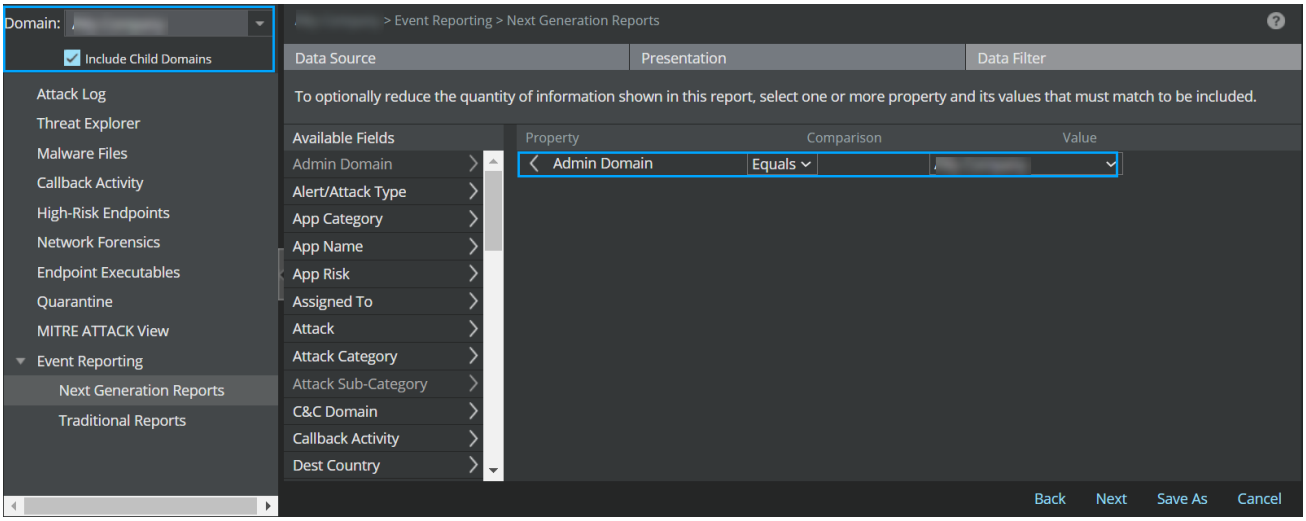


The available IPS Reports are:

- Big Movers Report — Provides a comparison view of attacks that occurred in recent time interval with those that occurred in a pervious time interval.
- Executive Summary Report — Provides a summary view of selected alert data presented in a variety of tables, graphs, and charts.
- Reconnaissance Attacks Report — Presents reconnaissance alerts during a specified time.
- Templates — Enables you to create custom IPS report templates that you can run on-demand at a later time, as well as manage the report templates you created for **Scheduled Reports**.
- Top N Attacks Report — Lists a specific number of alerts in order of frequency for one of four defining categories (for example, source IP address, most common attacks).
- Trend Analysis Report — Presents alert data based on common trends per specified frequency (for example, number of high severity alerts per hour for one day).
- User-Defined Report — Presents alerts based on a variety of defining parameters including interface, application protocol, and direction of alert.

This figure shows the difference between the admin domain filter available in the left pane, and the admin domain filter available for some reports.

Figure 212. Admin domain filters



1 — This admin domain filter has no impact on the reports generated.

2 — This is the admin domain filter that you can use to generate the report based on the admin domain selected.

Generate Big Movers reports

The Big Movers report is a comparison report of attacks occurred in recent time interval with those occurred in a pervious time interval. This is more clear because Recent time interval, and Previous time interval settings can be set in the UI.

You can define the time intervals of the two time periods and get a detailed report of attacks with percentage and direction.

Steps:

1. Select Analysis → Event Reporting → **Traditional Reports**.

   The **IPS Events** page is displayed.
2. Click the **Big Movers** link.
3. Select the required fields you need to configure:
   - **Admin Domain** — Select the admin domain in which to view alerts.

     NOTE

     The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.
   - **Sensor**
     - **All Devices** is checked by default. This displays information of all devices present at the selected Admin domain. To select your preference of devices, de-select **All Sensors** and select the devices from the list box.
     - **Include Child Admin Domains** — Displays device information for child domains.

- **Attack Severity** — Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities, which relate to attack impact.
- **Recent Time Interval** and **Previous Time Interval** — Enter the time period.
- **Ranking Basis** — Select one of the following:
  - Percentage change in attack count
  - Change in attack account value
- **Direction** — Select one of the following directions of how alerts occurred should be displayed:
  - Upward Movers only
  - Upward and Downward Movers
  - Downward Movers only
- **Maximum Movers** — Enter the value of maximum occurred alerts to be displayed.
- Select the **Report Format**.

4. Click **Run Report**.

   The report is displayed with attack details if any.

Generate Executive Summary reports

The Executive Summary report provides a summary view of alerts presented in a variety of tables, graphs, and charts. The alert information displayed results from filling out the report form by a narrowing set of parameters. The resulting report is a detailed snapshot of the most common parameters found in detected attacks.

> **TIP**
>
> This report is best used for displaying general alert information for the most common parameters in a presentation-style format.

Steps:

1. Select Analysis → Event Reporting → **Traditional Reports**.

   The **IPS Events** page is displayed.
2. Click the **Executive Summary** link.
3. Fill in the following fields to narrow your report:
   - **Admin Domain**— Select the admin domain in which to view alerts.

     > **NOTE**
     >
     > The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

   - **Sensor**:
     - **All Devices** is checked by default. This displays information of all devices present at the selected Admin domain. To select your preference of devices, de-select **All Devices** and select the devices from the list box.

    - **Include Child Admin Domains**— Displays device information for child domains.
- **Attack Severity**— Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities, which relate to attack impact.
- **Relevance**— Select one or more from the options, which is related to vulnerability relevancy.
- **Show Only Blocked Attacks?**— Select **Yes** to view alerts that indicate attacks blocked by the device. The default for this field is **No**.
- **Alert State**— Select one of the following to narrow the alerts:
    - **View unacknowledged alerts**— All unacknowledged alerts in the system for the specified time frame. If you have acknowledged alerts during your selected time range, this option suppresses those alerts.
    - **View all alerts**— (Default) both acknowledged and unacknowledged alerts for the specified time frame.
- **NSLookUp**— This feature lists the host name with the IP address in the generated report. The host names are retrieved using either the Source IP address, Destination IP address or using Both.
- For **Attacks**, choose one of the following time spans:
- **Select Attacks for this Day**— Format is **yyyy/mm/dd**. Default is Manager server system date.
- **Select Attacks Between these Dates**— Format is **yyyy/mm/dd hh:mm:ss**. Default **Begin Date** is "oldest alert detected time" and default **End Date** is Manager server system time.
- **Select Attacks in the past**— Selects alerts from a point in the past relative to the current time. This time in the past can be months, weeks, days (Default), or hours. Type a time (**yyyy/mm/dd hh:mm:ss**) when the span of reporting time ends (default is Manager server system time).

4. Enter the number of most frequent attacks (**Get summary of**) to view. A valid entry is between 1 and 20.
5. Select the **Sort By Attack Severity** check box to include the attack severity.
6. Select **Attack Count Per Relevance** or **Top N Source/Destination IP Pairs** to include information about vulnerability relevance and source/destination IP addresses, respectively.
7. Select the **Report Format**.
8. Click **Run Report**.

Generate Reconnaissance Attacks reports

The Reconnaissance report provides a summary of all reconnaissance (scans, sweeps, probes) attacks detected during a specified time frame.

> **TIP**
>
> This report is best used for analyzing only reconnaissance attacks detected by your device.

Steps:

1. Select Analysis → Event Reporting → **Traditional Reports**.

   The **IPS Events** page is displayed.

2. Click the **Reconnaissance Attacks** link.
3. Fill in the following fields to narrow your report:
   - **Admin Domain** — Select the admin domain in which to view alerts.

     NOTE

     The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

   - **Sensor**:
     - **All Devices** is checked by default. This displays information of all devices present at the selected Admin domain. To select your preference of devices, de-select the **All Devices** and select the devices from the list box.
     - **Include Child Admin Domains** — Displays device information for child domains.
   - **Attack Severity** — Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities, which relate to attack impact.
   - **Alert State** — Select one of the following to narrow the alerts:
     - **View unacknowledged alerts** — All unacknowledged alerts in the system for the specified time frame. If you have acknowledged alerts during your selected time range, this option suppresses those alerts.
     - **View all alerts** — (Default) both acknowledged and unacknowledged alerts for the specified time frame.
   - Choose one of the following time spans:
     - **Select Attacks for this Day** — Format is **yyyy/mm/dd**. Default is Manager server system date.
     - **Select Attacks Between these Dates** — Format is **yyyy/mm/dd hh:mm:ss**. Default **Begin Date** is "oldest alert detected time" and default **End Date** is Manager server system time.
     - **Select Attacks in the past** — Selects alerts from a point in the past relative to the current time. This time in the past can be months, weeks, days (Default), or hours. Type a time (**yyyy/mm/dd hh:mm:ss**) when the span of reporting time ends (default is Manager server system time).
4. Select the **Report Format**.
5. Click **Run Report**.

Generate Top N Attacks reports

The Top N report enables you to view alerts by count, for example the 10 most frequently detected attacks, during the designated time frame. The key field, **Desired Number ('N') of Attack Instances** for a certain parameter type, limits the number of different attacks to view. This field is in addition to those present in the Executive Summary report. For example, if you set the desired number to **10** and select the parameter to **Attack**, only the ten most frequently detected attacks are listed by attack name and the number of times the attack has been detected in the specified time frame.

The Top N report provides four viewing formats rather than just the three standard formats (HTML and PDF or Save as CSV). With Top N, you can supplement your view with alert information presented in bar and pie chart formats.

TIP

This report is best used for analyzing the most common attack type, source IP, destination IP, or source/destination IP pair found in alerts during a specific time frame.

Steps:

1. Select Analysis → Event Reporting → **Traditional Reports**.

   The **IPS Events** page is displayed.
2. Click the **Top N Attacks** link.
3. Fill in the fields to narrow your report. The following fields are noteworthy:
   - **Admin Domain** — Select the admin domain in which to view alerts.

     NOTE

     The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.
   - **Sensor**:
     - **All Devices** is checked by default. This displays information of all devices present at the selected admin domain. To select your preference of devices, de-select **All Devices** and select the devices from the list box.
     - **Include Child Admin Domains** — Displays device information for child domains.
   - **Attack Severity** — Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities, which relate to attack impact.
   - **Show only Blocked Attacks?** — Select **Yes** to view alerts that indicate attacks blocked by the device. The default for this field is **No**.
   - **Alert State** — Select one of the following to narrow the alerts:
     - **View unacknowledged alerts** — All unacknowledged alerts in the system for the specified time frame. If you have acknowledged alerts during your selected time range, this option suppresses those alerts.
     - **View all alerts** — (Default) both acknowledged and unacknowledged alerts for the specified time frame.
   - Choose one of the following time spans:
     - **Select Attacks for this Day** — Format is **yyyy/mm/dd**. Default is Manager server system date.
     - **Select Attacks Between these Dates** — Format is **yyyy/mm/dd hh:mm:ss**. Default **Begin Date** is "oldest alert detected time" and default **End Date** is Manager server system time.
     - **Select Attacks in the past** — Selects alerts from a point in the past relative to the current time. This time in the past can be months, weeks, days (Default), or hours. Type a time (**yyyy/mm/dd hh:mm:ss**) when the span of reporting time ends (default is Manager server system time).
   - Select the **Report Format**.
   - Select the **Report Content** delivery method. Choices are: **Chart Only**, **Table Only**, **Table and Chart**, **Bar chart** or **Pie chart**

- **Include other Attacks** — Applies only to **Pie Chart** format, displaying all alerts that are not included by the **Desired Number**. All other alerts appear as "Other" in the resulting pie chart.
- **Desired Number ('N') Of Attack Instances**. You can specify up to 1000 (10 by default). However, only the top 20 instances will be featured in the charts. Select the **Top N** field of interest (**Type**) from one of the following:
  - **Attack** — Sort by most commonly detected attacks.
  - **Source IP** — Sort by most common attack source IP address.
  - **Destination IP**— Sort by most common attack destination IP address.
  - **Source/Destination IP Pair** — Sort by most common occurrence of a specific source-to-destination IP address attack path.
  - **Attack Sub Category** — Sort by most commonly detected attack subcategories. Examples of subcategories are port scan, protocol violation, and worm.
  - **Protocol** — Sort by most commonly attacked protocols
  - **Service** — Sort by most commonly attacked services
- **NSLookUp** — Check the NSLookUp option to retrieve the host name corresponding to the IP address in the generated report.
- Select the **Sort By Attack Severity** check box to include the attack severity.

> **NOTE**
>
> NSLookUp is available only for Source IP, Destination IP or both.

- Select the **Sort By Attack Severity** check box to include the attack severity.

4. Click **Run Report**.

Generate Trend Analysis reports

The **Trend Analysis** report provides a high-level overview of trends and patterns in the collected alert data for a specified period of time or *interval*. A trend can be the number of alerts per hour for a day generated by all devices, the number of high severity exploit alerts per day for a week generated by a single interface on a device, and so on.

> **NOTE**
>
> You can generate a trend analysis report on all devices, a single device, a single interface on a device, or a single sub-interface.

Analyzing trends may provide an insight as to the type of alert activity being generated at different times of the day, week, or month. This data can help you devise a better security environment, or it may simply be used for presentation display when meeting to discuss your network security.

> **NOTE**
>
> Only users with root admin domain privileges can use the Trend Analysis Report.

The following categories and subcategories are available for trend analysis. During configuration, you must pick at least one category with a corresponding subcategory for your report. Each of the subcategories represents a specific trend during the interval you specify. If in one report you select multiple trend items for your report, each trend item has a separate graph and/or table for viewing the trend data. The categories and subcategories are as follows:

- **Severity**— Number of attacks by severity
  - **All** [severities]
  - **High** [severity alerts]
  - **Medium** [severity alerts]
  - **Low** [severity alerts]
  - **Informational** [alerts]
- **Attack Category**— Number of attacks by type
  - **Policy Violation**
  - **Reconnaissance Attacks**
  - **Volume DoS**
  - **Exploit**
  - **Malware Attacks**
- **Unique**— Number of attacks by specific parameter
  - **Attacks**— Unique attacks
  - **Destination IP**— Unique destination addresses
  - **Source IP**— Unique source addresses

> **TIP**
>
> This report is best used for displaying general alert information for the most common parameters in a presentation-like format.

Steps:

1. Select Analysis → Event Reporting → **Traditional Reports**.

   The **IPS Events** page is displayed.
2. Click the **Trend Analysis** link.
3. Select a **Resource**. A resource could be a device, interface on a device, or sub-interface. By default, only entire devices are available.

> **NOTE**
>
> Resource selection may include devices that have since been removed from your Manager. This is to provide you with the alert data generated by the now-deleted device during a period in the past.

4. Select one or more **Trend Item(s)**, then click **Add to List**. The trend data for the selected trend items can be viewed in the generated Trend Analysis Report. If you want to remove a Trend Item from the list, select the Trend Item, then click **Remove Selection**.
5. Select a **Trend Reporting Interval** from one of the following:
   - **Hour**— Display each Trend Item's alert count per hour
   - **Day**— Display each Trend Item's alert count per day
6. Select a **Trend Reporting Period** for Attacks. Choose one of the following time spans:
   - **Select Attacks for this Day**— Format is **yyyy/mm/dd**. Default is Manager server system date. It detects all the attacks for that particular date.
   - **Select Attacks Between these Dates**— Format is **yyyy/mm/dd hh:mm:ss**. Default **Begin Date** is "oldest alert detected time" and default **End Date** is Manager server system time. It detects all the attacks between the dates selected.
   - **Select Attacks in the past**— Selects alerts from a point in the past relative to the current time. This time in the past can be months, weeks, days (Default), or hours. Type a time **(yyyy/mm/dd hh:mm:ss)** when the span of reporting time ends (default is Manager server system time). It detects all the attacks for the number of days, weeks, or months selected.

   NOTE

   The Trend Reporting Period end date cannot be in the future.
7. Select the **Report Format**.
8. Select the **Report Content** delivery method. Choices are: **Bar Chart**, **Table Only**, or **Table and Chart**.
9. Click **Run Report**. The Trend Analysis Report is generated according to the configuration values set.

   NOTE

   The **Configure** button has multiple options.

Enable the Trend analysis and custom resource configuration

The engine used for trend analysis reporting is disabled by default. As the number of alerts in your database continues to grow, this engine may consume valuable processing cycles on your Manager server. The trend engine is required to maintain the tables that provide immediate trend analysis results for all of your database alerts. Without this engine, trend reports could take from several seconds to minutes to produce results. You may choose to disable this service if you are not currently interested in running trend analysis reports.

You can filter report information by assigning a specific resource, namely a single device, interface, or sub-interface for finer trend analysis.

Steps:

1. Click the **Analysis** tab from the Home page.

2. Select Event Reporting → Traditional Reports → **Trend Analysis** from the list of IPS Events.
3. Click **Configure**.
4. Do one of the following:
   - To disable the trend analysis engine, select **No** and click **Save**.
   - To assign a resource finer than an entire device, do the following:
     1. Click **Add**.
     2. Select the **Admin Domain** from the drop-down list in which the device you want to use resides.

        NOTE

        The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

     3. Select a **Sensor** you want to include in the trend analysis.
     4. Select an **Interface** on the device. The **Interface** field may also include any sub-interface resources.

        NOTE

        You cannot select just a device resource. When you select a device, you are also selecting an interface resource.

   - Click **Save**. Your added resource appears in the "Trend Resource" pane as well as in the Trend Analysis report's **Resource** field.

     NOTE

     At any time you can select a configured resource from the "Trend Resource" pane and click **Delete** to exclude a resource from trend analysis. However, you cannot delete a device resource.

5. Click **Back** to exit the Trend Analysis configuration page and return to the Trend Analysis report page.

Generate User Defined reports

The **User Defined** report presents alerts based on user-customized parameters. This report provides the most flexibility by enabling you to selectively minimize the report output through alert data filtering. For example, you can view alerts for all deployed devices, for one device, for a single interface, or even just a sub-interface of a device. In the same manner, you can filter based on a specific source IP, destination IP, and so forth. The depth of each category enhances the quality of your forensic analysis.

TIP

This report is best used for generating a custom report based solely on the parameters you require for alert analysis.

Steps:

1. Select Analysis → Event Reporting → **Traditional Reports**.

   The **IPS Events** page is displayed.

2. Click the **User Defined** link.

3. Fill out the form. The following fields are noteworthy:

   - **Admin Domain** — Select the admin domain in which to view alerts.

     NOTE

     The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

   - **Sensor**:
     - **All Devices** is checked by default. This displays information of all devices present at the selected Admin domain. To select your preference of devices, de-select **All Devices** and select the devices from the list box.
     - **Include Child Admin Domains** — Displays device information for child domains, but information about interfaces belonging to devices in child domain are not displayed.
   - **Interface** — Default is **All interfaces**. To narrow the result, clear the **All interfaces** check box, then select the desired interface(s). The **All interfaces** check box is enabled only if you have selected a specific device in the **Sensor** field.
   - **Detection Mechanism** — Default is **All detection mechanisms**. To narrow the result, clear the **All detection mechanisms** check box, then select the desired mechanism(s).
   - **Protocol** — The default is **Application Protocol**. Based on the selection, the fields change to display relevant protocols. Select **Reference Protocol** to view alerts based on the attack definition instead of the alert's application protocol. You may want to select Reference Protocol, if you want to search for a protocol that tunnels through another protocol and is, therefore, hidden. For example, P2P traffic is often tunneled through HTTP traffic.
   - **Application Protocol** — Default is **All protocols**. To narrow the result, clear the **All protocols** checkbox, then select the desired protocol(s).
   - **References Protocol** — Default is **All protocols**. To narrow the result, clear the **All protocols** checkbox, then select the desired protocol(s).
   - **Attack Category** — Default is **All Categories**. To narrow the result, toggle the drop down menu and select the category you require. The **Sub Category** field is a subset of the **Category** field.
   - **Attack Sub-Category** — Default is **All Sub Categories**. To narrow the result, clear the **All Sub Categories** check box, then select the desired sub category or sub categories.
   - **Source IP Address** — Default is **Any source IP address**. To enter a specific source IP address, clear the **Any source IP address** check box, then type your entry. You can enter a netmask (*) for Class B, C, and D addresses. You can select either IPv4 or IPv6 type of IP addressing.
   - **Source Port Number** — Default is **Any source port number**. To enter a specific port, clear the **Any source port number** check box and type your entry.
   - **Destination IP** — Default is **Any destination IP address**. To type a specific destination IP address, clear the **Any destination IP address** check box, then type your entry. You can enter a netmask (*) for Class B, C, and D addresses. You can select either IPv4 or IPv6 type of IP addressing.

> **NOTE**
>
> IP addresses can be expressed with netmasks as follows: XXX.*.*.*, XXX.XXX.*.*, and XXX.XXX.XXX.*.

- **Destination Port Number** — Default is **Any destination port number**. To enter a specific port, clear the **Any destination port number** check box and type your entry.
- **Direction of Attack (for Signature Attacks only)** — Default is **All** (both Inbound and Outbound). Selecting both options will include those attacks with "unknown" (common for SPAN or Hub mode) directions.
- **Attack Severity** — Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities, which relate to attack impact.
- **Relevance** — Select one or more from Relevant, Unknown, or Not Applicable levels, which is related to vulnerability relevancy.
- **Select Alert/Attack Type** — To view all alerts, blocked alerts, or alerts/attack type for which the source endpoints were quarantined and remediated.

  To select the alert/attack type based on Quarantine feature, select the check box **Quarantine**. Next, select either of the check boxes- **Quarantined** or **Quarantined & Remediated**.
- **Alert State** — Select one of the following to narrow the alerts:
  - **View unacknowledged alerts** — All unacknowledged alerts in the system for the specified time frame. If you have acknowledged alerts during your selected time range, this option suppresses those alerts.
  - **View all alerts** — (Default) both acknowledged and unacknowledged alerts for the specified time frame.
- **Attacks** — Choose one of the following attacks:
  - **Select Attacks for this Day** — Format is **yyyy/mm/dd**. Default is Manager server system date.
  - **Select Attacks Between These Dates** — Format is **yyyy/mm/dd hh:mm:ss**. Default **Begin Date** is "oldest alert detected time" and default **End Date** is Manager server system time.
  - **Select Attacks in the past** — Selects alerts from a point in the past relative to the current time. This time in the past can be months, weeks, days (Default), or hours. Type a time (**yyyy/mm/dd hh:mm:ss**) when the span of reporting time ends (default is Manager server system time).
- **Fields of Interest** — Checked fields appear as table columns in report output. All options are selected by default.
- **Organized by** — Specify how you want the information to be organized in the report. Choices are **Attack**, **Source IP**, **Destination IP**, or **Create Time**. For example, if you choose Attack, then the information is organized by attack name in the reverse alphabetical order. Create Time is the alert generation time.
- Select the **Report Format**.

4. Click **Run Report** to generate a report.

Templates reports

The **Templates** option enables you to create custom IPS report templates that you can run on-demand as well as manage the report templates you created for **Scheduled Reports**. IPS report templates simplify the process of generating a frequently used report by enabling you to create a template for a report, and simply return to this action to generate the report based on your settings at any given point in the future.

NOTE

You cannot create scheduled report templates under the **Report Templates** action. You must create those by following the steps in Scheduling a report.

The **Report Templates** table columns are described as follows:

- **Report Template Name**— User-given name of report template. Clicking column header sorts template names alphabetically.
- **Created by Admin Domain**—
- **Report Type**— List includes the IPS Report types as well as the Audit Report.
- **Last Modified Time**— Last date and time when template was modified. Clicking column header sorts template names chronologically.
- **Schedule**— Status of template as either automatic or manual. Automatic seen as "Daily" or "Weekly". Manual seen as "Template." Clicking column header sorts schedule names alphabetically.

NOTE

In Trellix IPS Central Manager, the **Templates** link is in Analysis → **Event Reports** main page helps you to create and manage report templates. Note that when you click **Add Report**, you can select only **User Activity Report**. The other functions from **Templates** link are similar to report templates in Manager as described in this section.

Add new report templates

To create a report template, do the following:

Steps:

1. Click the **Analysis** tab from the Manager Home page.
2. Select Event Reporting → Traditional Reports → Templates → **New**.
3. In **Add Report Template** page, select the **Report Type**. Based on this selection, the template fields change to fit the elements of the selected report. For example: Executive Summary

   Make sure you have specified values for all the mandatory fields including the following. The mandatory fields are indicated by a red asterisk.
4. Fill in the following fields to narrow your report:
   - **Admin Domain**— Select the admin domain in which to view alerts.
   - **Template Name**— Unique, user-given name for the template.
   - **Description**— Unique descriptive information about the template.
   - **Sensor**:
     - **All Devices** is checked by default. This displays information of all devices present at the selected Admin domain. To select your preference of devices, de-select **All Devices** and select the devices from the list box.

- **Include Child Admin Domains**— Displays device information for child domains.
- **By Device**— This helps to choose a particular device.

- **Alert Severity**— Select one or more from the **Informational**, **Low**, **Medium**, or **High** severities, which relate to attack impact.
- **Ranking Basis**— Select one of the following:
  - Percentage change in attack count
  - Change in attack count value
  - **Direction**— Select one of the following directions of how alerts occurred should be displayed:
    - Upward Movers only
    - Upward and Downward Movers
    - Downward Movers only
- **Maximum Movers**—
  - Enter the value of maximum occurred alerts to be displayed.
- **Comparison Interval (days)**— Select the interval of the comparison in days.

5. Click **Save** when finished.

   Once created, you can **Edit**, **Run**, or **Delete** the created report templates. Select the report template you want to edit/run/delete. By default, the last report template in the table is selected.

You can create a template by using a report type available in the **Report Type** field. When you click **Add**, by default, you will see a template created according to **Big Movers** report. For creating any other template, select the appropriate report type from the Report Type field. For specific information on the respective fields in a template, see the topic on the respective report. For example, if you are creating a template using Executive Summary report, see Generate Executive Summary reports (page 503).

Trellix Intrusion Prevention System Central Manager

About Trellix Intrusion Prevention System Central Manager

Trellix IPS provides a centralized, "manager of managers" capability, named Trellix Intrusion Prevention System Central Manager.

Trellix Intrusion Prevention System Central Manager (Central Manager) allows users to create a management hierarchy that centralizes policy creation, management, and distribution across multiple Trellix IPS Manager. For example, a policy can be created in a Trellix IPS Central Manager and synchronized across all Managers added to that Central Manager. This avoids manual customization of policy at every Manager.

The Central Manager provides you with a single sign-on mechanism to manage the authentication of global users across all Managers. Sensor configuration and threat analysis tasks are performed at the Manager level.

Central Manager architecture

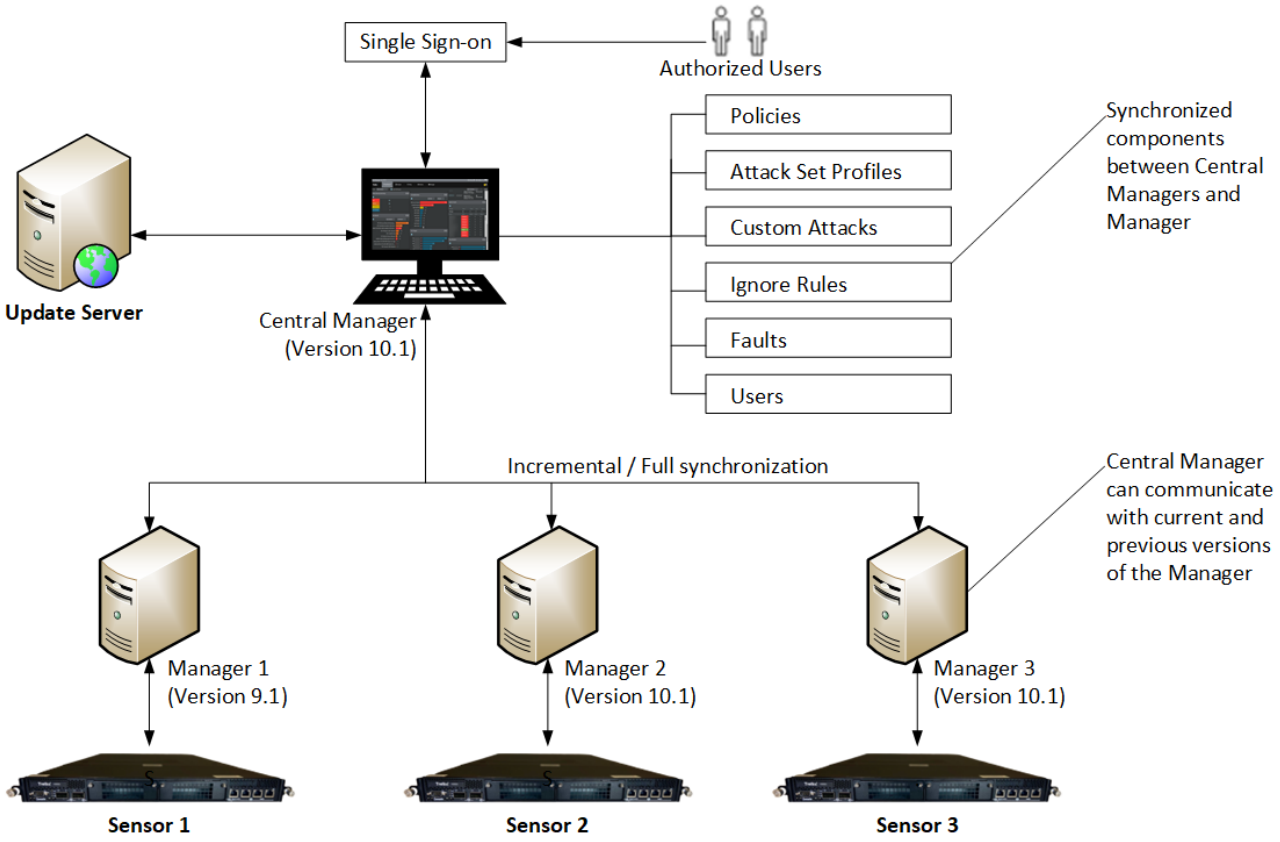
Central Manager is a centralized system managing multiple Managers. The Central Manager architecture consists of a Central Manager, which is interconnected to various Managers.

Central Manager manages configurations and pushes them globally to Managers. Configurations are pushed to the Sensors indirectly through Managers.

Suppose you are responsible for managing global security operations at a large multi-national corporation and you wish to delegate the management of specific security functions (including IPS) to the company's regional facilities. Your goal therefore, is to establish a master IPS security policy at the headquarters that can be pushed down to each region.

In this scenario, you can use the Central Manager at the headquarters and deploy a dedicated Manager for each region. When you use the Central Manager, your regional Managers can add their own region-specific rules, but cannot modify any configuration established by the Central Manager. Each Manager handles the daily operations and event management of the Sensors. The following diagram shows the Central Manager setup.

Figure 213. Central Manager architecture



The Central Manager's single sign-on mechanism manages the authentication of global users across Managers. The objective is to allow global users to access all Managers using a single sign-on. Once a global user is authenticated with the Central Manager, the user can access a Manager without having to re-enter the login credentials for the Manager.

The Central Manager supports heterogeneous Managers. It means that the Central Manager can communicate with the current version of Manager as well as the previous versions of the Manager.

NOTE

- Central Manager cannot directly handle any Manager resources. A Central Manager user has to log onto the Manager to do the same.
- You cannot add Sensors to the Central Manger.
- You cannot create admin domains in the Central Manager.

Installing and Configuring Trellix IPS Central Manager

This section provides information on installing and configuring a Trellix IPS Central Manager.

Installing the Central Manager

The system requirements and the installation procedure for the Central Manager are same as that of a Manager. To install the Central Manager, you should use the Manager installer. The Manager installer can be used to install a Manager or a Central Manager. For more information, see the following sections:

- System requirements for Central Manager - See [Preparation for the Manager installation] chapter in the [Trellix Intrusion Prevention System Installation Guide].
- Installing Central Manager - See [Install the Manager/Central Manager] chapter in the [Trellix Intrusion Prevention System Installation Guide].
- Starting the Central Manager - See [Starting the Manager/Central Manager] chapter in the [Trellix Intrusion Prevention System Installation Guide].

Log on to the Central Manager

To log on to the Central Manager:

Steps:

1. Do one of the following:

   For initial logon after a new installation:

   - For **Login ID**, type **`nscmadmin`**
   - For **Password**, type **`admin123`**

     TIP

     Trellix**strongly recommends** that you change the default user name and password as one of your first operations within the system. The new password must be at least 8 characters in length and must contain a combination of numbers, characters, and special characters.

   If you are not Trellix IPS System administrator/Super User:

   - Type the **Login ID** supplied to you by your administrator.
   - Type the valid **Password** for the specified Login ID.

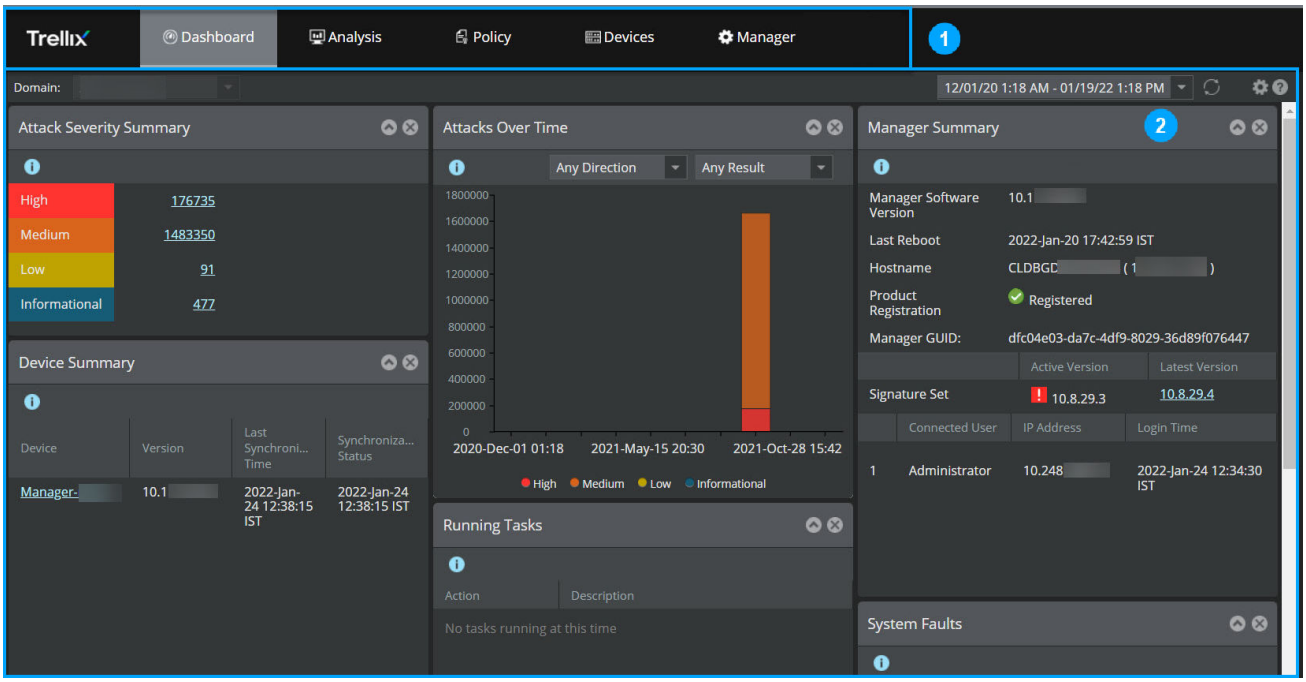
2. Click **Log In** or press **Enter**. The Central Manager Home page appears.

> **NOTE**
>
> You can opt to display your company's logo and accompanying text on the Central Manager Login page.

Central Manager Dashboard page

The Central Manager **Dashboard** page is the first page displayed after a successful login.

Figure 214. Central Manager Dashboard page



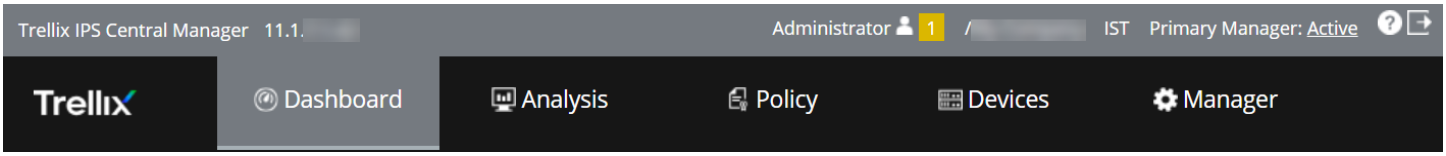
Item	Description
1	Menu bar
2	Display area

The **Dashboard** page is the central interface from which all Central Manager components are available. The **Dashboard** page is logically divided into two sections; the top menu bar and the lower summary display section.

Menu bar components

The menu bar of the Dashboard page presents you with navigation options (dependent on a user's assigned role) to the Central Manager components:

Figure 215. Menu Bar



- **Dashboard** — Displays key information summaries, such as Attack Severity Summary, Manager Synchronization Status, Release Announcements, Running Tasks, System Faults, and Manager Summary
- **Analysis** — Takes you to the Attack log page and the Reports page
- **Policy** — Links to the Policy page
- **Devices** — Enables you to add or remove Managers, view the devices, such as Sensors or NTBA appliances, that are connected to each Manager managed by the Central Manager (in Manager version 10.1.7.65 and higher), alert filters, synchronize faults and policies
- **Manager** — Enables you to handle all the Manager configurations, user role management, updating of signature sets, setup, reporting, maintenance, and troubleshooting

The menu bar of the Dashboard page also provides you with the following icons:

- — Links to the help page, which provides the complete system help
- — Logs you out of the system and returns to the login screen

Dashboard components

The **Central Manager Dashboard** page displays key information summaries such as the following:

- **Attack Severity Summary** — Displays statistics for the unacknowledged faults in the logged-in domain
- **Attacks Over Time** — Displays the number of attacks that have been detected at different time intervals
- **Manager Summary** — Displays information of Central Manager version, signature set version of Central Manager, user names, host names, Manager GUID, and times of Central Manager
- **Device Summary** — Displays information about connected Managers. Connected managers are treated as devices under this section. This section displays information such as device name (Manager name), Manager version, last synchronized time, and synchronization status.
- **Release Announcements** — Enables you to view any product or security-related messages. The messages can be related to operating system patches, signature set release, Central Manager software update, and so on.
- **Running Tasks** — Displays the status of activities currently running on your system that Trellix IPS identifies as long running processes
- **System Faults** — Displays the current faults of the Central Manager and the added Managers in the system

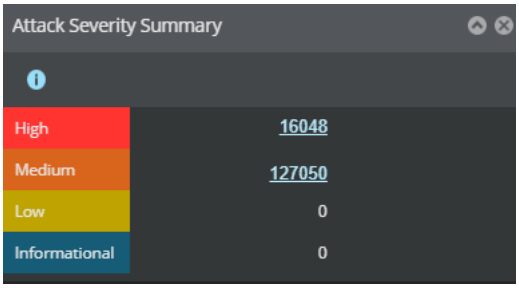
Attack severity summary

The **Attack Severity Summary** section of the Dashboard page displays statistics for the unacknowledged faults in the logged-in domain. Faults are categorized by system impact Severity level: High, Medium, Low, and Informational.

NOTE

If you want to hide the **Attack Severity Summary** monitor, you must manually do it using **Dashboard Settings** dialog. For more information on hiding a monitor, see Dashboard tab (page 353).

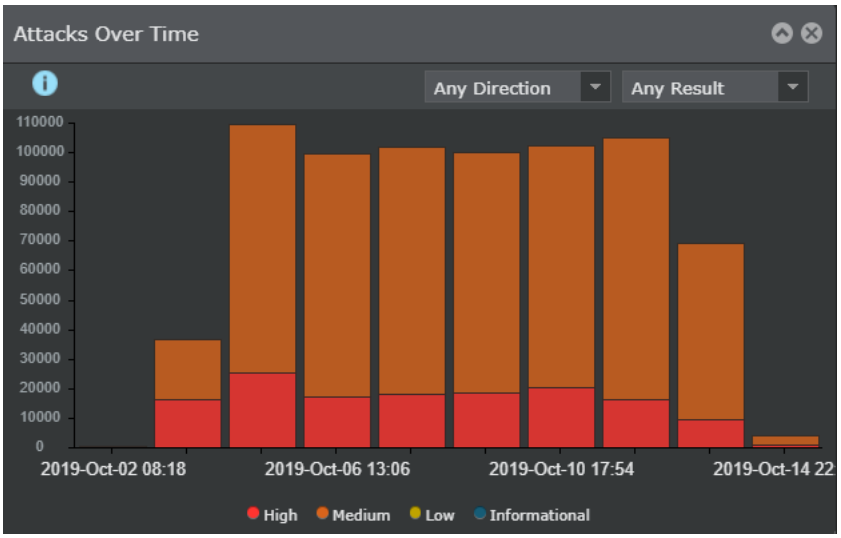
Figure 216. Attack Severity Summary



Attacks Over Time

The **Attacks Over Time** monitor enables you to view the number of attacks that have been detected at different time intervals. Each bar contains information related to the number of attacks and the time in which the attacks were detected.

Figure 217. Attacks Over Time



The following options in the first drop-down list are available in the monitor to view the attacks based on direction:

- **Inbound** - Displays the attacks on inbound traffic
- **Outbound** - Displays the attacks on outbound traffic
- **Any Direction** - Displays attacks on both inbound and outbound traffic

The following options in the second drop-down list are available in the monitor to view the attacks based on result:

- **Blocked** - Displays blocked attacks over a period of time
- **Unblocked** - Displays unblocked attacks over a period of time
- **Any result** - Displays both blocked and unblocked attacks over a period of time

Each bar represents the attacks based on severity level for different time intervals. Clicking on a bar redirects you to the **Attack Log** page where more details of the attack are displayed.

The legend at the bottom of the monitor indicates the color for each severity level of the attack displayed in the bar graph. The severity levels are as follows:

- **High**
- **Medium**
- **Low**
- **Informational**

NOTE

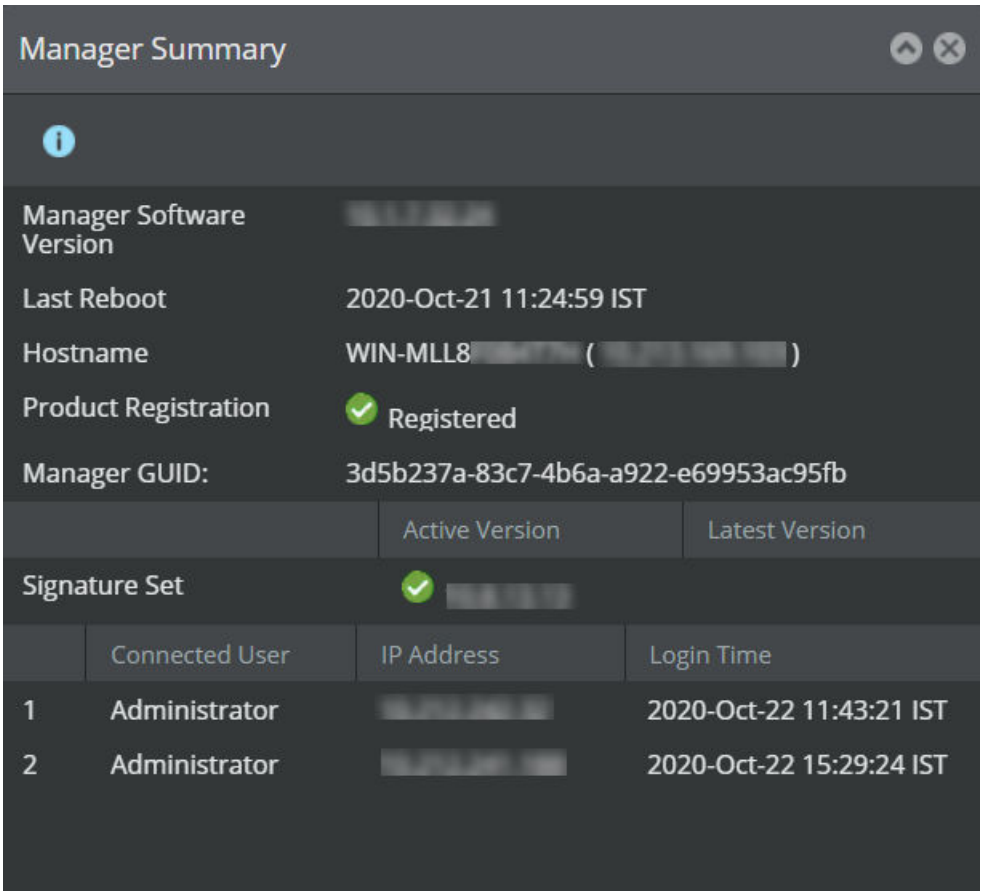
To view or hide the display of attack data in the monitor for different severities, click on the color indicator that represents the severity.

Manager Summary

The **Manager Summary** monitor (Central Manager → Dashboard → **Manager Summary**) displays the following details:

- **Manager Software Version** — Current Central Manager software version.
- **Last Reboot** — The most recent time when the Central Manager was restarted.
- **Hostname** — Host name and network identification of the Central Manager server (if host name is not available, only the IP address is displayed).
- **Product Registration** — The registration status of the Central Manager.
- **Manager GUID**— The unique identifier of the Manager server.
- **Signature Set - Active Version** — Current signature version available in Central Manager. The active version is preceded by a red or green button. A red button indicates that the active version is older than the current version. A green button indicates that the active version and the latest version are the same.
- **Signature Set - Latest Version** — The latest version of the signature set. If the active version is a version earlier to the latest version, the latest version number is a hyperlink which takes you to the **Download Signature Sets** page.
- **Connected User** — All currently open user session information by user name, host name (IP address) and logon time. If there is more than one user connected to the same Central Manager, you can see the user names one below the other in this column.
- **IP Address** — The IP address of the user.
- **Login Time** — The last logon time of the user.

Figure 218. Manager Summary



Device Summary

The **Device Summary** option (Central Manager → Dashboard → **Device Summary)** enables you to view details about Managers that are connected to the Central Manager. Similar to how a Manager manages devices such as Sensors, a Central Manager manages a set of Managers. So, in the Central Manager dashboard, the term *device* refers to a Manager managed by the corresponding Central Manager and does not refer to devices such as Sensors and NTBA appliances. Therefore, the **Device Summary** of the Central Manager displays details such as device name, version number, last synchronized time, and synchronization status of the corresponding Managers.

- **Device** — Name of the Manager connected to the Central Manager. This is the name that you entered for the Manager on Central Manager's **Add and Remove Manager's** page. The device name is actually a hyperlink which takes you to the respective Manager's **Manager** page.
- **Version** — Version of the Manager
- **Last Synchronized Time** — Time when the Manager was last synchronized with the Central Manager
- **Synchronization Status** — This column displays **Up-to-date** if the synchronization is up to date. If not, the column displays **Changes pending** as a hyperlink. The **Changes pending** hyperlink takes you to the **Synchronize Policies** page.

Release Announcements

The **Release Announcements** section enables you to view any product or security-related messages. The messages can be related to operating system patches, signature set release, and so on. Central Manager checks the Trellix IPS Update Server (Update Server) for such messages every 15 minutes and displays messages that are relevant to the version of Central Manager and signature set that you are using.

This feature ensures that all relevant messages from the Trellix IPS support team reach you on time. Because the new messages are displayed on the Central Manager home page, the chances of you missing out on any message are remote.

The Central Manager displays the release date and the message description of the relevant messages in the **Release Announcements** section. The release date is the date on which the message was posted on the Update Server. You can acknowledge the messages that you have already seen and they will not be listed again. The latest four unacknowledged messages are displayed on the Trellix IPS home page as well. Click the **View all messages** link on the home page to navigate to the **Release Announcements** tab (under Manager → **Trellix IPS Protection Status**) where all the messages are displayed.

NOTE

Though all users can view the messages, only users with the role of Super User in the root admin domain can acknowledge messages.

Background Tasks

The **Running Tasks** monitor of the **Dashboard** page displays the status of currently In-Progress activities on your system that Trellix IPS identifies as long running processes.

When a long running process is taking place in your Manager, the status is displayed as "In progress" in the **Running Tasks** monitor. You can also go to **Logs** page and select **Background Tasks** tab to view long running processes. Once the activity is completed, the entry for that activity is removed from the **Running Tasks** monitor and displayed only under **Background Tasks** tab in the **Logs** page.

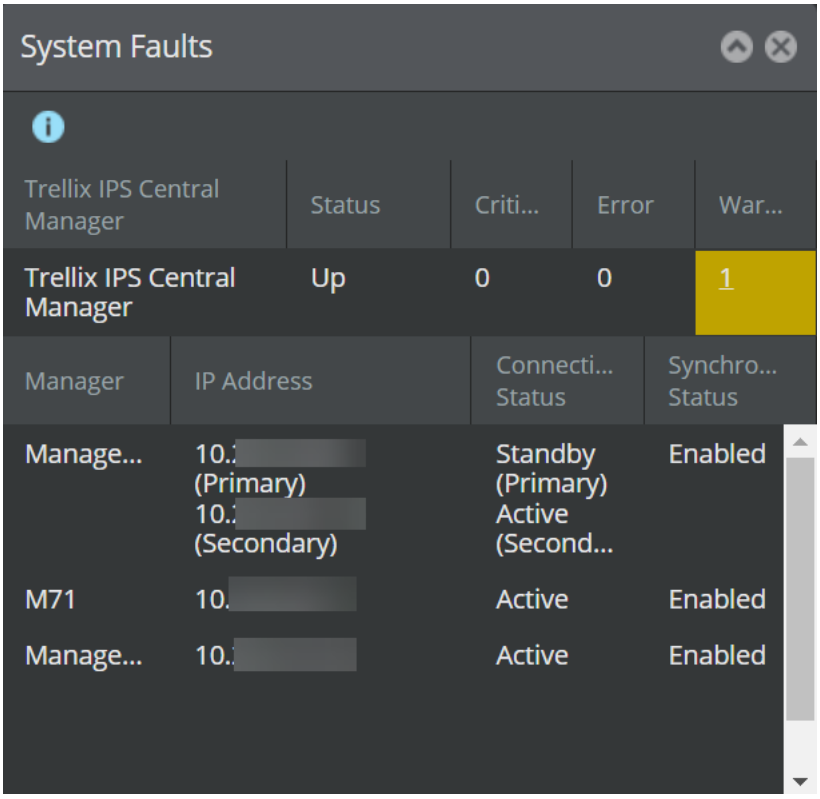
System Faults

The **System Faults** section of the **Dashboard** page displays the following information:

- **Trellix IPS Central Manager**— The Central Manager name
- **Failover Mode**— The failover mode of the Central Manager, whether primary or secondary as configured in MDR
- **Failover Status**— The failover status of the Central Manager, whether active or standalone
- **Status**— Operational status of the component. For Central Manager, up indicates proper functioning; down indicates the component is not functioning.
- **Critical**— Major faults, such as component failure.
- **Error**— Medium faults, such as a stopped process, incorrect port speed configuration, or a session time-out (automatic logoff).
- **Warning**— Minor faults, such as multiple bad logos or an attempt to delete a resource in System Configuration without properly clearing fields

- **Manager**— The name of the Manager entered in the Devices page
- **IP Address**— The IP address of the Managers managed by the Central Manager
- **Connectivity Status**— The connectivity status of the Managers managed by the Central Manager
- **Synchronization Status**— The synchronization status of the Managers managed by the Central Manager

Figure 219. System Faults window



Register the Central Manager

The Central Manager should be registered with Trellix for receiving automatic updates regarding the signature set, callback detectors, and device software from Trellix in real time.

The steps for registering a Central Manager are same as that of registering a Manager. For more information, see the [Product Registration] section in the [Trellix Intrusion Prevention System Product Guide].

Configure Managers in the Central Manager

Prerequisites:

Before you configure the Manager in the Central Manager, you should configure the Central Manager details in the Manager. To configure the Central Manager in the Manager, perform the following steps:

1. Login to the Manager instance.
2. Select Manager → <Admin domain> → Setup → **Central Manager**.

3. Enter the **Manager Name**.
4. Enter the **Central Manager IP Address**.
5. Enter the **Shared Secret** and **Confirm Shared Secret**.
6. Select **Synchronization Enabled**.
7. Click **Finish**.

Adding a Manager to the Central Manager enables the Manager to accept communication from Central Manager. Once trust is established, the Central Manager can view the Manager's configuration.

NOTE

Port 443 is used for communication between the Central Manager and the Manager.

To add a Manager to Central Manager perform the following steps:

Steps:

1. Select Devices → Manager Management → **Add and Remove Managers**.
2. Click +.
3. Type the **Manager Name** and the **Shared Secret** (repeat at **Confirm Shared Secret**).
   - The Name can be a maximum of 40 characters in length. The parameters you can use are:
     - 26 alpha — Uppercase and lowercase (a,b,c,...z and A, B, C,...Z)
     - 10 digits — 0 1 2 3 4 5 6 7 8 9
     - 2 symbols — _ and -

     NOTE

     The Manager name should match the name provided in the Manager when you configured the Central Manager details.
   - The secret must be a minimum of 8 characters and maximum of 64 characters in length. The **Secret** cannot start with an exclamation point nor have any spaces. The parameters you can use are:
     - 26 alpha — Uppercase and lowercase (a,b,c,...z and A, B, C,...Z)
     - 10 digits — 0 1 2 3 4 5 6 7 8 9

     NOTE

     The shared secret should match the secret provided in the Manager when you configured the Central Manager details.
4. Select the required severity level to be displayed in the Central Manager from **Alerts from this Manager to Show in the Central Manager** drop-down list.

5. Enter the number of days in the **Maximum Number of (Most Recent) Days of Alerts to Show** textbox (Default value -15).
6. Enter the number of alerts you want in the **Maximum Number of Alerts to Show** field (Default value - 100000).

   Maximum Number of (Most Recent) Days of Alerts to Show and **Maximum Number of Alerts to Show** provide a combined option for limiting the number of alerts that are displayed in the Central Manager Attack Log. For instance, the number of days is set to 15 and the number of alerts is set to 1000, the Central Manager **Attack Log** will display the first 1000 alerts from the current system to 15 days earlier. If the number of alerts during this period is more than 1000, only the first 1000 alerts will be displayed.
7. (Optional) Enter the contact information.
8. (Optional) Enter the location.
9. Select **Yes** to enable synchronization at **Synchronization Enabled**.
10. Click **Save** to save the configuration, and view the newly added Manager in the Managers page.

    The **Managers** page presents a read-only view of the configured information for connected Managers. The information displayed is configured during the trust establishment of the Managers.

    Once you have added a Manager to your Central Manager, you can **Edit** the Manager details as well as **Delete** the Manager configuration added to the Central Manager. Click **Refresh** to refresh the page.

Viewing Managers from the Central Manager

You can view all the Managers added to the Central Manager from the **Devices** page.

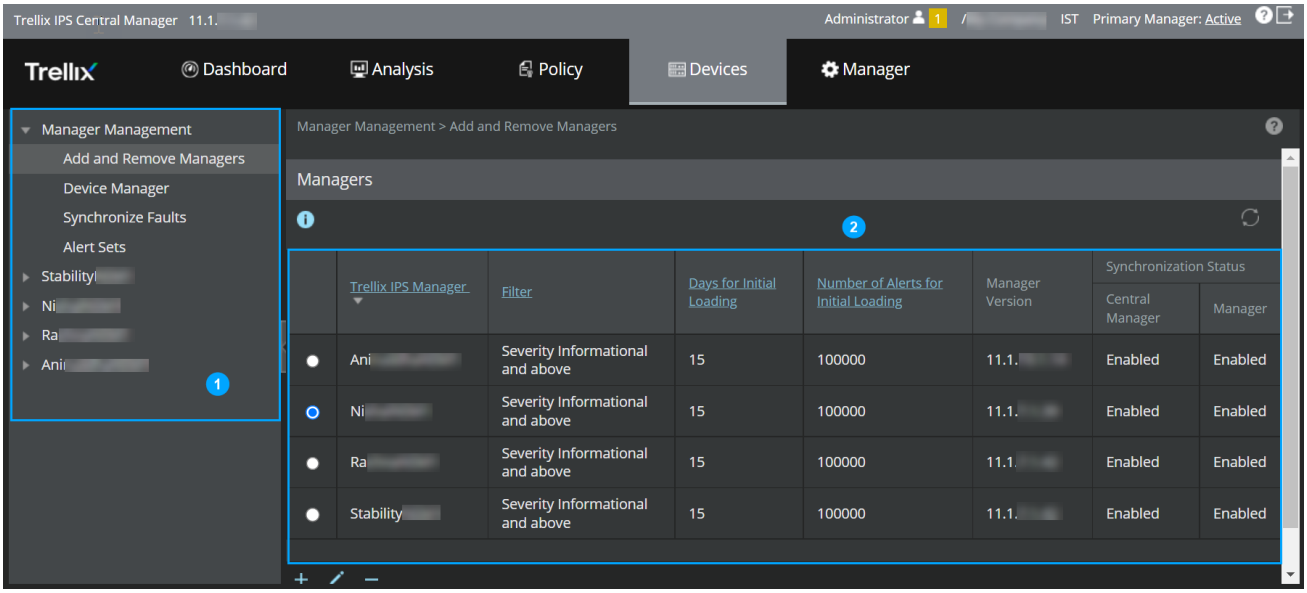
> **NOTE**
>
> Your access to the Managers is based on your role in the system.

To access the Central Manager systems page:

Steps:

- From the Central Manager home page, click the **Devices** tab.

Figure 220. Central Manager System page



Item	Description
1	Tree pane
2	Configuration pane

The page is divided into two sides, called panes:

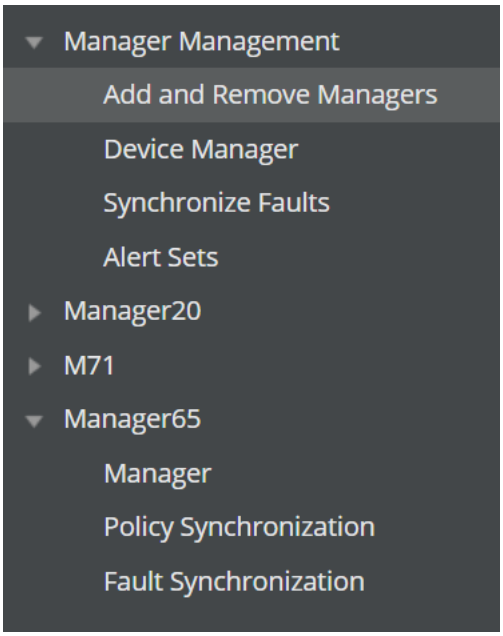
- The **Tree** pane is the left-side of the page. The Tree pane contains the hierarchical view of your Trellix IPS resources.
- The **Configuration** pane is the right-side of the screen. Depending on which item you select in the tree, this pane displays different action tabs, enabling you to perform configuration operations on the selected resource.

Tree pane

The **Tree** pane is in the left pane of the **Devices** page. The tree pane gives a hierarchical view of all your physical and virtual Trellix IPS resources reporting to the Central Manager server. The resources available are dependent upon the Trellix IPS products and features deployed in your system. The hierarchical view within the tree applies to the way the menus are managed by the system users and not necessarily to any networking or physical relationship between the resources.

Once you have configured a Manager as explained in Configure Managers in the Central Manager (page 523), you will be able to see the newly added Managers appearing as menus on the **Devices** tab.

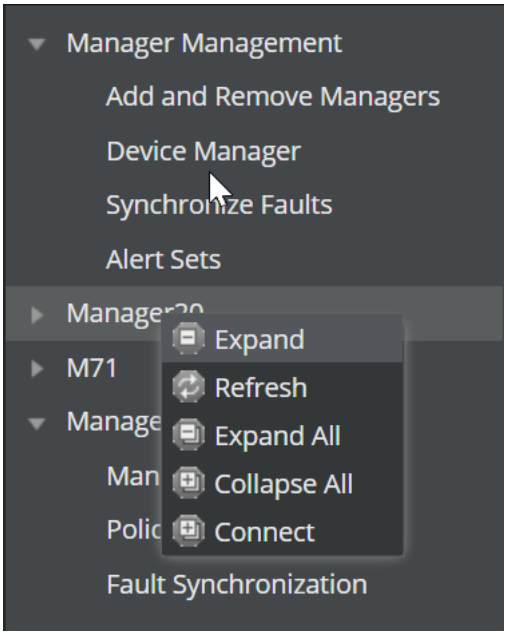
Figure 221. Newly added Managers in the Device tab



As you add more Managers, additional menus appear in the tree. To view details of any Manager, click **Manager** sub-menu under the **<Manager>** menu.

If you right-click on any of the menus, a shortcut menu offers the following options:

Figure 222. Right-click options in the Tree pane



- **Expand** — Expands a single resource from the tree
- **Refresh** — Updates the tree for immediate display of newly added/deleted Trellix IPS resources

- **Expand All** — Expands all the resource on the resource tree
- **Collapse All** — Collapses all the resource on the resource tree
- **Connect** — Allows you to connect to Managers

Accessing the Manager

From the **Manager** sub-menu, you can access a Manager using the **Connect** option. This opens the Manager Home page. To connect to the manager, perform the following steps:

1. On the Central Manager home page, click the **Devices** tab.
2. From any added <Manager> submenu, select **Manager**.
3. In the Manager details section, select **Connect**. The Trellix IPS Manager login page is displayed.
4. Type the Login ID and Password to log on to the Manager.

Editing Manager details

From the **Manager** tab, you can edit the Manager details.

You are allowed only to edit the contact and location details in the **Edit Trellix IPS Manager** page. You can enable/disable **Synchronization Enabled** while editing Manager details.

Removal of Managers from the Central Manager

The removal of Central Manager-Manager association can be initiated either from the Central Manager or the Manager.

If a Manager initiates the disassociation, all Central Manager details within that Manager are removed. This includes all Central Manager data, which has been synchronized as well as Central Manager-specific details. In this case, the Central Manager does not remove the Manager data. It is removed only when the Manager is disassociated in the Central Manager.

Proper shutdown of the Central Manager

A proper shutdown of the Central Manager prevents data corruption by allowing data transfer and other processes to gracefully end prior to machine shutdown.

Proper shutdown of the Central Manager services requires the following steps to be performed:

- **Windows based Manager**
    1. Close all client connections.
    2. RDP to the Central Manager server.
    3. Go to Control Panel → System and Security → Administrative Tools → **Services**.

       The **Services** window opens.
    4. Stop the following services:
        - Stop Trellix IPS Central Manager service.

- Stop Trellix IPS Manager Watchdog service.
- Stop Trellix IPS Manager Database service.

- **Linux based Manager**
  1. Close all client connections.
  2. Log in to the Central Manager shell.
  3. Execute the following commands:
     - Execute the **`manager stop`** command to stop Trellix IPS Central Manager service.
     - Execute the **`watchdog stop`** command to stop Trellix IPS Manager Watchdog service.
     - Execute the **`database stop`** command to stop Trellix IPS Manager Database service.

Synchronization of Managers with the Central Manager

After adding a Manager to the Central Manager, it appears as a menu under the **Devices** tab. You can now synchronize the Manager with the Central Manager.

The **Devices** tab represents the Trellix IPS Manager added to a Central Manager. Each Manager node is a uniquely named (user-defined) instance of a Manager. All actions available at the Manager level customize the settings for a specific Manager.

This section describes how to synchronize policies, attack set profiles, custom attacks, ignore rules, faults, and users between Managers and the Central Manager.

Synchronizing policies

All Central Manager policies (Trellix IPS-defined and user-defined) are synchronized with the Managers. While viewing the policies from the added Managers, the Central Manager policy names have *NSCM* prefixed to differentiate them from the Manager policies. For example, a **Default Prevention** policy defined in the Central Manager will be seen as **NSCM Default Prevention** in the Manager IPS Policy Editor. The same applies to user-defined Central Manager policies also.

The Central Manager policies are non-editable in the Managers. The Central Manager Attack Defaults settings are merged with the Central Manager policy. The Managers Attack Defaults settings do not affect any Central Manager policy and vice versa.

Each Manager must import signature sets independently. The policies and attack set profiles are evaluated based on the Manager signature set.

If the Central Manager removes a policy and the policy is being used in a Manager, then, during synchronization, the Central Manager policy in the Manager is renamed and the ownership changed to that of the Manager. A fault is raised in the Manager indicating that the policy has not been removed in that Manager.

For more information on configuring policies, refer to the chapter [Working with IPS policies].

Configuring policy synchronization

The **Synchronize Policies** menu from the **Policy** tab shows the synchronization status for all the Managers added to your Central Manager. This menu allows you to synchronize configurations between the Central Manager and all the Managers added to your Central Manager.

Field	Description
Synchronization Type	• **Incremental** (default: Enabled) — Based on last synchronization time • **Full**— Complete synchronization
Manager	Name of the Manager added
Last Synchronized	Time when last synchronization took place. Time is displayed as per the client time zone. For more information, see Viewing the server/client date and time (page 47).
Synchronization Required	If synchronization is required or not
Reason	Reason for synchronization
Synchronization Status	Enabled/Disabled for Central Manager or Manager

To trigger manual synchronization with the Manager, click **Synchronize**.

NOTE

You can also access **Synchronize Policies** menu from Policy → **Intrusion Prevention**.

NOTE

If the Central Manager contains a rule object with more than 10 entries, the Central Manager synchronizes only those rule objects containing 10 entries or lesser with a Manager running on or before 10.1.7.55.

Scheduling policy synchronization

You can configure the polices to be synchronized at regular time intervals. To set the policy scheduler in Central Manager, do the following:

1. Select Manager → Setup → Synchronization → **Policy Scheduler**

   NOTE

   Yes is selected by default at **Policy Scheduler**. Select **No** to turn off the scheduled synchronization.

2. Select time at **Recur every** (default 15 Min).
3. Click **Save**.

Synchronizing faults

Configuring fault synchronization

The **Synchronize Faults** menu (Devices → Manager Management → **Synchronize Faults**) allows automatic synchronization of faults between the Managers and the Central Manager.

Similar to **Synchronize Policy**, **Synchronize Faults** also provides both-incremental and full synchronization options.

Field	Description
Synchronization Type	• **Incremental** (default: Enabled)— Based on last synchronization time • **Full**— Complete synchronization
Manager	Name of the Manager added
Last Synchronized	Time when last synchronization took place. Time is displayed according to the client time zone. For more information, see Viewing the server/client date and time (page 47).

To trigger manual synchronization with the Manager, click **Synchronize**.

Scheduling fault synchronization

You can configure the faults to be synchronized at regular time intervals. To set the fault scheduler in Central Manager, do the following:

1. Select Manager → Setup → Synchronization → **Fault Scheduler**

   NOTE

   Yes is selected by default at **Fault Scheduler**. Select **No** to turn off the scheduled synchronization.

2. Select time at **Recur every** (default 10 Min).
3. Click **Save**.

Synchronizing alert sets

Alert sets specify the groups of alerts that can be sent from Managers to the Central Manager. You can configure alert sets in the Central Manager, and apply these filters to individual local Managers added to the Central Manager.

Configuring alert sets

To configure alert sets in the Central Manager, do the following:

Steps:

1. Select Devices → Manager Management → **Alert Sets** to view the list of alert sets.
2. Click ⊞ to view the list of available fields.
3. Select and move the required fields to the right pane by clicking the arrow button. The right pane displays **Property**, **Comparison**, and **Value** options.
4. Select **Equals** or **Does not equal** as the comparison value for each property. Select the values for the property from the **Value** drop down list.
5. Click **Next**.
6. Enter a name and description for the set.
7. Click **Save**.

The newly created alert set is listed in the **Alert Sets** page.

Synchronizing ignore rules

Ignore rules created in the Central Manager are synchronized with all the managers added to that Central Manager. In Central Manager, synchronization can be run manually (either as incremental or as full) or as scheduled. Ignore rules created in the Central Manager are pushed to the parent admin domains of individual Managers added to the Central Manager and are eventually applied to all levels such as admin domains, Sensors, and interfaces.

When you create an ignore rule from Central Manager Attack Log, it is effectively created and managed by the target Manager where the alert belongs. The target Manager user can edit or maintain that rule; however, rules and corresponding objects created on the Ignore Rules page of the Central Manager are created and managed by the Central Manager. Such rules are shown in read-only mode on the applicable Managers and exposed with an "owner of NSCM" name. This is because the Manager or admin domain is not the owner in this case.

You can use an ignore rule created at the Central Manager in the Manager. The ignore rules are pre-fixed with "NSCM" to distinguish between the ignore rules present in the Manager and the Central Manager. You cannot associate ignore rules at the Central Manager. However you can associate ignore rules created at Central Manager to Sensors at the Manager. You can export and import associated ignore rules from the Manager.

NOTE

- You cannot delete an ignore rule created by the Central Manager from the Manager.
- Ignore rules created at the Central Manager cannot be exported.

What happens to the synchronized ignore rules when communication between the Central Manager and the Manager is dissolved?

If the Manager uses an ignore rule created at the Central Manager, then the ignore rule is cloned and retained in the Manager as an ignore rule with an "NSCM" prefix. Even if the Manager has not used any of the synchronized ignore rules, they are retained in the Manager.

The key to synchronization of Central Manager rules objects and ignore rules with their respective local Manager is the object's name. For example, imagine that an ignore rule called "IG Rule A" is created in the Central Manager which is later synchronized with Managers. On the Managers' side, you will see the same ignore rule as "NSCM IG Rule A." These ignore rules synchronized from Central Manager are not editable but clonable.

Synchronizing custom attacks

You can create custom attacks in the Central Manager and publish it to the Managers. After creating custom attacks in the Central Manager, you should run policy synchronization for the custom attacks to reflect in the Manager.

Custom attacks defined in the Central Manager are synchronized with all Managers and are non-editable. The Attack ID format in the Central Manager custom attack is different from the Manager custom attack.

A specific Attack ID range within the existing format is allocated to a Central Manager custom attack. Policies are updated in the Manager after custom attack synchronization. The attack name is prefixed with "Central Manager" to represent custom attack policies defined at the Central Manager.

Synchronizing users

You can create users with specific roles in the Central Manager and assign the users the Managers. After creating users in the Central Manager, you should run policy synchronization for the users to reflect in the Manager. For more information on policy synchronization, see Synchronizing policies (page 529).

Monitoring Managers from Central Manager

One of the main advantages of having a Central Manager is that it allows you to manage and monitor multiple Managers spread across different geographies. In the Central Manager, you can view the reports, faults, and attacks of the individual Managers. This section describes how to monitor Managers from the Central Manager.

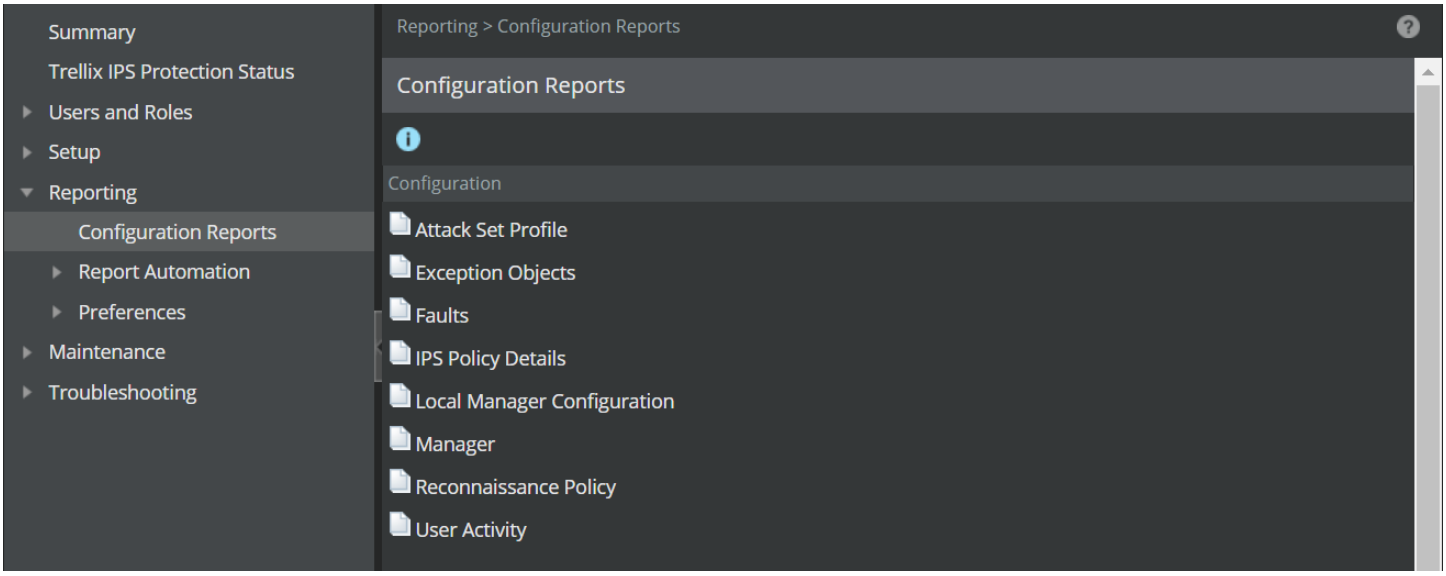
Viewing Manager reports in Central Manager

You can view Manager reports from Central Manager home page.

Access to the **Configuration Reports** main page is based on user roles. By definition, report generation is available for Super User, Security Expert, and Operator roles.

> **NOTE**
>
> Click **Back** to navigate to the **Configuration Reports** page from a generated report page.

Figure 223. Configuration Reports



The Central Manager provides the following configuration reports. The procedure for viewing these reports is similar to that in the Manager. For more information on the below reports, see the section Saving Configuration reports (page 243) and its following pages for individual reports.

- Attack Set Profile Reports

- Exception Objects Reports
- Faults Reports
- IPS Policy Details Reports
- Local Manager Configuration Reports
- Manager Reports
- Reconnaissance Policy Reports
- User Activity Reports

Templates

The **Templates** link found in **Event Reports** page under the **Analysis** tab helps you create and manage report templates. Note that while creating new report templates, you can select only **User Activity** in **Report Type** drop-down present in the **Add Report Template** page.

The other functions from **Templates** link are similar to report templates in Manager.

Reports Automation

To access this page, select Manager → Reporting → **Report Automation**.

Automation Settings

The **Automation Settings** sub-menu similar to that in the Manager.

Recipient List

The **Recipient List** sub-menu is similar to that in the Manager.

Report Scheduler

The **Report Scheduler** sub-menu is similar to that in the Manager.

Generate Exception Objects reports

The Exception Objects Report provides a detailed view of the exception objects available for application. Exception Object information includes address exclusion information configured for each user-customized filter.

To generate a report displaying all current Exception Object Editor filters, do the following:

Steps:

1. Click the **Manager** tab.
2. Select Reporting → Configuration Reports → **Exception Objects**.
3. Select a filter from the **Admin Domain** drop-down list.

> **NOTE**
>
> The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

4. Select one or more **Exception Objects**.

   This drop-down list displays the filters applied to the selected admin domain as well as the filters applied to its parent domains. However, for the parent-domain filters to be displayed in this list, they must be visible to their child domains.
5. Select or clear the checkboxes against **Matching Criteria** and **Assignment**.
6. Select the **Output Format**.
7. Click **Submit**.

Local Manager configuration reports

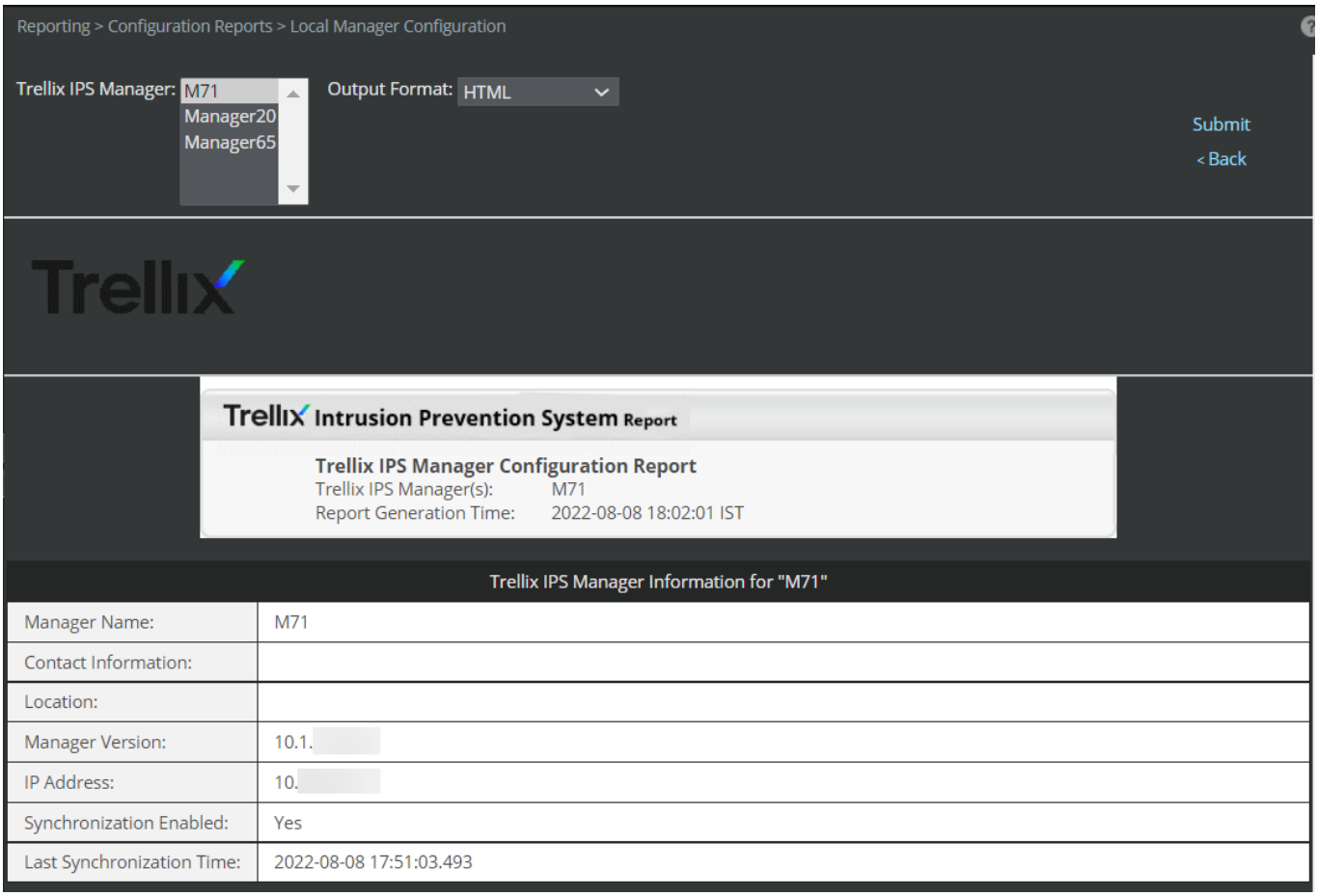
This report provides the configuration details of the local Manager added to the Central Manager.

1. Select Manager → Reporting → **Configuration Reports**.
2. Click the **Local Manager Configuration** link.

   The **Local Manager Configuration** report page is displayed.
3. Select a Manager from the Trellix IPS Manager list.
4. Select the **Output Format**.
5. Click **Submit**.

   The **Trellix IPS Manager Configuration Report** is displayed.

Figure 224. Trellix IPS Manager Configuration Report



The field description for the table in this report is as follows:

- **Manager Name**— Name of a Manager.
- **Contact Information**— The name of the user to contact.
- **Location**— Address of the user
- **Manager Version**— The current Manager version installed on your system.
- **IP Address**— IP address of the Manager
- **Synchronization Enabled**— Status of synchronization
- **Last Synchronization Time**— Time when the last synchronization took place

6. Click **Back** to go back to the **Configuration Reports** page.

Central Manager configuration report

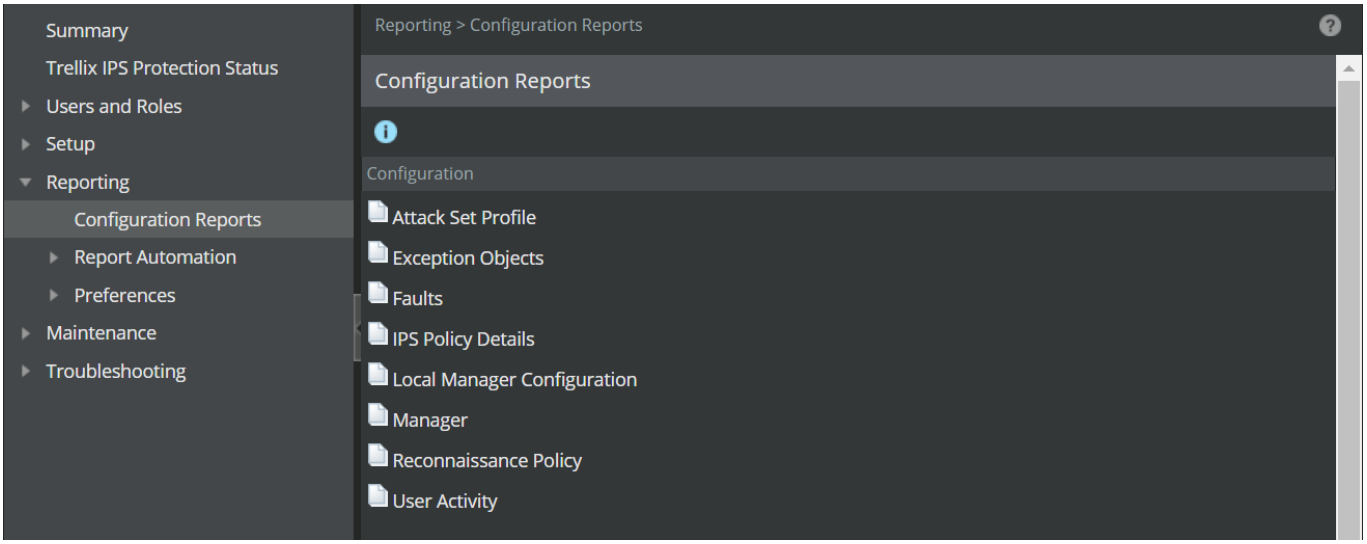
This report lists all the configuration details for the Central Manager. This report is displayed with the title **Manager Configuration Report**.

1. Select Manager → Reporting → **Configuration Reports**.
2. Click the **Manager** link.

   The **Manager** report is displayed.
3. Select the **Output Format**.
4. Click **Submit**.

   The **Manager Configuration Report** is displayed.

Figure 225. Manager Configuration Report



This report provides the following information regarding the Central Manager:

- Notification mail server settings
- Proxy server settings
- MDR information for Trellix IPS Central Manager
- Access Control
- Authorized hosts/networks
- Authentication details for RADIUS configuration and LDAP Configuration

Viewing Manger faults in Central Manager

You can view the system faults generated by the Managers in the Central Manager.

Faults

The Faults tab in Manager → Troubleshooting → **Logs** page displays messages that are generated to detail the system faults experienced by each of your Trellix IPS components installed.

NOTE

When management faults are raised and cleared too frequently on the Manager, the Manager may not have sufficient time to forward those faults to the Central Manager. As a result, there can be a fault count mismatch between the Manager and Central Manager for management faults.

To view the faults, follow the steps below:

Steps:

1. Go to Manager → Troubleshooting → **Logs**.

   The **Logs** page opens.

2. Select **Faults** tab to view the system faults.

   The data displayed in the table is based on the time frame of the core attribute in the faults table. By default, the logs for [last 7 days] are displayed. The data can be filtered for the time period of your preference using the **Custom Time Period** option.

   The following table lists the fields on the **Faults** tab:

Options	Definition
Time	Displays date and time of fault occurrence
Fault	Displays severity and summary of the activity • **Severity**: Displays severity level of the activity Different severity levels are as follows: • **INFORMATIONAL** • **WARNING** • **ERROR** • **CRITICAL** • **Summary**: Displays brief summary of the activity
Details	Displays brief report on nature of the activity
Duration	Displays the time period of fault existence
Device	Displays the details of the device that has generated the fault The **Device** column contains two sub-columns: • **Generated By** - Specifies the device that generated the fault. The device can be the Central Manager or a Manager • **Forwarded By** - Provides more information about the device that generated a fault. For example, if a Manager generates a fault, this column specifies if the device is a primary Manager, secondary Manager, or a Sensor attached to the Manger.

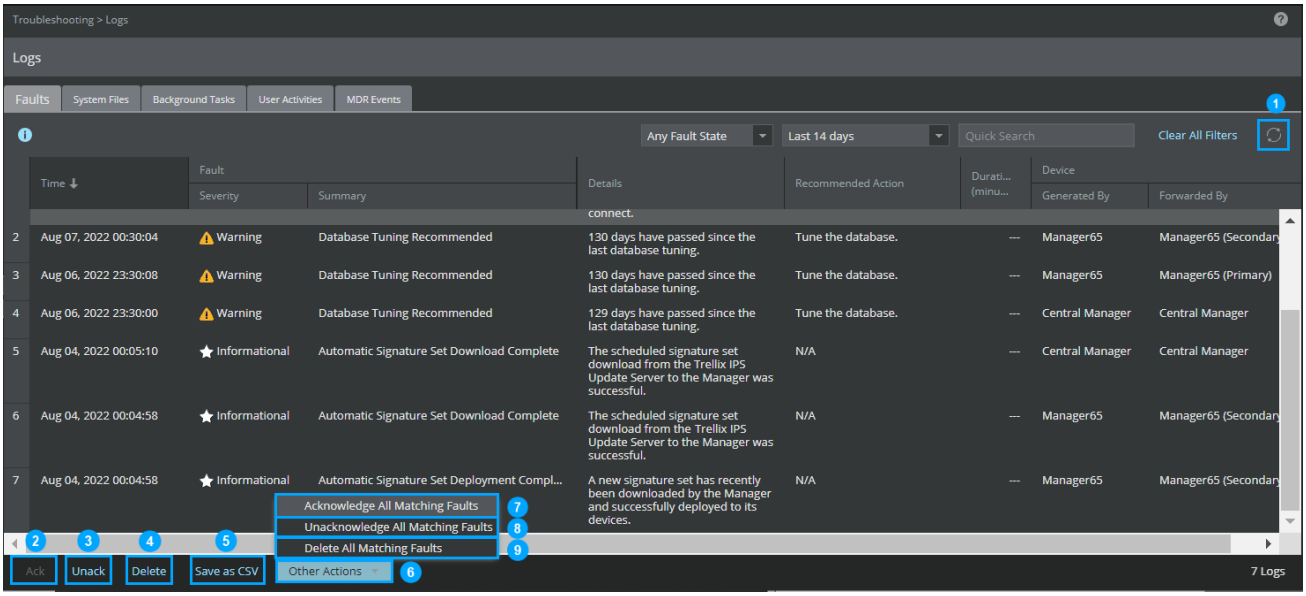
3. You can save a copy of faults by clicking **Save as CSV**.

NOTE

The **Save as CSV** option saves a copy of system faults based on the filters applied. To save a copy of all system faults, clear all filters before saving it as **Save as CSV**.

Faults tab action buttons

The following action buttons are available in the **Faults** tab:



Callout	Action button
1	**Refresh**—Updates the Manager faults log with new faults from the database.
2	**Acknowledge**— Marks the fault as acknowledged/read. Acknowledging a fault means that you are aware of its existence and plan to take appropriate action. To acknowledge a fault, select the fault and click the **Ack** button. When you acknowledge a fault, the fault will still be available in the Central Manager which can be used for analysis later.
3	**Unacknowledge**— Marks the fault as unrecognized. By default all faults are unacknowledged. You can unacknowledge an acknowledged fault. To unacknowledge a fault, select the fault and click the **Unack** button.
4	**Delete**— Deletes the selected faults from the Central Manager.
5	**Save as CSV**— Saves a copy of the faults displayed with filters applied.
6	**Other Actions**— You can perform further actions on the faults using the option available under **Other Actions**. The **Other Actions** has the following options: • Acknowledge All Matching Faults • Unacknowledge All Matching Faults • Delete All Matching Faults

Callout	Action button
7	**Acknowledge All Matching Faults**— Acknowledges all faults of the same type for the selected filter range.
8	**Unacknowledge All Matching Faults**— Unacknowledges all faults of the same type for the selected filter range.
9	**Delete All Matching Faults**— Deletes all faults of the same type for the selected filter range.

For a complete listing of system fault messages and their interpretation, see [System fault messages] in the [Trellix Intrusion Prevention System Product Guide].

Forward faults to a Syslog server

The Manager → Setup → Notification → Faults → **Syslog** option enables the forwarding of Trellix IPS faults to a syslog server. Syslog forwarding enables you to view the forwarded faults via a third-party syslog application. For syslog forwarding, the root domain and parent domains have the option to include faults from all corresponding child domains.

Following are the Syslog variables for fault notification:

Table 19. Syslog variables for fault notification

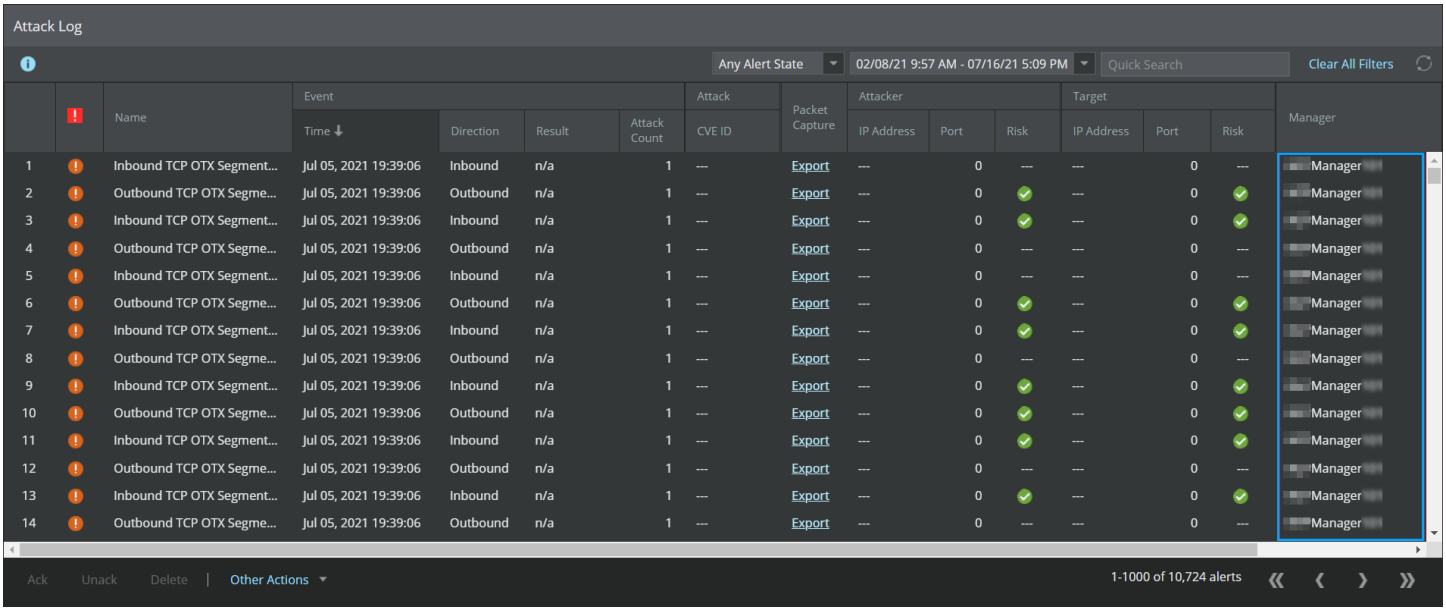
Syslog variable name	Description
$IV_ACK_INFORMATION$	Displays additional acknowledgment information when a created fault is acknowledged after the hysteresis period.
$IV_ADDITIONAL_TEXT$	Displays additional text for the raised fault.
IV_ADMIN_DOMAIN	Name of the domain.
$IV_DESCRIPTION$	Description of the fault.
IV_DEVICE_NAME	Name of the device.
$IV_FAULT_COMPONENT$	The component for which the fault is generated.
IV_FAULT_LEVEL	Displays the fault level (Manager system level, Sensor level, or Sensor interface level)
IV_FAULT_NAME	The name of the fault.
IV_FAULT_SOURCE	Indicates if the fault is generated by the Manager or sent by the Sensor.
IV_FAULT_TIME	The time at which the fault is generated.
IV_FAULT_TYPE	Indicates if the event is created, acknowledged, or cleared.
IV_OWNER_ID	ID of the Manager or the Sensor.
$IV_RECOMMENDED_ACTION$	The next steps recommended for the fault.
$IV_SEVERITY$	The severity of the fault (critical, error, or warning).

Viewing Manager attacks in Central Manager

Trellix IPS Central Manager provides you with a single sign-on mechanism to manage the authentication of global users across all Managers configuration. Threat analysis tasks are performed at the Manager level and aggregated at the Central Manager. Local Managers attached to the Central Manager push new alerts and modifications into the Central Manager. These alerts are aggregated in the Central Manager Attack Log.

Alerts from the Managers managed by the Central Manager can be monitored and managed from the Central Manager. The Attack Log of the Central Manager consolidates alerts from the local Managers and displays them for monitoring purposes.

Figure 226. Attack log in Central Manager

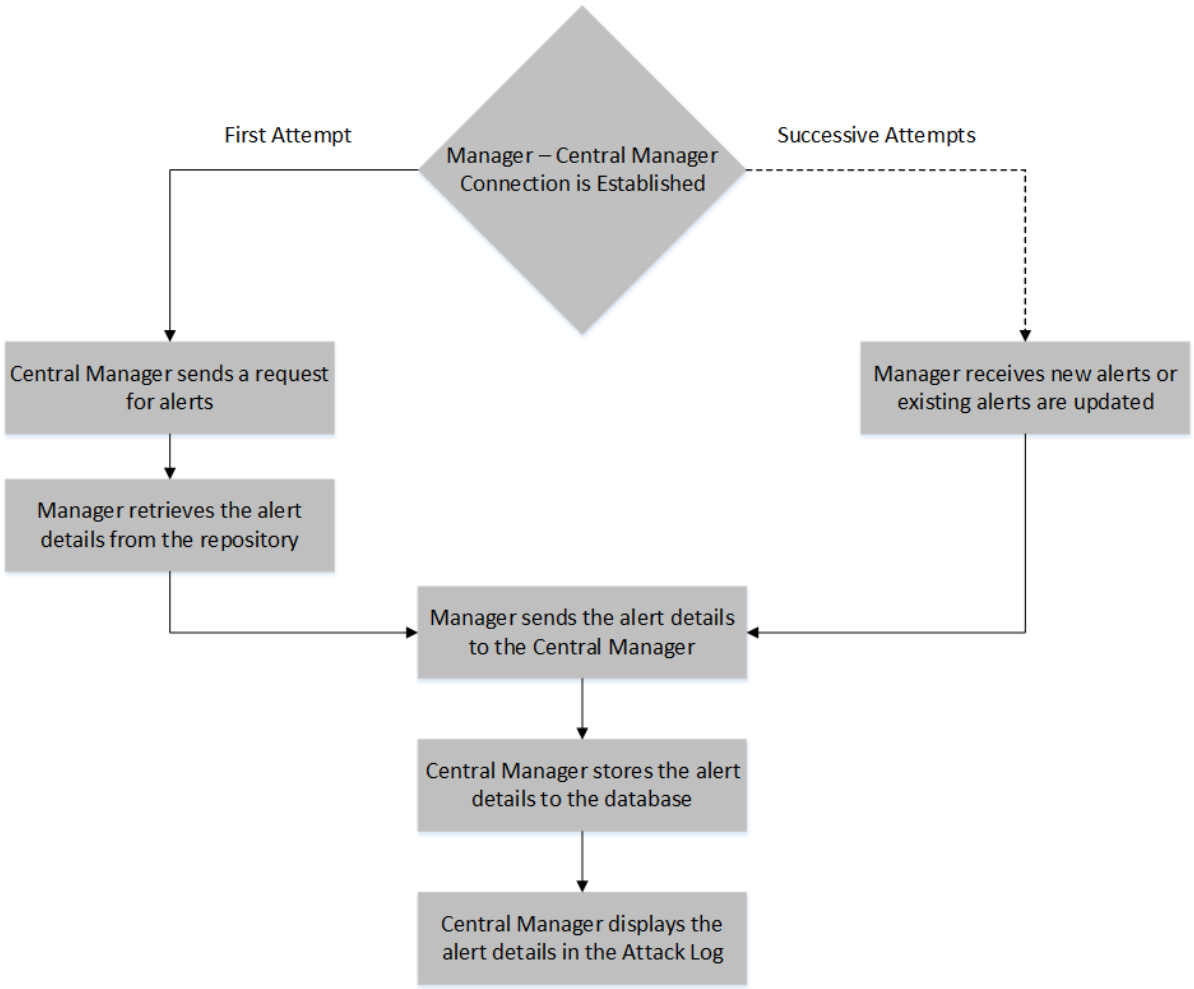


Once the Manager and the Central Manager establish a connection, the Central Manager sends a request to the Manager for alert details. The Manager retrieves the existing alert details and sends the information to the Central Manager.

When the Manager receives new alerts the next time or if an existing alert is updated, it retrieves the alert details from the repository and sends the information to the Central Manager. Once it receives the alert details from the Manager, the Central Manager stores alert details in its database and displays those details along with the Manager name in the Attack Log.

When a Manager is removed from the Central Manager, all the alerts synchronized from that Manager are also removed from the Central Manager repository.

Figure 227. Display of alerts in the Central Manager Attack Log



NOTE

To view **Endpoint** information, go to Analysis → <Admin Domain Name> → **Quarantine** in the corresponding Manager.

For more information on Attack Log, refer to the [Attack Log] section this guide.

Managing users in the Central Manager

Users defined at Central Manager are called global users or Central Manager users. They have the same roles as in the Manager, such as Super User, System Admin, or Security Expert. This global user can log on to every Manager associated with that Central Manager, and has the same permissions associated with the role as assigned at Central Manager level. Therefore, if a user is an operator at Central Manager, the user has operator permissions across all associated Managers by default.

NOTE

Custom roles cannot be created in Central Managers.

User authentication

Users created at a Manager level can log onto that Manager alone. LDAP and RADIUS configurations can be inherited or customized in Managers.

If the user credentials are changed, but synchronization has not yet taken place with the Central Manager, the user needs to enter the old credentials to log onto the Manager.

Authentication using LDAP

The LDAP communication from the client Managers is over a secure communication. Therefore, LDAP configuration information is valid and can be passed onto all the Managers.

The LDAP server configuration in the Central Manager should be synchronized with all Managers.

If a LDAP configuration is done at the Central Manager, and no LDAP server exists at the Manager level, then after synchronization, the Manager will inherit the configuration with a suffix "Inherited".

If the Manager has its own LDAP configuration, it will not inherit the configuration from the Central Manager level; it will have its own customized configuration with a suffix "Customized".

At any time, if a user deletes the configuration made at the Manager level, the inherited configuration is displayed.

For more information on configuring a LDAP server, see Configuration of LDAP servers (page 209).

NOTE

If LDAP servers are configured with the Central Manager, and the LDAP servers exist in private networks and Managers exist in public network, the LDAP configuration needs to be customized at the Manager in a way that it reaches the LDAP server through translated public IP address.

Authentication using RADIUS

If RADIUS configuration is done at the Central Manager, and no RADIUS server exists at the Manager level, then after synchronization, the Manager will inherit the configuration with a suffix "Inherited".

If the Manager has its own RADIUS configuration, it will not inherit the configuration from the Central Manager level; it will have its own customized configuration with a suffix "Customized".

At any time, a user deletes the configuration made at the Manager level, the inherited configuration is displayed.

For more information on configuring a RADIUS server, see Configuration of RADIUS server in the Manager (page 213).

NOTE

If the RADIUS servers are configured with the Central Manager, and the RADIUS servers exist in private networks and Managers exist in public network, the RADIUS configuration needs to be customized at the Manager in a way that it reaches the RADIUS server through translated public IP address.

User role assignment

The roles such as super user, restricted user, and operator roles are the same for both the Central Manager and the Manager.

The Central Manager acts as a parent domain for every Manager. User roles which are defined at the Central Manager level can be used at the Manager level and will have the same privileges as defined at the Central Manager level.

It is possible to upgrade the role of a Central Manager user at an individual Manager level.

For example, an operator role has been assigned to a user at the Central Manager level. After synchronization, at the Manager level, the role is edited to a Super user. The user now has an operator role at the Central Manager as well as other Managers, but has a Super user role in a single Manager. If the operator uses the single sign-on option, the operator has the operator rights for that Manager, but if the operator logs onto that Manager directly, the operator has Super user rights.

The prefix "Central Manager" is added to the global user to distinguish the role from the Manager user role.

Overriding users with the same name

There can be two users created with the same name, one in the Central Manager and another in the Manager. If their passwords are same, then the Manager will let the user log onto either.

NOTE

If two users with the same name, user1, are created at Central Manager and Manager respectively, then during synchronization, the role defined for user1 at the Central Manager level will be inherited by the user1 at the Manager level.

Central Manager users and roles

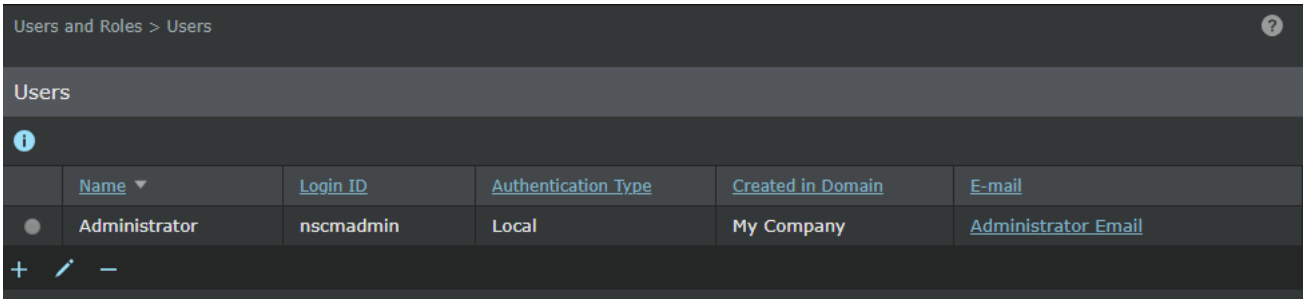
Trellix IPS enables the creation of users for various administrative functions. This enables selected entities (users/groups/business units) to manage specific domain resources.

User management in the Trellix IPS environment consists of creating users and granting them permissions. Network security requires careful planning when creating users to ensure the integrity of the environment. All users must authenticate at the Central Manager logon page before to performing *any* activities. The user name and password are securely stored in the database with matching permissions rules. A class of user permissions termed **Roles** determines the authorized activities of the various users in the system. Once a user logs in, the Central Manager makes available activities based on the role.

User management

The **Users** page (Manager → Users and Roles → **Users**) enables you to create, edit, and delete users.

Figure 228. Users page



When you are in **Edit** ( )mode, you will see the **Reset GUI Presentation** button. This version of the Manager allows you to make changes to a column or panel presentation. For example, you can resize the width of a column in a table or apply a filter by using a small arrow situated next to a column. Once you customize the width of a column or apply a filter, it stays that way even when you log out and log in next time. If you want to reset these changes and revert to the default settings, click **Reset GUI Presentation**.

These functions have similar steps to that in the Manager. See the following sections:

- Adding users
- Editing users
- Deleting users

NOTE

Users created in Central Manager are synchronized with all associated Managers. These users cannot be edited or deleted in any of the Managers.

Super users

Trellix IPS resources are governed by users with super user access; a super user is allowed to configure every resource and function in the system. Each shipped Central Manager is configured with one built-in super user account, including a default password.

CAUTION

The default super user account username is **`nscmadmin`** and password is **`admin123`**. Trellix **strongly recommends** that you change the default super user password for security purposes. The new password must be at least 8 characters in length and must contain a combination of numbers, characters, and special characters. For more information on the password control, see Configure password complexity settings (page 229).

Role Assignment

A **Role** is defined as a group of actions that a user is allowed to perform in Trellix IPS. Users authenticate themselves by logging into the Central Manager prior to performing any configuration activity. Not all users are allowed to fully administer the Central

Manager; thus, user management controls the roles, the list of authorized activities, and the users that belong to that role. The roles assigned to a user in Central Manager, are carried forward to all associated Managers. The roles can however be changed to a higher role in an individual Manager. This upgraded role will apply only to that particular Manager.

Managing roles for Central Manager is similar to that of Manager. Roles can be default user roles such as Super User, or custom roles such as Operator, Security Expert, or System Administrator.

Role Assignments tab in Central Manager

The **Role Assignments** page (Manager → Users and Roles → **Role Assignments**) enables administrator to assign roles to users in the Trellix IPS. Adding a user requires the application of a *role*, or privilege, thus limiting a user's configuration abilities.

NOTE

You must first create a user through the **Users** action before assigning a role.

Role descriptions

The following section summarizes the Trellix IPS-provided user roles in the Central Manager.

Table 20. Roles and Descriptions

Role	Descriptions
ePO Dashboard Data Retriever	The **ePO Dashboard Data Retriever** has rights to retrieve information from Trellix IPS to ePO for displaying Trellix IPS information in the ePO.
NOC Operator	The **NOC Operator** monitors the security environment.
Report Generator	The **Report Generator** runs reports.
Security Expert	The **Security Expert** role largely pertains to managing intrusion policies. The **Security Expert** administers the IPS and NTBA environments. The **Security Expert** can create, edit, and delete policies, view alerts, manage software and signature update downloads, generate reports, manage system faults, and handle security alerts.
Super User	The **Super User** role (not represented by an icon) enjoys all privileges. Each shipped Manager is configured with one built-in Super User account including a default password. The **Super User** role provides: • all the privileges possible in the current domain • all the privileges a **Super User** has in all the children of the current domain • the special privilege to assign (or remove) the Super User role for a user in the current domain A **Super User** can be defined at any level, and the role applies to the current domain and all of its children, but not for its parent domain or any other "sibling" domains.

Role	Descriptions
System Administrator	The **System Administrator** role pertains strictly to administration of the system itself. The **System Administrator** administers the Manager and the Device List. Tasks permitted to the **System Administrator** include managing software and system performance; adding, deleting, or configuring Sensors, and handling system faults.
No Role	No role is assigned to the user.

Modify user roles

A role determines the actions a user can perform in a given domain. Roles enable task-specific actions to multiple users of your Trellix IPS security environment. As your security implementation grows, utilizing multiple users to perform the various role-based tasks can facilitate security management.

A created user is not required to have a role. You can assign or remove a role to/from a user at any time.

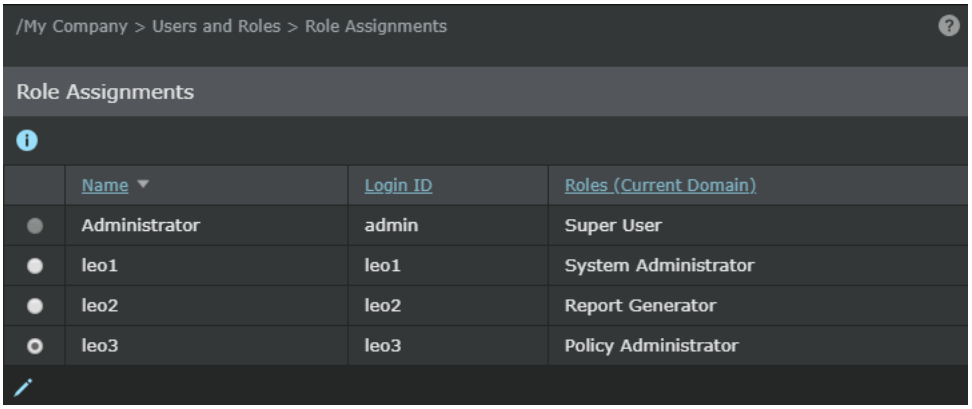
To edit the role assigned to a user, do the following:

Steps:

1. Go to, Manager → Users and Roles → **Role Assignments**.
2. Select a user in the role assignment table.
3. Click .
4. View the user's role assigned.
5. Select the role you want the user to have.
6. Click **Save**.

   The new role assigned is updated in the Role Assignments table.

Figure 229. Role Assignment window



Custom roles

The **Roles** page (Manager → Users and Roles → **Roles**) is used to define the required custom role to a user.

The custom roles defined in Central Manager are similar to that in Manager.

Account information management

The **My Account** action displays the **My Account** page, which lists the account information for the logged-in user. The navigation path for this page is Manager → Users and Roles → **My Account**.

If you want to edit the information (password, address, and so forth), clear the appropriate field, type the new information, and click **Save**. Click **Cancel** to exit without saving the changes.

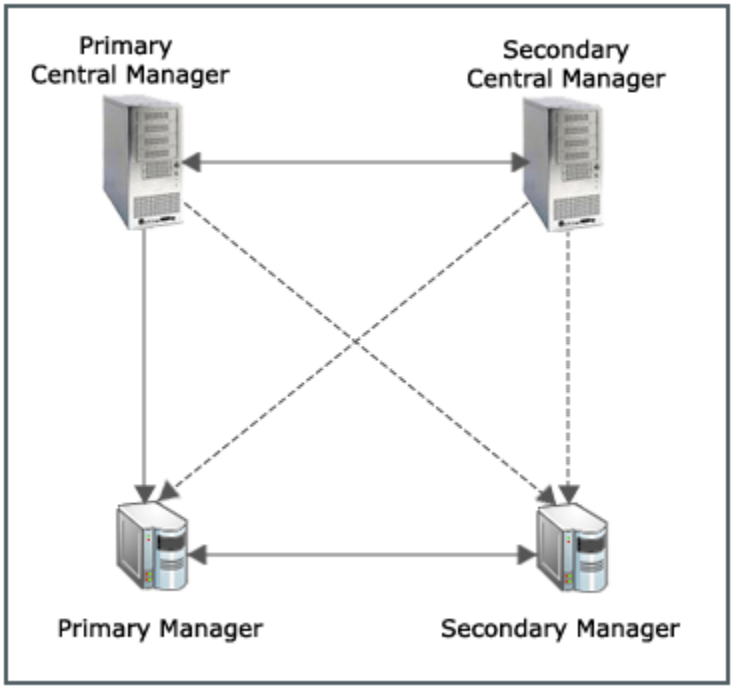
When you are in **Edit** mode, you will see the **Reset GUI Presentation** button. This version of the Manager allows you to make changes to a column or panel presentation. For example, you can resize the width of a column in a table or apply a filter by using a small arrow situated next to a column. Once you customize the width of a column or apply a filter, it stays that way even when you log out and log in next time. If you want to reset these changes and revert to the default settings, click **Reset GUI Presentation**.

Managing your account for Central Manager is similar to that of Manager.

MDR support for the Central Manager

The MDR feature is supported at the Central Manager level as well as the Manager level. The active Central Manager has the ability to synchronize with the active Manager.

Figure 230. MDR layout for Central Manager



Similarly, in case a switchover happens at the Central Manager level, the Secondary active Central Manager can communicate with the Manager.

The **MDR** page enables you to have a standby Central Manager available in case the primary Central Manager fails.

The Central Manager Disaster Recovery (MDR) feature is available for deployments where the following conditions are met:

- Two Central Managers (called Primary and Secondary) are available. The Primary is in active mode and the Secondary in standby mode.
- The Primary and Secondary use the same Central Manager software release version. MDR is supported on Central Managers with version numbers that match in the first three places.
- The Primary and Secondary have a similar database structure.

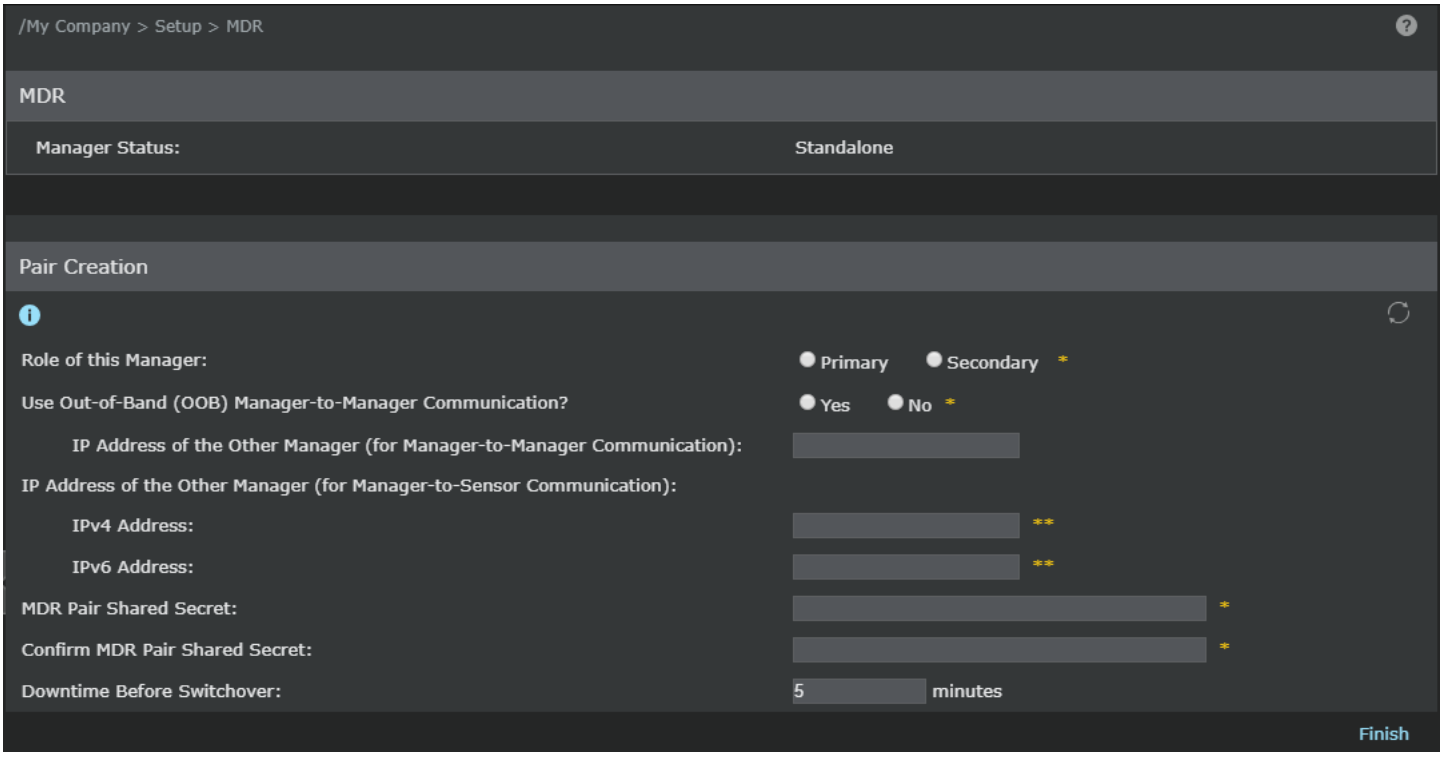
The **MDR** page in Central Manager provides the following functions:

- Configuring the Central Manager for MDR
- Switchover History

Configure MDR in Central Manager

You can configure the MDR pair in Central Manager from Manager → Setup → **MDR**.

Figure 231. Manager Pair



NOTE

The configuration for Central Manager in MDR is similar to that in the Manager. For more information on the fields in **Pair Creation**, see the section Configure MDR (page 128).

When you enter the Peer Manager IP Address in the Manager Pair, consider the following:

Enter the IP address of the peer Manager (that is, use the address of the Secondary Manager if you have designated this Manager as Primary). You can configure either IPv4 address or IPv6 address or both, as given in the following scenarios:

Steps:

1. If a Manager is configured in Central Manager over IPv4 network, or you want to add a Manager from the IPv4 network to the Central Manager, you need to enter the IPv4 address of the peer Manager (Central Manager).
2. If a Manager is configured in Central Manager over IPv6 network, or you want to add a Manager in the IPv6 network to the Central Manager, you need to enter the IPv6 address of the peer Manager (Central Manager).
3. If there are Managers configured in Central Manager over both IPv4 and IPv6 networks, you need to configure both IPv4 address and IPv6 address of the peer Manager (Central Manager).

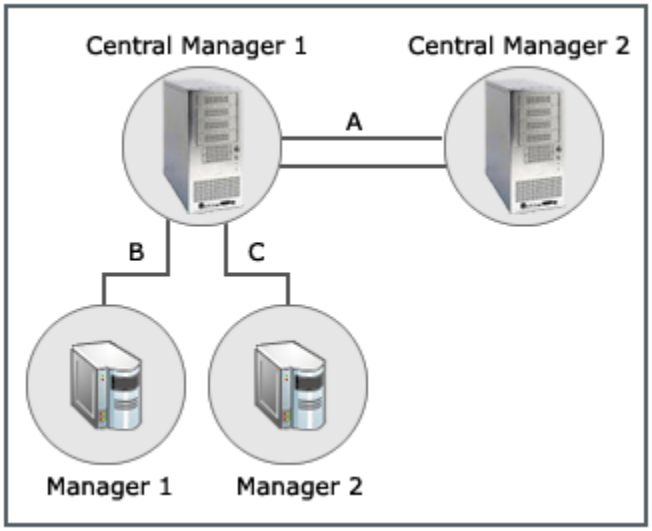
> **NOTE**
>
> While configuring the **Peer Manager IP Address**, ensure that the operating system supports both IPv4 and IPv6 stacks.

Scenario - MDR pair configuration for Central Manager

The following scenario explains the above points.

One Central Manager (Central Manager 1) is standalone (not part of an MDR pair), and you want to add another Central Manager 2 to the standalone Central Manager 1 to form an MDR pair.

Figure 232. MDR pair configuration for Central Manager



If the communication between Managers and Central Manager 1 (that is, B and C in the figure) is over IPv4 network, the communication between Central Manager 1 and Central Manager 2 (that is, A) should also be configured for IPv4 network.

Similarly if the communication between Managers and Central Manager 1 (that is, B and C in the figure) is over IPv6 network, the communication between Central Manager 1 and Central Manager 2 (that is, A) should also be configured for IPv6 network.

If the communication between Managers and Central Manager1 is over both IPv4 and IPv6 networks (that is, B is in IPv4 and C is in IPv6), the communication between Central Managers 1 and 2 (that is, A) can be configured to support either IPv4 or IPv6 networks.

NOTE

If you want to setup a MDR for the Managers, connect Primary Manager of MDR to the Central Manager. On the next MDR configuration synchronization, the Central Manager gets the details of the Secondary Manager and the Central Manager lists both the Primary Manager and the Secondary Manager.

MDR Events

You can view the previous MDR activities, including the date and time on which the activity occurred, the users performing the activity, and the nature of the activity. For more information, see MDR Events (page 352).

Synchronize faults in an MDR set up

Faults are synchronized from the Manager to the Central Manager. The faults (real-time faults or alarms) generated in the Managers are seen in the **System Faults** page of the Central Manager. You can customize your view of the alarms based on severity and alarm status. The Central Manager can acknowledge, unacknowledge and delete the Manager alarms. The changes are reflected in the **System Faults** page.

Alarms are resynchronized after every disconnect and reconnect between the Manager and the Central Manager and is shown in the Central **System Faults** page.

Alarms (displayed in the **System Faults** page) are automatic and are displayed as and when the alarm occurs in the Managers. For example, if there is a network disruption between Manager and Central Manager, an alarm is generated at the Manager. This alarm is immediately shown in the Central Manager. Once the connection is restored, the alarm is removed from the Manager as well as Central Manager.

Historical Faults can be viewed in the Fault Log reports. These historical faults are synchronized to the Central Manager to get a consolidated view of Faults of all the Managers. This synchronization can be done manually or can be scheduled.

All the fault logs are reported in the Fault log report and is available to the Central Manager only after synchronization.

The Fault synchronization scheduler synchronizes the faults from the Manager database to the Central Manager database. You can see the audit log messages for the fault log synchronization in the Central Manager.

Faults are sent to both Central Managers when in MDR mode. Real-time faults (Alarms) are automatically sent to both the Managers. But fault logs are sent only to the active Manager and copied to the secondary Manager as part of the MDR synchronization.

In the Manager, the Alarm synchronization is enabled by default. That is, the Manager starts the synchronization of alarms as soon as it connects to the Central Manager. In case the user wants to turn it off due to some reason for a particular Manager, the user can do so using the iv.mom.alarmSync.enabled property in ems.properties file by setting its value to false.

Fault synchronization in an MDR set up

There are four possible scenarios of fault synchronization in an MDR set up.

1. **Real-time alarms for Manager in MDR**— In such a case both the active and standby MDR alarms are synchronized with both Central Managers, if Central Manager is in MDR.
2. **Fault log for Manager in MDR**— Both the primary and secondary Manager's fault logs are synchronized only with the active Central Manager.

3. **Real-time alarms for Central Manager in MDR**— In active Central Manager, only the alarms of the active Manager can be acknowledged or unacknowledged or deleted. The standby Manager's alarms are read-only. In the standby Central Manager, all the synchronized alarms are read-only.
4. **Fault log for Central Manager in MDR**— Fault log is sent only to the active Central Manager and NOT copied to the secondary Central Manager. But when the standby Central Manager becomes active, a full fault log sync is made.

IPS Administration

Network security and Trellix Intrusion Prevention System

The network-security landscape is ever-changing. As technology gets sophisticated, so do the threats. The Internet explosion exposed corporate networks to even teenagers sitting in their garages at home. The hackers of those days were continuously trying to test the security of various systems and networks. Some were simply seeking some sort of intellectual high, while others were fueled by more treacherous motives, such as revenge or stealing for profit.

Hacking these days is very organized and focused. It involves a lot of planning, collaboration, and persistence. Contemporary hackers are no more just the amateur individuals of yesteryears. On one hand, you need to protect your network from hackers working for rich corporations and nation states. On the other, you are up against ideology-driven hacktivism. In addition to these, the biggest challenge for governments and defense establishments is cyber-terrorism.

These days your network is perpetually under one attack or the other. So, it is not enough if you just ensure that all the doors and windows to your network are locked, and the alarm is turned on. In addition to alerting on intrusions, malware, and policy violations, your security system needs to provide you complete visibility into your network. Some of the things that you need to continuously monitor are:

- The current users on your network
- The devices on your network
- The applications being used on your network
- The type and quantity of traffic traversing your network
- The source and destination of the traffic

This section discusses some of the current threats to your network and how you can use Trellix IPS to mitigate those threats.

Network security threats and trends

As always, the challenges for security experts are on the rise. The technological advancements in the availability of the Internet, mobile computing devices such as smart phones, social networks and other Internet applications have all contributed to the current realm in network security.

As a security expert, you need to be aware of your challengers, the probable points of entry for hackers, and the current techniques in hacking.

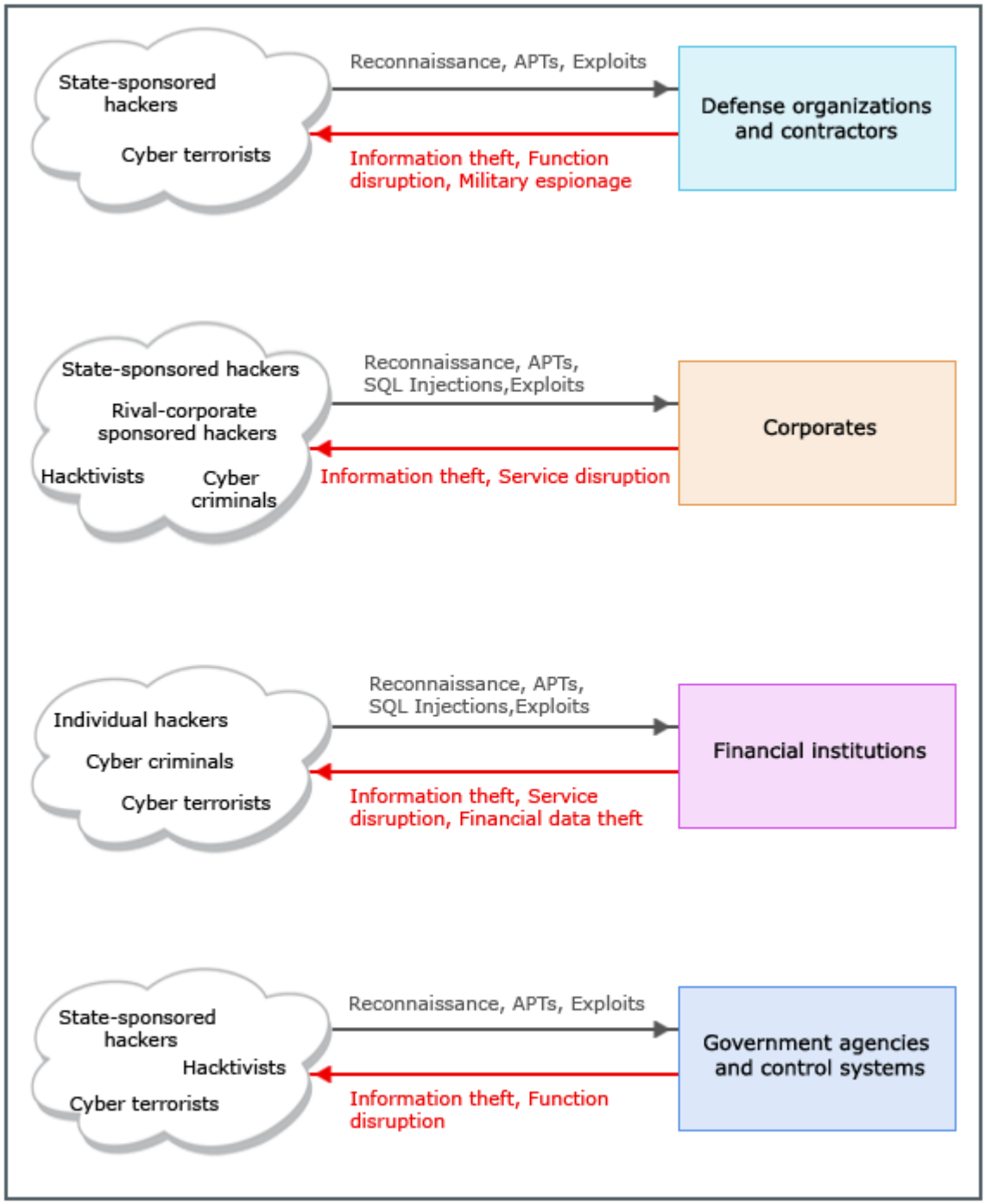
Who are you up against

With the challenges from individual, unorganized hackers still remaining true, the new generation of hackers can be broadly classified into categories.

- **Hackers sponsored by corporations and nations (not necessarily rogue)**: The purpose here is industrial or military espionage. As a security expert working for enterprises, the advantage that you had over the previous generation hackers is the funds to buy the required facilities and technology. This advantage is fast vanishing since your challengers are also equally funded if not more.
- **Hacktivists**: The purpose of these hackers is to retaliate against corporations or government agencies for their decisions.
- **Cyber terrorists**: These hackers are ideology-driven but sponsored by rogue nation states.

- **Cyber criminals**: These hackers work for international organized crime with the sole purpose of targeting financially sensitive data.

Figure 233. Categories of hackers



Contributing factors to security threats

Technological advancements have contributed to the growth of businesses. However, this has also put security professionals in an unenviable position. Some of the main contributing factors to the current security threat environment are:

- **Internet-based business world**: Across industries, organizations depend on the Internet to run their business. Their network is open to their vendors, partners, customers, and even the public.
- **Mobile computing devices and BYOD**: Handheld devices are now available with a very high computing power and storage capacity. More and more organizations are encouraging the Bring Your Own Device (BYOD) concept, wherein the employees bring their personal mobile devices to their offices and use them for official purposes as well. While it is true that BYOD can save money and space for the organization, the flipside is that it is a huge security threat. To mitigate this threat, your security system must be able to:
  - Detect the device and its type as soon as it comes on to your network.
  - Quickly assess the device's posture, detect the user logged on, and the Wireless Access Point to which it is connected and grant the appropriate access.
  - Detect and report any undesired activity involving the device.
- **Internet applications and their usage**: Internet-based applications such as social networking sites and multimedia-based applications come with their own set of vulnerabilities. More the features, more are the chances for vulnerabilities. It is not just the recreational applications, but business and productivity applications that users find to be more powerful and capable compared to the equivalents approved by your organization. In some cases, organizations do allow some of the open Internet applications to be used for business purposes. This means that your security system must be capable of identifying each and every application on your network for you to control the undesired ones.

  In addition to the vulnerabilities of the applications, the network bandwidth consumed by these applications is also a concern. For example, you cannot allow a video-based recreational application to cause network bandwidth deficiency during business hours.
- **Storage devices**: Over the years, storage devices have been increasing in capacity but decreasing in size and cost. Your security system must be capable of validating the data coming from and going to such devices.
- **Easy availability of hacking tools**: You do not need to be technical savvy to be a hacker. One can buy the required hacking tools over the Internet.

What are you up against?

Every technological advancement provides new options to hackers. Some of the popular trends that are used to attack networks are:

- **Exploits**: A hacker attempts to take advantage of hidden features or bugs in a system in order to gain unauthorized access. Examples include buffer overflows, directory traversal, and DNS cache poisoning.
- **Advanced persistent threats (APTs)**: APTs are unrelenting attacks against specific networks over a long period of time. APTs are purpose oriented. They target specific networks for specific goals. The attackers probe the target network for the most feasible entry point and then launch the attacks using the most appropriate technique. It could be a simple or complex technique, but they choose one that can help them achieve their goals. The attackers take care to remain undetected and persist with different methods until they succeed. The usual purpose is to gain financially or intellectually. It is very difficult to trace the source because APTs are mostly sponsored by nation states. Therefore, they are backed up by people, technology, and almost unlimited funds.
  - **Advanced malware**: Earlier users received malware as attachments in their emails. With the upsurge in Internet applications, users only need to click on a link to download files. Today, there are many other options to post such files - blogs, social networking sites, websites, chat messages, webmails, message boards, and so on. Your security system must not only be able to detect known malware but zero-day ones as well.

  - **Bots**: These are malware running on compromised systems. They are part of a larger, centrally managed network of such compromised systems. This network of compromised systems reporting to one command and control system is referred to as a botnet.
  - **DoS and DDoS**: Denial of Service (DoS) attack is a malicious attempt to render a service, system, or network unusable by its legitimate users. The previous generation DoS attacks do not require the attacker to gain access or entry into the targeted server. The primary goal of such DoS attacks is to deny legitimate users access to the service provided by that server. Distributed Denial of Service (DDoS) involves many compromised hosts across the Internet, to launch a DoS attack. Attackers typically use various tools to launch DoS and DDoS attacks.

    DoS attacks have now evolved to exploit vulnerabilities in the web applications themselves. The aim is to turn off the service, thereby denying access to legitimate users. This technique produces the same result as the traditional DoS but costs less in terms of time and money.
- **Reconnaissance**: These include host sweeps, TCP or UDP port scans, e-mail recons, brute force password guessing, and possibly indexing of public web servers to find CGI holes or other system vulnerabilities that might later be exploited.
- **SQL injections**: Because of their location and their functionality, web servers are usually the favorites for hackers. Mere signature-based detection cannot adequately protect your servers. You need an IPS that can quickly and intelligently detect SQL injections.
- **Bandwidth-consuming applications**: As a security expert, you must be concerned not just about attacks but also about multimedia-rich applications bringing your network to a halt by consuming the majority of the available bandwidth. Your security system must be capable of identifying and regulating application traffic.
- **Virtual environments**: Organizations are increasingly moving towards virtual environments. So, your security system must be capable of inspecting traffic between virtual machines residing on the same host.
- **Applications using non-standard ports**: Current threats involve exploiting the use of non-standard ports to evade the IPS boxes. Your security system must be intelligent enough to address this issue.
- **Browser-based attacks**: Browsers have become feature-rich and very user friendly with the support for new features, including HTML 5. However, this also offers new opportunities for hackers.
- **Policy violations**: This denotes to all activities for which the underlying traffic content may not be malicious by itself, but are explicitly forbidden by the usage policies of your network as defined by your security policy. These can include "protocol violations" wherein packets do not conform to network protocol standards. (For example, they are incorrectly structured, have an invalid combination of flags set, or contain incorrect values.) Examples might include TCP packets with their SYN and RST flags enabled, or an IP packet whose specified length does not match its actual length. A protocol violation can be an indication of a possible attack, but can also be triggered by buggy software or hardware.

Figure 234. The network security threat landscape

Fortifying your network using Trellix Intrusion Prevention System

Contemporary hackers have more resources at their disposal, especially when backed up by rival corporations and nation states. Your security system must be very dynamic, intelligent, and proactive to help you meet evolving techniques and successfully defend your network every time. As a reactive strategy, it must be capable of blocking attacks and warn you of any strange activity in your network. For the proactive part, your security system must be capable of notifying the vulnerabilities in your network and also provide you the visibility of even the normal traffic on your network. A proactive security system enables you to be a step ahead of your challengers.

Trellix IPS is a network-based IPS that combines purpose-built network security devices and management software for the accurate detection and prevention of known attacks using signature detection and zero-day attacks using anomaly detection. It also provides you next-generation IPS features such as internal-firewall and QoS.

The add-on McAfee™ Network Threat Behavior Analysis appliance monitors and presents you a real-time view of your network traffic. Trellix IPS also collaborates with other Trellix products on your network to provide you complete network protection.

What are attacks and intrusions?

Trellix IPS considers any unauthorized action taken with the intent of hindering, damaging, incapacitating, or breaching the security of your network as an attack. An attack typically prepares for or carries out threats to your critical assets. Attacks can be active, wherein the goal is to directly exploit some vulnerability in a system or software package. In contrast, passive attacks generally consist of monitoring or eavesdropping on traffic with the intention of viewing or capturing sensitive data.

The result of a successful active attack is an intrusion-disruption of the normal services, unauthorized access, and/or some form of tampering with the system. When you install Trellix IPS in the prevention (IPS) mode, it detects and blocks attacks. In the detection (IDS) mode, it reports the attacks. However, based on the type of attack, the attack traffic might have reached the intended target.

How Trellix IPS protects your network

Trellix Intrusion Prevention System offers multi-gigabit performance, flexible deployment, robust scalability, and easy-to-use intrusion detection and prevention. Trellix IPS goes beyond the simple string matching. Sensors analyze and validate the traffic to its basic protocol elements and inspect specific protocol fields to improve accuracy, while maintaining full flow and application state. The Sensors perform IP fragment reassembly and TCP stream reassembly, and perform thorough protocol analysis all way up to the Application Layer. The signature engine searches in a flow for multiple triggers (that is, sub-signatures) in multiple fields of a protocol using Trellix IPS embedded signature files to increase the precision by which an attack can be unambiguously detected.

Once the packet is captured, it is analyzed into its corresponding protocol fields. The Sensor analyzes a frame completely and thoroughly from Layers two through seven, and understands the semantics of the protocol fields even at the Application Layer. After it analyzes the protocols, it verifies that the packet conforms to the protocol specification. Trellix IPS then passes the parsed packet through its other engines, such as the DoS, Signature and Anomaly detection engines, Malware engine, and internal Firewall engine. This enables Trellix IPS to be very efficient in terms of packet processing because the packet is "peeled" only once and then fed to the corresponding detection engines. All these processes are designed to provide the required wire-speed performance.

If the detection engines detect something abnormal, they pass an alert and corresponding data to the management process that is running on the Sensor. The management process can then trigger the appropriate response, based on policy, and send alerts to the Manager. This response can include blocking the corresponding traffic entirely and even quarantining the attacking host.

In addition to dropping malicious traffic, Trellix IPS provides "packet scrubbing" functionality to remove protocol inconsistencies resulting from varying interpretations of the TCP/IP specification, which can be used by hackers to evade IDS/IPS and other security devices.

The accuracy level of Trellix IPS is exceptionally high due to the following factors:

- Full protocol analysis and state tracking
- Multi-trigger, multi-field pattern matching
- Trellix IPS's ability to see all the traffic in a variety of deployment modes, including active/active, active/passive, and asymmetrically routed traffic environments.

Protection against APTs: Trellix IPS performs deeper inspection of traffic to detect malicious file downloads and bots. It uses various malware scanning options for advanced malware protection. This includes an embedded PDF emulator that detects zero day java script threats in PDF downloads. It also runs the gateway anti malware engine on the NTBA appliance.

For bot-detection, Trellix IPS correlates multiple attacks across different flows by observing a host over a given period of time. It also forwards the attack information to the NTBA appliance for similar correlation.

Trellix IPS detects DoS and DDoS through threshold-based and self- learnt profile-based detection techniques. In addition, it provides a connection-limiting feature that limits the number of connections a host can establish.

Protection for web applications: Trellix IPS provides various features to protect your web application servers. For example, it employs a heuristic engine to detect SQL injections. Trellix IPS can inspect HTTP responses to ensure your servers are not compromised.

For inbound SSL traffic, in case of Known-Key method, the Sensor decrypts and analyses the SSL traffic based on the server's private key. In case of Agent-based method, the Sensor decrypts traffic based on the key exchanged by the agent installed on the web server with the Sensor. Based on the result of the inspection, the traffic is either allowed to go the client or blocked.

In case of outbound SSL traffic, the Sensor decrypts the traffic by matching with the trusted CA certificates in the Manager. After the Sensor inspects the traffic, the traffic is encrypted using the re-signing certificate.

Application Identification: Trellix IPS can identify the applications traversing your network and act on them as configured. So, you can allow or block specific applications or application features on your network. For example, you can block the connections to Facebook from your network while allowing all other HTTP traffic.

Identifying users and user groups: Trellix IPS integrates with Trellix Logon Collector to identify the Windows AD users on your network and also the user groups to which they belong. This means that you can now control based on users rather than their IP addresses, which are not always reliable. For example, a dynamic IP address might differ based on whether the user connects from office or outside office.

Next-generation IPS features: Trellix IPS provides next-generation IPS features, such as internal Firewall and QoS.

You can create different Firewall rules for different segments of your network. You can base these rules on the traditional 5-tupple with support for IPv6. In addition, you can base them on the applications, application features, Windows AD user data, geographical location, and time. This enables you to control the privileges of your network users regardless of whether they log on from home, airport, or office.

The Sensor evaluates the traffic against the Firewall rules before checking it for attacks. So, you can use this feature to filter the traffic that must be inspected for attacks.

You can create QoS rules based on similar criteria as for Firewall. These rules ensure that the required network bandwidth is always available for your business applications and not consumed by other applications, such as social-network or video-streaming applications.

Identifying the host type: Trellix IPS profiles devices to address risks due to BYOD. It integrates with Trellix ePO - On-prem and NTBA to identify the device type and the operating system for each host on your network. You are now aware of the types of devices on your network. If a specific host is targeted for an attack, you can also assess if that attack is relevant based on the device type and OS.

Protection for virtual machines: Virtual instances of Sensors enable you to monitor peer-to-peer traffic between virtual machines even within the same virtual host. Trellix Virtual Intrusion Prevention System Sensors are called as Virtual IPS Sensors or Virtual Sensors. You can deploy a Virtual IPS Sensor as a virtual appliance in a virtualization platform such as VMware ESXi server. Then, you can configure the Virtual IPS Sensor to protect the virtual network within the virtualization platform or even outside. Based on the network design and security requirements, you can configure a Virtual IPS Sensor to be inline between virtual machines or configure it in the IDS mode. It is also possible to use a Virtual IPS Sensor to inspect traffic between physical hosts.

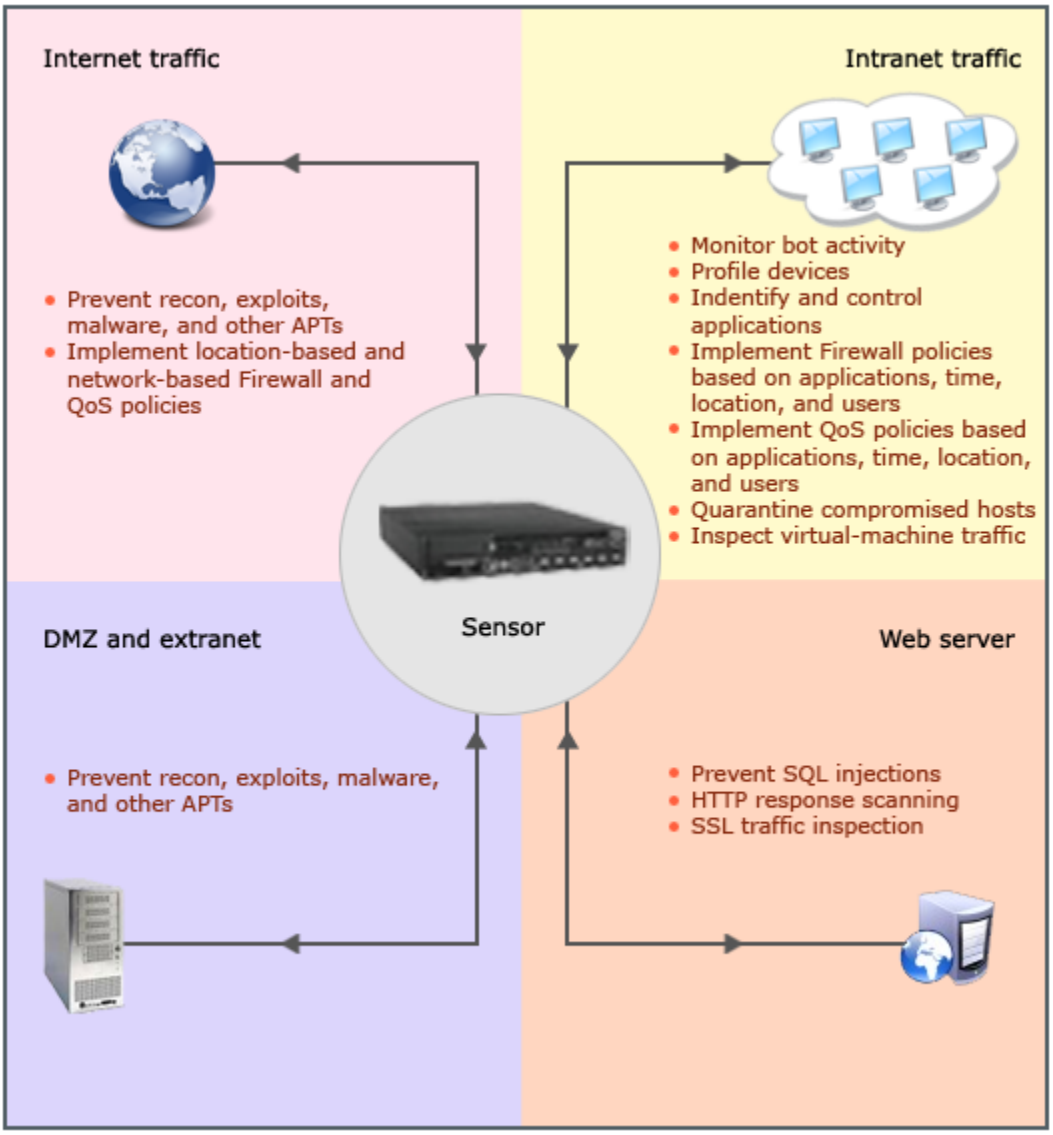
Cloud-based IP and file reputation: To protect your network from known and near zero-day malware, Trellix IPS integrates with Trellix GTI. It can check if an email, URL, or a file is known malware. It can also check the reputation of IP address and port combination when an external host attempts to communicate with a host on your network.

Quarantine host and enforce remediation: If an internal host generates attack traffic, it could be that it is compromised. You can use Trellix IPS to manually or automatically quarantine such hosts until they are remediated.

Analyzing your network traffic: The IPS Sensor integrates with the NTBA appliance to proactively provide visibility into any anomalous behavior on your network. They passively monitor your network to help identify threats from APTs and to even

troubleshoot network issues. NTBA collects a vast amount of data, which is converted to meaningful and relevant information, and presented to you in an easy-to-understand graphical format.

Figure 235. Analyzing your network traffic

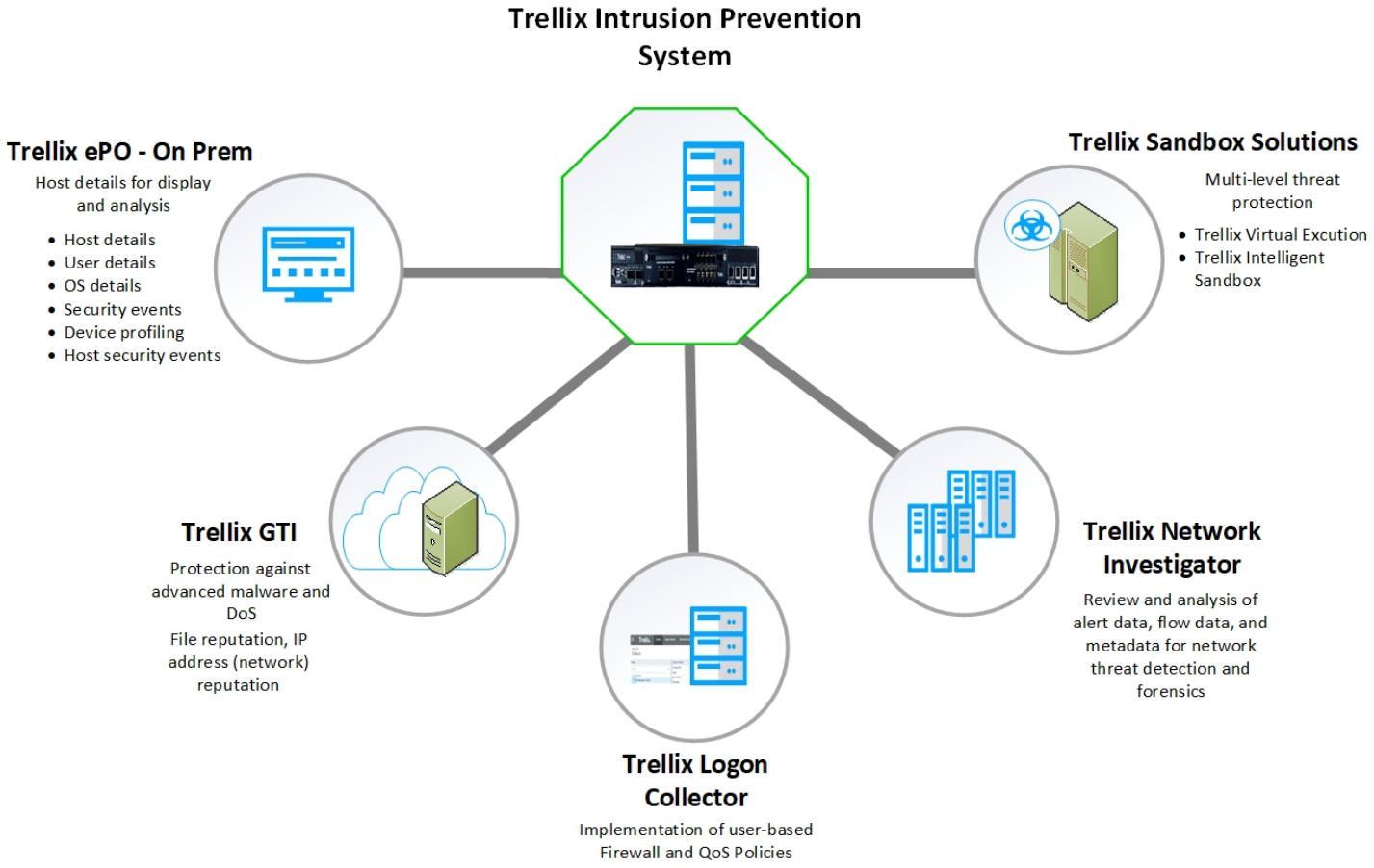


Integrating with other Trellix products: One of the biggest advantage that Trellix IPS provides is the ability to integrate with other Trellix products. A few of the Trellix products that Trellix IPS integrates with are given below:

- Integration with **Trellix ePolicy Orchestrator - On-prem**: As mentioned earlier, this integration enables Trellix IPS in identifying the devices on your network. You can also query for the complete details of any ePO-managed host on your network.
- Integration with **Trellix GTI**: As explained previously, this integration facilitates Trellix IPS to check the reputation of a file, URL, email, IP, and network.

- Integration with **Sandbox Solutions**: Trellix enables integration with Trellix Intelligent Sandbox and Trellix Virtual Execution. Both these solutions facilitate detection and prevention of malware. They provide protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.
- Integration with **Trellix Network Investigator**: With integration enabled with Trellix Network Investigator (NI), Trellix IPS exports netflows and Layer 7 metadata from IPS Sensors, and alert data from IPS Manager to Network Investigator, as per the configuration and filter parameters set by the user. The alert data, L7 metadata information, and net flow records exported by Trellix IPS are displayed on the **Dashboard** of NI's web-based UI which users can review and utilize further for the detection and analysis of network threats.
- Integration with **Trellix Logon Collector**: This integration enables Trellix IPS to identify the Windows AD users and their hosts to apply the security policies accordingly.

Figure 236. Integration with a few Trellix products



Flexible deployment options: Trellix IPS provides devices of various throughput capacities to meet today's higher speed network segments. The throughput of these devices range from 100 Mbps to 100 Gbps that are designed to provide comprehensive protection without compromising on network performance. Trellix IPS provides wire-speed monitoring and analysis up to multi-Gbps network segments in three flexible modes of deployment, enabling you to easily integrate it into your network and adapt to any network or security changes that you may encounter in the future. Some Sensor models contain built-in 10/100 Mbps Ethernet taps, thus making it extremely easy to switch between tap and in-line modes through software reconfiguration; no physical rewiring is required. The multi-port configuration of all Sensors empowers comprehensive network-wide IPS deployment with significantly fewer Sensors.

The latest Trellix IPS devices come with hardware acceleration for supporting encryption, decryption, and decompression. They use Intel's high-performance processors to deliver higher throughput.

VIPS - Applying policies at the interface and sub-interface levels: The VIPS feature enables you to configure multiple policies for multiple unique environments and traffic directions all monitored with a single Sensor. The goal of virtualization is scanning granularity. Virtualization allows you to apply multiple policies to traffic flowing through a single interface. In this way, a unique scanning policy can be applied to a single host or group of hosts, when their traffic will not travel through a unique Sensor port. For example, suppose port G0/1 of an NS9500 Sensor is connected to the SPAN port on a switch. Port G0/1 is configured with a specific environment detection policy. The rest of the ports on the Sensor can have policies completely different than the policy on G0/1, or they can use the same policy. In this case, each monitoring port of the Sensor is an interface. The other option is to segment each monitoring port by multiple VLAN tags or CIDR addresses, each customized with its own security policy. In this case, each monitoring port is segmented into virtual sub-interfaces.

High-availability: Sensors support high-availability deployment, using stateful Sensor failover between two hot-standby Sensors. The Sensors are interconnected, copy traffic between themselves, and maintain synchronization. If one Sensor fails, the standby Sensor automatically takes over and continues to monitor the traffic with no loss of session state or degradation of protection level. Trellix IPS also supports Manager Disaster Recovery (MDR) for its management console. If, for any reason, the primary Trellix IPS Manager goes off-line, its secondary can automatically take its place, processing alerts and managing Sensor configuration.

Scalable IPS management: A scalable web-based architecture allows customers to efficiently manage their IPS deployment while reducing operational costs. Trellix IPS's real-time signature and software update mechanism automate the process of keeping the complete system current with little or no human intervention, thus reducing on-going operating costs. Also, Virtual IPS Sensors are remarkably quick and easy to deploy. Therefore, they greatly enhance scaling up your next-generation IPS deployment without any compromise on security features.

Trellix IPS Basics

This section provides an overview of Trellix Intrusion Prevention System and its components.

Trellix Intrusion Prevention System overview

Trellix Intrusion Prevention System is a combination of network appliances and software built for the accurate detection and prevention of intrusions, denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, malware download, and network misuse. Trellix Intrusion Prevention System provides comprehensive network intrusion detection, and can block or prevent attacks in real time, making it truly an intrusion prevention system (IPS).

Trellix IPS components

The following are the major Trellix Intrusion Prevention System components for IDS and IPS:

- Trellix Intrusion Prevention System Sensor
- Trellix Intrusion Prevention System Manager, with its Web-based graphical user interface

Trellix IPS Sensors

Trellix IPS Sensors are high-performance, scalable, and flexible content processing appliances built for the accurate detection and prevention of intrusions, misuse, malware, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks. Sensors can be physical or virtual appliances. IPS Sensors are specifically designed to handle traffic at wire-speed, efficiently inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise

environment. When deployed at key network access points, a Sensor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

Once deployed and the communication is established, Sensors are configured and managed through the Manager server.

- In this chapter, the term *Sensor* applies to both physical as well as Virtual IPS Sensors unless otherwise specified.
- In this guide, the term *Sensor resources* refers to the monitoring ports, interfaces, and subinterfaces of a physical or a Virtual IPS Sensor.

Sensor functionality

The primary function of a device is to analyze traffic on the selected network segments and to respond when an attack is detected. The device examines the header and data portion of every network packet, looking for patterns and behavior in the network traffic that indicate malicious activity. The device examines packets and matches the packets against the applied policies. These policies determine what attacks to watch for, and how to respond with countermeasures if an attack is detected.

If an attack is detected, a physical or a Virtual IPS Sensor responds according to its configured policy. A Sensor can perform many types of attack responses, including generating alerts and packet logs, resetting TCP connections, “scrubbing” malicious packets, and even blocking attack packets entirely before they reach the intended target.

In addition to its primary function of preventing exploit, recon, and DoS attacks, a Sensor can also do the following:

- **Detect malware**— A Sensor uses various methods to inspect files being downloaded for embedded malware. If a malware is detected, the Sensor blocks the download and takes further response actions.
- **Enforce Firewall access rules**— You can define Firewall access rules (similar to ACLs) in the Manager. Then you can configure a Sensor to enforce these rules on your network.
- **Provide and facilitate Quality of Service (QoS)**— A physical Sensor can facilitate Differentiated Services and IEEE 802.1p by differentiating traffic and tagging them accordingly.
- **Provide connection limiting services**— Based on how you configure, a Sensor can limit the number of connections a host can establish. One of the advantages of connection limiting is that it can minimize connection-based DoS attacks.
- **Export NetFlow data**— If Network Threat Behavior Analysis (NTBA) is deployed, you can configure a Sensor to export NetFlow data to the NTBA Appliance.

NOTE

The Sensor generates an auditlog file that is no more than 128MB. The file is purged from the disk when the audit log is uploaded to the Manager and a new auditlog file is started with a start marker.

All the manager-sensor communications happen over TLS.

Sensor platforms

Trellix IPS offers several types of Sensor platforms providing different bandwidth and deployment strategies.

- NS-series: NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3600, NS3500, NS3200, and NS3100
- Virtual IPS Sensors: IPS-VM600, IPS-VM5000

NS-series Sensor

Ports	NS9500	NS9300	NS9100/ NS9200
Fixed Gigabit Ethernet— Copper Ports (inline fail-open)	NA	16	8
Fixed 100/ 40-Gigabit Ethernet	2	NA	NA
Fixed 40- Gigabit Ethernet	NA	4 40 Gigabit Ethernet (used as interconnect ports between NS9300P and NS9300S)	2 40 Gigabit Ethernet
Fixed 10 GigE/1 GigE (SFP+) Ports	NA	NA	NA
Fixed 10 Gigabit Ethernet— Copper Ports (inline fail-open)	4	NA	NA
Network I/O Slots	2	4	2

Ports	NS9500	NS9300	NS9100/ NS9200
Network I/O Modules (four options)	8-port SFP/SFP+ 1/10 Gigabit 6-port RJ-45 10/100/1000 Mbps with internal fail-open 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open 4-port 10/1 Gig MM 62.5 micron with internal fail-open 4-port 10/1 Gig MM 50 micron with internal fail-open 4-port 10/1 Gig SM 8.5 micron with internal fail-open 4-port QSFP+ 40 Gigabit 2-port QSFP+ 40 Gigabit 2-port 100/40 Gig SR MTP/MPO passive fail-open 2-port QSFP28 100 Gigabit	8-port SFP/SFP+ 1/10 Gigabit 6-port RJ-45 10/100/1000 Mbps with internal fail-open 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open 4-port 10/1 Gig MM 62.5 micron with internal fail-open 4-port 10/1 Gig MM 50 micron with internal fail-open 4-port 10/1 Gig SM 8.5 micron with internal fail-open 4-port QSFP+ 40 Gigabit 2-port QSFP+ 40 Gigabit	8-port SFP/SFP+ 1/10 Gigabit 6-port RJ-45 10/100/1000 Mbps with internal fail-open 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open 4-port 10/1 Gig MM 62.5 micron with internal fail-open 4-port 10/1 Gig MM 50 micron with internal fail-open 4-port 10/1 Gig SM 8.5 micron with internal fail-open 4-port QSFP+ 40 Gigabit 2-port QSFP+ 40 Gigabit
External fail- open kits (New and Old variants)	Yes	Yes	Yes
10 Gigabit Ethernet	Up to 20	Modular up to 32	Modular up to 16
40-Gigabit Ethernet	Up to 10	Modular up to 16	Modular up to 8
100-Gigabit Ethernet	Up to 6	NA	NA
10/100/ 1000 Mbps	Modular up to 12	Modular up to 24	Modular up to 12
100/1000/ 10000 Mbps	Up to 12	Modular up to 16	Modular up to 8
Dedicated Response Ports (RJ-45)	1 (10G/1G)	1 (10G/1G/100M) on NS9300S	1 (10G/1G/100M)

Ports	NS9500	NS9300	NS9100/ NS9200
Dedicated Management Ports (RJ-45)	1 (10G/1G)	1 (10G/1G/100M) on NS9300P	1 (10G/1G/100M)
Dedicated Auxillary Port (RJ45)	NA	2 (10G/1G/100M)	1 (10G/1G/100M)
USB ports	2	4	2

Ports	NS7600	NS7500	NS7x50	NS7x00
Fixed Gigabit Ethernet— Copper Ports (inline fail-open)	NA	8	8	8
Fixed 100/40-Gigabit Ethernet	NA	NA	NA	NA
Fixed 40-Gigabit Ethernet	NA	NA	NA	NA
Fixed 10 GigE/1 GigE (SFP+) Ports	4 (in G0)	2	2	2
Fixed 10 Gigabit Ethernet— Copper Ports (inline fail-open)	NA	NA	NA	NA
Network I/O Slots	3	2	2	2

Ports	NS7600	NS7500	NS7x50	NS7x00
Network I/O Modules (four options)	6-port RJ-45 10/1 Gig with internal fail-open 8-port 10/1 Gig SM (8.5 micron) with internal fail-open 8-port 10/1 Gig MM (50 or 62.5 micron) with internal fail-open	8-port SFP/SFP+ 1/10 Gigabit 6-port RJ-45 10/100/1000 Mbps with internal fail-open 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open 4-port 10/1 Gig MM 62.5 micron with internal fail-open 4-port 10/1 Gig MM 50 micron with internal fail-open 4-port 10/1 Gig SM 8.5 micron with internal fail-open	8-port SFP/SFP+ 1/10 Gigabit 6-port RJ-45 10/100/1000 Mbps with internal fail-open 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open 4-port 10/1 Gig MM 62.5 micron with internal fail-open 4-port 10/1 Gig MM 50 micron with internal fail-open 4-port 10/1 Gig SM 8.5 micron with internal fail-open	8-port SFP/SFP+ 1/10 Gigabit 6-port RJ-45 10/100/1000 Mbps with internal fail-open 4-port RJ-45 10 Gbps/1 Gbps/100 Mbps with internal fail-open 4-port 10/1 Gig MM 62.5 micron with internal fail-open 4-port 10/1 Gig MM 50 micron with internal fail-open 4-port 10/1 Gig SM 8.5 micron with internal fail-open
External fail-open kits (New and Old variants)	Yes	Yes	Yes	Yes
10 Gigabit Ethernet	Up to 28	Up to 18	Modular up to 16	Modular up to 16
40-Gigabit Ethernet	NA	NA	NA	NA
100-Gigabit Ethernet	NA	NA	NA	NA
10/100/1000 Mbps	NA	Up to 20	Modular up to 12	Modular up to 12
100/1000/10000 Mbps	Up to 18 (1000/10000 Mbps)	Modular up to 8	Modular up to 8	NA
Dedicated Response Ports (RJ-45)	1 (10G/1G)	1 (10G/1G)	1 (10G/1G)	1 (1G/100M/10M)
Dedicated Management Ports (RJ-45)	1 (10G/1G)	1 (10G/1G)	1 (10G/1G)	1 (1G/100M/10M)
Dedicated Auxillary Port (RJ45)	NA	NA	NA	1 (DB9 port)
USB ports	2	2	2	2

Ports	NS5200/ NS5100	NS3600	NS3500	NS3200/ NS3100
Fixed Gigabit Ethernet—Copper Ports (inline fail-open)	8	8	4	8
Fixed 100/ 40-Gigabit Ethernet	NA	NA	NA	NA
Fixed 40- Gigabit Ethernet	NA	NA	NA	NA
Fixed 10 GigE/1 GigE (SFP+) Ports	2	2	NA	NA
Fixed 10 Gigabit Ethernet— Copper Ports (inline fail-open)	NA	NA	NA	NA
Network I/O Slots	12	1	NA	NA
Network I/O Modules (four options)	NA	4-port RJ-45 1 Gbps/100 Mbps/10 Mbps 4-port 10/1 GigE MM 50/62.5 µm	NA	NA
External fail- open kits (New and Old variants)	Yes	Yes	Yes	Yes
10 Gigabit Ethernet	Modular up to 2	Up to 6	NA	NA
40-Gigabit Ethernet	NA	NA	NA	NA
100-Gigabit Ethernet	NA	NA	NA	NA
10/100/ 1000 Mbps	Up to 8	Up to 12	Up to 4	Up to 8
100/1000/ 10000 Mbps	NA	NA	NA	NA
Dedicated Response Ports (RJ-45)	1 (1G/100M)	1 (1000/100/10 Mbps)	1 (10/100/1000 Mbps)	1 (10/100/1000 Mbps)

Ports	NS5200/ NS5100	NS3600	NS3500	NS3200/ NS3100
Dedicated Management Ports (RJ-45)	1 (1G/100M)	1 (1000/100/10 Mbps)	1 (10/100/1000 Mbps)	1 (10/100/1000 Mbps)
Dedicated Auxillary Port (RJ45)	NA	NA	NA	NA
USB ports	2	2	2	1

Virtual IPS Sensor models

The table describes the available Virtual IPS Sensor models.

Model	Maximum Sensor throughput	Number of monitoring ports	Management port	Response port	Logical CPU Cores	Memory	Storage
IPS-VM600	Up to 1 Gbps	6	1	1	4	8 GB	8 GB
IPS-VM5000	Up to 5 Gbps	6	1	1	12	16 GB	32 GB

NOTE

The kind of traffic being inspected and the features that you enable are some of the primary factors that affect the throughput of a Sensor. For these details and other capacity values for Virtual Sensors, refer to Virtual IPS Sensor capacity.

Trellix IPS Manager components

The Manager is a term that represents the hardware and software resources that are used to configure and manage the Trellix IPS. The IPS Manager consists of the following components:

- Manager server platform
- The Manager software
- A back-end database that is installed along with the Manager
- A connection to Trellix IPS Update Server
- Signature Set

Manager server platform

The Manager server platform hosts the Manager software and the Manager database. It is a server running on an operating system as specified in the [Trellix Intrusion Prevention System Installation Guide.] You can remotely access the Manager user interface from a client machine using a browser. Refer to the [Trellix Intrusion Prevention System Installation Guide] to know the supported browsers and the supported operating systems for the clients.

Sensors use a built-in 10/100 Management port to communicate with the Manager server. You can connect a segment from a Sensor Management port directly to the Manager server; however, this means you can only receive information from one Sensor

(typically, your server has only one 10/100 network port). During the Sensor configuration, you will establish communication between your Sensors and your Manager server.

Manager software

The Manager software has a web-based user interface for configuring and managing Trellix IPS. Users connect to the Manager server from a supported client using a supported browser, the details of which are in the [Trellix Intrusion Prevention System Installation Guide.] The Manager functions are configured and managed through a GUI application, which includes complementary interfaces for alerts, system status, system configuration, report generation, and fault management. All interfaces are logically parts of the Manager program.

The Manager user interface has five main tabs:

- **Dashboard** — The **Dashboard** is the first page displayed after the user logs on to the system. Options available within the page are determined by the current user's assigned roles. The Dashboard enables you to view all the critical information regarding Trellix IPS deployment in the same page. The Dashboard is very user configurable. You can configure the information that you want to view, the timeframe for which you want to view the information, the frequency with which the Dashboard must auto-refresh, and so on. All these information can be customized to view for a particular admin domain. You can select the admin domain from the **Domain** drop-down list to display data for the selected admin domain.

  Some of the information displayed on the dashboard includes:

  - Release announcements
  - Information regarding the frequently seen malicious activities on your network. This includes things, such as the most downloaded malware, most callback activity, the most targeted hosts, the most detected attack and so on.
  - System faults of Trellix IPS components which show whether all those are functioning properly, the number of unacknowledged alerts in the system, and the configuration options available to the current user
  - Manager-related details, such as the version, signature set version, users logged on to the Manager, and so on
  - Information like whether the devices are up-to-date
- **Analysis** — This tab presents the options using which you can view the granular details of all the malicious activities on your network. The intention here is to provide you all the critical information needed for further analysis for the selected admin domain.

  One of the key options on the **Analysis** tab is the **Attack Log**, which displays the alerts triggered by the Sensors. The **Attack Log** page displays the hosts detected on your network as well as the detected security events that violate your configured security policies. The Attack Log provides powerful drill-down capabilities to enable you to see all of the details on a particular alert, including its type, source and destination addresses, and packet logs where applicable.
- **Policy** — All the major features in Trellix IPS are policy based. For example, to block exploit and recon attacks, you use the IPS and the recon policies; for Firewall, you use the Firewall policies; for QoS, you use the QoS policies and so on. The **Policy** tab provides the options to manage all these policies and other related functionality.
- **Devices** — You can use the same instance of the Manager to manage both the physical and virtual devices. The **Devices** tab provides all system configuration options, and facilitates adding and configuration of your devices - Sensors, NTBA Appliances, HA pairs of Sensors, etc. This tab provides configuration options on per device basis as well. Access to various activities is based on the current user's role(s) and privileges, administrative domains, attack policies and responses, user-created signatures, and system reports.
- **Manager** — This tab provides the configuration options related to the Manager software. This includes managing administrative domains, users, and roles, downloading signature sets and other software such as Sensor software, integrating the Manager with other Trellix products, maintenance activities such as database backups, and so on.

Other key features of Manager include:

- **Integration with other Trellix products** — You can integrate Trellix IPS with other Trellix products to provide you with a comprehensive network security solution.
    - **Trellix ePolicy Orchestrator - On-prem** — Trellix ePolicy Orchestrator - On-prem is a scalable platform for centralized policy management and enforcement of your system security products, such as anti-virus, desktop firewall, and anti-spyware applications. You can integrate Trellix IPS with Trellix ePO - On-prem 5.0 and above. The integration enables you to query the Trellix ePO - On-prem server from the Manager for viewing details of a network host.
    - **Trellix Global Threat Intelligence** — Trellix Global Threat Intelligence is a global threat correlation engine and intelligence base of global messaging and communication behavior including reputation, volume, trends, email, web traffic and malware. By having Trellix Global Threat Intelligence integration, you can report, filter, and sort hosts involved in attacks based on their network reputation and the country of the attack origin.
    - **Trellix Intelligent Sandbox** — Trellix Intelligent Sandbox is an on-premise appliance that facilitates detection and prevention of malware. Trellix Intelligent Sandbox provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.
    - **Trellix Intelligent Virtual Execution (IVX)** — Intelligent Virtual Execution (IVX) Engine is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature-based and policy-based defenses. The IVX engine detects zero-day, multiflow, and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyberattack kill chain by identifying never-before-seen exploits and malware.

      Trellix IPS offers integration capability with Intelligent Virtual Execution - Server and Intelligent Virtual Execution - Cloud which utilize IVX engine's technology to perform malware analysis.
    - **Trellix Network Investigator** — Network Investigator (NI) is a security analytics solution that allows the analysis of alerts and network metadata gathered from all devices connected to it. Network Investigator can ingest alerts and collect Layer 7 metadata from other Trellix products, including Network Security (NX), Packet Capture (PX), and End-point Security (HX), and provides a high-level view of the network metadata gathered over customizable dashboards supporting multiple configurations. It thus enables users to have a metadata-based view of network activities and search indexed metadata from various network protocols, which allows them to zero down on threat information critical for performing further investigation.

      Trellix IPS offers integration capability with Trellix Network Investigator using which it exports netflows and Layer 7 metadata from IPS Sensors, and alert data from IPS Manager to NI, as per the configuration and filter parameters set by the user. The alert data, L7 metadata information, and net flow records exported by Trellix IPS are displayed on the **Dashboard** of NI's Web UI which users can review and utilize further for the detection and analysis of network threats.

  For more information on all the above mentioned integration options, see [Trellix Intrusion Prevention System Integration Guide].
- **Integration with third-party products** — Trellix IPS enables the use of multiple third-party products for analyzing faults, alerts, and generated packet logs.
    - **Fault/Alert forwarding and viewing** — You have the option to forward all fault management events and actions, as well as IPS alerts to a third-party application. This enables you to integrate with third-party products that provide trouble ticketing, messaging, or any other response tools you may want to incorporate. Fault and/or alert forwarding can be sent to the following ways:
        - **Syslog Server** — forward IPS alerts and system faults
        - **SNMP Server (NMS)** — forward IPS alerts and system faults

    - **Java API** — forward IPS alerts
- **Packet log viewing** — View logged packets/flows using third-party software, such as Wireshark.

Manager database

The Manager server operates with an RDBMS (relational database management system) for storing persistent configuration information and event data. The compatible database is MariaDB. Refer to the [Trellix Intrusion Prevention System Installation Guide] for the current version of MariaDB.

The Manager server includes a database that is installed (embedded) on the target Windows server during Manager software installation.

The database can be tuned on-demand or by a set schedule through the Manager user interface configuration. Tuning promotes optimum performance by defragmenting split tables, re-sorting and updating indexes, computing query optimizer statistics, and checking and repairing tables.

Signature Set

Signature set is a comprehensive set of attack definitions developed and provided by Trellix Advanced Research Center. An attack definition contains one or more signatures, which indicate suspicious or malicious activity. These signatures are then matched against traffic passing through the Sensor monitoring ports.

Each attack definition can be configured to perform response actions like sending an alert to the Manager, dropping traffic, capturing packets, or generating an email. It is used to detect threats and anomalies in the network traffic.

Signature sets are available in Trellix IPS Update Server (Update Server). Trellix regularly updates the signature set with latest attack definitions which you can download from the Update Server.

The threat landscape is constantly evolving, and new attacks are regularly added to the signature set to keep the network protection up-to-date. The attack definitions in the signature set are categorized as high, medium, and low priority attacks. This helps optimize Sensor resources on older Sensor models and Sensors running older software versions, thereby protecting against the most critical and relevant attacks.

Based on the priority attribute configured for the Sensor models, the Manager dynamically compiles the signature set using the current signature set version available in the Manager. The corresponding set of attack definitions are then pushed to the Sensors.

For more information about downloading signature sets, see the Download signature set updates.

Trellix IPS Update Server

For your Trellix IPS to properly detect and protect against malicious activity, the Manager and Sensors must be frequently updated with the latest signatures and software patches available. Thus, the Trellix IPS team constantly researches and develops performance-enhancing software and attack-detecting signatures that combat the latest in hacking, misuse, and denials of service (DoS). When a severe-impact attack happens that cannot be detected with the current signatures, a new signature update is developed and released. Since new vulnerabilities are discovered regularly, signature updates are released frequently.

New signatures and patches are made available to customers via Trellix IPS Update Server (Update Server). The Update Server is a Trellix IPS owned and operated file server that houses updated signature and software files of Managers and Sensors for customer installations. The Update Server securely provides fully automated, real-time signature updates without requiring any manual intervention.

NOTE

Communication between the Manager and the Update Server is SSL-secured.

Obtaining updates from the Update Server

You have the following options for obtaining updates from the Update Server:

1. Connecting directly from your Manager server (via Manager interface action).
2. Connecting through a proxy server (through Manager interface action). You will then authenticate as in option 1.

Configuring software and attack signature updates

You can configure interaction with the Update Server using the Manager. You can pull updates from the Update Server on demand or you can schedule update downloads. With scheduled downloads, the Manager polls the Update Server (over the Internet) at the desired frequency. If an update has been posted, that update is registered as “Available” in the Manager interface for on-demand downloaded. Once downloaded to the Manager, you can immediately download (via an encrypted connection) the update to deployed Sensors or deploy the update based on a Sensor update schedule you define. Acceptance of a download is at the discretion of the administrator.

- **Automatic update to Manager, manual update from Manager to Sensors** — This option enables Manager server to receive updates automatically, but allows the administrator to selectively apply the updates to the Sensors.
- **Manual update to Manager, automatic update from Manager to Sensors** — This option enables the administrator to select updates manually, but once the update is selected, it is applied to the Sensors automatically without reboot.
- **Fully manual update** — This option allows the security administrator to determine which signature update to apply per update, and when to push the update out to the Sensors. You may want to manually update the system when you make some configuration change, such as updating a policy or response.
- **Fully automatic update** — This option enables every update to pass directly from the Update Server to the Manager, and from the Manager to the Sensors without any intervention by the security administrator. Note that fully automatic updating still happens at the scheduled intervals.
- **Real-time update** — This option is similar to fully automatic updating. However, rather than waiting for a scheduled interval, the update is pushed directly from Update Server to Manager to Sensor. No device needs to be rebooted; the Sensor does not stop monitoring traffic during the update, and the update is active as soon as it is applied to the Sensor.

Trellix Intrusion Prevention System deployment - an overview

The process of setting up and running Trellix IPS falls into these basic stages:

1. Deciding where to deploy Trellix Intrusion Prevention System Sensor and in what operating mode
2. Setting up your Sensors for the desired deployment mode(s)
3. Installing the Manager software and establishing Sensor-to-Manager communication
4. Configuring your deployment using the Manager
5. Viewing and working with data generated by Trellix IPS
6. Tuning your deployment

7. Updating your signatures and software

Each of these stages consists of a number of tasks; some are simple, some are complex. You will generally perform steps 1 through 3 only once per Sensor.

For information on how to deploy Virtual IPS Sensors, see [Trellix Virtual Intrusion Prevention System Product Guide].

Decide where to deploy Sensors and in what operating mode

This is one of the very first decisions that you need to make. Where you deploy your Sensors and which Sensor model to use depends on your network topology, the amount of traffic on the network, and your security goals, which ideally are based on your company's security requirements.

- **Determine where you will place the Sensors**. This is an individual decision your company will need to make. Questions to ask yourself in making this decision are covered at a high level in the [Pre-deployment Considerations] section of this document. Some things to consider are what assets you want to protect, the configuration of your network, the location of your aggregation points, the type of traffic, how the traffic is routed, and so on.
- **Establish a naming convention for your Sensors**. The Sensor name is used to identify the Sensor in the Manager interface, in certain reports, and in the alert data generated by the Sensor. Trellix recommends you to establish a naming convention that is easy to interpret by anyone working with the Trellix IPS deployment. After you name a Sensor, you cannot rename it without de-installing the Sensor-to-Manager communication. After renaming the Sensor, you must reinstall this communication.

Review of pre-deployment considerations

Deployment of Trellix IPS requires specific knowledge of your network's security needs. Read this section to determine which Sensor model will best suit your environment, and in what operating mode you'll need to employ each Sensor port.

Size of your network

The size of your network will determine the number of Sensors you will require to successfully and efficiently protect your network. A large network with many access points, file servers, and machines in use may require a larger level of IPS deployment than a small office with just a single access point and few machines. You must also factor in the redundancy requirements for your network.

Knowing how your business will grow can help determine the amount of equipment you will require and the proper strategy for network placement. Trellix IPS is built with growth in mind. The Trellix IPS can manage multiple Sensors, and Sensors can scale in performance from 100 Mbps to multi gigabits per second (up to 80 Gbps) for monitoring network segments.

Access points between your network and the extranets or Internet

Large corporations have several points of access that can be exploited by parties with malicious intent. Protecting the various points of access to your network is the key to any successful IDS installation. You're only as strong as your weakest link.

Intrusions coming in from the Internet are important to combat, but misuse and intrusions attempted through the extranets or inside the corporate network are equally as critical to defend against. In fact, research statistics show that insiders are the most common source of attacks.

Critical servers that require protection within your network

File servers containing financial, personnel, and other confidential information need protection from those people wishing to exploit your critical information. These machines are extremely appealing targets. And, as discussed in the previous section, insiders pose a threat that must be addressed.

You should also consider whether you need different levels of security for different parts of the organization. Assess how much of your sensitive material is on-line, where it is located, and who has access to that material.

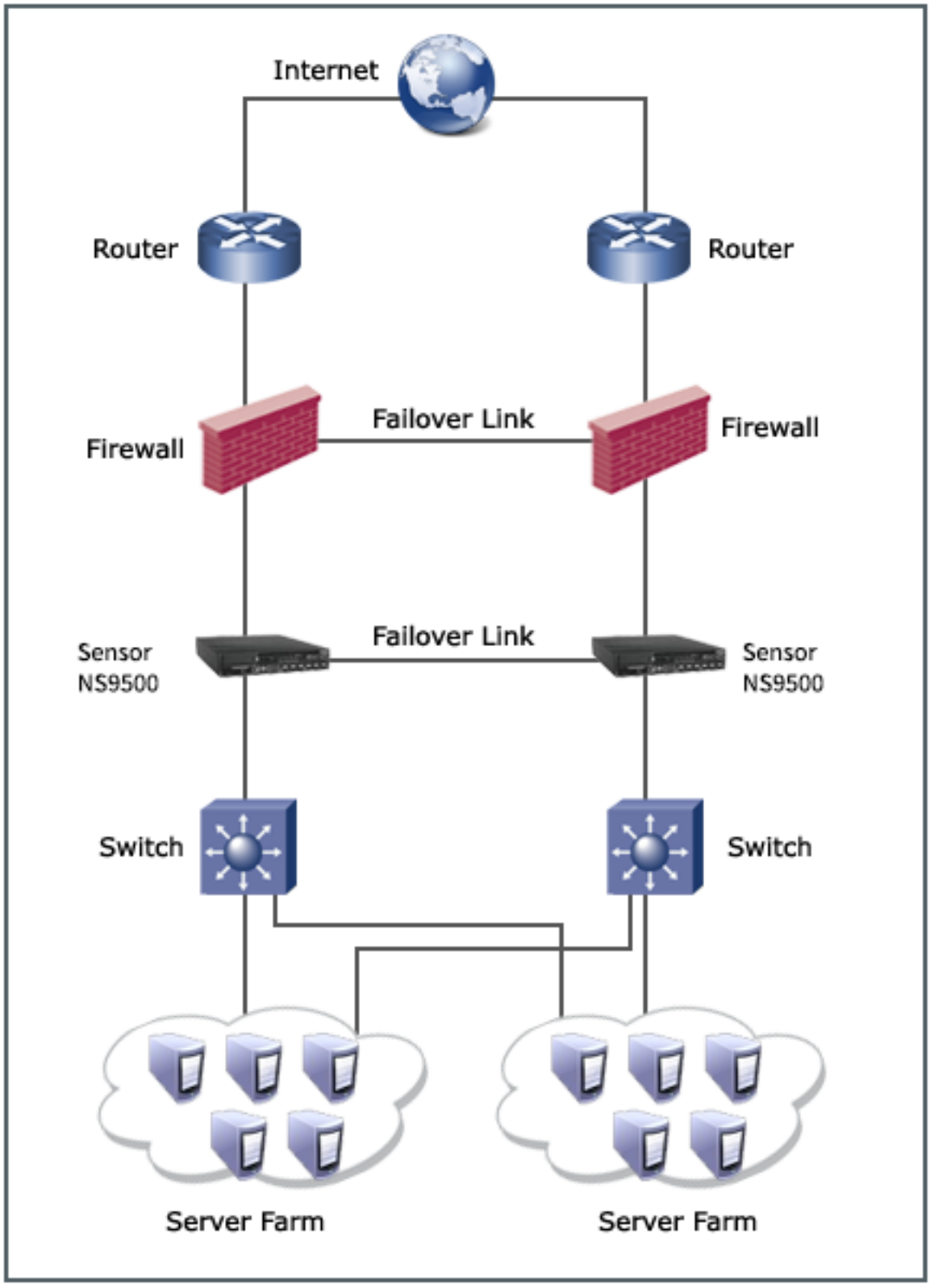
Determination of complexity of your network topology

Asymmetrically routed networks are complex environments that require careful planning and execution.

The following figure shows a network protected by the Sensor in tap operating mode. Since both links are monitored by the same Sensor, the state machine remains in sync. The Sensor can support an Active-Active configuration as long as the aggregate bandwidth does not exceed the total processing capacity of the Sensor.

Furthermore, a Sensor can also monitor asymmetrically routed traffic where the traffic comes in on one link and goes out another link, because the state machine on the Sensor associates the inbound and outbound traffic efficiently.

Figure 237. Network topology



Traffic flow across your network

Bandwidth and traffic flow are crucial to running a successful enterprise network. Bandwidth requirements will vary in an enterprise network, as different applications and business functions have different needs. Bandwidth utilization on the network segments that you need to monitor will determine what type of Sensor will work best for you. Trellix IPS offers multiple Sensors providing different bandwidths:

Sensor bandwidth

NS-series Sensor	Aggregate performance
NS9500 stack - 100 Gbps throughput	100 Gbps
NS9500 stack - 60 Gbps throughput	60 Gbps
NS9500 stack - 40 Gbps throughput	40 Gbps
NS9500 standalone - 30 Gbps throughput	30 Gbps
NS9500 standalone - 20 Gbps throughput	20 Gbps
NS9500 standalone - 10 Gbps throughput	10 Gbps
NS9300	40 Gbps
NS9200	20 Gbps
NS9100	10 Gbps
NS7600 - 15 Gbps throughput	15 Gbps
NS7600 - 10 Gbps throughput	10 Gbps
NS7600 - 5 Gbps throughput	5 Gbps
NS7500 - 7.5 Gbps throughput	7.5 Gbps
NS7500 - 5 Gbps throughput	5 Gbps
NS7500 - 3 Gbps throughput	3 Gbps
NS7350	5 Gbps
NS7250	3 Gbps
NS7150	1.5 Gbps
NS7300	5 Gbps
NS7200	3 Gbps
NS7100	1.5 Gbps
NS5200	1 Gbps
NS5100	600 Mbps
NS3600 - 5 Gbps throughput	5 Gbps
NS3600 - 3 Gbps throughput	3 Gbps
NS3600 - 1 Gbps throughput	1 Gbps
NS3500	750 Mbps
NS3200/NS3100	750 Mbps

Virtual IPS Sensor	Aggregate performance
IPS-VM600	1 Gbps
IPS-VM5000	5 Gbps

Find where your security operations are located

To successfully defend against intrusions, Trellix recommends dedicated monitoring of the security system. Network intrusions can happen at any given moment, so having a dedicated 24-hour-a-day prevention system will make the security solution complete and effective.

Where are your security personnel? How many users are involved? Knowing who will be configuring your policies, monitoring events, running reports, and performing other configuration tasks will help you manage your users and determine where you locate your Trellix IPS Manager server. The Manager should be placed in a physically secure location, should be logically accessible to users, and must have reliable connectivity so as to be able to communicate with all deployed Sensors.

Deployment of Sensors

Should you deploy Sensors at the perimeter of your network, in front of the servers you want to protect, or at a convenient nexus where all traffic passes?

Deployment at the perimeter does not protect you from internal attacks, which are some of the most common source of attacks. Perimeter monitoring is also useless if a network has multiple ISP connections at multiple locations (such as one Internet connection in New York and one in San Jose) and if you expect to see asymmetric traffic routing (that is, incoming traffic comes through New York and outgoing traffic goes out through San Jose). The IPS simply will not see all the traffic to maintain state and detect attacks. Deployment in front of the servers that you want to protect both detects attacks from internal users and deals effectively with the geographically diverse asymmetric routing issue.

A better illustration of the advantage of Sensors' multiple segment monitoring is to consider the question of installing Sensors with respect to firewalls. It is very common to deploy Sensors around firewalls to inspect the traffic that is permitted by the firewall. A common question when installing Sensors around the firewall is: *Do you put the Sensors on the inside (Private and DMZ) or put them outside (Public) the firewall*? There are benefits to both scenarios, and the more complete solution includes both. For example, if you detect an attack on the outside of the firewall and you detect the same attack on the inside of the firewall, then you know your firewall has been breached. This is obviously a much higher severity event than if you were just to see the attack on the outside and not on the inside, which means that your firewall blocked the attack.

When using the existing, single monitoring port products available, you would have to deploy multiple Sensors to get the required coverage (as shown in Scenario 1 below). Furthermore, you would need to figure out how to connect them to the segments that you want to monitor, and only via a SPAN or hub port.

Consider the same scenario using the NS9500 Sensor (as shown in Scenario 2 below). You can simultaneously monitor all three segments with one Sensor, and, with the integrated taps, you can easily monitor the full-duplex uplinks between your routers and the firewall. You can also run the inside connections in in-line mode, which provides intrusion protection/prevention, while running the outside connection in tapped mode.

Figure 238. Scenario 1

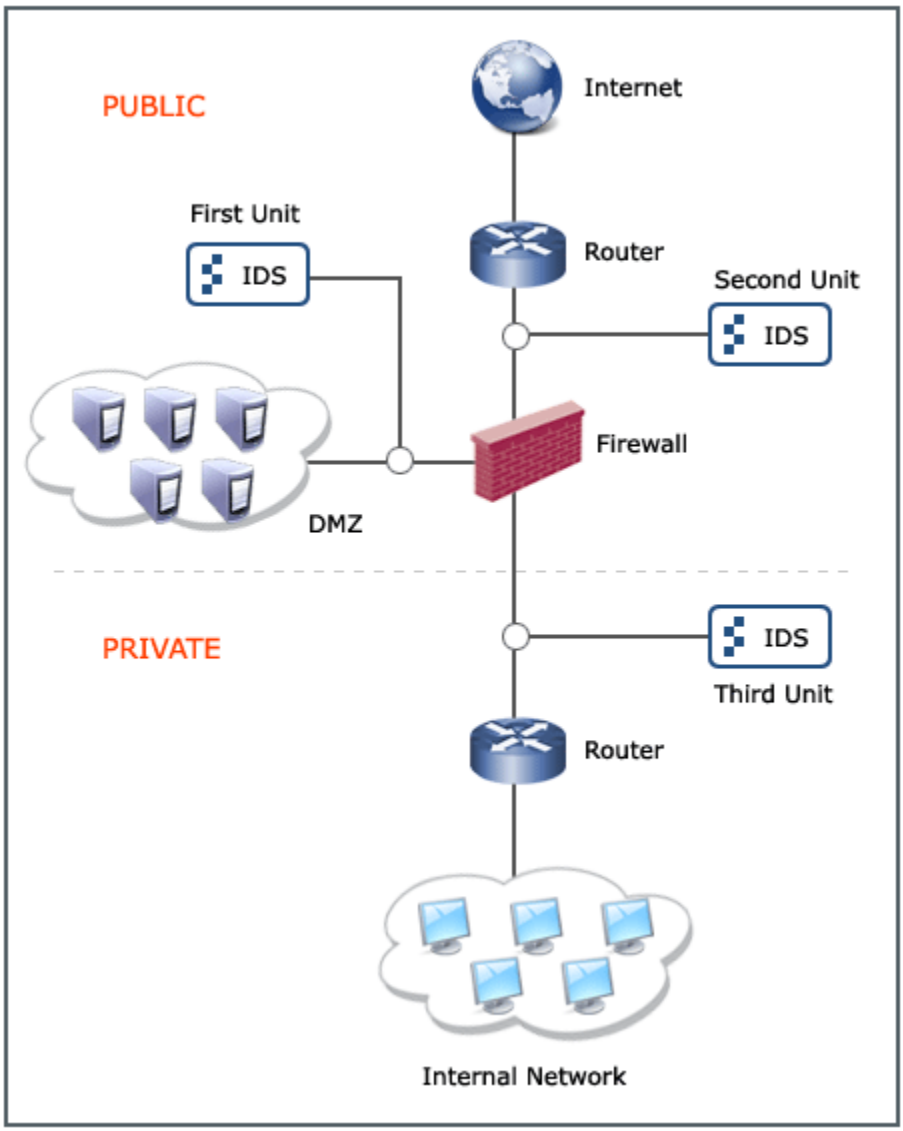
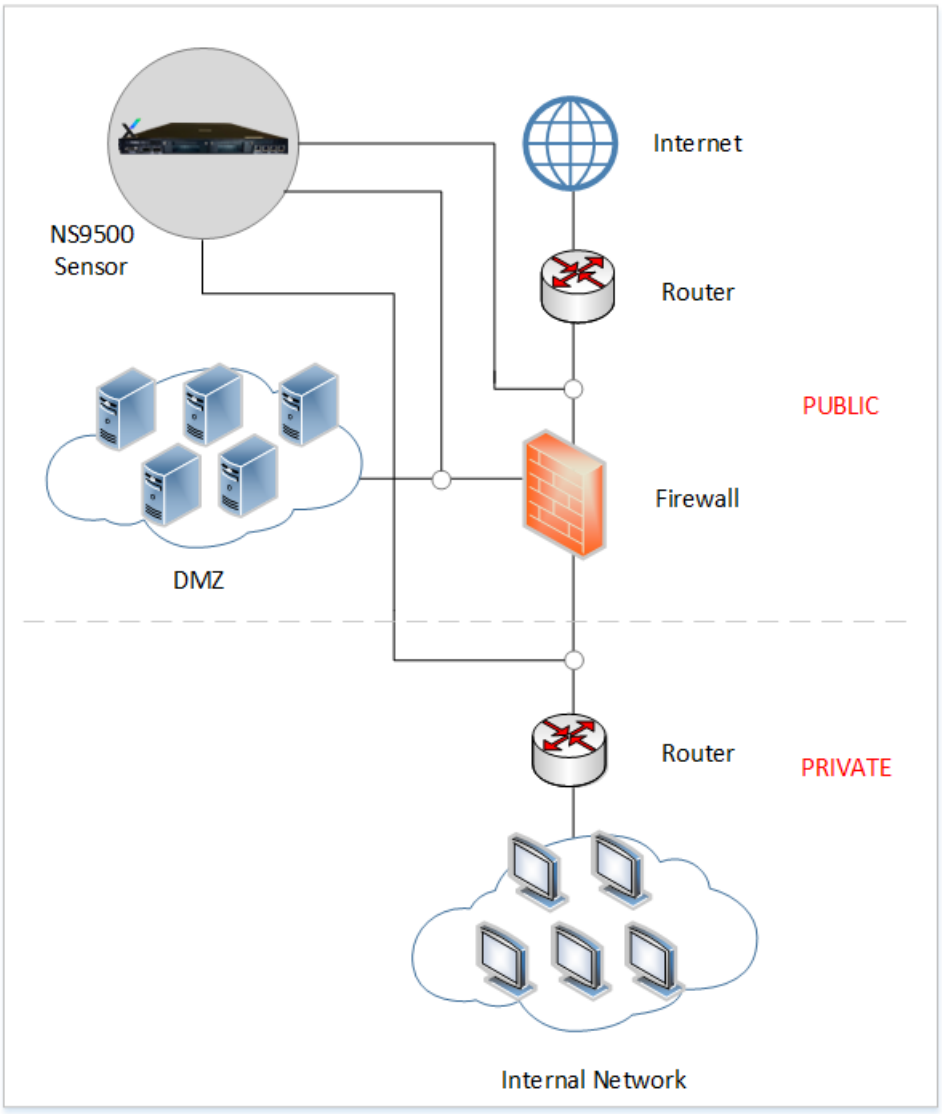


Figure 239. Scenario 2



Sensor deployment modes

This section presents suggestions for implementing Trellix Intrusion Prevention System in a variety of network environments.

Flexible deployment options

Trellix Intrusion Prevention System offers unprecedented flexibility in Sensor deployment. Sensors can be deployed in a variety of topologies and network security applications, providing industry-leading flexibility and scalability. Most PC-based IDS Sensors on the market today can monitor only one network segment at a time, and only via the SPAN port on a switch. Thus, to monitor a switched environment with multiple segments and multiple switches deployed in a High Availability environment, you would need multiple Sensors.

Multi-port Sensor deployment

Unlike single-port Sensors, a single multi-port Sensor can monitor many network segments in any combination of *operating modes*—that is, the *monitoring* or *deployment* mode for the Sensor—SPAN, Tap, or In-line mode. Additionally, Trellix IPS's Virtual IPS (vIPS) capability enables you to further segment a port on a Sensor into many "Virtual Sensors".

This makes deployment easy; not only can you use one Sensor to monitor multiple network segments, but you also can configure the Sensor to run whatever mode best suits each network segment. What more, you can enforce policies that are tailor-made for each of those network segments.

Supported deployment modes

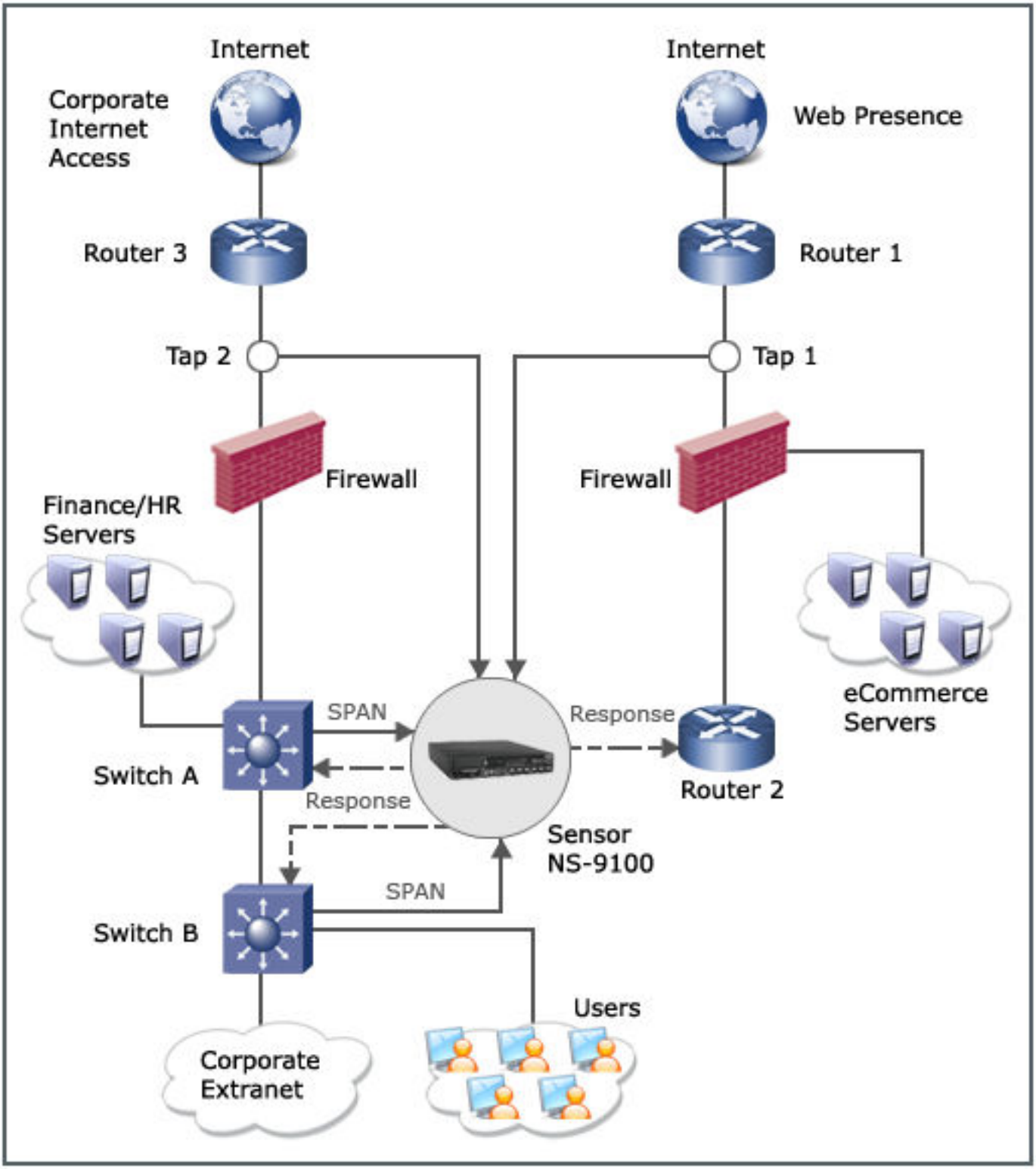
Every port on the Sensor supports the following deployment modes:

- SPAN or Hub
- Tap
- In-line, fail-closed
- In-line, fail-open

Additionally, Trellix IPS provides features vital to today's complex networks: *interface groups* (also called *port clustering*), and *High-Availability*.

In the following example, a single Trellix IPS NS-9100 Sensor is deployed to monitor the several external and internal points of exposure of an enterprise network. This includes the Web Presence, Corporate Internet Access for employees, employee Remote Access, Extranet connections, and internal attacks on critical department servers such as Finance and HR.

Figure 240. Deployment example



In this example, the ports on this NS-9100 Sensor might be configured as such:

- Tap 1: Ports G1/1 and G1/2 run in Tap mode and respond to attacks via Response port R1.
- Tap 2: Ports G2/1 and G2/2 run in Tap mode and respond to attacks via Response port R2.
- SPAN from Switch A: Port G2/3 runs in SPAN mode and inject response packets back to the switch through the SPAN port.
- SPAN from Switch B: Port G2/4 runs in SPAN mode and responds to attacks via Response port R3.

Full-duplex and half-duplex monitoring

Sensors are equipped with multiple Monitoring and Response ports. By default, the Sensor ports are internally wire matched to monitor traffic in full-duplex pairs, that is, two detection ports work together to monitor traffic flowing in both directions.

To monitor a full-duplex segment in In-line or Tap mode, you use two Sensor ports (one port for transmit, one for receive). SPAN port monitoring receives on one port and can respond via the same port (if the switch supports this feature).

NS-series Sensor model	Supported number of full-duplex links	Supported number of half-duplex links
NS9500	6	4
NS9300	20	16
NS9200	10	8
NS9100	10	8
NS7x50	10	8
NS7x00	10	8
NS5x00	22	20
NS3500	4	4
NS3x00	8	8

- In-line mode and tap mode can both monitor full-duplex links.
- SPAN monitoring works in either half- or full-duplex mode (depending on the switch).
- Hub monitoring works in half-duplex mode.

SPAN port and hub monitoring

Sensors can connect to the SPAN port of a switch or to a port on a hub. Most vendors' IDS Sensors are deployed in this manner, and many beginning Trellix IPS users choose to deploy in this mode. The Switch Port Analyzer (SPAN) port is designed for troubleshooting and network analysis so that an attached network analyzer can receive a copy of every single packet that is sent from one host to another through the switch. The SPAN port forwards all incoming and outgoing traffic within the switch to a predetermined port where a Sensor or a sniffer is connected. This is called *port forwarding* or *port mirroring*, and it allows an attached device to monitor all traffic of that switch.

When monitoring SPAN ports and hubs, traffic is typically half-duplex. Only one monitoring port is required to monitor each SPAN or hub port. You can send a response back through a hub; if you choose to send a response back through the SPAN port, you can do so if the switch supports transmit back through the SPAN port.

NOTE

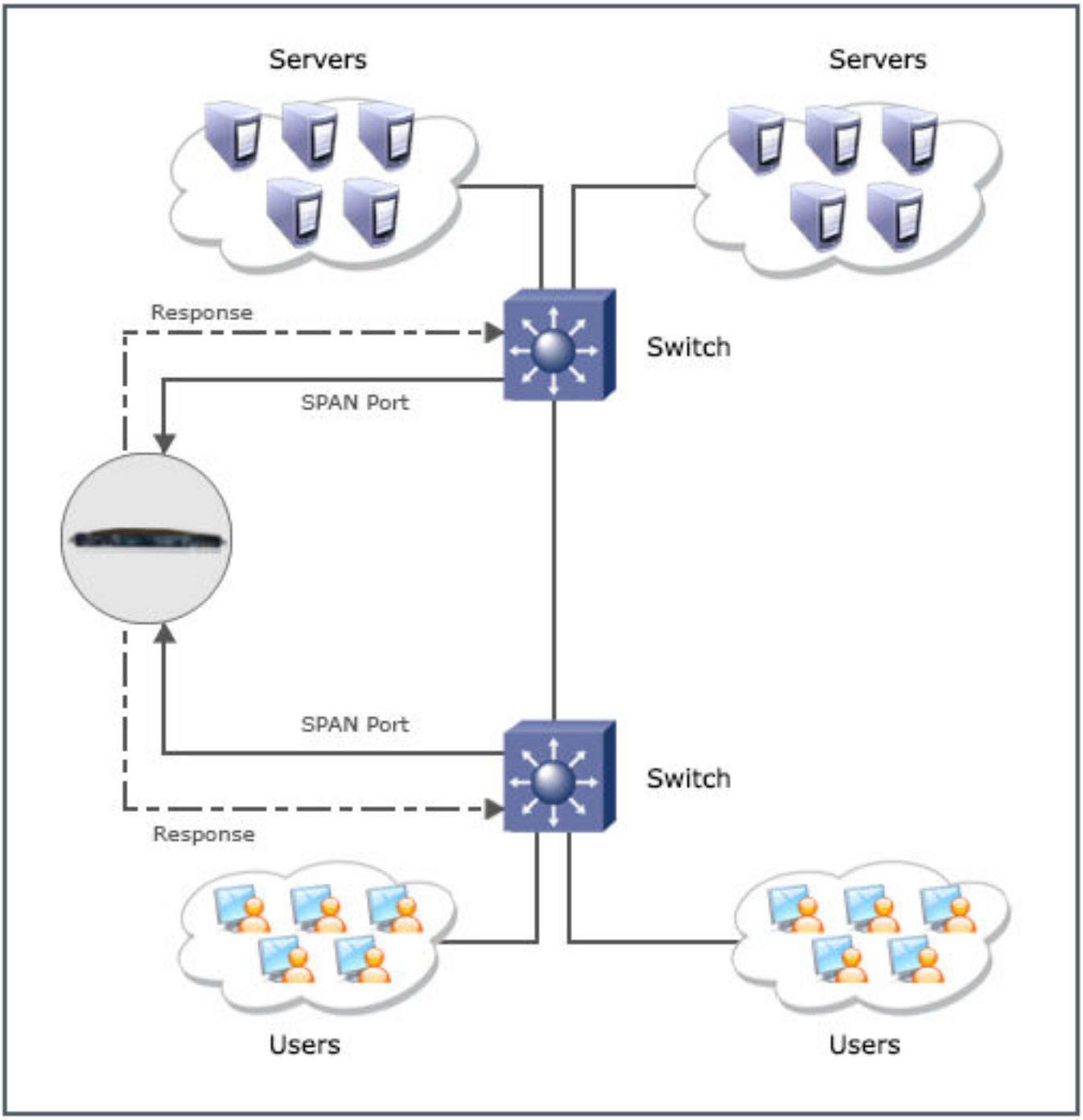
If the switch does not support transmit back through the SPAN, you can send a response via a Sensor response port.

SPAN port and hub monitoring

When monitoring a SPAN or hub port, Sensors with internal taps are disabled.

In the following figure showing an NS9500 base Sensor model, Port G0/1 receives data from the SPAN port of SwitchA. Port G0/2 gets data from the SPAN port of SwitchB. Two distinct network links from two separate switches are monitored by the one active NS9500 Sensor with a 5 Gbps rate per link to the Sensor, allowing a total of 10 Gbps traffic to the IPS engine.

Figure 241. SPAN port monitoring



Deployment of Sensors in tap mode

A *tap*--internal or external--is a passive wiring device that copies traffic on full-duplex Ethernet segments, and sends this copied traffic information to the S processors for analysis.

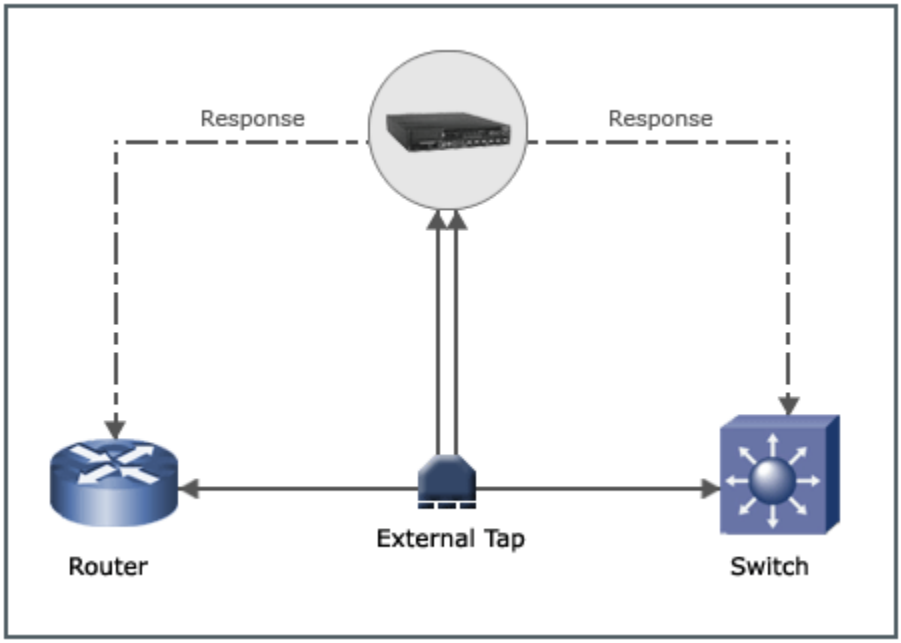
Full-duplex taps split a link into separate transmit and receive channels. Sensors provide multiple monitoring interfaces to monitor the two channels, and Sensor ports are wired in pairs in order to accommodate full-duplex taps. Two monitoring ports are used to monitor one full-duplex link using a tap.

The benefits to using Sensors in tap mode are:

- **Monitor uplinks passively** -- Taps cause no latency in your network traffic. You essentially sniff traffic as it passes.
- **Traffic continues to flow if the tap fails** -- Completely passive and fault tolerant, taps provide fail-safe operation with no impact on network connectivity or performance. Taps *fail open*, meaning that a failed Sensor permits traffic to continue to flow unimpeded.

The downside of tap mode is that, unlike in-line mode, you cannot prevent attacks. Tap mode is passive; the Sensor essentially sees malicious traffic as it passes, so sensing an attack in tap mode triggers a response post-attack. You also cannot inject response packets back through a tap; the Sensor provides Response ports to inject response packets.

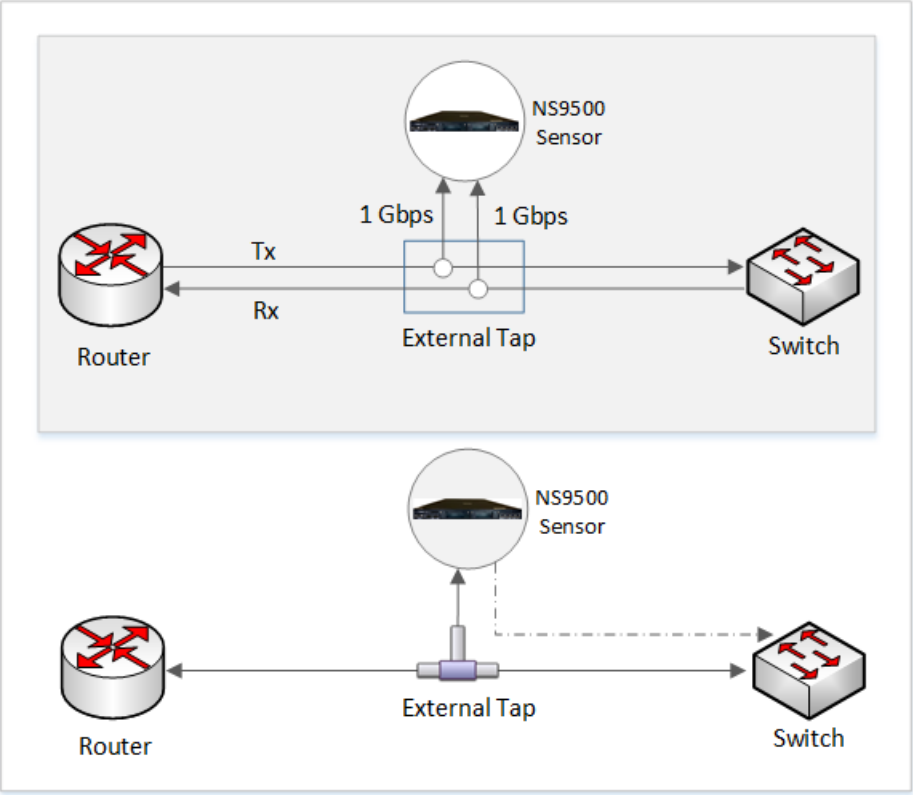
Figure 242. Tap mode



Deployment of Sensors with GE ports in external tap mode

Sensors with GE monitoring ports require external taps. The external taps are full-duplex; they connect in-line with the network segment, copy the traffic, and send the copies to the Sensor for analysis.

Figure 243. NS-9500 Sensor deployed in external tap mode



Shifting from tap mode to in-line mode

You can easily shift from tap to in-line mode. If you are running a Sensor with built-in taps in internal tap mode, you can toggle between tap and in-line mode with a simple software configuration change from the Manager interface. Thus, you can run in tap mode until you feel comfortable with the Sensor's reliability, and then shift into in-line mode without needing to touch the Sensor. You can also mix modes using different ports of a Sensor. You can run one pair in in-line mode and others in tap mode. With the GE port-Sensors, you will have to do some minimal reconnecting to convert from tap to in-line mode.

Deployment of Sensors in in-line mode

In-line mode is achieved when the Sensor is placed directly in the path of a network segment, becoming, essentially, a "bump in the wire," with packets flowing through the Sensor. In this mode, the Sensor can prevent network attacks by dropping malicious traffic in real time. Preventative actions can be at a highly granular level, including the automated dropping of DoS traffic intended for a specific Web server.

NOTE

Sensors are configured by default to run in in-line mode.

When running in in-line mode, network segments are connected to two matched ports of the Sensor (for example, ports G0/1 and G0/2), and packets are examined in real time as they pass through the Sensor.

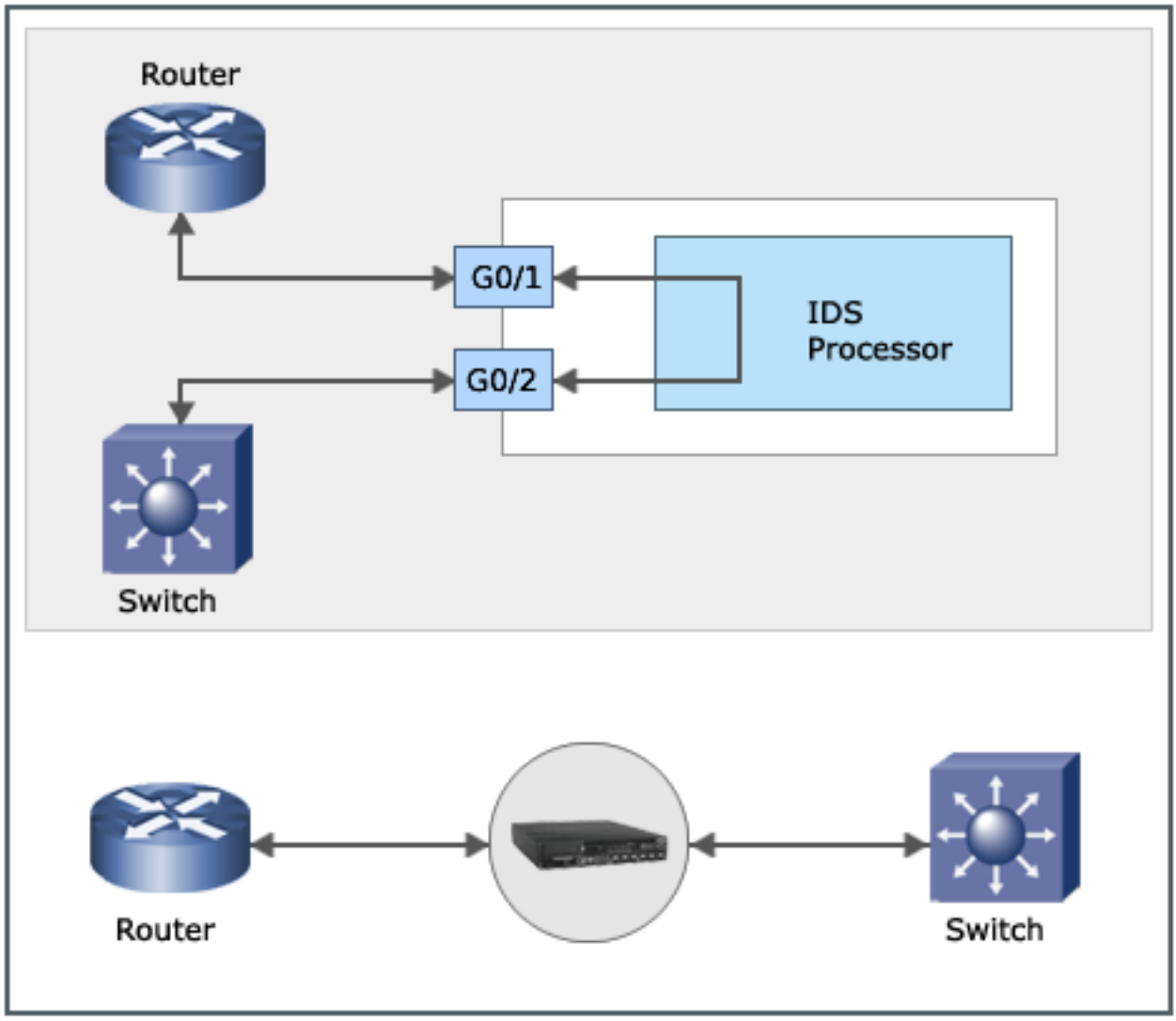
The benefits of using Sensors in in-line mode are:

- **Protection/Prevention** – Prevention is a feature unique to in-line mode. Basically, if you are running in any "sniffing" mode, there is no way for the IPS to prevent malicious packets from reaching their intended target. In a sniffing mode, the Sensor sees the attack at the same time it hits the target. You can apply some countermeasures, like TCP Resets, but these are post-detection actions. The only way to prevent the malicious packets from reaching the target is to mediate the traffic flow.

  When running in-line, the Sensor can drop malicious packets and not pass them through the network. This acts sort of like an "adaptive firewall," with your detection policy dictating what is dropped. Furthermore, when dropping packets, Trellix IPS is very precise and granular. The Sensor can drop only those packets it identifies as malicious or all of the packets related to that flow (a choice that is user configurable).

  One of the problems with using firewall reconfiguration actions with current IDS products is that an attacker can spoof large address ranges and mislead you into blocking legitimate traffic with the firewall, creating your own denial of service condition. Trellix IPS only drops the malicious packets, so spoofed traffic doesn't have the same effect.
- **Packet "scrubbing"** – In addition to dropping malicious traffic, Trellix IPS can *scrub*—or normalize—traffic to take out any ambiguities in protocols that the attacker may be using to try to evade detection. Current IDS products are susceptible to these techniques, and an example of this attempt is IP fragment and TCP segment overlaps. The Sensor can reassemble the IP fragments and TCP segments and enforce a reassembly mode of the user's choice to accept either the old or the new data.
- **Processing at wire-speed** – An obvious requirement with running in-line is to avoid dropping packets and your IDS Sensor becoming a bottleneck. Sensors are able to process packets at wire rates.
- **High Availability** – In in-line mode, the Sensor does become a single point of failure, so the Sensors support complete stateful fail-over, delivering the industry's first true high-availability IPS deployment, similar to what you would find with firewalls. If you're running in-line, Trellix recommends that you deploy two Sensors redundantly for failover protection.

Figure 244. In-line mode



- **Traffic prioritization** – When you deploy a port in inline mode and enable the inline traffic prioritization feature, the Sensor prioritizes packets emerging from the port in inline mode, during heavy network load conditions, over packets emerging from a port in SPAN mode.

  The Sensor periodically checks for latency in inline packets. If latency is higher than a stipulated limit and, at the same time, there are several inline packets and SPAN packets in queue to be analyzed by the Sensor, some of the SPAN packets are dropped to prioritize inline packets.

  When traffic density returns to normal operating levels, the Sensor stops prioritizing inline packets and traffic is analyzed in the order that it arrives.

NOTE

Prioritization of inline traffic is disabled by default. You can view or change its status only through the Sensor CLI **Debug** mode using the following commands:

- **`show inline traffic prioritization status`** — Displays whether it is enabled or disabled
- **`set inline traffic prioritization <enable | disable>`** — Enables or disables the feature

In inline mode (seen in the previous figure), the Sensor logically acts as a transparent repeater with minimal latency for packet processing. Unlike bridges, routers, or switches, the Sensor does not need to learn MAC addresses or keep an ARP cache or a routing table.

When deployed in-line, you must specify whether the Sensor port is monitoring inside or outside of the network it is protecting. For example, the Sensor shown in the figure in the section [Determination of complexity of your network topology?] is monitoring links both inside and outside the network.

Fail-open versus fail-closed

Sensor ports deployed in In-line Mode have the option of failing open or closed. Similar in terminology to firewall operation, ports failing *open* allow traffic to continue to flow. Thus, even if the ports fail, your Sensor does not become a bottleneck; however, monitoring ceases which may allow bad traffic to impact systems in your network. When ports are configured to fail *closed*, the Sensor does not allow traffic to continue to flow, thus the failed ports become a bottleneck, stopping all traffic at the Sensor.

Inline Fail Open - Passive option for GE ports

Gigabit Ethernet Sensor ports require the connection of a Passive Fail Open (PFO) kit if configured in **Inline Fail Open - Passive** operation mode. Passive Fail Open Kits are sold separately.

NOTE

This mode is only supported in NS5x00, NS7x00 and NS7x50

For more information on hardware connection, see [Trellix Intrusion Prevention System Fail-Open Kit Product Guide]. And, for more information on port configuration, see Configuring the monitoring and response ports of a Sensor (page 611).

Layer 2 passthru mode

Fail-open operation provides a measure of network integrity when a Sensor fails. When a Sensor with ports operating in In-line Fail-Open Mode experiences a critical fault, the Sensor might restart; during the restart, the Sensor goes into fail-open mode until it restarts. If a critical fault occurs again, another restart cycle might be initiated. In some cases, this can continue until acted upon through human intervention.

You can enable a failure threshold to automatically initiate fail-open, or *passthru*, mode by configuring the **Layer 2 Passthru** feature from the Manager user interface. This feature enables you to set a threshold on the number of critical failures within a configured period of time that the Sensor can experience before being forced into Layer2 passthru mode.

For example, you configure Layer 2 Passthru mode to be enabled if there are three critical faults in any 10-minute period. At minutes 1, 3, and 7, faults occur; L2 mode is enabled. Here is another scenario: at minutes 1, 4, 11, and 13, faults occur. In this case, the last three faults occurred within 10 minutes of each other, thus the Sensor enters L2 mode.

Sensor restart may take a few minutes to complete. This downtime is not counted against the L2 duration; only Sensor uptime is counted.

The L2 feature is supported by all NS-series Sensor models.

High Availability

Redundancy is a key element for any network that needs to operate all the time. Using an identical pair of Sensors (same model, software image, signature set) deployed redundantly in In-line Mode, Trellix IPS can provide high availability with no administrator intervention.

How to understand failover in Trellix IPS

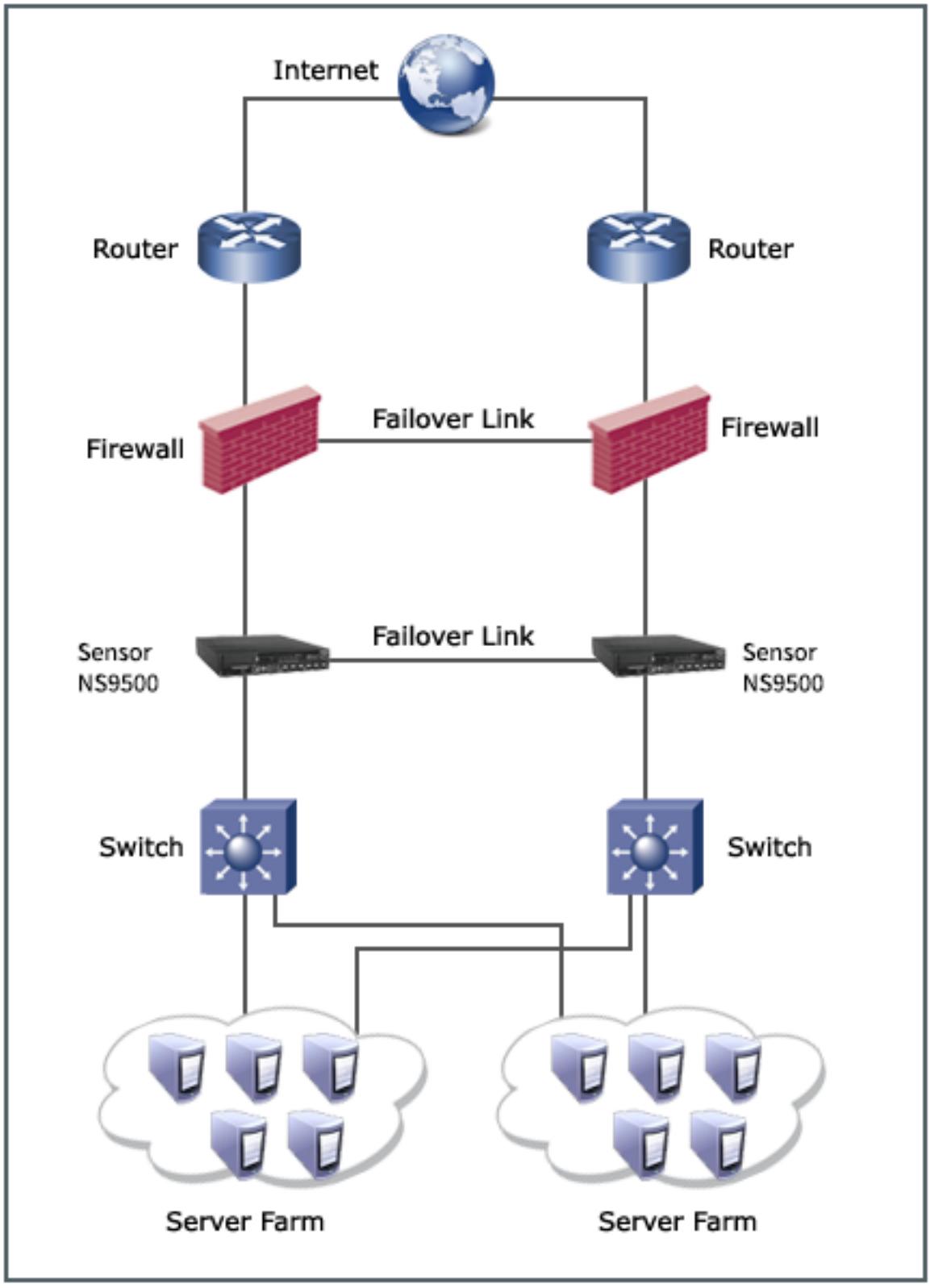
In typical failover configurations, one device is the *template* device while the other is the *peer*. As its name implies, when you create the HA pair, the configurations applied on the template device is applied on the peer. The template device is the active device and performs normal network functions while the peer is the standby, which monitors, ready to take control should the template/active device fail. When you delete the HA pair, the template device's configuration is what remains on the peer device. So, it is recommended that you export the configuration of the peer device before you create a HA pair.

In Trellix IPS, because both failover Sensors must be ready to process packets on their monitoring ports at all times, both Sensors are actually active at all times; neither Sensor is inoperative, or 'standing by' unless the unit has failed. Instead, both Sensors operate normally.

In the following figure, two Sensors are placed in-line, connected to each other via cables, and configured to act as a *HA pair*. All traffic is copied and shared between them in order to maintain state. One Sensor copies the packets received on its monitoring ports to the other Sensor using the interconnection ports and vice versa. Since both Sensors see all traffic and build state based on it, their state information is synchronized at all times.

All packets are seen by both Sensors (when both are operational); however, only one Sensor in the pair raises an alert whenever an attack is detected.

Figure 245. Two NS9500s in a high availability configuration



Primary vs. Active

You configure a HA pair using the Manager. You designate one Sensor as the *template* Sensor and the other as *peer*. This designation is used purely for configuration purposes and has no bearing on which Sensor considers itself active.

Once configured, the two Sensors exchange information to determine their respective roles; the Sensor that has been online the longest becomes the active Sensor. If they have been online for exactly the same amount of time, the Sensor with the higher serial number takes the active role. The Sensors communicate every second to determine if their peer is available. If the HA pair cannot communicate with each other, each Sensor will assume its peer Sensor is down, and both will issue alerts. If communication is re-established, the two Sensors communicate to determine their respective failover roles.

When one Sensor is brought up well after the other, the new Sensor synchronizes state with the old Sensor and builds on the synchronized state based on the packets received on its monitoring and interconnect ports.

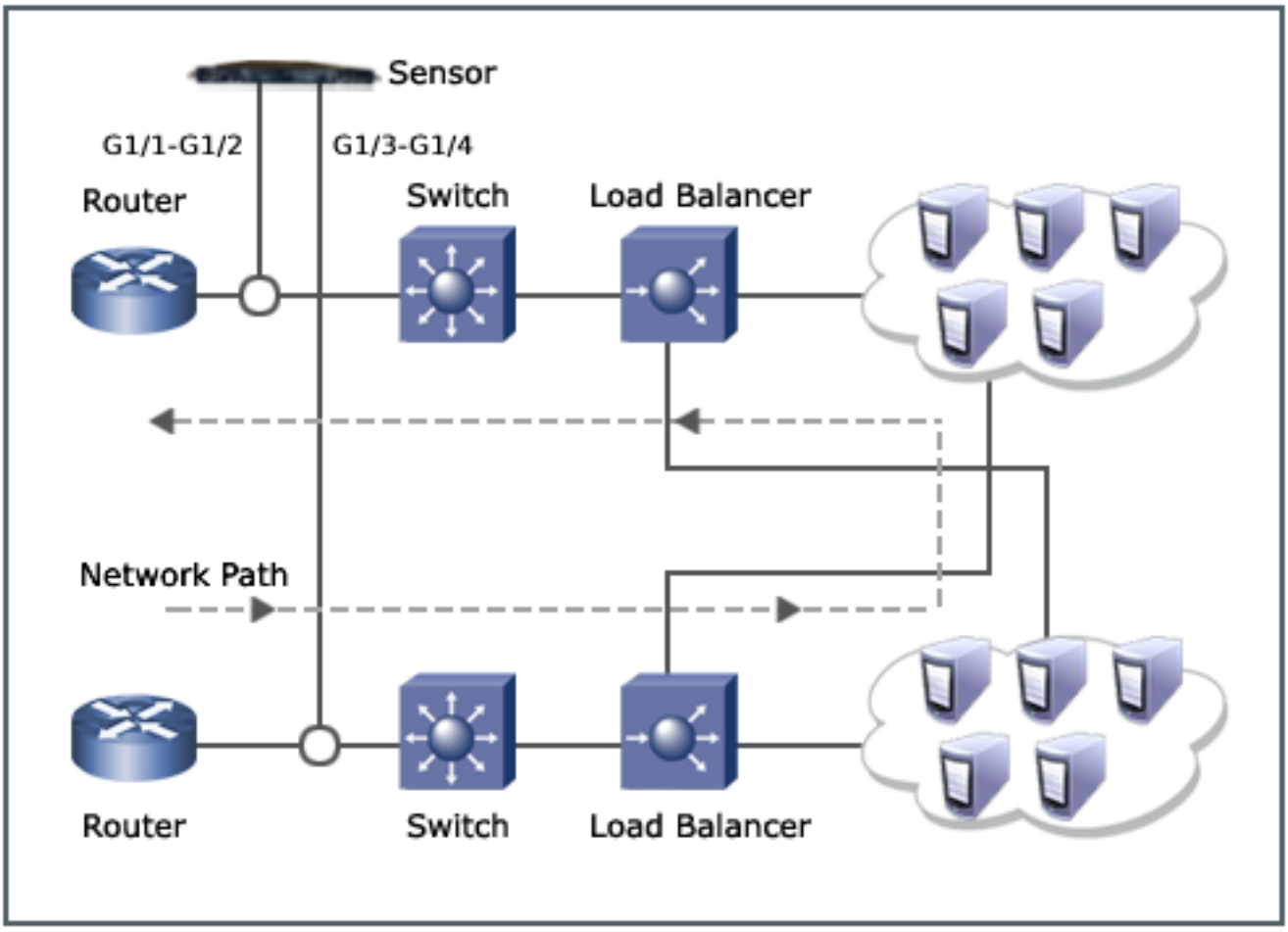
This Active-Active configuration provides the added benefit of supporting asymmetric traffic flows (that is, when packets belonging to the same TCP/UDP flow are divided across Sensors). Thus, the Trellix IPS HA pair will detect attacks even when the traffic is asymmetric. This topic is discussed, in the section [Interface groups.]

Interface groups (port clusters)

An interface group, also known as *port clustering* in networking parlance, combines the traffic processed on separate Sensor interfaces—or, in the case of a HA pair, on separate Sensors—into a single logical interface for state and intrusion analysis. Asymmetric routing is a good example of where an interface group is recommended. In asymmetric routing, a TCP connection does not always send and receive along the same network path. Therefore, a single-interface Sensor monitoring this transmission may only see the traffic received, not the traffic sent in response; thus not seeing all data from a transmission.

Sensors' multiple interfaces make the monitoring of asymmetric traffic possible. For example, consider an NS9500's G1 interface module that has 4 ports. The ports are wired in pairs by default. Peer ports G1/1 and G1/2 can monitor one direction of an asymmetric transmission, while peer ports G1/3 and G1/4 can monitor the other direction. By making an interface group of G1/1-G1/2 and G1/3-G1/4, the Sensor is able to see all the traffic for all sessions in the asymmetrically routed network and still is able to maintain state and accurately detect all attacks.

Figure 246. Interface groups in an asymmetric network



Create a port cluster

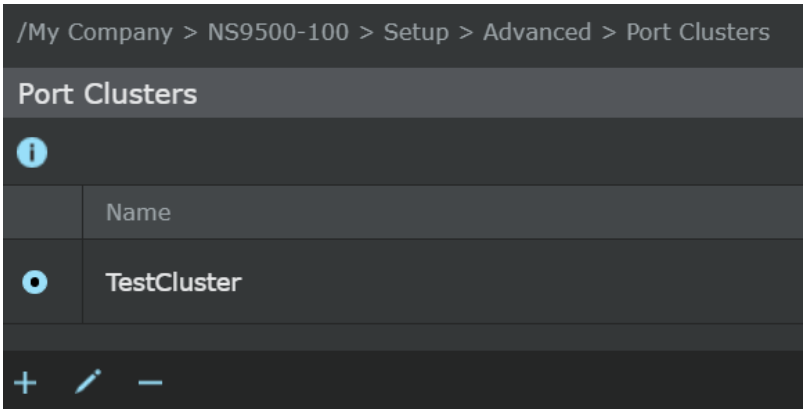
The **Port Clusters** action enables multiple Sensor ports to be grouped together for the effective monitoring of asymmetric environments. Asymmetric networks are common in load balancing and active/passive configurations. Port clusters normalize the impact of traffic flows split across multiple interfaces, thus maintaining state to avoid information loss.

Once configured, an interface group appears in the IPS interfaces as a single interface node (icon) under the <Device Name> where it is located. All of the ports that make up the interface are configured as one logical entity, keeping the configuration consistent.

> ⚠ **CAUTION**
>
> If you decide to change your settings after the initial interface group configuration, all of the previous configurations performed for the interface group are erased in favor of the new port configuration. This can affect sub-interfaces and policy settings.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **Port Clusters**.

Figure 247. Port cluster list area



2. Click +.
3. Type a **Name**.
4. Select a **Template Port** from the drop-down list.
   - For standalone Sensors, the template port will display the port pair (G3/3-G3/4)
   - For a stack of Sensors, the template port will display the member Sensor along with the port pair (<Stack-name_node-Id>/G3/3-G3/4).

     NOTE

     G0/1 and G0/2 ports will be excluded from the drop-down list because they are used to create the stack.

   - For HA pair of Sensor stacks, the template member port will display both peer member sensors along with the port pair (<Stackname_node-Id>:<Stackname_node-Id>/G3/3-G3/4).

     NOTE

     G1/1 and G1/2 ports will be excluded from the drop-down list because they are the interconnect ports used to create HA pairs.

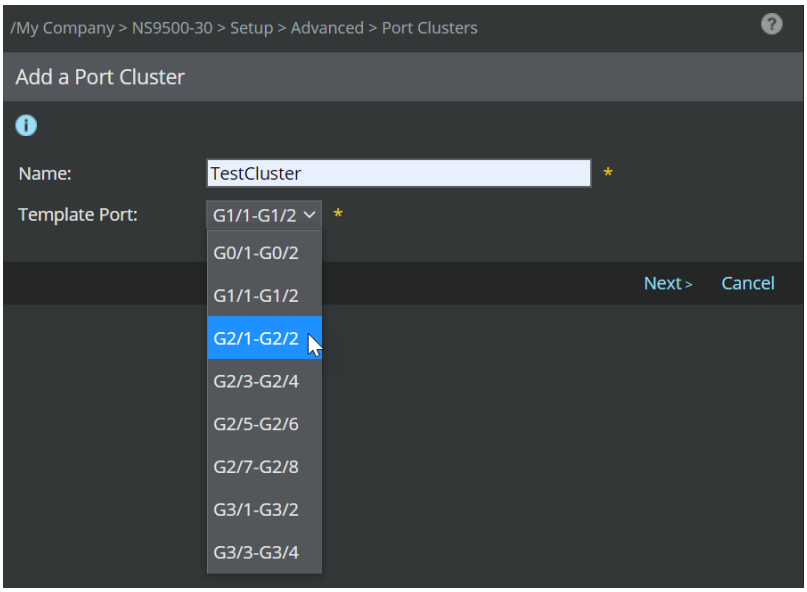
   The template member port determines the policy that is enforced by the group.

   NOTE

   An interface changed from Dedicated to VLAN or CIDR traffic types is not eligible for interface group combination until VLAN or CIDR IDs are added.

5. Click **Next**.

Figure 248. Create Cluster dialog



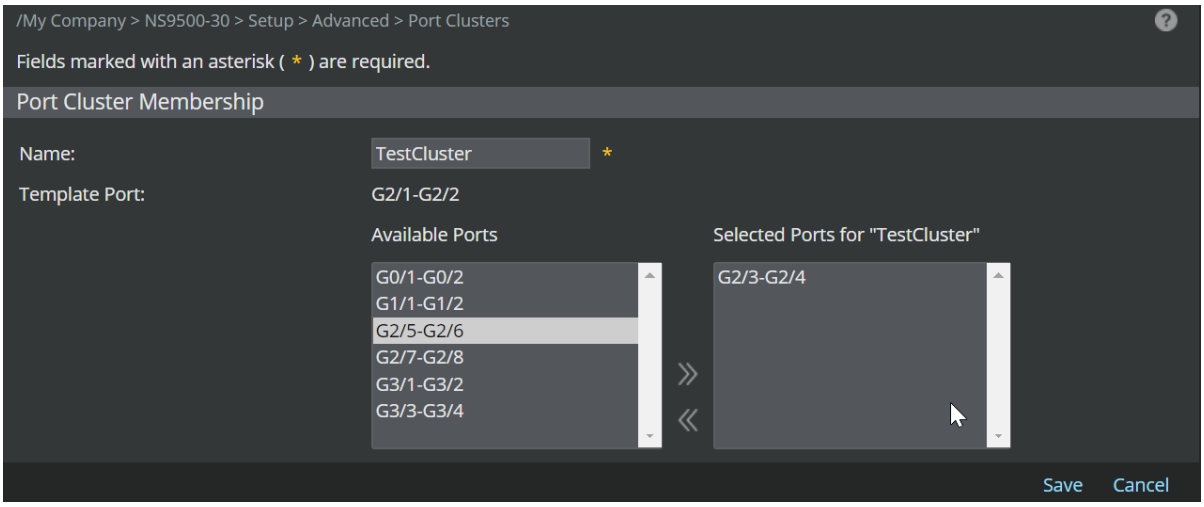
6. Select interfaces to add to the group.

   For Sensors in a stack, the list of available ports displays interfaces of each member Sensor in the stack.

7. Click **Save** to complete the creation of a port cluster, or click **Cancel** to exit the window.

   If interfaces are functioning as a port pair, they cannot be separated within an interface group.

Figure 249. Add/Delete Interfaces To Port Cluster Member dialog



8. Download the changes to your Sensor by clicking **Deploy Pending Changes**.

Managing interfaces

Sensors support four traffic types:

- Dedicated

- VLAN
- Bridge VLAN
- CIDR

By default, all interfaces monitor traffic in *Dedicated* mode: the interface monitors all transmissions without regard to network segmentation. Traffic segmentation by *VLAN* tag or *CIDR* addressing is supported. If your traffic is segmented into VLANs, for example between switches in a building, you can change the interface type to VLAN. More commonly, if you have used CIDR addressing in your network, changing the traffic type to CIDR helps you better protect specific networks/hosts in your system. For VLAN and CIDR interfaces, you are able to add the network IDs, either VLAN tags or CIDR addresses, in order to specify unique networks in your domain.

By segmenting the network traffic into VLAN or CIDR, the user has more flexibility in applying multiple policies to traffic subflows. This is accomplished by configuring one or more traffic subflows (VLAN tag(s)/CIDR block(s)) into a sub-interface.

A Bridge VLAN interface functions exactly like a VLAN interface except that post-IPS, if the traffic is OK, the Sensor changes the VLAN ID to that of the peer ID.

The VLAN Bridging feature enables you to subject inter-VLAN traffic to IPS with the least number of Sensors. You can also use the VLAN Bridging feature in conjunction with EtherChannel Load Balancing on your switches, to incrementally increase the IPS bandwidth of your Trellix IPS infrastructure.

NOTE

You cannot change the traffic type of an allocated interface. Since the interface has been allocated, it is the "virtual" property of the child domain. Therefore, full ownership cannot be granted. Only the admin domain in which the physical port(s) — thus interface — reside owns the interface and can make this type of change.

CAUTION

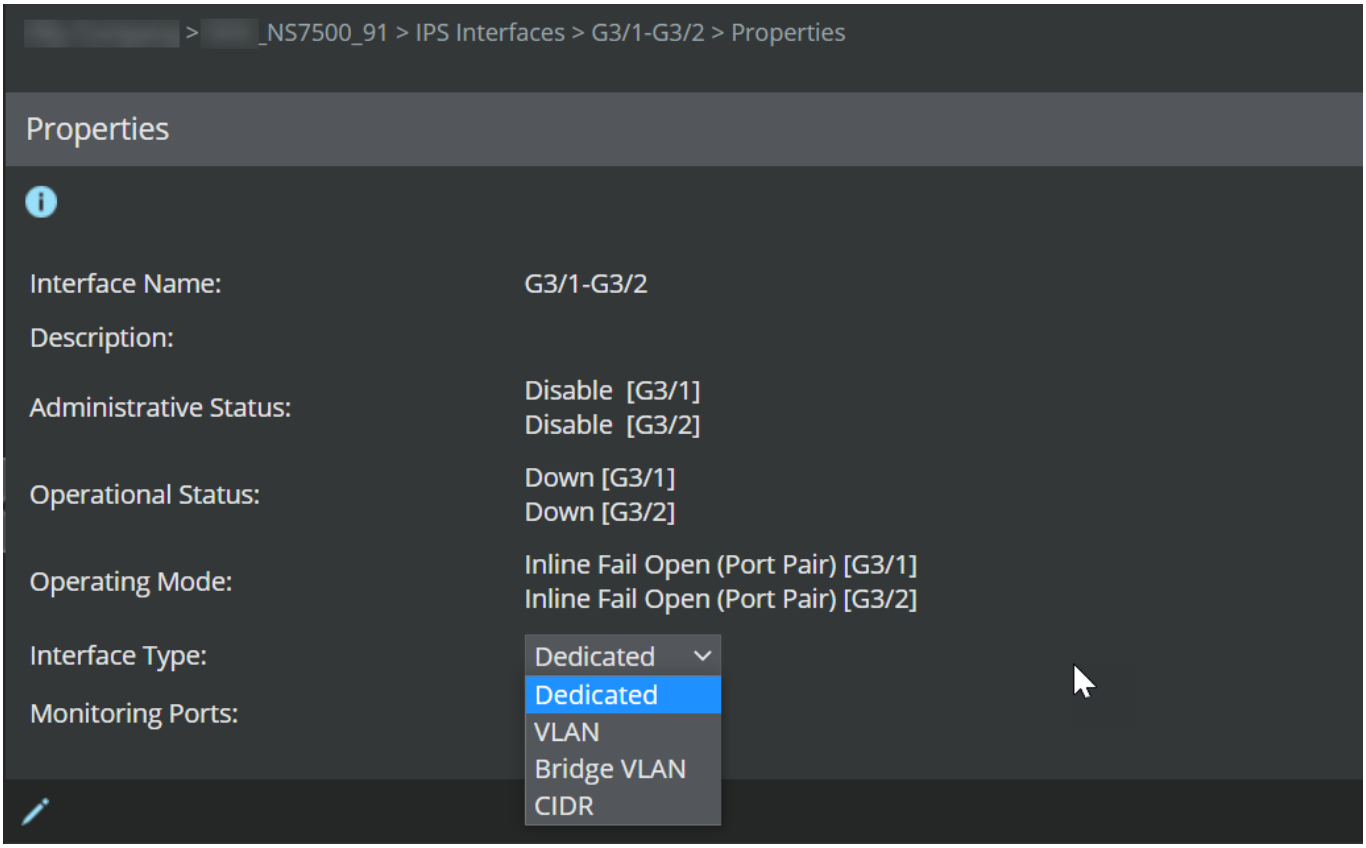
If you decide to again change your traffic type settings after having once changed from Dedicated to VLAN or CIDR, all of the previous configurations performed at the interface and sub-interface levels for the interface are erased in favor of the new configuration. This can affect many scenarios including the creation of a child admin domain to where an interface has been allocated.

To change the traffic type of an interface and add VLAN or CIDR network IDs, do the following:

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Interface_Name> → **Properties**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Stackname-node id> → <Interface_Name> → **Properties**.

Figure 250. Manage Interface - changing traffic type



2. Select the **Interface Type** as one of the following:
   - **Dedicated**: (default) no segmentation of traffic
   - **VLAN**: enables segment of interface into multiple networks by VLAN tags
   - **Bridge VLAN**: enables bridging of traffic between VLANs

     NOTE

     When the Sensor is down, the traffic is forwarded through the peer port with the same VLAN ID with which it came to the Sensor. So, if your switches are not configured to handle such a scenario, the packets may get dropped. You can set up a fail-over Sensor to mitigate this risk.

   - **CIDR**: enables segment of interface into multiple networks by CIDR addressing

     If you selected **VLAN** or **CIDR**, go to Step 3. If you selected **Dedicated**, you are done.
3. Click from the new VLAN or CIDR window to add the VLAN/CIDR IDs.
4. (Optional) Clear the port number(s) and type new text in the **Interface Name** field. The custom name can have up to 45 alphanumeric characters including hyphens, underscores, and periods. The text you enter appears under IPS Interfaces where the interface node is located; the physical port number is still listed in parentheses at the end of your text. For example, if you typed "VLANs 1-5" as the Interface Name for port pair G3/1-G3/2, IPS Interfaces list the node as **VLANs 1-5(G3/1-G3/2)**.

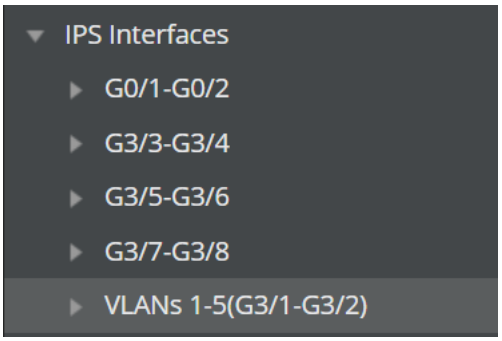
NOTE

If you had changed the **Interface Name** earlier and if you want to restore the default, click **Reset Name to Default**. This action has no effect on the **Description** field.

NOTE

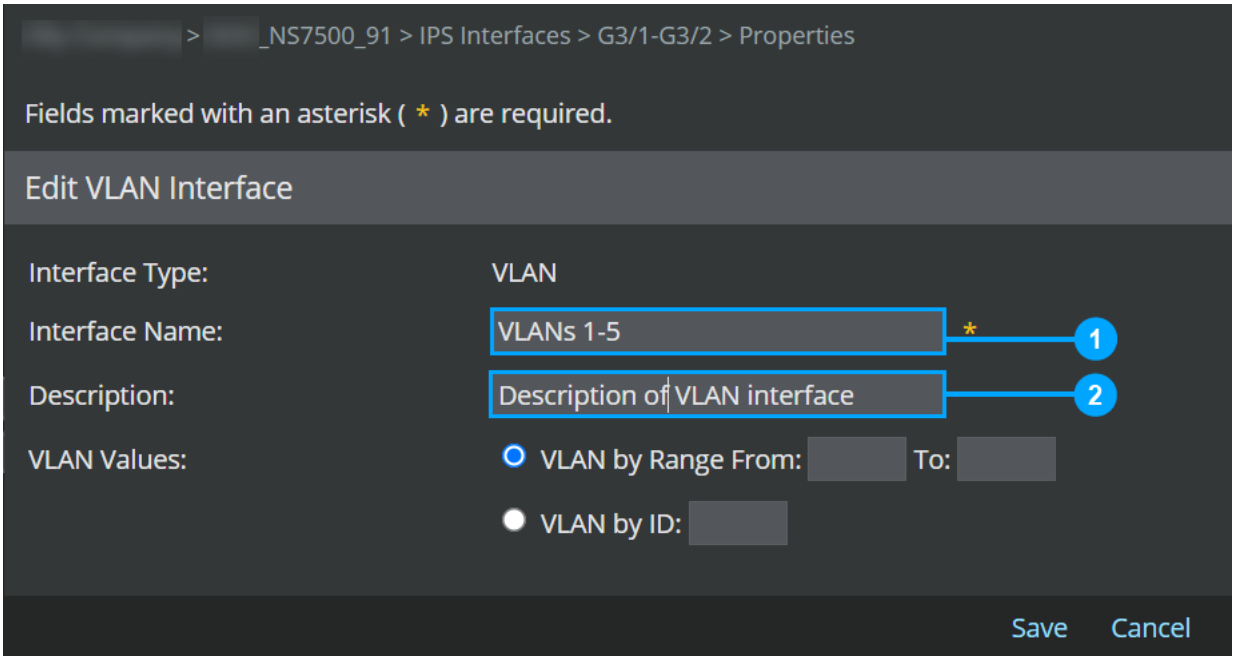
If you have given a custom name to an interface and later allocated the interface to a child domain, the custom name is not inherited by the child.

Figure 251. Interface name change under IPS Interfaces



5. (Optional) Type an interface **Description**. This text does not display under IPS Interfaces, only in the interface detail. A unique description can only be entered when the interface type has been changed to VLAN or CIDR.

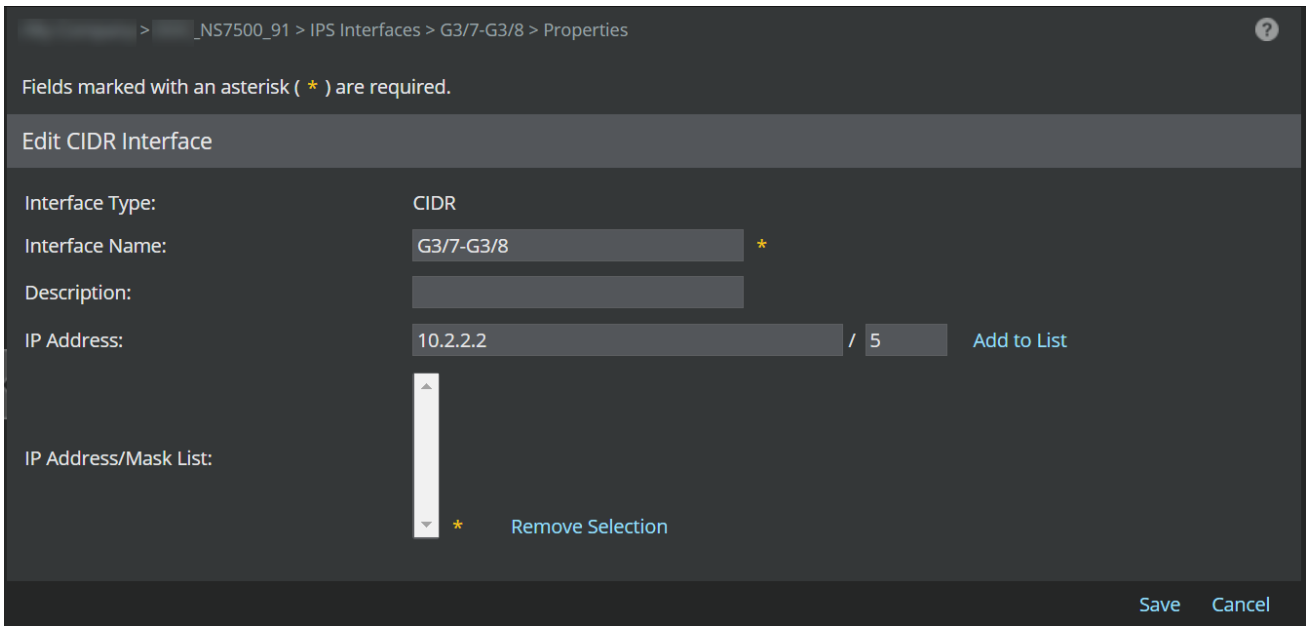
Figure 252. Edit VLAN IDs



Item	Description
1	Custom name (default is port number). This name appears under IPS Interfaces.
2	Only appears in interface description dialog

6. Add the VLAN/CIDR IDs you want to monitor.
   - For VLAN, you can type the VLAN tags by range or by individual ID. The valid range is 0 to 4095, and the maximum number of VLAN tags per interface is 254. If you create a sub-interface and assign all the 254 VLANs to the sub-interface, you can create more number of VLANs in the interface.
   - For CIDR, type the network **IP Address** in the text box provided and the mask length value in the box provided after the forward slash, and click **Add to List**. This network address must follow standard CIDR addressing rules (correct IP and mask length combination) to be valid. For example, in the figure below, the CIDR range of 10.2.2.2/5 is about to be added to the selected interface.

Figure 253. Edit CIDR Interface



> **TIP**
>
> If you are unsure about your exact VLAN/CIDR IDs and you do not enter IDs, you can always add your IDs later.

7. Click **Save** to save your interface additions; click **Cancel** to abort.
8. Download the changes to your Sensor by clicking **Deploy Pending Changes**.

The IPS Sensor interface node

The **Interface-x** nodes under **IPS Interfaces** represent an interface (a single physical port, peer ports, or an interface group) on a particular Sensor. The number of interface nodes displayed depends upon the type of Sensor. Interface nodes are displayed individually by default because the default monitoring mode is SPAN mode.

Full-duplex Tap and Inline modes require two physical ports, and each mode uses these two ports to form a single logical interface. Therefore, all configuration and policy decisions are made at a logical interface level.

After a new Sensor is installed, a policy is inherited from the admin domain and enforced on all Sensor interfaces. Subinterfaces are user created within this resource, and can be edited here or from the **Sub-interface-x** resource node.

TIP

Interfaces can be allocated to child domains for specialized management.

The navigation path to the interface nodes is as follows:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. For a standalone Sensor, select IPS Interfaces → **<interface name>**.

   For Sensors in a stack, select IPS Interfaces → <Stackname-node id> → **<interface name>**.

The primary tasks that you can perform are customizing policies, assigning policies, and configuring inspection options.

Configuration of general interface settings

The **Policy Manager** page at the interface level provides options for applying the general settings of an interface.

- Managing policies at the interface level — Configure the policies at the interface level under **Interfaces** tab; manage the inspection options.
- Managing an interface — Change the traffic type and name the interface; enable segmentation of the interface by changing the traffic type to CIDR or VLAN.
- Creating subinterfaces — Create a subinterface for policy application and traffic management.

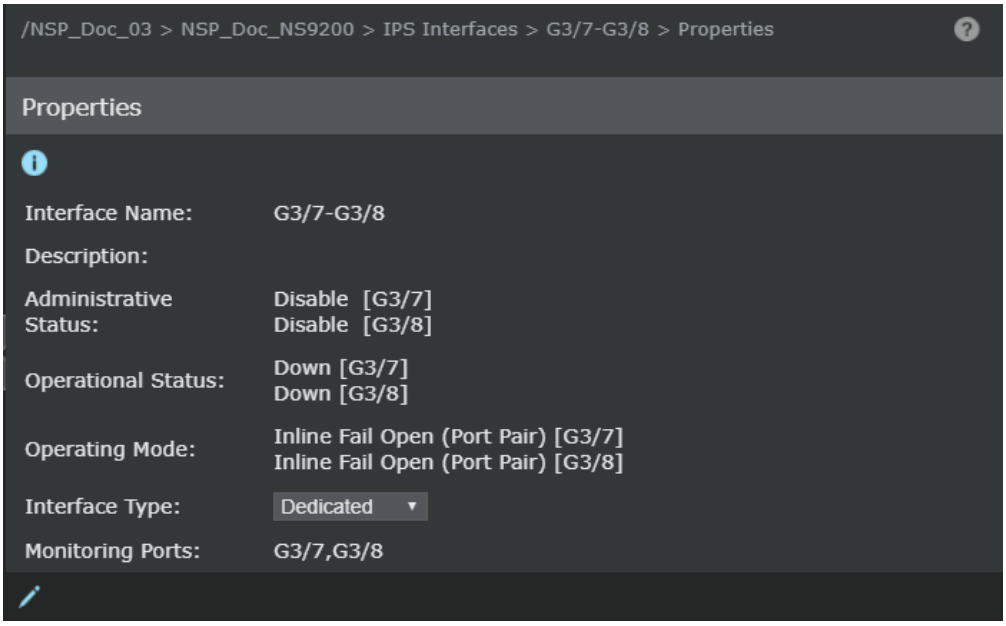
Viewing interface details

To view the details of an interface, select an interface node under IPS Interfaces:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. For a standalone Sensor, select IPS Interfaces → <interface name> → **Properties**.

   For Sensors in a stack, select IPS Interfaces → <Stackname-node id> → <interface name> → **Properties**.

Figure 254. Interface detail



The dialog details are as follows:

- **Interface Name** — Identification of ports that make up the interface. For peer ports, format is xA-xB. If this is an interface group, multiple Sensor ports are listed. This name is user-configurable if the traffic type is changed to VLAN or CIDR; a unique name enables easy recognition.
- **Description** — Description of the interface
- **Administrative Status** — State defined by user. **Enable** is up, **Disable** is down.
- **Operational Status** — State defined by Sensor (functional) operation. **Up** is working and user-enabled, **Down** is user-disabled or a malfunction has occurred.
- **Operating Mode** — The monitoring configuration of the interface
- **Interface Type** — Traffic type; Dedicated by default and can be changed to VLAN or CIDR
- **Monitoring Ports** — The physical Sensor ports which comprise the interface

Click to edit the interface level settings.

Delete a VLAN or CIDR ID from an interface

You can delete a VLAN or CIDR ID from a segmented interface.

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Interface_Name> → **Properties**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Stackname-node id> → <Interface_Name> → **Properties**.

2. Select the ID to delete.

3. Click − and confirm deletion.
4. Download the changes to your Sensor by clicking **Deploy Pending Changes**.

Create sub-interfaces

If there is VLAN,Bridge VLAN or CIDR traffic transmitting across a monitored segment, you can create one or more sub-interfaces. Before creating a sub-interface, the "Interface Type" must be set to VLAN or CIDR in Managing an interface, and you must have already entered VLAN or CIDR IDs.

NOTE

If you entered IDs that do not flow in the monitored link, the parent interface's policy protects all traffic.

NOTE

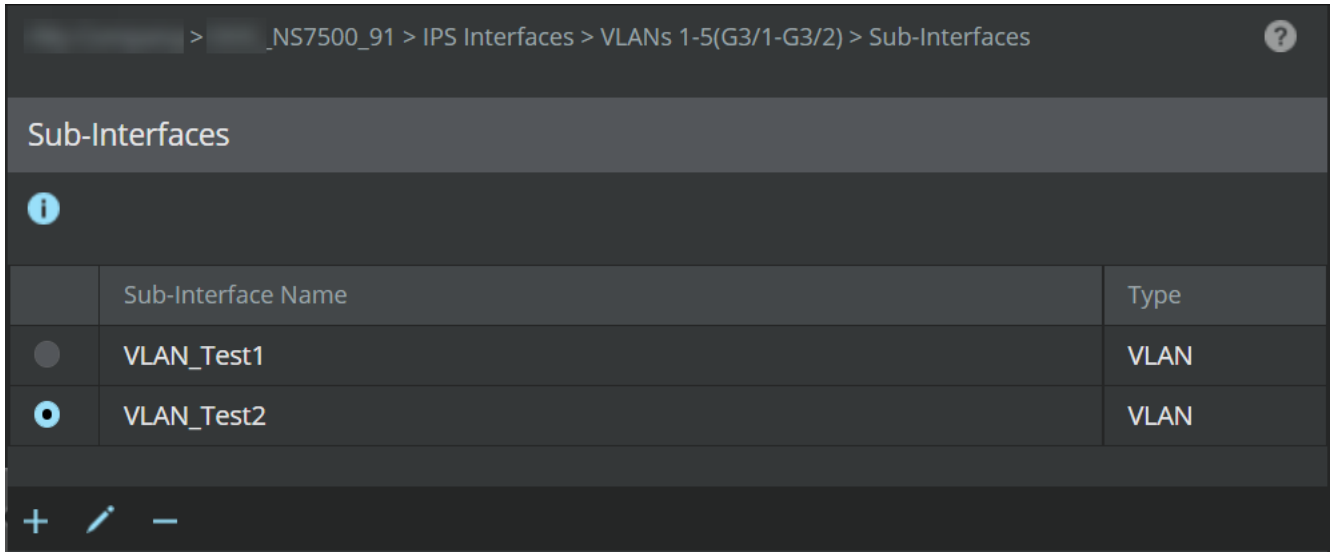
Before creating sub-interfaces, it is important to note that you will not be able to perform the **Manage DoS IDs** action at the interface level once a sub-interface is created. If you create a sub-interface, then you must utilize **Manage DoS IDs** at the sub-interface level.

If you added more than one VLAN or CIDR ID to an interface, you can create a sub-interface with one or multiple IDs or you can create multiple sub-interfaces. To create more than one sub-interface, you must repeat the steps that follow.

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Interface_Name> → **Sub-interfaces**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Stackname-node id> → <Interface_Name> → **Sub-interfaces**.

   Figure 255. Manage Sub-Interface

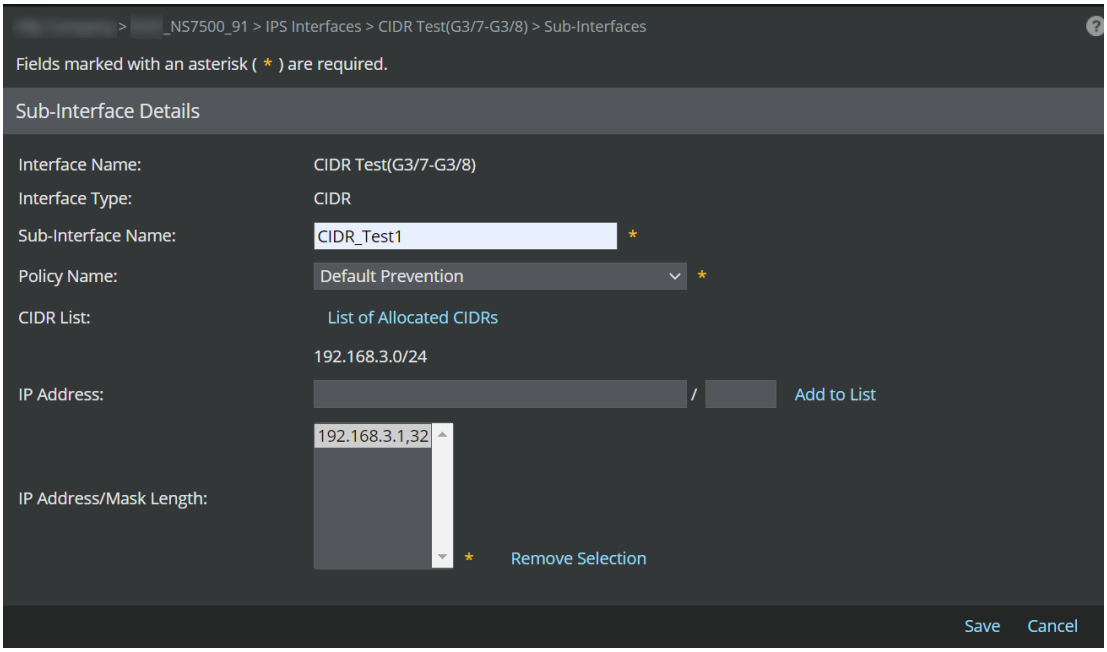
2. Click +.

NOTE

To edit an existing sub-interface, select the sub-interface and click ; then follow the steps below. To delete a sub-interface, select the sub-interface and click ; then confirm the deletion.

3. Type a **Sub-interface Name**.
4. Select a policy (**Policy Name**) to be enforced on the sub-interface(s).

Figure 256. Create Sub-Interface - CIDR



5. Do one of the following:
   - For VLAN and Bridge VLAN, move an ID from "Available" to "Allocated" by selecting the ID and clicking the button.
   - For CIDR, type the network **IP Address** in the text box provided and the mask length value in the box provided after the forward slash, and click **Add to List**. A valid CIDR can be from the list you entered on clicking at IPS Interfaces → **Interface_Name** (For Sensors in stack, IPS Interfaces → <Stackname-node id> → **Interface_Name**), or a CIDR host(s) within a network in your entered list. For example, if you had entered 192.168.3.0/24, you can enter 192.168.3.1/32 and 192.168.3.2/32 here for sub-interface creation.

NOTE

If you are creating another sub-interface from a CIDR address that has not been allocated, you can check to see which have already been allocated by clicking **List of Allocated CIDRs**.

6. Click **Save**.

   The new sub-interface appears in the **Sub-Interfaces** list table as well as under **IPS Interfaces** as a node under the interface node within which it was created.

7. Download the changes to your Sensor by clicking **Deploy Pending Changes**.

How to plan your IPS deployment

IPS deployment can be daunting and complex. Trellix IPS, while complex, provides great flexibility in deployment so you can start monitoring your network even while you familiarize yourself with its features and capabilities and tune your security policies.

Trellix IPS deployment can be simple or complex, depending on your needs and your skill with the product. If you are a **Beginner**, you can use Trellix IPS straight out of the box and get your entire deployment up and monitoring in an extremely short period of time. An **Intermediate** approach might be to customize your policies a bit and shift to another operating mode, such as Tap mode. An **Advanced** user might use all of the features available, tracking traffic at extremely granular levels, creating multiple administrative domains managed by a variety of users with various privileges, tailored policies and custom responses to detected attacks, and so on.

Deployment scenario for beginners

Trellix IPS includes a variety of pre-configured security policies targeting different environments. These policies enable you to start monitoring your network right away.

1. Install the Manager as described in [Trellix Intrusion Prevention System Installation Guide].
2. The **Default Prevention** policy is applied by default. You can leave this policy in place or pick the policy that best matches your needs. The Sensor you add will inherit this policy and pass it along to all interfaces of the Sensor.

   NOTE

   This policy enables blocking for certain attacks; immediately upon in-line deployment, Sensors will begin blocking these attacks when they are detected.

3. Configure the Sensor and add it to the Manager as described in [Trellix Intrusion Prevention System Sensor Reference Guide], and [Trellix Intrusion Prevention System Installation Guide].
4. On the Manager, check the Sensor's port configuration to be sure that it matches the way you have deployed the Sensor. Make changes as necessary.
5. Download and apply the latest Sensor software and signature file from the Update Server.
6. Send all configuration changes to the Sensor.
7. If you want, set up alert notification to email or pager by attack severity.
8. Using the information and features available in the Dashboard and Analysis pages, examine the resulting alerts for patterns to help you tune your policies.
9. Back up your data.

Deployment scenario for intermediate users

The pre-configured policies have an umbrella effect — you are protected from all the critical attacks defined in the policy. This enables you to get up and running quickly, but it also may protect you against attacks you do not care about. This would mean wasting the Sensor resources on things that are not relevant for your network. For example, if you have an entirely Solaris environment, you may not care if someone is initiating IIS attacks against the network, because these attacks are irrelevant to you. Some administrators prefer to see all network activity, including unsuccessful attacks, to get a complete picture of what is occurring on the network. Others want to reduce the "noise" generated by irrelevant attacks. Tuning your policies to delete attacks that do not apply to your environment reduces the amount of unimportant alerts generated by your Sensors.

To tune your deployment, you might do the following:

- Try a more advanced deployment mode. If you were running in SPAN mode, you may choose to try another deployment mode, such as tap mode.
- Take advantage of the Sensor's ability to apply multiple policies to multiple interfaces. Instead of applying a single policy to the entire Sensor, you may try applying different policies to dedicated interfaces of the Sensor. You can go a step further and segment your traffic into VLAN tags or CIDR blocks, create sub-interfaces, and apply policies to the Sensor's sub-interfaces.
- Tune your policies. Pick the policy that best matches your needs and clone the policy (or create a policy from scratch). Then remove any irrelevant attacks, add any additional attacks, and configure appropriate response actions to respond to detected attacks.
- Generate reports, view alerts, view the information presented in the Dashboard. Look at the data generated by the system to help you further tune your policies, and if necessary, implement more granular monitoring or delegation of monitoring activities to others.

Deployment scenario for advanced users

An advanced deployment of Trellix IPS utilizes more of its features to best tune your system. After you are more familiar with Trellix IPS, you might do the following:

- **Try running in in-line mode**. In-line mode enables you to drop malicious traffic and thus prevents attacks from ever reaching their targets.
- **Split your deployment into multiple Admin Domains**. You may want to organize your deployment by geographical location, business unit, or functional area (such as HR, Finance, etc).
- **Segment your network traffic into VLAN tags and CIDR blocks**. You can thus monitor various traffic with distinct policies using the sub-interfaces feature.
- **Create (or clone) policies on a sub-interface basis**. Create policies tuned for specific traffic flows within a network segment, and apply them on an extremely granular level.
- **Define user roles**. Delegate the day-to-day management of the IPS to specific individuals, providing each person with only enough access to the system to carry out his/her responsibilities.
- **Define DoS policies**. Configure DoS policies for specific hosts or a subset of your network.

Establish Sensor-to-Manager communication

The process of setting up a Sensor is described at a high level.

1. Set up the Manager software on the server machine.
   a. Install the Manager software on the server machine. For more information on this process, see [Trellix Intrusion Prevention System Installation Guide].
   b. Start the Manager software as described in [Trellix Intrusion Prevention System Installation Guide]. You can establish communication with a Sensor through the Manager server or from a browser on a client machine that can connect to the Manager server.

      Trellix recommends you connect to the Manager server through a browser session from a separate client machine to perform your configuration tasks.
   c. You can choose a specific policy to apply by default to the root admin domain (and thus all monitoring interfaces on the Sensor). By default, the pre-defined Default Prevention policy is applied to all of your Sensor ports upon Sensor addition.

      Whatever policy you've specified will apply until you make specific changes; the default policy gets you up and running quickly. Most users tune their policies over time, in conjunction with VIPS, to best suit their environments and reduce the number of irrelevant alerts.
2. Use the **Sensors** tab in **Device Manager** page of the Manager and add the Sensor to required domain.
   a. On the **Devices** tab of the Manager, select the domain where you want to add the Sensor and go to Global → **Device Manager**. The **Device Manager** page is displayed. Select the **Sensors** tab and click +.
   b. Specify the required information in the **Add Device - Step 1 of 2** window.
      - Enter the Name of device. This must be the same name (case-sensitive) that you assigned to the Sensor through Sensor CLI.
      - Enter and confirm the **Shared Secret**. You must enter the same shared secret (case-sensitive) in the Sensor CLI when you establish Sensor-to-Manager communication.
      - Select **IPS Sensor** or **NTBA Appliance** as the Device Type.
      - Specify the deployment mode as either **Direct** or **Indirect**.
      - If required, provide the information for the optional fields.
      - Click **Save**.
3. Configure the Sensor.
   - From a serial console connected physically or logically to the Sensor, configure the Sensor with network identification information (that is, IP address, IP address of the Manager server, and so on), and configure it with the same case-sensitive name and shared secret key value you provided in the Manager.

     For more information on configuring the Sensor using the Sensor CLI, see [CLI commands] section.
4. Verify communication between the Sensor and the Manager.
   - Verify the health of the Sensor on the Sensor CLI and that the Sensor has established communication with the Manager. Use the **`status`** command.
   - Verify in the Manager interface that the Sensor's name is listed. On the **Devices** tab of the Manager, select the corresponding domain and check if the Sensor is listed in the **Device** drop-down.
5. Troubleshoot any problems you run into.
   - If you run into any problems, check your configuration settings and ensure that they are correct. For more troubleshooting tips, see [Troubleshooting] section.

6. Verify the operating mode of the ports on your Sensor.
    - Your Sensor ports are configured by default for monitoring in in-line mode; that is, connected via a port pair on the Sensor to a segment of your network. If you've set up the Sensor to monitor in in-line mode, check your settings to make sure everything is correct.

Configure your deployment using the Manager

After you are up and running and reviewing the data generated by the system, you can further configure and maintain your system. For example, you can do the following:

- **Apply IPS policies to each interface of your multi-port Sensor (instead of applying one policy to all interfaces, as when you chose the default policy to establish Sensor-to-Manager communication)** — You can ensure that all of your interfaces use IPS policies specifically for the areas of your network they are monitoring. For example, you can apply a **Web Server** policy to one interface, **Mail Server** policy to another, **Internal Segment** policy to another, and so on. More information on the provided policies is available in the subsequent sections.
- **Configure responses to alerts** — Developing a system of actions, alerts, and logs based on impact severity is recommended for effective network security. For example, you can configure Trellix IPS to send a page or an email notification, execute a script, disconnect a TCP connection, send an **ICMP Host Not Reachable** message to the attack source for ICMP transmissions, or send address-blocking for a host.
- **Filter alerts** — An ignore rule limits the number of alerts generated by the system by excluding certain source and Destination IP address parameters. If these address parameters are detected in a packet, the packet is not analyzed further (and is automatically forwarded when in Inline mode).
- **View the system's health** — The **Faults** tab in the **Logs** page details the functional status for all of your installed Trellix IPS system components. Messages are generated to detail system faults experienced by your Manager, Sensors, or database. For more information, see the [Troubleshooting] section.
- **View a port's performance** — The **Traffic Statistics** action enables you to view performance data for a port on a Sensor. You can view the statistics of the total number of packets received (Rx) and transmitted (Tx) for a given device per port. You can also view the reason and the packet drop rate on a port for a device. The data collected is a reflection of the traffic that has passed through the port.
- **View datapath statistics for ports** — Datapath statistics include data on the traffic such as number of frames, bytes, and count of the traffic that are received and sent by the Sensor ports. It also contains the count of error packets for TCP, IP, and UDP traffic. These statistics can be viewed by using the **`datapath intfport`** command. For more information, see the [CLI commands] section.
- Back up all or part of your Manager configuration information to your server or other location. Trellix IPS provides the following backup options:
    - **All Tables** — All Trellix IPS data (configuration, audit, and alert)
    - **Config Tables** — All information related to system configuration, such as port configuration, users, admin domains, policies for all Trellix IPS resources in all domains
    - **Audit Tables** — All information related to user activity and alerts
    - **Event Tables** — All information related to alerts, packet log host and Sensor performance
    - **Trend Tables** — All information related to trend patterns of alerts and Sensor performance events

> **NOTE**
>
> The **All Tables** and **Audit Tables** options can be rather large in size, depending upon the amount of alert data in your database. Trellix recommends saving these types of backups to an alternate location.

For more information on how to back up your data, see the [Manager Administration] section.

View and work with data generated by Trellix IPS

Once you have completed the steps in the previous sections, you are up and running. While actively monitoring network traffic, your Sensor will generate *alerts* and other data for traffic that is in violation of the set security policy.

The Manager processes all the information that it receives from the Sensors and presents them in a form that is readily understandable to you. The **Dashboard** displays the information in a graphical format, whereas the **Analysis** tab displays the information in a tabular format.

- The Attack Log enables you to drill down to the details of an alert, such as what triggered the alert, when it was triggered, which Sensor detected it, the source IP address of the attack that triggered the alert, the destination IP address of the attack, and so on. You can access the **Attack Log** from the **Analysis** tab. You use the Attack Log to perform forensic analysis on the alert to help you tune the Trellix IPS system, provide better responses to attacks, and otherwise shore up your defenses. You can view the Attack Log for specific admin domains.
- The **Event Reporting** page provides you detailed reports based on your alerts, and reports on your Trellix IPS configuration. You can use these reports to communicate incidents to other members of your team and to your management.

> **NOTE**
>
> For more information on these tools, see [Reporting] section.

Tune your deployment

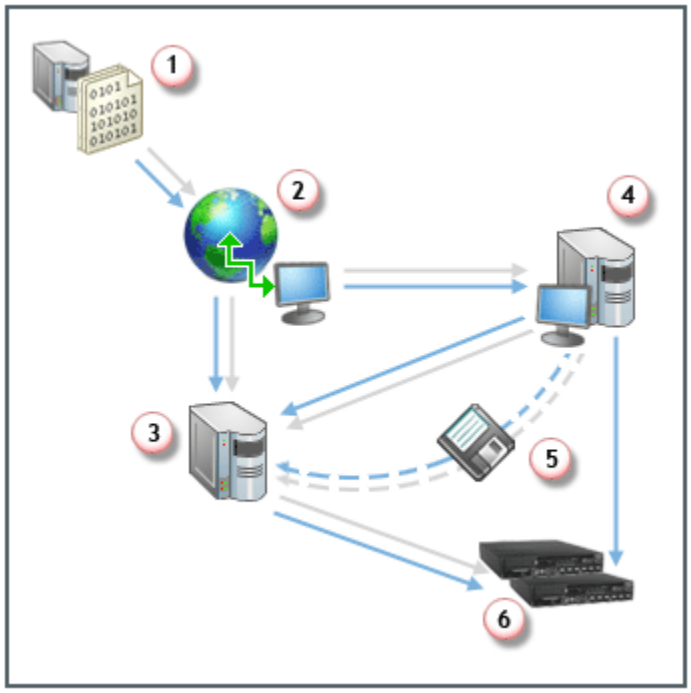
Once you become familiar with the basics of the Manager program, you can further enhance your deployment by utilizing some of the more advanced features. These features include:

- **Cloning and modifying the Trellix IPS-provided policy**. This information is provided in the subsequent sections.
- **Deploying your Sensor to monitor traffic in Tap mode or, ultimately, in Inline mode**.
- **Adding users and assigning management roles**. For more information, see the chapter [Users and Roles] in [Trellix Intrusion Prevention System Product Guide.]
- **Adding admin domains for resource management**. For more information, see the topic [Configuration of administrative domains] in [Trellix Intrusion Prevention System Product Guide.]
- **Changing your interface type to CIDR or VLAN depending on your network configuration**.
- **Using other features such as Firewall to block traffic or pass traffic without sending it through the IPS engine**.

Update your signatures and software

An essential element to a reliable IPS is updating the system signature and software images. Trellix periodically releases new Manager software and Sensor signature and software images, and makes these updates available via the Trellix IPS Update Server to registered support customers.

Figure 257. Update signatures and software



Field	Description
1	Update Server
2	Internet
3	Manager Server
4	PC/TFTP server
5	Import/disk
6	Sensor

NOTE

Manager software installation includes a default signature set image.

There are several options for loading updates to your Manager and Sensors.

1. **Download images from the Trellix IPS Update Server (Update Server) to your Manager.**

You can use the Manager interface to download Sensor software and signature updates from the Update Server to the Manager server, and then download the Sensor image to the Sensor. For more information, see the [Manager Administration] section.

2. **Import image files from a remote workstation to your Manager.**

   If your Manager server is not connected to the Internet, you can download the updates from the Update Server to any host, then do one of the following:

   - Download the image to a remote host, then log in to the Manager via browser session on the remote host and import the image to the Manager server. You can then download the Sensor image to the Sensor. For more information, see the [Manager Administration] section.
   - Similar to above, download the image from the Update Server to any host, put it on a disk, take the disk to the Manager server, and then import the image and download it to the Sensor.

3. **Download Sensor software from the Update Server to a TFTP client then to a Sensor.**

   You can download the software image from the Update Server onto a TFTP server, and then download the image directly to the Sensor using commands on the Sensor CLI. This is useful if you prefer not to update Sensor software via the Manager, or you may encounter a situation wherein you cannot do so. For more information on this method, see the [Manager Administration] section.

Configuring the monitoring and response ports of a Sensor

Configuration of device monitoring and response ports

The **Monitoring Ports** action enables you to view/edit the parameters of the monitoring and response ports on a specific device. Monitoring port configuration allows you to change device deployment modes, select port speeds or indicate whether you are using Trellix certified modules, enable/disable ports, and choose the path for device responses. Response port configuration allows you to choose the receiving device and change the link speed. Port Settings are configured using the virtual device action buttons available within every device settings page in the Manager UI.

The following table contains the default values for device ports in different operating modes. You must ensure that the switch or router ports connected to the device ports match these settings for the configurations as shown below:

Interface Type	Mode	Auto-negotiation	Speed	Duplex
100 Gigabit Ethernet	Tap	OFF	N/A	N/A
100 Gigabit Ethernet	SPAN	OFF	N/A	N/A
100 Gigabit Ethernet	In-line	OFF	N/A	N/A
40 Gigabit Ethernet	Tap	OFF	N/A	N/A
40 Gigabit Ethernet	SPAN	OFF	N/A	N/A
40 Gigabit Ethernet	In-line	OFF	N/A	N/A
10 Gigabit Ethernet	Tap	OFF	N/A	N/A
10 Gigabit Ethernet	SPAN	OFF	N/A	N/A
10 Gigabit Ethernet	In-line	OFF	N/A	N/A
Gigabit Ethernet	Tap	OFF	N/A	N/A

Interface Type	Mode	Auto-negotiation	Speed	Duplex
Gigabit Ethernet	SPAN	ON	N/A	N/A
Gigabit Ethernet	In-line	ON	N/A	N/A

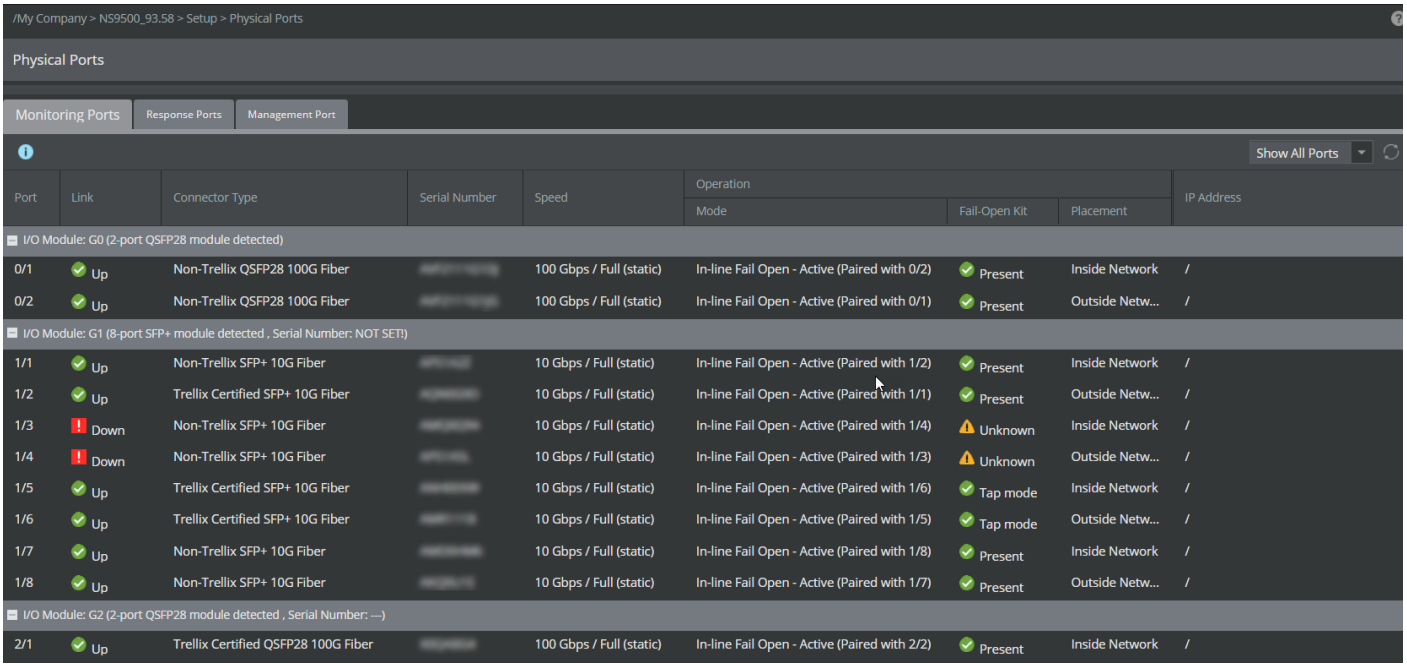
Ports for NS-series devices

You can view or configure the settings of the monitoring ports for Trellix IPS NS-series devices on the configuration page. To access the configuration page for a standalone Sensor, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Physical Ports**.

To access the configuration page for Sensors in a stack, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Setup → **Physical Ports**.

A page is displayed with the list of ports available for the device you selected. Following is a port description for the Sensors. To view the list of ports supported by each Sensor model, refer to *NS-series Sensor* (page 564).

Figure 258. Ports for NS9500



Monitoring port details

The following are the details of the monitoring ports displayed on the **Monitoring Ports** tab.

Table 21. Monitoring port details

Column	Description
Port	Specifies the monitoring port

Column	Description
Link	Specifies the status of the monitoring port. The available statuses are: • **Up** • **Down** • **Disabled**
Connector Type	Displays the connector type
Serial Number	Displays the serial number
Speed	Specifies the speed of the port. The following are the available speed: • **Auto-negotiate** • **1 Gbps(full)** • **100 Mbps(full)** • **100 Mbps(half)** • **10 Mbps(full)** • **10 Mbps(half)** • **10 Gbps(full)** • **40 Gbps(full)** • **100 Gbps(full)**
Operation	
Mode	Specifies the mode of operation. The following are the available modes: • **Inline Fail Open - Active** • **Inline Fail Open - Passive** • **Inline Fail Closed** • **SPAN or Hub** • **Tap**
Fail-Open Kit	Displays the status of the fail open kit. The following are the available status: • **Present** • **Built in** • **Unknown** • **n/a**
Placement	Displays the area of the network where the port is connected. The options are: • **Inside Network** • **Outside Network**

Column	Description
Response Port	Specifies the path of response for the device. The available options are: • **This port** • **R1** • **R2**

Display options for Monitoring ports

Display options for Serial Number

The following Serial Numbers are displayed on **Monitoring Ports** tab:

- **Transceiver Serial Number** - Displays the Transceiver Serial Number in the **Serial Number** column
- **I/O Module Serial Number** - Displays the network module serial number in a grid view
- **Last Seen Serial Number** - Displays the **Last Seen** Serial Number as , when the Manager fails to read active Serial Number or if the Transceiver/Network module is removed.

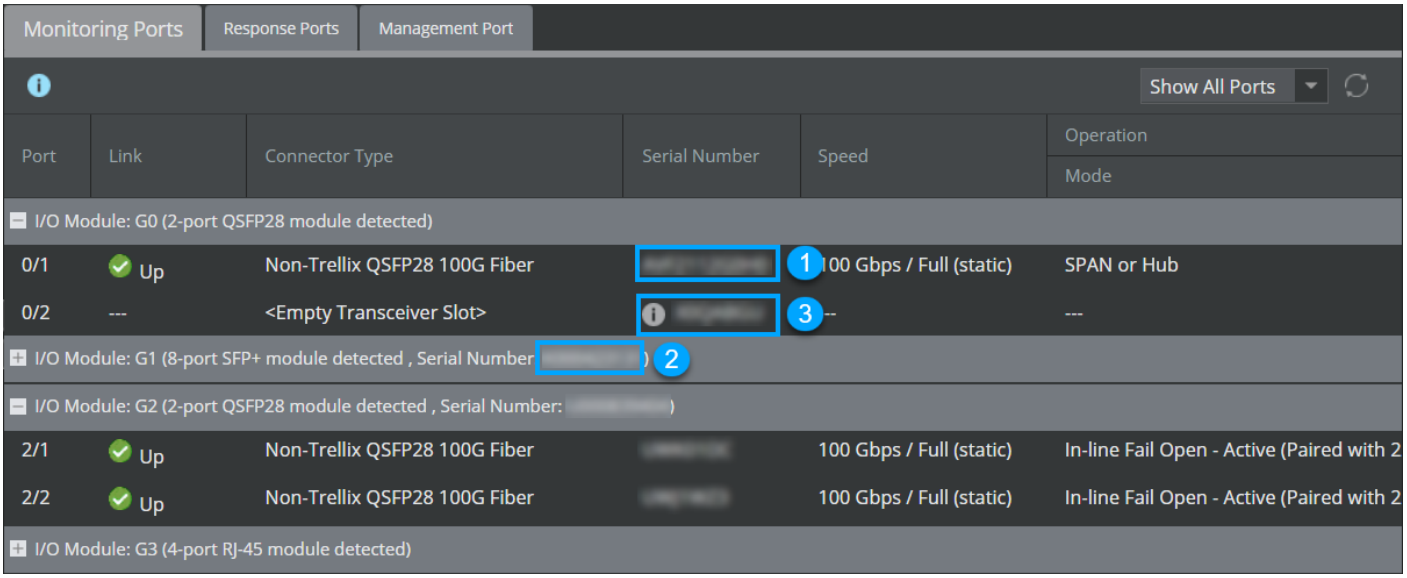
NOTE

If users see any anomaly in the displayed Transceiver Serial Number, it is recommended that they make the link up and then check the Serial Number again. By doing so, the last seen Serial Number is also updated properly.

NOTE

Whenever a Transceiver is replaced, the port gets disabled and user has to enable the port irrespective of the operating mode.

Figure 259. Display options for Serial Number



Callout	Description
1	Displays the Transceiver Serial Number
2	Displays the I/O Module Serial Number
3	Displays the **Last Seen** Serial Number

NOTE

For RJ-45 module, the Serial Number is displayed as **Not Applicable**.

You have the following options to view the details of the list of monitoring ports:

- **Show All Ports** - Displays the list of all monitoring ports
- **Hide Empty Slots** - Hides ports that have empty slots and displays only those ports that are configured

Enable or disable a monitoring port

This section explains about enabling and disabling a monitoring port from the **Monitoring Ports** tab.

To view or configure the settings of the monitoring ports for Trellix IPS, you access the configuration page in Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**. A list of ports available for the device you selected are displayed on the **Monitoring Ports** tab of a new page.

To disable a monitoring port:

1. Click on the row of the monitoring port that you wish to disable.

   NOTE

   - To disable multiple monitoring ports, press the **Ctrl** key and click on multiple monitoring ports that you wish to disable.
   - Since monitoring ports are internally wired, when you disable one of the ports in a pair, the corresponding port is also disabled.

2. Click on the **Disable** button. The monitoring port(s) are disabled.

To enable a monitoring port:

1. Click on the row of the monitoring port that you wish to enable.

   NOTE

   To enable multiple monitoring ports, press the **Ctrl** key and click on multiple monitoring ports that you wish to enable.

2. Click on the **Enable** button. The monitoring port(s) are enabled.

NOTE

The configurations made to the monitoring port will not be pushed to the Sensor automatically when the port is in **Disable** state. Trellix recommends you to perform **Deploy Pending Changes** immediately after changing the port status.

Port color key

This section describes a port's status color under the **Link** column in the **Monitoring Ports** tab.

Table 22. Port color key

Color	Description
Green	Port is enabled and operating correctly.
Red	Port is enabled, but not operating due to some failure. Check system faults.
Gray	Port has been disabled by the user.
Orange	Device or NTBA Appliance is disconnected. The port data is retrieved from the database.
Beige	Port has been modified.

Hardware for monitoring ports

Before you configure the monitoring and response ports of a physical Sensor, make sure you have correctly cabled the ports as per your network design and requirements. Based on the Sensor model and the port that you plan to use, you might be required to connect some hardware to the monitoring ports. This section introduces the various hardware that might be required to configure monitoring ports.

- Transceivers — Based on the Sensor model, monitoring ports use different types of transceivers to connect to peer devices. The transceiver types that are supported are as follows:
  - Small Form-factor Pluggable (SFP) (fiber or copper)
  - SFP+
  - QSFP+
  - QSFP28

NOTE

NS9500 Sensors support SFP (fiber or copper) 1 Gbps, SFP+ (fiber) 10 Gbps, QSFP+ (fiber) 40Gbps, and QSFP28 (fiber) 100Gbps transceiver modules.

NOTE

NS9x00 Sensors support SFP (fiber or copper) 1 Gbps, SFP+ (fiber) 10 Gbps, and QSFP+ (fiber) 40Gbps transceiver modules.

NOTE

NS7600 and NS3600 Sensors support SFP+ (SM and MM), SFP Fiber (SM and MM), and SFP Copper transceiver modules.

NOTE

NS7500, NS7x50, and NS7x00 Sensors support only SFP (fiber or copper) 1 Gbps and SFP+ (fiber) 10 Gbps transceiver modules.

NOTE

NS5x00 Sensors support only SFP (fiber or copper) 1 Gbps transceiver modules.

NOTE

NS3x00 Sensors do not need transceiver modules.

Refer to the corresponding Sensor product guide to know the transceivers type used by the monitoring ports and how to cable them.

- Fail-open kits — Fiber monitoring ports are fail-closed by default. Thus, if these ports are deployed in-line, a Sensor hardware failure, for example, results in network downtime. Fail-open operation for fiber ports requires the use of the an external bypass switch. Fail-open bypass kits minimize the potential risks of in-line Sensor failure on critical network links. There are two types of fail-open kits available - active and passive. To know the difference between the two and the active and passive fail-open kits available, see the section [Using active fail-open kit] in [Trellix Intrusion Prevention System Product Guide]. For information on how to deploy a particular fail-open kit, refer to the corresponding guide. For example, for information on how to deploy gigabit optical Active fail-open switch, see the [Trellix Intrusion Prevention System Fail-Open Kit Product Guide.]
- External tap device, if you plan to deploy monitoring ports in the tap mode. Refer to Deployment of Sensors in tap mode (page 585).

Configuration of monitoring ports

Configuration of monitoring ports enables you to set the operating mode of your ports, change port speeds or specify whether you are using Trellix certified modules, and/or choose the corresponding response port for device action.

NOTE

For information on properly connecting your device for the various operating modes, see the appropriate [Trellix IPS <Sensor > Product Guide].

Configuration of ports for NS-series devices

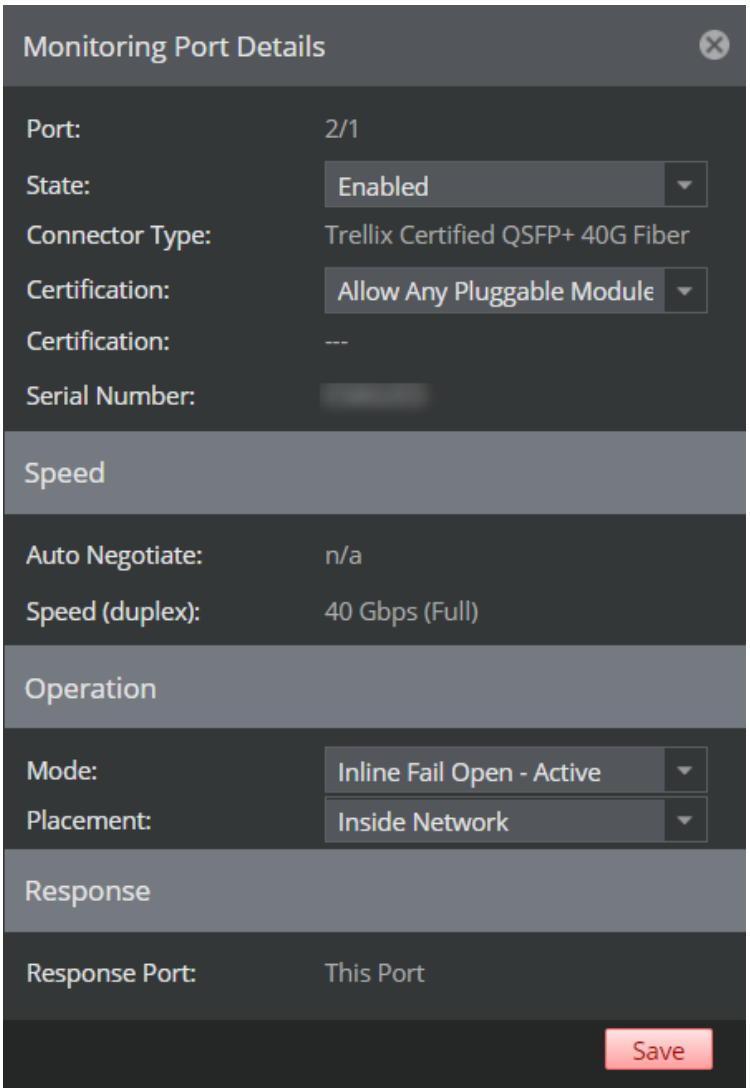
To view or configure the settings of the monitoring ports for Trellix IPS NS-series devices. To access the configuration page, go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.

Configure 40 Gbps (QSFP+) monitoring ports

Configuration of monitoring ports enables you to set the operating mode of your ports, change port speeds or specify whether you are using Trellix certified modules, and/or choose the corresponding response port for device action.

1. Go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Double-click on the row of numbered 40 Gbps (QSFP+) monitoring port. The **Monitoring Port Details** window is displayed.

Figure 260. Configure Monitoring Port window



NOTE

The speed is automatically set to **40 Gbps** on the 40 Gigabit Ethernet ports. However, you can specify whether the modules are Trellix Certified.

3. Select the **State** as either **Enabled** (on) or **Disabled** (off). The **Link** displays **Up** (on) or **Down** (off) accordingly.

NOTE

If your **Link** displays as **Down** and your **State** is **Enabled**, there may be a problem. Check the system faults in the **Faults** tab in **Logs** page for more information.

4. Select a **Mode** from the following:

CAUTION

Your device connections must match the selected operating mode for correct system functionality. Improper deployment may result in system faults, including missed attacks and system failure.

- **Inline Fail Open – Active**
- **Inline Fail Closed**

NOTE

Inline fail-open and Inline fail-closed are determined by how the port cables are connected. Fail-open operation for GE ports requires use of the optional Bypass Switch provided in the Gigabit Optical Fail-Open Bypass Kit (sold separately). You should *not* select the **Inline Fail Open** option if the optional external Bypass Switch is not present.

- **SPAN or Hub**
- **Tap**

  GE ports can only be configured for External Tap mode.

NOTE

The **Inline Fail Open – Passive** mode is not supported with the NS9x00-series Sensors. Since the QSFP+ transceivers are supported only with the NS9x00-series Sensors, the **Inline Fail Open – Passive** mode is not supported as well.

If a port is functioning as part of a *Port Pair*, the *Peer Port* is listed. For example, if port G2/1 is configured for Tap mode, port G2/2 is listed as the Peer Port. All ports are wire-matched internally with a single peer. For example, G2/1-G2/2 make up a port pair.

5. Select **Placement** of your network where the current port is connected: **Inside Network** or **Outside Network**. This step applies to **Tap** or **Inline** modes only.
6. Wherever applicable, select a **Response Port**. The following choices are available:
   - **This Port**: Respond out of the detection port to the segment. This is selected by default for Inline and SPAN operating modes.
   - **R1**: Sends responses through a R1 port
   - **R2**: Sends responses through a R2 port

TIP

You can assign a response port to more than one device monitoring port. However, knowing where your response ports are connected in the network will make for the best response system.

7. Click **Save** to save changes.

   A confirmation page is displayed. A window is displayed to confirm the changes. Click **OK** to confirm changes.

Configure 10 Gbps (SFP+) Monitoring Ports

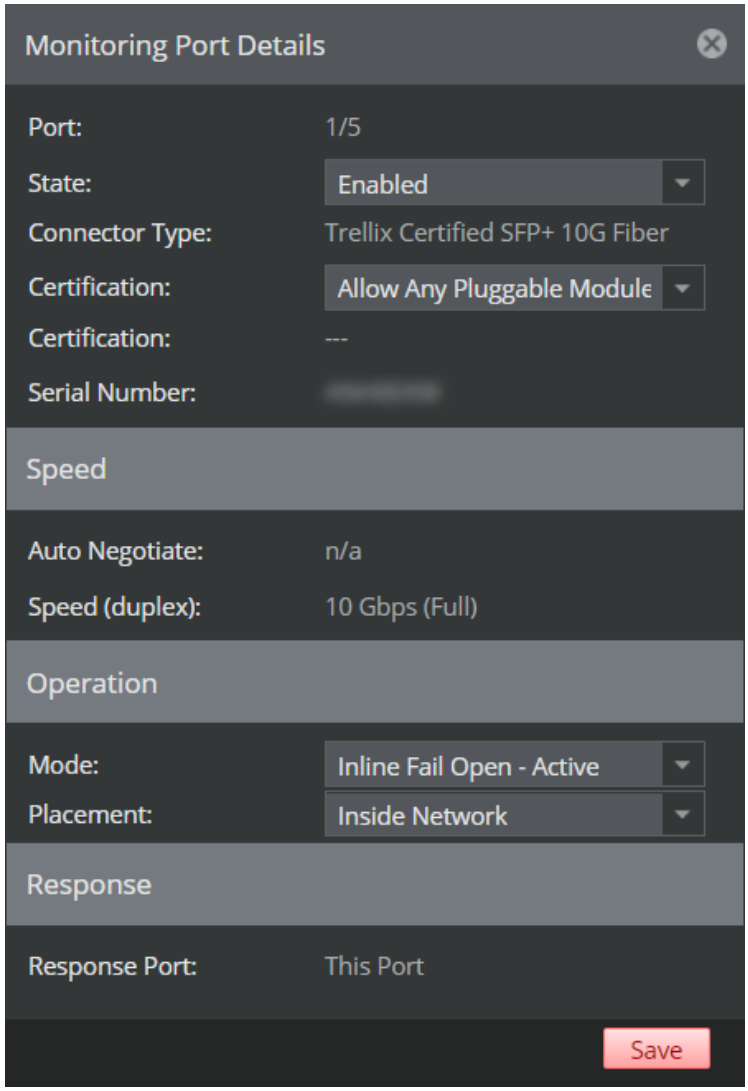
You can view or configure settings for the 10 Gbps monitoring ports.

1. Go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Double-click on the row of numbered 10 Gbps (SFP+) monitoring port. The **Monitoring Port Details** window is displayed.

NOTE

The speed is automatically set to **10 Gbps** on the 10 Gigabit Ethernet ports. However, you can specify whether the modules are Trellix certified.

Figure 261. Monitoring port window



3. Select the **State** as either **Enabled** (on) or **Disabled** (off). The **Link** displays **Up** (on) or **Down** (off) accordingly.

> **NOTE**
>
> If your **Link** displays as **Down** and your **State** is **Enabled**, there may be a problem. Check the system faults on the **Faults** tab in **Logs** page for more information.

4. Select a **Mode** from the following:

> **CAUTION**
>
> Your device connections must match the selected operating mode for correct system functionality. Improper deployment may result in system faults, including missed attacks and system failure.

- **Inline Fail Open – Active**
- **Inline Fail Closed**

> **NOTE**
>
> Inline fail-open and Inline fail-closed are determined by how the port cables are connected. Fail-open operation for GE ports requires use of the optional Bypass Switch provided in the Gigabit Optical Fail-Open Bypass Kit (sold separately). You should *not* select the **Inline Fail Open** option if the optional external Bypass Switch is not present.

- **SPAN or Hub**
- **Tap**

  GE ports can only be configured for External Tap mode.

> **NOTE**
>
> The SFP+ transceivers do not support **Inline Fail Open – Passive** mode.

If a port is functioning as part of a *Port Pair*, the *Peer Port* is listed. For example, if port G2/1 is configured for Tap mode, port G2/2 is listed as the Peer Port. All ports are wire-matched internally with a single peer. For example, G2/1-G2/2 make up a port pair.

5. Select **Placement** of your network where the current port is connected: **Inside Network** or **Outside Network**. This step applies to **Tap** or **Inline** modes only.
6. Wherever applicable, select a **Response Port**.The following choices are available:
   - **This Port**: Respond out of the detection port to the segment. This is selected by default for Inline and SPAN operating modes.
   - **R1**: Sends responses through a R1 port
   - **R2**: Sends responses through a R2 port

> **TIP**
>
> You can assign a response port to more than one device monitoring port. However, knowing where your response ports are connected in the network will make for the best response system.

7. Click **Save** to save changes.

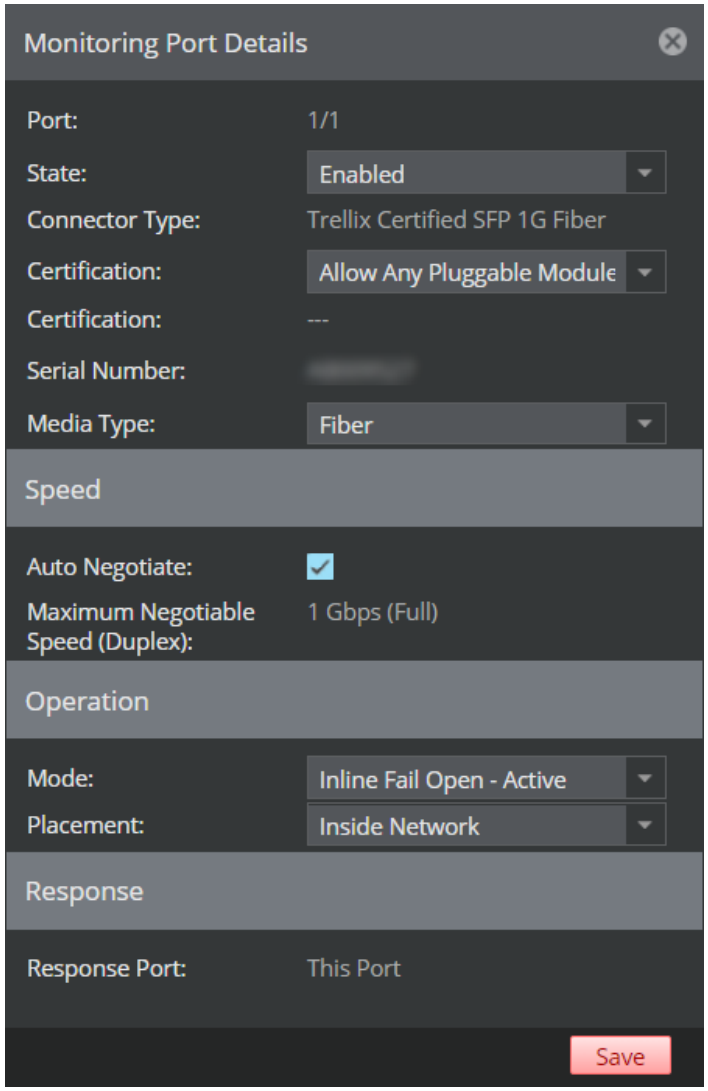
   A confirmation page is displayed. A window is displayed to confirm the changes. Click **OK** to confirm changes.

Configure 1 Gbps (SFP) Monitoring Ports

You can view or configure settings for the 1 Gbps monitoring ports.

1. Go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Double-click on the row of numbered 1 Gbps (SFP) port. The **Monitoring Port Details** window is displayed.

Figure 262. View Monitoring Port window



3. Select the **Auto Negotiate** checkbox if the speed of the port has to match with the rest of the network.
4. Select the **Speed(Duplex)** of the port. Port speed details the speed of traffic being monitored. You can set the port speed to from the following values on the drop down list:
   - **1 Gbps(full)**
   - **100 Mbps(full)**
   - **100 Mbps(Half)**
   - **10 Mbps(full)**
   - **10 Mbps(Half)**
5. Select the **State** as either **Enabled** (on) or **Disabled** (off). The **Link** displays **Up** (on) or **Down** (off) accordingly.

NOTE

If your **Link** displays as **Down** and your **State** is **Enabled**, there may be a problem. Check the system faults on the **Faults** tab in **Logs** page for more information.

6. Select a **Mode** from the following:

CAUTION

Your device connections must match the selected operating mode for correct system functionality. Improper deployment may result in system faults, including missed attacks and system failure.

- **Inline Fail Open – Active**
- **Inline Fail Open – Passive**
- **Inline Fail Closed**

NOTE

Inline fail-open and Inline fail-closed are determined by how the port cables are connected. Fail-open operation for GE ports requires use of the optional Bypass Switch provided in the Gigabit Optical Fail-Open Bypass Kit (sold separately). You should *not* select the **Inline Fail Open** option if the optional external Bypass Switch is not present.

- **SPAN or Hub**
- **Tap**

  GE ports can only be configured for External Tap mode.

If a port is functioning as part of a *Port Pair*, the *Peer Port* is listed. For example, if port G2/1 is configured for Tap mode, port G2/2 is listed as the Peer Port. All ports are wire-matched internally with a single peer. For example, G2/1-G2/2 make up a port pair.

7. Select **Placement** of your network where the current port is connected: **Inside Network** or **Outside Network**. This step applies to **Tap** or **Inline** modes only.
8. Wherever applicable, select a **Response Port**.The following choices are available:
   - **This Port**: Respond out of the detection port to the segment. This is selected by default for Inline and SPAN operating modes.
   - **R1**: Sends responses through a R1 port
   - **R2**: Sends responses through a R2 port

TIP

You can assign a response port to more than one device monitoring port. However, knowing where your response ports are connected in the network will make for the best response system.

9. Click **Save** to save changes.

A confirmation page is displayed. A window is displayed to confirm the changes. Click **OK** to confirm changes.

Configuration of gigabit ethernet inline fail open - passive status

When deploying your Gigabit Ethernet ports in **Inline Fail Open - Passive mode**, you must verify RJ-11 to RJ-45 control cable connection is in place between X1(RJ-11)NS7500 and PFO(RJ-45) control ports.

NOTE

Fail-open operation for GE ports requires use of the optional Bypass Switch provided in the Gigabit Fail-Open Bypass Kits (sold separately).

TIP

For more information on steps on how to properly connect your Sensor for GE Inline Fail-Open functionality, see [Trellix Intrusion Prevention System Installation Guide].

The port status and operating mode status for Manager fail-open passive for NS-series Sensors are as follows::

Inline Fail Open - Passive port status	Operating Mode Status on PFO
Present	The inline fail open - passive kit is in inline fail-open mode.
Bypassing	The inline fail open - passive kit is in bypass mode. The bypass switch has been activated. The sensor does not monitor traffic during this time. For example, when sensor ports are administratively disabled.
Unknown	Unable to get the status of the inline fail-open passive kit. For example, when the control cable is unplugged.
N/A	Not Applicable; the operating mode is not in inline fail open - passive mode.

Change a monitoring port from SPAN mode to TAP or Inline mode (and vice versa)

You must disable both ports required for port pair operation when changing the operating Mode from single port (SPAN or Hub) Mode to a port pair (Tap or Inline) mode. Device monitoring ports are configured by default to operate in SPAN or Hub mode.

1. Go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Double-click on the row of the port to be configured. The **Monitoring Port Details** panel is displayed on the right side.
3. Select **Disabled** from the **State** drop-down list.
4. Click **Save**.
5. Select the peer port (for example, G0/2).
6. Select **Disabled** at the **State** drop-down list.
7. Select **Tap** or **Inline Fail Open** mode as the **Mode**.

> **NOTE**
>
> To configure from port pair mode to single port mode, select **SPAN or Hub** as the **Mode**.

8. Click **Enabled** at **State**.
9. Configure your port settings (port speed or Trellix certification, duplex, response port usage).
10. Click **Save**.
11. Select port G0/1 to verify the **State** reads **Enabled** and the **Mode** matches your new setting.
12. Click **Save**.

Change a monitoring interface from external tap to inline (and vice versa)

You can change your monitoring configuration from External Tap mode to Inline mode, or you can change from Inline Mode back to External Tap mode.

> **NOTE**
>
> Changing from one port pair mode to another port pair mode does not require disabling of ports.

1. Disconnect the segments from the external tap and connect the segments appropriately to your device port pair.

> **NOTE**
>
> If going from an Inline mode to External Tap mode, disconnect the segments from the device and connect the segments appropriately to the external tap and device ports.

2. Go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
3. Double-click on the row of the monitoring port to be configured, example, G0/1. The **Monitoring Port Details** panel is displayed on the right side.
4. Select an **Inline Fail Open** mode as the **Mode**.

> **NOTE**
>
> Select **Tap** as the **Mode** if going from Inline to External Tap mode.

5. Configure port settings (port speed or Trellix certification, duplex, response port setting—you will need to select a response port if changing from Inline Mode to Tap Mode).
6. Click **Save**.

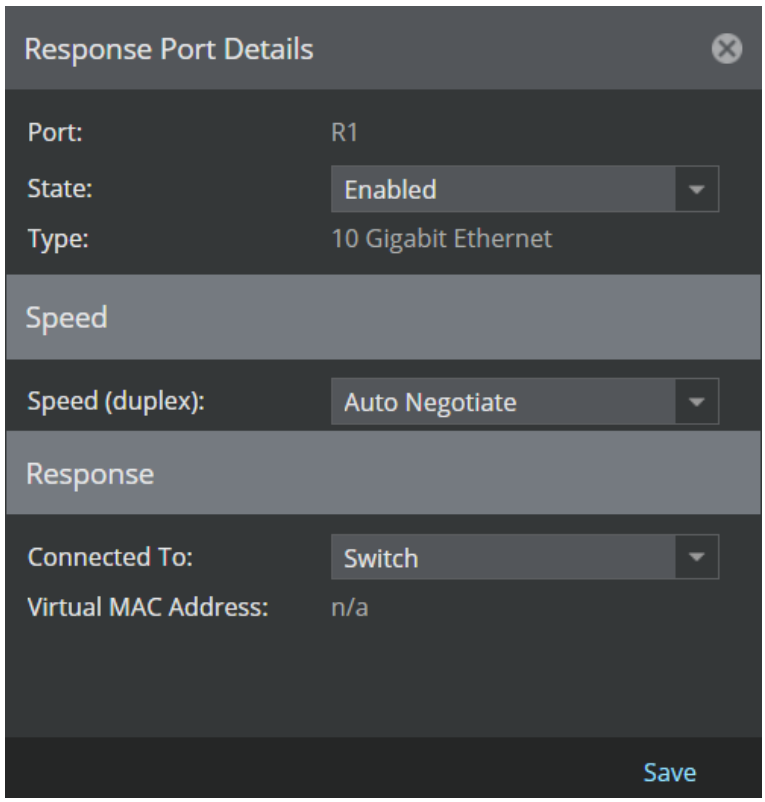
Configure response ports

Utilizing device response ports enables your device to send preset responses (enabled in policy configuration), such as a TCP reset, as well as post-detection responses, such as firewall blocking of traffic, upon detection of malicious traffic. The device

response ports are most commonly used with an external tap operating configuration. The other operating modes allow responses to be injected back through the interface ports. Since responses cannot be injected into a segment through an external tap, response port configuration is necessary.

1. Go to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Click on the **Response Ports** tab.
3. Double-click on the row of the response port to be configured. The **Response Port Details** window is displayed.

Figure 263. Configure Response Port window



4. Select a **Speed (Duplex)**. The following are the supported options for NS-series Sensor models.
   - NS-series:
     - **Auto-Negotiate**
     - **1 Gbps**
     - **10 Gbps**
5. Select the **State** as either **Enabled** (On) or **Disabled** (Off). For example, you need to disable the port if you connect a new wire, then enable it after re-connection.
6. Select the network component the response port connects to (**Connected To**): either a **Switch** or a **Router**.
   - If you select **Router**, in the **Virtual MAC Address** type the MAC address of the router to which you are connecting. The MAC address **cannot** be the broadcast address "ff:ff:ff:ff:ff:ff."
7. Click **Save** to save your port changes.

View management port settings

You can view the details of the management port settings.

1. Navigate to Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Click on the **Management Port** tab. The following information is displayed.

Settings	Description
IPv4	
IP Address	Displays the IPv4 IP address
Network Mask	Displays the Network mask for IPv4
Default Gateway	Displays the Default Gateway for IPv4
IPv6	
IP Address	Displays the IPv6 IP address
Network Mask	Displays the Network mask for IPv6
Default Gateway	Displays the Default Gateway for IPv6
Physical	
Speed(duplex)	Specifies the speed and duplex of the management port

NOTE

You will not be able to modify any settings in this page. The settings can be modified only from the device CLI.

Deployment of Sensors in inline mode

Inline monitoring mode provides prevention of attacks by enabling Security Administrators to select the types of attacks/traffic to drop, thus preventing the negative end-system impact common with today's network attacks. Inline mode is achieved when the Sensor is placed directly in the path of a network segment, becoming, essentially, a "bump in the wire," with packets flowing through Sensor. In this mode, the Sensor inspects all traffic at wire-speed and can prevent network attacks by dropping malicious traffic in real time—the Sensor actually ends the attacking transmission before it can reach and impact the target. Preventative actions can operate at a highly granular level, including the automated dropping of DoS traffic intended for a specific host.

When operating in inline mode, network segments are connected to two wire-matched Sensor ports (For example, peer ports G0/1 and G0/2), and packets are examined in real time as they pass through the Sensor. In this mode, a packet comes in through the first interface of the pair of the Sensor and out the second interface of the pair. The packet is sent to the second interface of the pair unless that packet is being denied or modified by a signature.

The Sensor ports are configured by default for monitoring in inline mode; that is, connected inline on a network segment (For example, between a switch and a router or two switches).

NOTE

This change will not override user-configured settings.

Benefits of running inline mode

The benefits to using Sensors in inline mode are:

- **Protection/Prevention** — Prevention is a feature unique to inline mode. When running inline, a Sensor can drop malicious packets and not pass them through the network. This acts sort of like an "adaptive firewall," with your detection policy dictating what is dropped. Furthermore, when dropping packets, Trellix IPS is very precise and granular. The Sensor can drop only those packets it identifies as malicious or all of the packets related to that flow (a choice that is user configurable).
- **Packet "scrubbing"** — In addition to dropping malicious traffic, Trellix IPS can *scrub*—or normalize—traffic to take out any ambiguities in protocols that the attacker may be using to try to evade detection. Current IDS products are susceptible to these techniques, and an example of this attempt is IP fragment and TCP segment overlaps. The Sensor can reassemble the IP fragments and TCP segments and enforce a reassembly mode of the user's choice to accept either the old or the new data.
- **Processing at wire-speed** — Sensors are able to process packets at wire rates.

  In inline mode, the Sensor logically acts as a transparent repeater with minimal latency for packet processing. Unlike bridges, routers, or switches, the Sensor does not need to learn MAC addresses or keep an ARP cache or a routing table.
- **Traffic prioritization** – When you deploy a port in inline mode and enable the inline traffic prioritization feature, the Sensor prioritizes packets emerging from the port in inline mode, during heavy network load conditions, over packets emerging from a port in SPAN mode.

  The Sensor periodically checks for latency in inline packets. If latency is higher than a stipulated limit and, at the same time, there are several inline packets and SPAN packets in queue to be analyzed by the Sensor, some of the SPAN packets are dropped to prioritize inline packets.

  When traffic density returns to normal operating levels, the Sensor stops prioritizing inline packets and traffic is analyzed in the order that it arrives.

  NOTE

  Prioritization of inline traffic is disabled by default. You can view or change its status only through the Sensor CLI **Debug** mode using the following commands:

  - **`show inline traffic prioritization status`** – Displays whether it is enabled or disabled.
  - **`set inline traffic prioritization <enable | disable>`** – Enables or disables the feature.

Inline deployment walkthrough

In-line mode enables you to run the Sensor in a *protection/prevention* mode, where packet inspection is performed in real time, and intrusive packets can be dealt with immediately; you can actively drop malicious packets because the Sensor is physically in the path of all network traffic. This enables you to actually prevent an attack from reaching its target.

1. Determine the optimal high availability strategy for the Sensor.

   This indicates how you would like the Sensor to behave when it fails (that is, fail-open, fail-closed, or support a fail-over/high-availability configuration).
2. Physically install the Sensor on your network, and connect the Sensor cables for the deployment mode of your choice.

   For example, connect one Sensor standalone (to fail-open, if applicable, or configure two Sensors as part of a HA pair).
3. Configure the Sensor monitoring ports.
4. Configure one or more policies for the inline ports.
5. Understand how blocking works, and configure blocking.

> **NOTE**
>
> You must use Manager to configure most aspects of your Sensor(s), including port configuration, pairing two Sensors for failover operation, and configuring and applying policies to detect and drop malicious traffic.

Determine your high availability strategy

Before you move your Sensor inline, consider the impact of a Sensor outage and its effect on your network. In inline mode, the Sensor does become a single point of failure. Trellix IPS provides a variety of options to minimize network downtime in the event of Sensor failure. For example, Sensors support complete stateful failover, delivering the industry's first true high-availability IPS deployment, similar to what you'd find with firewalls. If you're running the Sensor in inline mode, Trellix recommends that you deploy two Sensors redundantly for failover protection.

Failover or high availability

Where redundancy is an essential requirement, it is best practice to implement Trellix IPS 'high-availability' configuration. When running Sensors inline, this option is available to an identical pair of Sensors (same model, software image, signature set) deployed redundantly in inline mode. Both Sensors in the pair are active and share full state, so that the information on both Sensors is always current. Latency is very minimal compared to other devices providing failover, such as, firewalls.

The keys to the Trellix IPS failover architecture are as follows:

- Sensors configured for failover confirm a *heartbeat* once each second.
- Sensors configured for failover share flow information in real time.
- Sensors are invisible at Layer 2 and above; the monitoring ports do not have MAC addresses.

As a result, you do not have to worry about Layer 2 and 3 topology changes when you introduce Trellix IPS failover into the environment, and in the unlikely event of a Sensor failure, failover is instantaneous and connection state is maintained.

All NS-series Sensor models except NS3500 support failover.

Fail-open or fail-closed functionality

Sensor ports deployed in inline mode have the option of failing open or closed. Similar in terminology to firewall operation, ports failing open allow traffic to continue to flow. Thus, even if the ports fail, your Sensor does not become a bottleneck. However, the

monitoring ceases, allowing all traffic to continue to flow through the network, which can allow attacks to impact systems in your network. When ports are configured to fail-closed, the Sensor does not allow traffic to continue to flow. Thus, the failed ports become a bottleneck, stopping all traffic at the Sensor.

NOTE

There are security consequences when the Sensor is in bypass mode. When bypass mode is on, the traffic bypasses the Sensor and is not inspected; therefore, the Sensor cannot prevent malicious attacks.

There are two fail-open options available:

Fail-open with external hardware

Inline fail-open mode, available for both 10/100 and GE links, guarantees that data will be forwarded over a monitored link in the event that the Sensor's processes are temporarily stopped for upgrades or when the Sensor fails. This guarantee is delivered for 10/100 port pairs using an internal mechanical tap that connects the monitoring ports when hardware failure is detected. The 10/100 configuration is a choice made per port pair. The Gigabit fail-open implementation involves the use of the external Gigabit Fail-Open Kit, which includes a Bypass Switch.

CAUTION

Note that Sensor outage breaks the link connecting the devices on either side of the Sensor and requires the renegotiation of the network link between the two peer devices connected to the Sensor.

CAUTION

Depending on the network equipment, this disruption introduced by the renegotiation of the link layer between the two peer devices may range from a couple of seconds to more than a minute with certain vendors' devices.

CAUTION

A very brief link disruption may also occur while the links between the Sensor and each of the peer devices are renegotiated to place the Sensor back in inline mode. This outage, again, varies depending on the device, and can range from a few seconds to more than a minute.

Fail-open with the layer 2 passthru (L2) feature

Layer 2 Passthru is also known as *software fail-open*. The L2 feature, when triggered, causes traffic to flow through the Sensor without being copied to the detection engine.

NOTE

The Layer 2 Passthru option is provided specifically to handle internal Sensor errors; it is not provided as an alternative to other HA options, such as the Fail-Open kit.

Setting up the Sensor

NS-series Sensor port fail-open behavior

Each Sensor model is shipped with documentation on how to set up the Sensor and configure it to communicate with the Manager. This documentation consists of model-specific product guides and quick start guides. These documents provide detailed installation, configuration and cabling instructions for your Sensor.

The following table shows the monitoring port types for each Sensor model.

Table 23. NS-series Sensors: Port fail-open behavior

NS-series Sensor	Monitoring port type	Default port operation mode	Internal Fail-open ports	External Active Fail-open Kit	External Passive Fail-open Kit
NS9500	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi, 2x100G/40G Fi) • RJ45 10G (G3/1-2 to G3/3-4)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2 Group Slots • RJ45 10G (G3/1-2 to G3/3-4) • QSFP+ 40G(G0/1-2) • QSFP28 100 GigE	Not supported
NS9300	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2,G5,G6(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi) • RJ45 1G (G3/1-2 to G3/7-8) • RJ45 1G (G7/1-2 to G7/7-8)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2,G5,G6 Group Slots • RJ45 1G (G3/1-2 to G3/7-8) • RJ45 1G (G7/1-2 to G7/7-8)	Not supported

NS-series Sensor	Monitoring port type	Default port operation mode	Internal Fail-open ports	External Active Fail-open Kit	External Passive Fail-open Kit
NS9200	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi) • RJ45 1G (G3/1-2 to G3/7-8)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2 Group Slots • RJ45 1G (G3/1-2 to G3/7-8) • QSFP+ 40G(G0/1-2)	Not supported
NS9100	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi) • RJ45 1G (G3/1-2 to G3/7-8)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2 Group Slots • RJ45 1G (G3/1-2 to G3/7-8) • SFP+ 10G/1G (G0/1-2)	Not supported
NS7600	GE ports	In-line fail-open on pluggable I/O modules In-line fail-close on built-in G0	Supports built-in internal Fail-open on the following ports: • G1,G2,G3 (I/O: 6x10/1G Cu; 8x10G/1G Fi)	Supports Active Fail-open on the following ports: • Built-in G0 slot • All in I/O Modules supported in G1,G2, G3 Group Slots	Not supported

NS-series Sensor	Monitoring port type	Default port operation mode	Internal Fail-open ports	External Active Fail-open Kit	External Passive Fail-open Kit
NS7500	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi) • RJ45 1G (G3/1-2 to G3/7-8)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2 Group Slots • RJ45 1G (G3/1-2 to G3/7-8) • SFP+ 10G/ 1G(G0/1-2)	Supported on G0/1 and G0/2 interface only.
NS7350 / NS7250 / NS7150	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi) • RJ45 1G (G3/1-2 to G3/7-8)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2 Group Slots • RJ45 1G (G3/1-2 to G3/7-8) • SFP+ 10G/ 1G(G0/1-2)	Supported on G0/1 and G0/2 interface only.
NS7300 / NS7200 / NS7100	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • G1,G2(I/O: 6x1G Cu; 4x10G Cu; 4x10G/1G Fi) • RJ45 1G (G3/1-2 to G3/7-8)	Supports Active Fail-open on the following ports: • All in I/O Modules supported in G1,G2 Group Slots • RJ45 1G (G3/1-2 to G3/7-8) • SFP+ 10G/1G (G0/1-2)	Supported on G0/1 and G0/2 interface only.

NS-series Sensor	Monitoring port type	Default port operation mode	Internal Fail-open ports	External Active Fail-open Kit	External Passive Fail-open Kit
NS5200 / NS5100	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • RJ45 1G (G2/1-2 to G2/7-8)	Supports Active Fail-open on the following ports: • SFP+ 10/SFP 1G (G0/1-2) • SFP 1G Cu/Fi(G1/1-2 to G1/11-12) • RJ45 1G(G2/1-2 to G2/7-8)	Supported on G0/1-2, G1/1-2 to G1/11-12 interface ports.
NS3600	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • RJ45 1 Gbps/100 Mbps/10 Mbps (1-4, 7-14) • Fiber ports 10 Gbps/1 Gbps (11-14)	Supports Active Fail-open on the following ports: • RJ45 1 Gbps/100 Mbps/10 Mbps (1-4, 7-14) • Fiber ports 10 Gbps/1 Gbps (5-6, 11-14)	Not supported
NS3500	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • RJ45 1G(1-2 and 3-4)	Supported • RJ45 1G(1-2 and 3-4)	Not supported
NS3200/ NS3100	GE ports	Inline fail-open	Supports built-in internal Fail-open on the following ports: • RJ45 1G(1-2 to 7-8)	Supports Active Fail-open on the following ports: • RJ45 1G(1-2 to 7-8)	Not supported

The NS-series Sensors support network interface modules in the G1, G2 and G3 slots. Based on the type of modules, the ports have fail-open behavior as briefed below.

Table 24. Interface modules: Only for NS9500 Sensor (G1 and G2 slot ports)

I/O modules	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External AFO Kit	External PFO Kit
2-port (QSFP28) 100 GigE	GE ports	Inline fail-closed	No	Required for active fail-open	Not supported
4-port (QSFP+) 40 GigE					
2-port (QSFP+) 40 GigE					
2-port 100/40 GigE SR MTP/MPO with Internal fail-open		Inline-fail open	Yes		

Table 25. Interface modules: Only NS9x00 Sensors (G1 and G2 slot ports)

I/O modules	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External AFO Kit	External PFO Kit
4-port (QSFP+) 40 GigE	GE ports	Inline fail-closed	No	Required for active fail-open	Not supported
2-port (QSFP+) 40 GigE					

Table 26. Interface modules: Only NS7600 Sensors (G1, G2, and G3 ports)

I/O modules	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External AFO Kit	External PFO Kit
6-port RJ45 10/1 GigE with internal fail-open	GE ports	Inline fail-open	Yes (All port pairs)	Required for active fail-open	Not supported
8-port 10/1 GigE SM and MM with internal fail-open					

Table 27. Interface modules: NS9x00, NS7500, NS7x50, and NS7x00 Sensors (G1 and G2 ports)

I/O modules	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External AFO Kit	External PFO Kit
8-port (SFP+/SFP) 10/1 GigE	GE ports	Inline fail-closed	No	Required for active fail-open	Not supported

I/O modules	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External AFO Kit	External PFO Kit
4-port RJ-45 10 GigE with internal fail-open	GE ports	Inline fail-open	Yes (All port pairs)	Required for active fail-open	Not supported
6-port RJ-45 1 GigE with internal fail-open					
4-port SFP+ 1/10 GigE SR Optical 50 micron with internal fail-open					
4-port SFP+ 1/10 GigE SR Optical 62.5 micron with internal fail-open					
4-port SFP+ 1/10 GigE LR Optical with internal fail-open					

Table 28. Interface modules: Only NS3600 Sensor (Ports 11-14)

I/O modules	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External AFO Kit	External PFO Kit
4-port RJ-45 1 Gbps/100 Mbps/10 Mbps with internal fail-open	GE ports	Inline fail-open	Yes (All port pairs)	Required for active fail-open	Not supported
4-port 10/1 GigE MM 50/62.5 µm with internal fail-open					

VM-IPS Sensor port fail-open behavior

Virtual IPS Sensor	Monitoring port type	Default port operation mode	Internal (Fail-open built-in)	External Active Fail-open Kit	External Passive Fail-open Kit
IPS-VM600 and IPS-VM5000	GE ports	Inline fail-closed	No	Required for active fail-open	Not supported

NOTE

External AFO kit is applicable to scenarios where the Virtual Sensor is between two physical network devices. For inline inspection of traffic to virtual machines, only fail-closed mode is applicable.

How to connect the gigabit ethernet monitoring ports

Inline Fail Open - (Active or Passive) mode for Gigabit Ethernet (GE) ports requires the use of the external Gigabit fail-open Kit. The Passive Fail Open kit requires a RJ-45 control cable connecting to X1, for example, RJ-11 on NS7500.

NOTE

Fail-closed mode for GE ports requires no extra hardware; simply connect your fiber cables to the GE port pair (For example: G0/1-G0/2).

For information on how to connect the Sensor with a Gigabit Fail-Open Kit, see the documentation that accompanies the kit. For example, the Active-Fiber (850 nm) 10G (62.5 µm) Bypass Kit includes [Trellix IPS 1/10 Gigabit Modular Active Fail-Open Bypass Kit Guide].

HA pair cable connections

Failover requires connecting the paired Sensors via an interconnection cable or cables. Communication between paired Sensors maintains the failover heartbeat and state information.

There is no standard heartbeat port across all the Sensor models. The port or ports you use to connect the two Sensors depends on the Sensor model. The Sensor models and their failover interconnection ports are described below.

NS-series Sensor	Failover port
NS9500	G0/1
NS9300	G1/1 and G1/2
NS9200	G0/1
NS9100	G0/1
NS7600	• G0/1 in Sensor with 5 Gbps throughput • G0/1 and G0/2 in Sensor with 10 and 15 Gbps throughput

NS-series Sensor	Failover port
NS7500	G0/1
NS7350	G0/1
NS7250	G0/1
NS7150	G0/1
NS7300	G0/1
NS7200	G0/1
NS7100	G0/1
NS5200	G1/1 and G1/2
NS5100	G1/1 and G1/2
NS3600	5
NS3200/NS3100	1

NOTE

High availability is not supported in NS3500 Sensor.

The following is a quick summary of the rules for connecting cables:

- Connecting the heartbeat cable must be direct; you must not connect the heartbeat cable through another network device, such as a switch.
- When using a copper SFP, make sure to change the **Media Type** of the port to **Copper** in the **Physical Ports** page before creating the HA pair.
- When 2 ports are used on each Sensor for the heartbeat connection, always connect cables between identical port names. For example, in NS9500 high availability configuration, port G0/1 on Sensor 1 must be connected to port G0/1 on Sensor 2 (not G0/2).

How to configure the Sensor monitoring ports

After you have installed and connected the Sensor, you must configure the Sensor ports. The following list summarizes the port configuration requirements:

- Make sure the ports are enabled.
- You must set the port speed depending on your network.
- You must match Sensor cable connections to the port configuration: for example, if you do not connect a fail-open kit to the port, you can configure the port as inline fail-open if it supports built-in passive fail-open. If not, you must configure it as inline fail-closed.
- Select the placement of the port depending on the direction of traffic. This step is also crucial since enabling the incorrect placement will configure the Sensor to examine the wrong traffic.

About Sensor port configuration

Before you configure the Sensor ports, you must have installed the Sensor and added to the Manager interface.

Configure inline mode for a single Sensor

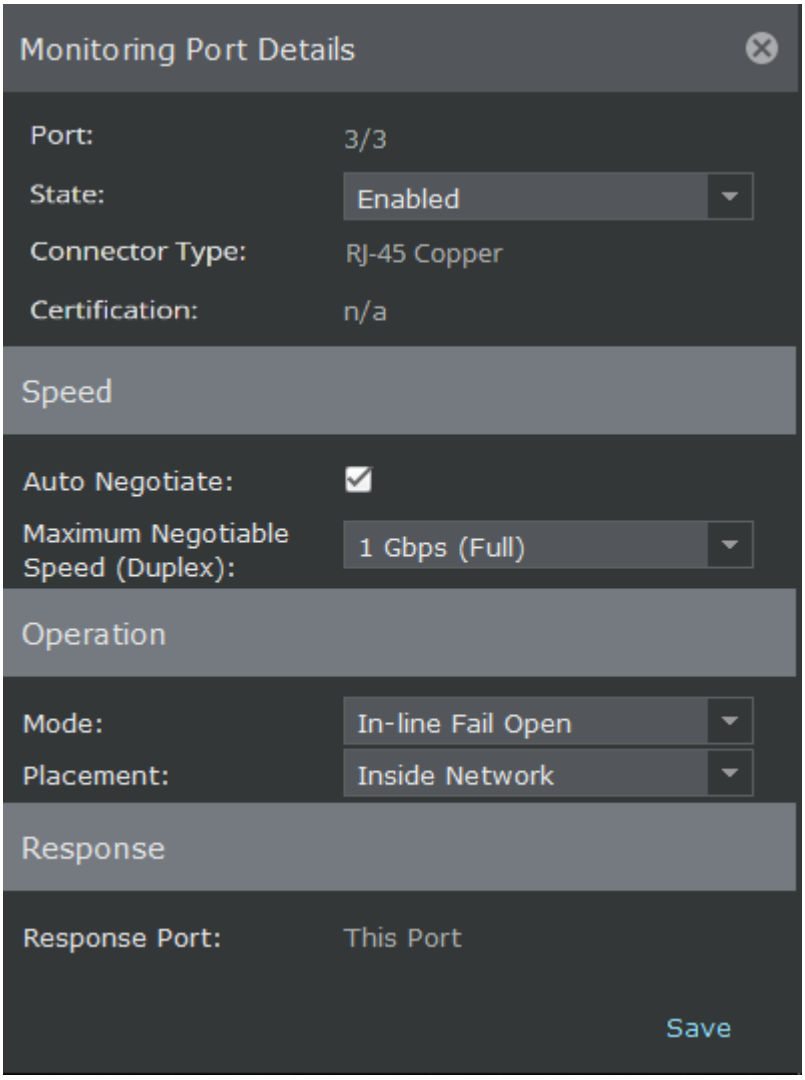
This section contains recommendations for deploying a single Sensor in inline mode.

> **NOTE**
>
> Configuration for a fail-open kit is described in the fail-open kit documentation. For example, to configure the Sensor to work with the copper fail-open kit, see the [Trellix Intrusion Prevention System Fail-Open Kit Product Guide].

1. In the Manager interface, select Devices → <Admin Domain Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Double-click on a numbered port (for example, 3/1) from **Monitoring Ports**.

   Monitoring Port Details panel displays current port settings.

Figure 264. Verifying ports for inline fail-open mode



3. Set the Administrative **State** to **Disable** (off).
4. Select the other port (for example, 3/2) and set the Administrative **State** to **Disable** (off).
5. Now select the aforesaid port (port 3/1) and select the **Auto Negotiate** checkbox.
6. Select the port **Speed**.
7. Do one of the following:
   - For inline fail-closed operation, select **Inline Fail Closed** as the operating Mode.
   - For inline fail-open operation, select **Inline Fail Open** or **Inline Fail Open - Active** as the operating Mode. Confirm (**Yes**) that you have already connected a fail-open kit. However, if your Sensor supports in-built fail-open on that port, you might not require a fail-open kit.

> **NOTE**
>
> **Inline Fail Open** indicates in-built passive fail-open which is supported on different Sensors differently.

8. Select the area of your network to which the current port is connected: **Inside** (traffic generated internally, destined for the external network) or **Outside** (traffic generated externally, destined for the internal network).
9. Set the Administrative **State** to **Enable** (on).
10. Click **Save**.
11. Repeat for any other ports you need to configure.
12. Download the changes to your Sensor by clicking the **Deploy Pending Changes** option.

Failover — Configuration of two Sensors in inline mode

In a failover configuration, the two Sensors are placed inline, connected to each other via cables, and configured to act as a *failover pair*. All traffic is copied and shared between them in order to maintain state. Sensor A copies the packets received on its monitoring ports to Sensor B using the interconnection ports and vice versa. Since both Sensors see all traffic and build state based on it, their state information is synchronized at all times.

All packets are seen by both Sensors (when both are operational); however, only one Sensor in the pair raises an alert whenever an attack is detected.

When deploying the two Sensors in failover mode, you must ensure the following:

- The Sensor interconnection ports must be connected appropriately so that both the Sensors can communicate.
- Both Sensors must be of the identical model type, and have the same signature set and software loaded. (One of the two Sensors may be a "Failover (FO)" Sensor model, which is a fully functional Sensor limited to operation as part of a failover pair; it cannot operate standalone.)
- Additionally, all ports on both the Sensors must be configured to run in inline mode.

Creating a HA pair

Prerequisites:

- By design, the configuration of the primary Sensor is copied to the secondary Sensor, overwriting the original configuration on the secondary. If you intend to configure both Sensors as fail-closed or fail-open, you need to configure the ports on the Sensor you intend to designate as the primary during the HA pair creation. However, if you intend to have one Sensor as fail-closed and the other as fail-open, you must revisit the **Physical Ports** page of each Sensor after creating the HA pair and make the appropriate changes.
- When using a copper SFP, make sure to change the **Media Type** of the port to **Copper** in the **Physical Ports** page before creating the HA pair.
- Ensure failover (interconnect cable) is connected between the Sensor pair before creating the HA pair.

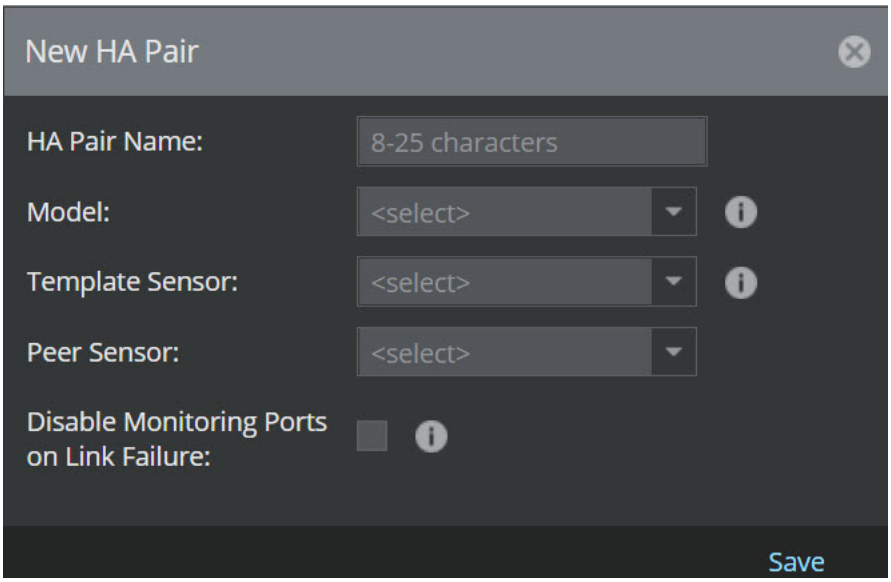
You can create a HA pair using **Device Manager** page. A HA pair creation happens in real time; there is no need to explicitly update the configuration. To create a HA pair, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Global → **Device Manager**.

   The **Device Manager** page is displayed.

2. Select the **HA Pairs** tab and click +.

   The **New HA Pair** details panel is displayed.



3. Enter the name of HA pair that uniquely identifies the grouping in **HA Pair Name**.

   Both Sensors in a HA pair must use same model and same version.

4. Configure the Primary Sensor as **Template Sensor** from the drop-down option.
5. Configure the Secondary Sensor as **Peer Sensor** from the drop-down option.
6. Enable or disable the **Disable Monitoring Ports on Link Failure** as required. By default, it is disabled.

   Enabling this option enables the ability of monitoring ports to permit fail-open configuration. It signifies your intent on whether to prioritize transport over security or prioritize no-network-disruption over traffic monitoring by IPS.

   Trellix recommends one of the following:

   - Enabled fail-open configuration:
     - However, configure the monitoring ports on the primary Sensor as **Inline Fail Closed** so that they do not fail-open but indicate primary Sensor failure. This causes upstream traffic to be routed to the secondary Sensor thereby continuing traffic monitoring.
     - Additionally, configure the monitoring ports on the secondary Sensor as **Inline Fail Open** so that, in case both Sensors have failed, traffic bypasses the HA pair.
   - Disabled fail-open configuration:
     - This ensures that the primary Sensor will not fail-open in case of a failure.
     - Nevertheless, configure the monitoring ports on the primary Sensor as **Inline Fail Closed** so that they do not fail-open but indicate primary Sensor failure. This causes upstream traffic to be routed to the secondary Sensor thereby continuing traffic monitoring.
     - Additionally, explicitly configure the monitoring ports on the secondary Sensor as **Inline Fail Open** so that, in case both Sensors have failed, traffic bypasses the HA pair.

7. Click **Save**.

   A **Confirmation** dialog box is displayed. Click **OK**. The configured HA pair can be viewed in the list.

   NOTE

   - In the Manager, if at least two Sensors are not using same model and software version, an **Error** dialog box is displayed.
   - An option to edit the existing HA pair is not provided. If you double-click a row in the grid, an **Error** dialog box is displayed. You change the configuration by deleting and re-creating a HA pair.

   Most configuration options are done at the HA pair node level. For example, you can now apply a policy or update the configuration at the HA pair node level and it automatically propagates to each of the member Sensors. On the other hand, you still configure the port settings, view interface statistics, and upgrade the Sensor software at the Sensor node level. The easiest way to get a feel for the HA pair configuration process is to examine the user interface once the pair has been created.

   NOTE

   The Sensors must be running the same software version to run in a failover configuration. However, you upgrade software at a Sensor level, even those that are part of a HA pair. The recommended upgrade procedure is to therefore upgrade the software version on both Sensors, and then restart them sequentially. That is, once the upgrade process is complete on both, restart (for example) the secondary, confirm that it has restarted without error, and then restart the primary.

Download configuration, signature set, and software updates to the Sensor

After configuring your ports for inline mode, setting the TCP/IP parameters, and customizing and applying policy, you will need to download this configuration to the Sensor in order for all of your changes to be active.

- Configuration changes, including port configuration, policy, and signature set updates: Devices → <Admin Domain Name> → Devices → <Device_Name> → **Deploy Pending Changes**
- Software updates only: Devices → <Admin Domain Name> → Devices → <Device_Name> → Member Sensors → <HA Pair Node> → Maintenance → **Deploy Device Software**

Fail-open operation in Sensors

When a Sensor is deployed inline, it monitors traffic at wire speed and, depending on your policies, prevents attacks from occurring. However, if the Sensor fails, depending on your configuration, the Sensor becomes a bump in the wire which results either in no traffic passing through or in all traffic passing through without being monitored. The former configuration is called inline fail-closed and the latter configuration is called inline fail-open.

To deploy Sensors in a fail-open configuration, you might require additional hardware which comprises a compatible fail-open switch, appropriate cables, and depends on which port you want to configure – SFP, SFP+, QSFP+, or QSFP28 transceivers. The only exception to this rule is if you decide to use the in-built fail-open option available in some Sensor models.

To deploy Sensors in fail-closed configuration, you will not require any additional hardware. When enabled, Sensor ports requiring the use of SFP, SFP+, QSFP+, or QSFP28 transceivers are configured inline fail-closed by default .

Evaluation of fail-open modes

It all begins with estimating the requirements of your organization's network. If it is paramount to allow uninterrupted traffic flow to the network, a fail-open deployment will work best. However, if security cannot be compromised at any instant, you must choose a fail-closed configuration. Both deployments come with inherent advantages and disadvantages. While a fail-closed setup ensures that all traffic entering the network is monitored, it results in network outages which may not be favorable if you host business-critical servers in the network. On the other hand, a fail-open setup ensures that traffic is never interrupted but can result in malicious traffic entering the network during a Sensor outage. So, this is the first choice that you, as a security analyst, need to make.

Broadly, these are the benefits of choosing a fail-open network architecture.

- It reduces network downtime to seconds during any Sensor reboot or Sensor failure.
- It protects your network during link failure on the Sensor.
- It bypasses the Sensor when troubleshooting network issues. This will help you identify or eliminate the Sensor as the cause of network issues.

Fail-closed configuration

To configure your network for fail-closed operation, you will simply need to make sure that a port pair on the Sensor is set to inline fail-closed configuration.

Fail-open configuration

Should you decide to go the fail-open route, you have two options:

- Internal fail-open: Fail-Open is built into some of the Sensor ports

  NOTE

  When a port pair is configured for internal fail-open, the downtime between link failure on the Sensor and bypass can be a maximum of 3 seconds.

- External fail-open: Fail-Open is carried out using external hardware

If you use a Sensor that supports internal fail-open, you simply need to configure the appropriate port pair for inline fail-open.

If you use a Sensor that supports external fail-open, you will need to make sure you have the additional hardware necessary for an inline fail-open deployment. Trellix IPS provides a range of fail-open kits to accommodate diverse requirements. You must purchase a fail-open kit that best suits your requirements and one that is compatible with your existing network infrastructure. The primary component in a fail-open kit is the fail-open switch, which can be active or passive.

An active fail-open switch sends a signal to the Sensor at regular intervals and awaits a response. A response indicates that the Sensor is operating normally. This signal is called a "heartbeat" signal. If the switch does not receive a response for a set number of signals, it removes the Sensor from the path of traffic and routes all traffic through its own ports, thereby ensuring continuous traffic flow.

A passive fail-open switch relies on the Sensor to send an electrical signal to determine if the Sensor is operating normally. If the switch does not receive a signal in a specified period, it removes the Sensor from the path of network traffic and bypasses the Sensor, routing traffic through its own ports.

NOTE

A heartbeat signal is a data packet that is sent by the Sensor or by the fail-open switch (depending on whether it is passive or active). Regardless of whether it is passive or active, a signal is sent at regular intervals and is used by the fail-open switch to determine the operational state of the Sensor. The interval between each signal varies with the type of fail-open switch you are using.

Physical description

All fail-open switches are provided with four basic ports. Two of these connect to monitoring ports of the Sensor and while the other two connect to network devices that route traffic to the network.

Active fail-open switches have two power ports for a primary and a secondary power source. They also have LEDs that show bypass status. Certain models also have LEDs to show utilization threshold status for each port.

There are several types of fail-open switches that enable you to choose the one that best suits your requirements. When you make your choice of fail-open kit, be sure to consider the following factors:

- How quickly you need traffic to bypass the Sensor during an outage – Depending on how quickly you require traffic to bypass a Sensor during an outage, you can decide between an active or a passive fail-open switch and a copper or a fiber fail-open switch. For more details about the differences between the speed of active switching and passive switching, refer to the following sections:
  - Passive fail-open switches (page 648)
  - Active fail-open switches (page 649)
- Distance between the fail-open switch and Sensor – All fail-open switches have an upper limit that is set by the type of cable used for data transport.
- Cost – Finding the right balance between cost and your requirements is another factor in determining the ideal fit for a fail-open switch.

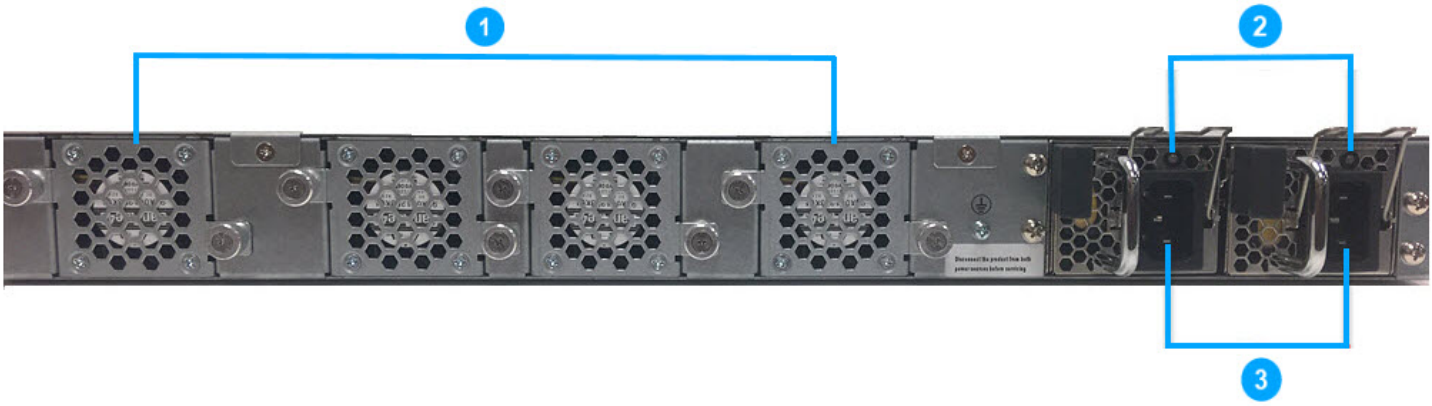
Images below show the front and rear views of 100G active fiber fail-open switch.

Figure 265. Front view of 100G active fiber fail-open switch

Callout	Description
1	Ethernet management port (1)
2	RS232 (RJ45) console port (1)

Callout	Description
3	USB port (1)
4	100G Fail-open module ports with hot swappable QSFP28 transceivers (2)

Figure 266. Back view of 100G active fiber fail-open switch



Callout	Description
1	Fan units (4)
2	LED on the power supply unit
3	Power supply 1/2

Types of fail-open

Internal fail-open

Some Sensor models provide fail-open through their in-built copper ports. Sensor models that provide in-built fail-open are:

- **NS-series**: NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3600, NS3500, NS3200, and NS3100

External fail-open

Fail-open switches are categorized in several ways. One categorization, as seen above, is based on functionality – active or passive. In addition, they are also categorized based on the type of ports and the corresponding type of cables that connect them to the Sensor and network device – copper or fiber. Copper and fiber fail-open switches are further categorized based on the maximum throughput that each model supports. Finally, every fail-open switch optionally has the facility to trigger alarms and send notifications to an SNMP manager.

IMPORTANT

While choosing a fail-open switch, you must remember that certain fail-open switches are compatible only with certain Sensors. The comparison in the tables in upcoming sections provide details about which fail-open switches work with which Sensors. These tables contain a **Model no.** for each fail-open switch. The rest of the chapter frequently refers to the **Model no.** of each fail-open kit when explaining steps to perform various functions.

IMPORTANT

All active fail-open switches support SNMP traps regardless of whether the switch is copper or fiber. The switch in such fail-open kits consists of a Management port. This allows you to assign an IP address to the fail-open switch and establish communication with an SNMP server through the network.

Fiber fail-open switches consist of two types: single mode and multi-mode fibers. The table below gives you some relevant details about both types of fiber optic fail-open switches. This is especially relevant because you must determine the type of fiber that is used your organization network before you decide which type of fail-open switch to use. Also, all product documentation for fail-open kits and decals on the fail-open switches will repeatedly refer to these parameters.

Table 29. Single mode and multi-mode fiber optic fail-open switches

Type	Fiber thickness	Wavelength range
Single mode (Long reach)	8.5 µm	1300 nm to 1550 nm
Multi-mode (Short reach)	50 µm or 62.5 µm	850 nm to 1300 nm

Support for External Active Fail-Open Kits in Sensors with internal fail-open functionality

All Sensor port-pairs with internal or in-built fail-open functionality can also support active fail-open kits (refer to the section Active fail-open switches (page 649) for compatibility information). For additional details, refer to the specific fail-open kit guides.

Using an external (active) fail-open switch has the following advantages over the in-built mode:

- Lower latency in a bypass mechanism
- Elimination of risk associated with a single point of failure

Passive fail-open switches

A passive fail-open switch depends on the Sensor to send a control signal or heartbeat signal from its **Control** port at regular intervals.

A passive copper or fiber fail-open switch receives a control signal every second. If the fail-open switch does not receive a signal for 4 seconds consecutively, it transitions to bypass mode thereby removing the Sensor from the path of traffic.

During normal operation, the bypass status of the switch remains ON. To confirm this, you must see the **Control** port LED ON on the switch. When the Sensor fails or reboots, bypass status is activated, which is indicated by the **Control** port LED going off. When the fail-open switch is in bypass mode, there is no traffic monitoring by the Sensor.

NOTE

Passive fail-open kits are not compatible with NS9500, NS9x00, NS3500 and NS3x00 Sensors since these Sensors do not have control ports. Refer to the table which lists all fail-open switches and the Sensors with which they are compatible for more details.

Active fail-open switches

An active fail-open switch sends control signals or heartbeat signals to the Sensor to determine its operational state. Active fail-open switches are faster than passive fail-open switches in its transition from normal mode to bypass mode during a Sensor outage.

An active fiber fail-open switch sends a heartbeat signal to the Sensor. This signal returns to the fail-open switch during normal operation. If the fail-open switch does not receive a response, it transitions to bypass mode thereby removing the Sensor from the path of traffic.

During normal operation, the bypass status of the switch remains OFF. To confirm this, you must see the OFF LED on the switch lit up. When the Sensor fails or reboots, bypass status changes to ON, which is indicated by the ON LED coming on. When the fail-open switch is in bypass mode, there is no traffic monitoring by the Sensor.

NOTE

Active fail-open kits are not compatible with NS3500 Sensors.

Fail-Open switch model 1

The table below shows fail-open switch model 1 with all applicable NS-series Sensors.

Table 30. NS-series Sensors compatible with fail-open switch models

Model no.	Fail-open switch	SKU	NS3x00	NS5x00	NS7x00	NS7x50	NS9x00
1	Active-Fiber 40G (8.5 µm, 50 µm, 62.5 µm)	IAC-2P40FO-KIT	No	No	No	No	Yes

Fail-Open switch models 2 thru 20

The tables below show all NS-series Sensor models that are compatible with fail-open switches 2 thru 20.

Table 31. NS-series models compatible with fail-open switch models 2 thru 20 (Modular based Active Fail-Open kits)

No.	Fail-open switch	SKU	NS3x00	NS3500	NS3600	NS5x0
2	Passive-Fiber (850 nm) 10G (50 µm)	IAC-PF85050-KT1	No	No	No	Yes (suppo on G0 ly)

No.	Fail-open switch	SKU	NS3x00	NS3500	NS3600	NS5x0
3	Passive- Fiber (850 nm) 10/1G (62.5 µm)	IAC-PF85062- KT1	No	No	No	Yes (10/1G suppo on G0, only 1 suppo on G1)
4	Passive- Fiber (1310 nm) 10/1G (8.5 µm)	IAC-PF131010- KT1	No	No	No	Yes (10/1G suppo on G0, only 1 suppo on G1)
5	Passive- Copper 10/100/1000	IAC-PFOCG- KT2	No	No	No	Yes (1000M suppo on G0 G1 onl
6	Active- Fiber (850 nm) 10G (62.5 µm)	IAC-AF85010- KT1*	No	No	Yes (supported on ports 5 and 6 and ocp fiber is sup-ported on ports 11-14)	Yes (suppo on G0 ly)
7	Active- Fiber (1310 nm) 10G (8.5 µm)	IAC-AF131010- KT1*	No	No	Yes (supported on ports 5 and 6)	Yes (suppo on G0 ly)

No.	Fail-open switch	SKU	NS3x00	NS3500	NS3600	NS5x0
8	Active- Fiber (850 nm) 1G (62.5 µm)	IAC-AF85062- KT1*	No	No	Yes (supported on ports 5 and 6 and ocp fiber is supported on ports 11-14)	Yes
9	Active- Fiber (1310 nm) 1G (8.5 µm)	IAC-AF131085- KT1*	No	No	Yes (supported on ports 5 and 6)	Yes
10	Active -Copper 10/100/1000 module	IAC-AFOCG- KT2*	Yes	No	Yes (supported on ports 1-4 and 7-10 and ocp copper is supported on ports 11-14)	Yes
11	Active Fail-Open Chassis: Module based for 10G/1G	IAC-AFOCH- KT2	Yes	No	Yes (supported on ports 5 and 6 and ocp fiber is supported on ports 11-14)	Yes
12	Active Fiber 40G - SR4 (50µm MTP/ MPO)	IAC-2P40FOSR4- KIT **	No	No	No	No

No.	Fail-open switch	SKU	NS3x00	NS3500	NS3600	NS5x0
13	Active Fiber 10G - SR (LC 62.5µm)	IAC-4P10FOSR- KIT **	No	No	Yes (supported on ports 5 and 6 and ocp fiber is supported on ports 11-14)	Yes
14	Active Fiber 40G -LR4 (LC 8.5µm)	IAC-2P40FOLR4- KIT **	No	No	No	No
15	Active Fiber 10G - LR (LC 8.5µm)	IAC-4P10FOLR- KIT **	No	No	Yes (supported on ports 5 and 6)	Yes
16	Active Fiber 40G - BiDi (LC 50µm/ 62.5µm)	IAC-2P40FOBD- KIT**	No	No	No	No
17	Active Fail-Open Chassis: Module based for 40G	IAC-AFOCH40- KT2 **	No	No	Yes	No
18	Active Fiber 100G - QSFP28-SR4 (50µm MTP/ MPO)	IAC-2P100FOSR- KIT***	No	No	No	No

No.	Fail-open switch	SKU	NS3x00	NS3500	NS3600	NS5x0
19	Active Fiber 100G - QSFP28-LR4 (LC 8.5um)	IAC-2P100FOLR-KIT ***	No	No	No	No
20	Active Fail-Open Chassis: Module based for 100G	IAC-AFOCH100-KT2 ***	No	No	No	No
	* Active Fail-Open Chassis is required with these kits (10G/1G). Each chassis can hold up to 4 modules.					
	** Active Fail-Open Chassis is required with these kits. Each chassis can hold up to three 40G or 10G modules in any combination.					
	*** Active Fail-Open Chassis is required with these kits (100G). Each chassis can hold up to 2 modules.					

Table 32. NS-series models compatible with fail-open switch models 2 thru 20 (Modular based Active Fail-Open kits)

No.	Fail-open switch	SKU	NS7x00	NS7x50	NS7500	NS7600
2	Passive- Fiber (850 nm) 10G (50 µm)	IAC-PF85050-KT1**	Yes (supported on G0 only)	Yes (supported on G0 only)	Yes (supported on G0 only)	No
3	Passive- Fiber (850 nm) 10/1G (62.5 µm)	IAC-PF85062-KT1**	Yes (supported on G0 only)	Yes (supported on G0 only)	Yes (supported on G0 only)	No
4	Passive- Fiber (1310 nm) 10/1G (8.5 µm)	IAC-PF131010-KT1**	Yes (supported on G0 only)	Yes (supported on G0 only)	Yes (supported on G0 only)	No

No.	Fail-open switch	SKU	NS7x00	NS7x50	NS7500	NS7600
5	Passive- Copper 10/100/1000	IAC-PFOCG- KT2**	Yes (1000Mbps supported on G0 only)	Yes (1000Mbps supported on G0 only)	Yes (1000Mbps supported on G0 only)	No
6	Active- Fiber (850 nm) 10G (62.5 µm)	IAC-AF85010- KT1*	Yes	Yes	Yes	Yes
7	Active- Fiber (1310 nm) 10G (8.5 µm)	IAC-AF131010- KT1*	Yes	Yes	Yes	Yes
8	Active- Fiber (850 nm) 1G (62.5 µm)	IAC-AF85062- KT1*	Yes	Yes	Yes	Yes
9	Active- Fiber (1310 nm) 1G (8.5 µm)	IAC-AF131085- KT1*	Yes	Yes	Yes	Yes
10	Active -Copper 10/100/1000 module	IAC-AFOCG- KT2*	Yes	Yes	Yes	Yes
11	Active Fail-Open Chassis: Module based for 10G/1G	IAC-AFOCH- KT2	Yes	Yes	Yes	Yes

No.	Fail-open switch	SKU	NS7x00	NS7x50	NS7500	NS7600
12	Active Fiber 40G - SR4 (50µm MTP/ MPO)	IAC-2P40FOSR4- KIT ***	No	No	No	No
13	Active Fiber 10G - SR (LC 62.5µm)	IAC-4P10FOSR- KIT ***	Yes	Yes	Yes	Yes
14	Active Fiber 40G -LR4 (LC 8.5µm)	IAC-2P40FOLR4- KIT ***	No	No	No	No
15	Active Fiber 10G - LR (LC 8.5µm)	IAC-4P10FOLR- KIT ***	Yes	Yes	Yes	Yes
16	Active Fiber 40G - BiDi (LC 50µm/ 62.5µm)	IAC-2P40FOBD- KIT***	No	No	No	No
17	Active Fail-Open Chassis: Module based for 40G	IAC-AFOCH40- KT2 ***	No	No	No	Yes
18	Active Fiber 100G - QSFP28-SR4 (50µm MTP/MPO)	IAC-2P100FOSR- KIT****	No	No	No	No
19	Active Fiber 100G - QSFP28-LR4 (LC 8.5um)	IAC-2P100FOLR- KIT ****	No	No	No	No
20	Active Fail-Open Chassis: Module based for 100G	IAC-AFOCH100- KT2 ****	No	No	No	No

No.	Fail-open switch	SKU	NS7x00	NS7x50	NS7500	NS7600
* Active Fail-Open Chassis is required with these kits (10G/1G). Each chassis can hold up to 4 modules.						
** For NS7500, NS7x00, and NS7x50 Sensors, these kits work with G0/1 and G0/2 interface only.						
*** Active Fail-Open Chassis is required with these kits. Each chassis can hold up to three 40G or 10G modules in any combination.						
**** Active Fail-Open Chassis is required with these kits (100G). Each chassis can hold up to 2 modules.						

Table 33. NS-series models compatible with fail-open switch models 2 thru 20 (Modular based Active Fail-Open kits)

No.	Fail-open switch	SKU	NS9x00	NS9500
2	Passive- Fiber (850 nm) 10G (50 µm)	IAC-PF85050- KT1**	No	No
3	Passive- Fiber (850 nm) 10/1G (62.5 µm)	IAC-PF85062- KT1**	No	No
4	Passive- Fiber (1310 nm) 10/1G (8.5 µm)	IAC-PF131010- KT1**	No	No
5	Passive- Copper 10/100/1000	IAC-PFOCG- KT2**	No	No
6	Active- Fiber (850 nm) 10G (62.5 µm)	IAC-AF85010- KT1*	Yes	Yes

No.	Fail-open switch	SKU	NS9x00	NS9500
7	Active- Fiber (1310 nm) 10G (8.5 µm)	IAC-AF131010- KT1*	Yes	Yes
8	Active- Fiber (850 nm) 1G (62.5 µm)	IAC-AF85062- KT1*	Yes	Yes
9	Active- Fiber (1310 nm) 1G (8.5 µm)	IAC-AF131085- KT1*	Yes	Yes
10	Active -Copper 10/100/1000 module	IAC-AFOCG- KT2*	Yes	Yes
11	Active Fail-Open Chassis: Module based for 10G/1G	IAC-AFOCH- KT2	Yes	Yes
12	Active Fiber 40G - SR4 (50µm MTP/MPO)	IAC-2P40FOSR4- KIT ***	Yes	Yes
13	Active Fiber 10G - SR (LC 62.5µm)	IAC-4P10FOSR- KIT ***	Yes	Yes
14	Active Fiber 40G -LR4 (LC 8.5µm)	IAC-2P40FOLR4- KIT ***	Yes	Yes

No.	Fail-open switch	SKU	NS9x00	NS9500
15	Active Fiber 10G - LR (LC 8.5µm)	IAC-4P10FOLR-KIT ***	Yes	Yes
16	Active Fiber 40G - BiDi (LC 50µm/62.5µm)	IAC-2P40FOBD-KIT***	Yes	Yes
17	Active Fail-Open Chassis: Module based for 40G	IAC-AFOCH40-KT2 ***	Yes	Yes
18	Active Fiber 100G - QSFP28-SR4 (50µm MTP/MPO)	IAC-2P100FOSR-KIT****	No	Yes
19	Active Fiber 100G - QSFP28-LR4 (LC 8.5um)	IAC-2P100FOLR-KIT ****	No	Yes
20	Active Fail-Open Chassis: Module based for 100G	IAC-AFOCH100-KT2 ****	No	Yes
* Active Fail-Open Chassis is required with these kits (10G/1G). Each chassis can hold up to 4 modules.				
** For NS7500, NS7x00, and NS7x50 Sensors, these kits work with G0/1 and G0/2 interface only.				
*** Active Fail-Open Chassis is required with these kits. Each chassis can hold up to three 40G or 10G modules in any combination.				
**** Active Fail-Open Chassis is required with these kits (100G). Each chassis can hold up to 2 modules.				

Configure fail-open kit model 1

Prerequisites:

For each fail-open configuration, you will need to make sure you have all these components.

- Determine the IP address for the fail-open switch or, if you are deploying multiple switches, a range of IP addresses
- Determine a network mask and the default gateway for the fail-open switch
- 4 cables to connect the fail-open switch and the Sensor
- (Optional) A DB-9 RS232 female-female cable to access the fail-open switch CLI
- 2 QSFP+ for the fail-open switch and 2 QSFP+ for the Sensor
- Cables for a fiber fail-open switch
    - 2 LC or MTP/MPO cables for network ports

- 2 LC or MTP/MPO cables for monitoring ports

Broadly, these are the steps you will need to follow to set up a fail-open kit.

1. Install the fail-open switch.
2. (Optional) Configure bypass switch parameters.
3. (Optional) Configure notification by SNMP traps
4. Cable bypass switch to a Sensor using the appropriate cables.
5. Configure Sensor ports as inline fail-open.
6. (Optional) Use the Web Manager to configure the fail-open switch settings.

1. Install the fail-open switch

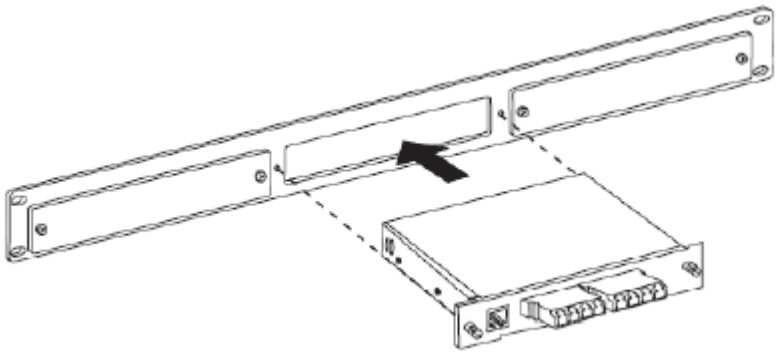
Prerequisite:

Depending on whether you can physically connect the fail-open switch to a computer using an RS232 cable, you might consider swapping this step with configuring fail-open switch parameters.

These steps explain the procedure to install fail-open switch model 1.

1. Slide the switch into the opening in the center of the rack-mount panel, until the faceplate of the switch rests against the panel.

Figure 267. Slide the fail-open switch into the rack plate



2. Secure the switch to the rack-mount panel by inserting screws through the holes on the switch faceplate and into the panel.
3. Install the panel and fail-open switch on the rack.
   a. Place the 1U panel against the front of a standard 19-inch rack.
   b. Secure the rack-mount panel by inserting the screws (included with the rack-mount panel) through the holes on the front of the panel and the sides of the rack.
4. Additional fail-open switches can be installed without removing the rack-mount panel from the rack. To install up to two additional switches:
   a. Remove the screws holding one of the removable blank plates from the front of the panel.
   b. Follow the procedure for installing a switch in the rack-mount panel for the additional fail-open switch.

2. Configure fail-open switch parameters

Prerequisite:

To proceed with this setup you will require:

- One DB9 RS-232 cable
- One RJ-45 cable

The steps below explain the configuration of parameters for your fail-open switch.

1. Connect the applicable cable to the fail-open switch.
2. Connect the other end to a computer which runs a terminal emulation software, such as HyperTerminal or PuTTY.
3. Launch the terminal emulation software, and set the communications parameters as shown below:
   - Baud rate: 19200
   - Data bits: 8
   - No parity
   - Stop bits: 1
   - No flow control
4. Power up the fail-open switch.

   The CLI banner and login prompt are displayed.
5. At the login prompt, type the username and password, and press **Enter**.

Table 34. Username and password for both sets of fail-open switches

For fail-open switch model 1	
Username	**Trellix00**
Password	**Trellix00**

The fail-open switch CLI prompt is displayed.

6. Use these commands for fail-open switch model 1.

Table 35. CLI commands for fail-open switch model 1

Command	Description
set username <username>	Change the username of the fail-open switch.
set password <password>	Change the password of the fail-open switch.
set time <date & time>	Set the time and date of the fail-open switch in mm/dd/yyyy-hh:mm:ss.
set ip <ip address>	Configures the IPv4 address of the fail-open switch.
set mask <mask>	Configures the gateway IPv4 address to be used by the fail-open switch.

Command	Description
`set manager <ip address>`	Configures the SNMP server IPv4 address.
`show display`	View the state of the web interface.
`display`	Enable or disable the Web Manager and management port of the fail-open switch. **NOTE** The Web Manager enables you to view and manage all settings for a fail-open switch through a web console using administrator credentials. The management port enables you to establish communication between the fail-open switch and SNMP manager. You can enable or disable this view and the management port depending on your preferences. The default state is set to ON.
`show set`	Displays the current settings for the fail-open switch.

3. (Optional) Configure notification by SNMP traps

Prerequisites:

- To configure SNMP traps, you will require a server that will act as an SNMP server. The SNMP server can be any Windows or Linux system installed with a MIB browser such as iReasoning. To view requirements and download a copy of iReasoning MIB browser, follow the link: https://ireasoning.com/mibbrowser.html.
- Make sure your fail-open switch IP address can be reached within the network.
- Make sure your SNMP server and fail-open switch are able to communicate.
- In addition, you will need to obtain MIB files to decode alert codes sent by the fail-open switch. These files are specific to the fail-open switch and can be obtained by clicking on this link: KB86247.
- You will require the RJ-45 cable.

1. Connect an RJ-45 cable to the Management Port at the back of the fail-open switch.
2. Connect the other end to a network device so that the SNMP server is reachable through the network.
3. Copy the fail-open switch MIB files to a suitable location on the SNMP server.

   When any of the following events occur, an SNMP trap is generated:

   - Utilization exceeds the threshold on any port (Only for model 1)
   - Bypass state changes
   - Any port link status changes
   - Either power supply state changes
4. Set up the fail-open switch IP address, network mask, and SNMP manager IP address using the commands provided in the section [Configure the fail-open switch parameters].
5. Make sure the SNMP manager and fail-open switch are able to communicate.

Configuration of SNMP traps is complete when you can see a trap appear in the MIB browser.

4. Connect the switch to an inline Sensor

After you have secured the fail-open switch in its rack, use copper or fiber connecting cables to connect the switch with the Sensor. The underlying principle in connecting these cables is to connect the Sensor and the switch such that traffic gets routed through the fail-open switch in case of a Sensor outage.

Regardless of the Sensor and fail-open kit models, the connections remain the same. The only difference between the connections for the active and the passive fail-open kits is that you must connect the switch to the Sensor control ports in a passive fail-open deployment.

If you are using an active fail-open kit, you will require four cables in all.

Figure 268. Active fail-open switch connections

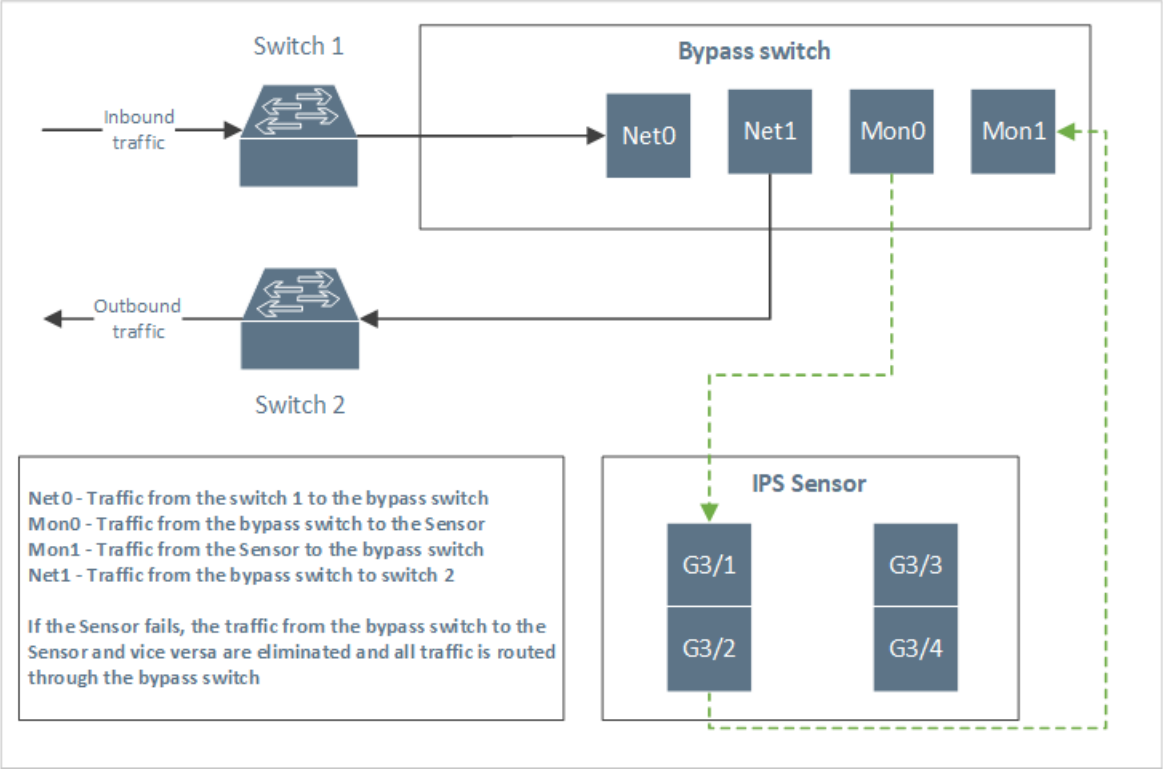
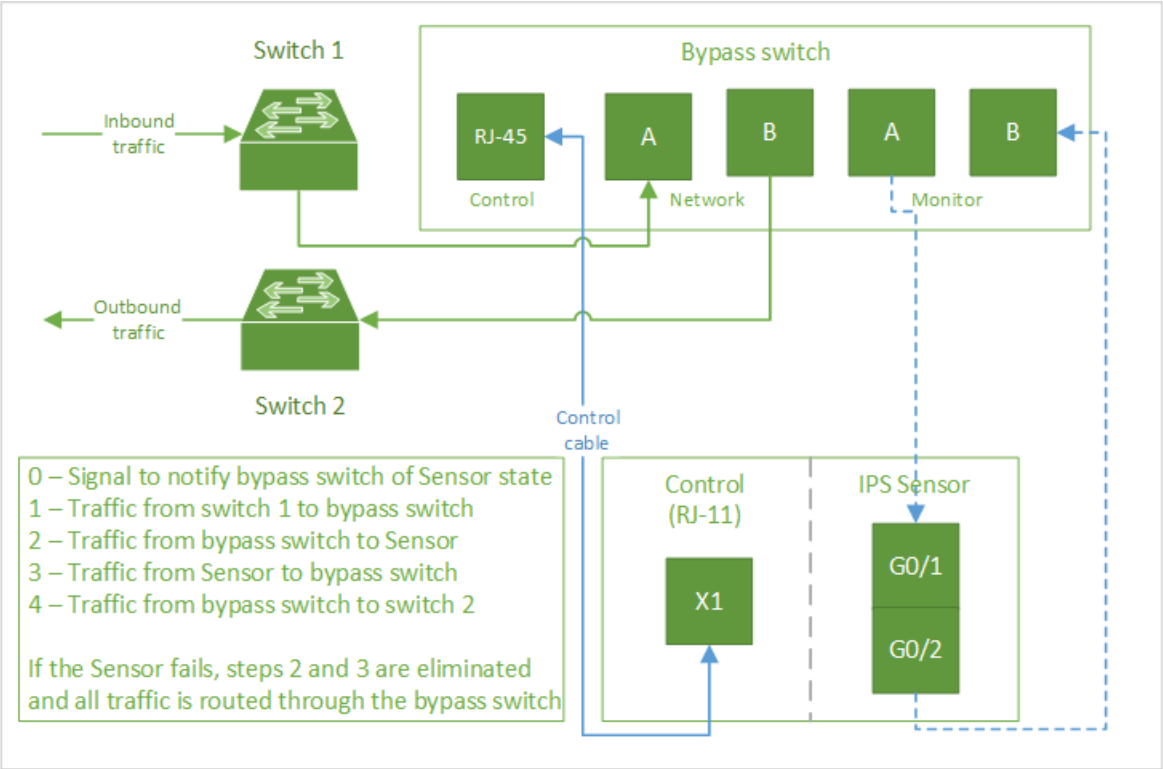


Figure 269. Passive fail-open switch connections



If you are using a passive fail-open kit, you will require five cables. One of these cables is the RJ-45 to RJ-11 cable which is used to connect the Console port in the fail-open switch with the Monitor port in the Sensor.

You require the RS-232 cable and RJ-45 cable if you plan to configure the SNMP manager.

1. If you are connecting a passive fail-open switch, connect the RJ-11 connector of the Control cable to the Control port of the fail-open switch and the RJ-45 connector of the Control cable to a Control port on the Sensor (X2 in the illustration). If you are connecting an active fail-open switch, proceed to step 3.

   This cable is used to transport control signals from the Sensor to the fail-open switch. When the fail-open switch does not receive four consecutive control signals (about 4 seconds), it changes to bypass mode.

   NOTE

   Each Sensor Control port is used in conjunction with a corresponding port pair.

2. Connect the GBIC port or RJ-45 port on your network device to Network Port A of the fail-open switch.
3. Insert QSFP+ into each of the slots of one of the unused port pairs on your Sensor. We will use port pair G0/1-G0/2 for this illustration.
4. Connect **Monitor** port **A** on the fail-open switch to port **G0/1** on the Sensor.
5. Connect **Monitor** port **B** on the fail-open switch to port **G0/2** on the Sensor.
6. Connect the network device that carries traffic into the network to **Network** port **B** on the fail-open switch.

This completes the connections between the Sensor and fail-open switch. The link lights may not come on as yet if the Sensor has not yet been deployed inline.

5. Deploy a Sensor in inline Active Fail-Open mode

Prerequisites:

- The Sensor must be set up and have established trust with a Manager server.
- The Sensor has a free port pair which can be deployed in inline Active Fail-Open mode.
- It is assumed that you have inserted necessary transceiver modules into the Sensor if you have completed cabling the Sensor and Active Fail-Open module.

To configure a fail-open switch you must configure the port pair to operate as an inline fail-open port.

1. After cabling the Sensor and the fail-open switch, log on to your Manager.
2. Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Physical Ports**.
3. Double-click port one of the configurable ports, say **2/1** (Gx/1).

   A configuration panel appears on the right side of the window.
4. Click the **State** drop-down and select **Enabled**.

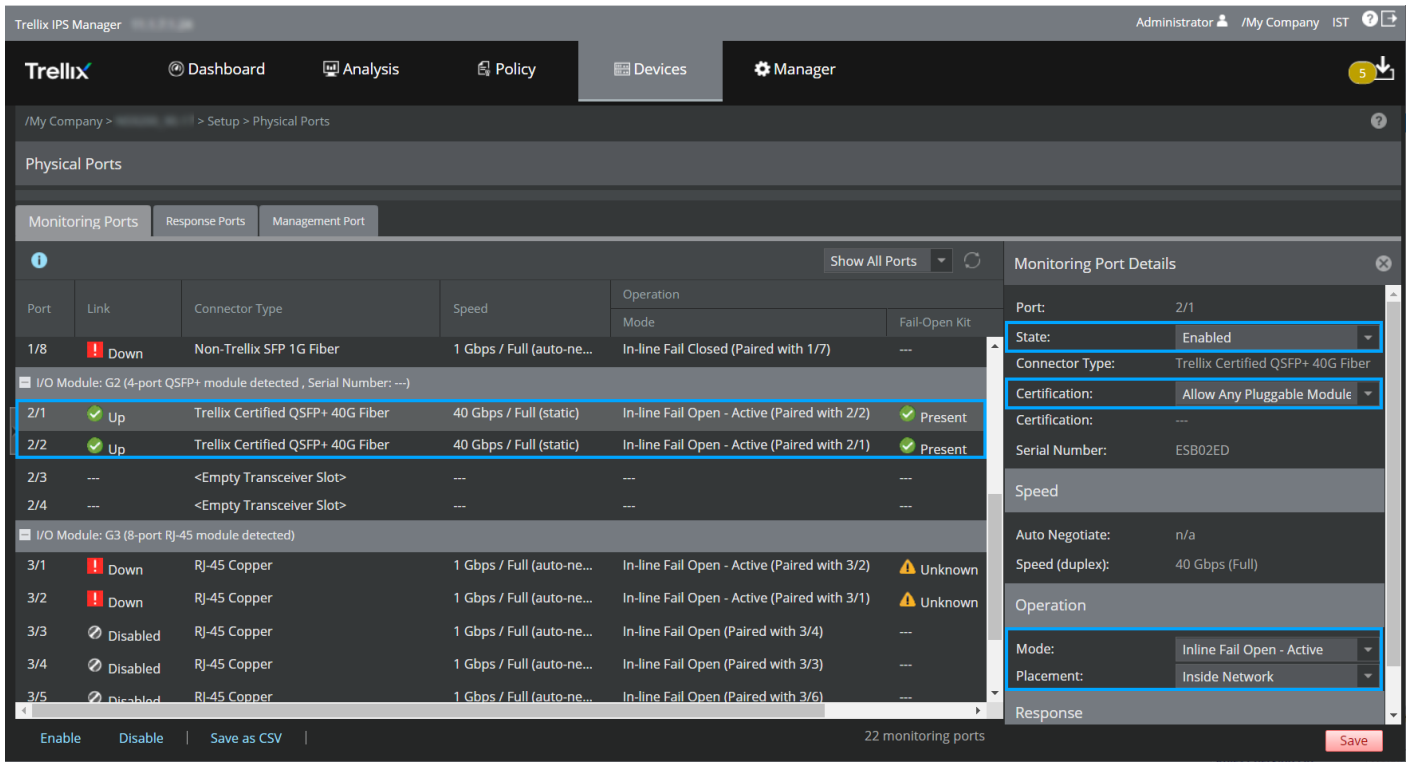
   This will impact the port 2/2 (Gx/2) as well. So, ports **2/1-2/2** (Gx/1-Gx/2) are enabled.
5. Click the **Certification** drop-down and select an option depending on your requirement.

   > **NOTE**
   >
   > Based on the I/O module and port selected, you may be required to select the **Auto Negotiate** checkbox and set the speed under **Maximum Negotiable Speed (Duplex)**. For certain ports, the speed is automatically selected and you will not be able to edit it.
6. Click the **Mode** drop-down and select **Inline Fail Open – Active**.

   This means port pair 2/1-2/2 is now configured for inline fail-open.
7. Under **Placement**, select **Inside Network** or **Outside Network** from the drop-down list, depending on how you want to configure your ports.

   Placement refers to the area of the network which that individual port is connected.

Figure 270. Configuration of a port pair for inline fail-open active operation



8. Click **Save**.

> **NOTE**
>
> An **Alert!** pop-up displays stating the changes made on port x/1 impacts x/2 as well. Click **OK**.

If traffic is passing through the ports, you will notice the port link status changes to **Up** and goes green.

6. Use the Web Manager to configure the fail-open switch

Besides using CLI commands, you can view and configure fail-open switch settings for an active fail-open switch through a web console called the Web Manager. You can restrict or permit access to the Web Manager depending on your preferences.

The web interface for fail-open switch model1 allows you to manage the following functions:

- Configuration of general fail-open switch parameters, such as IPv4 address, subnet mask, and gateway IPv4 address.
- Enabling tap mode for the fail-open switch
- Returning from tap mode to inline mode
- Configuration of notifications through SNMP traps

Follow these steps to access the Web Manager.

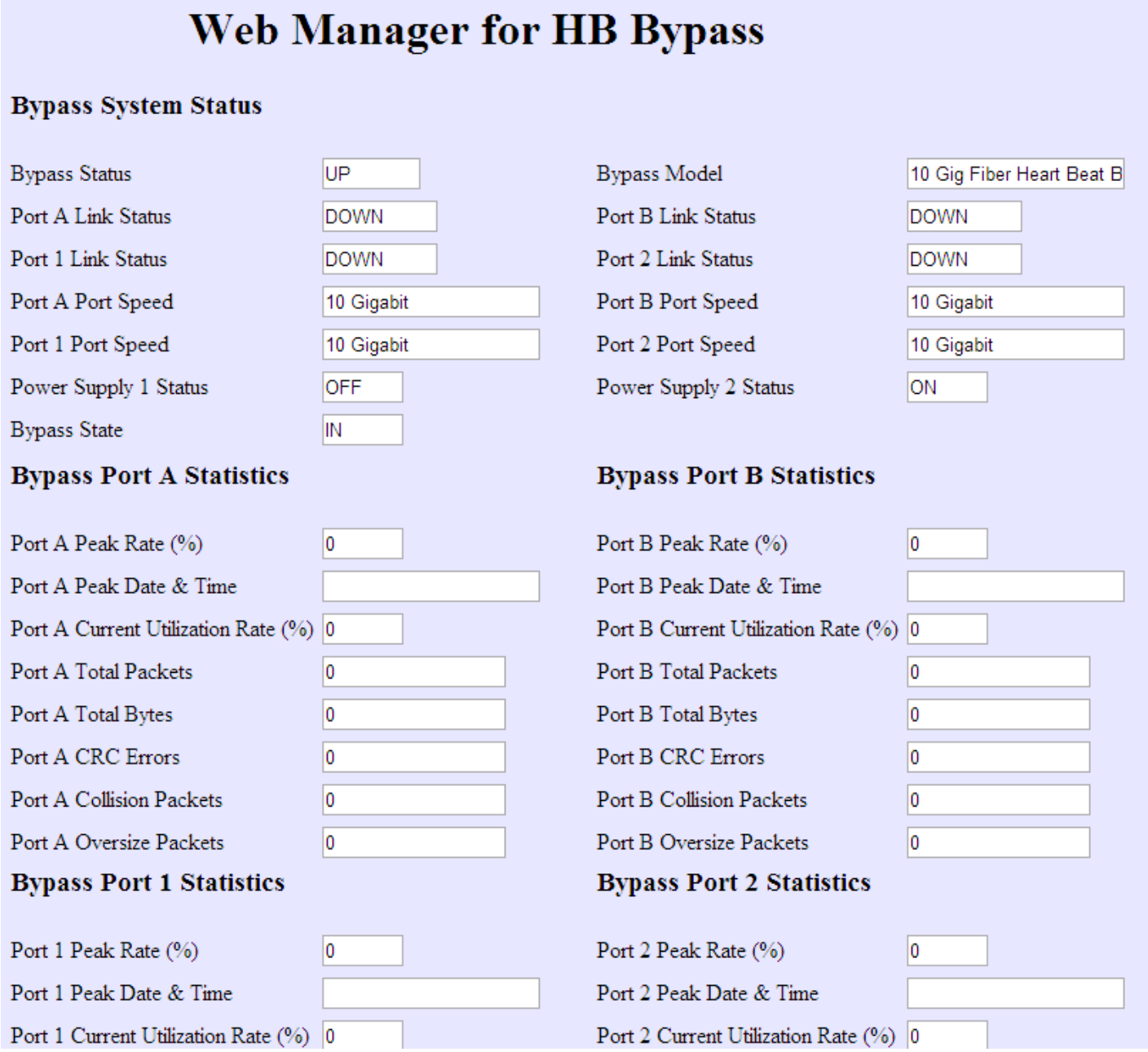
1. Open a browser such as Internet Explorer or Mozilla Firefox.
2. In the address bar, enter the fail-open switch IP address.

   You will be prompted for the username and password.

3. Enter the username and password. The default username and password are **`Trellix`**.
4. Submit credentials.

The Web Manager appears where you can modify the fail-open switch parameters.

Figure 271. Web Manager page - Upper half



Web Manager for HB Bypass

Bypass System Status

Bypass Status	UP	Bypass Model	10 Gig Fiber Heart Beat B
Port A Link Status	DOWN	Port B Link Status	DOWN
Port 1 Link Status	DOWN	Port 2 Link Status	DOWN
Port A Port Speed	10 Gigabit	Port B Port Speed	10 Gigabit
Port 1 Port Speed	10 Gigabit	Port 2 Port Speed	10 Gigabit
Power Supply 1 Status	OFF	Power Supply 2 Status	ON
Bypass State	IN		

Bypass Port A Statistics

Bypass Port B Statistics

Port A Peak Rate (%)	0	Port B Peak Rate (%)	0
Port A Peak Date & Time		Port B Peak Date & Time	
Port A Current Utilization Rate (%)	0	Port B Current Utilization Rate (%)	0
Port A Total Packets	0	Port B Total Packets	0
Port A Total Bytes	0	Port B Total Bytes	0
Port A CRC Errors	0	Port B CRC Errors	0
Port A Collision Packets	0	Port B Collision Packets	0
Port A Oversize Packets	0	Port B Oversize Packets	0

Bypass Port 1 Statistics

Bypass Port 2 Statistics

Port 1 Peak Rate (%)	0	Port 2 Peak Rate (%)	0
Port 1 Peak Date & Time		Port 2 Peak Date & Time	
Port 1 Current Utilization Rate (%)	0	Port 2 Current Utilization Rate (%)	0

Configure fail-open kits 6 thru 10

Prerequisites:

For each fail-open configuration, you will need to make sure you have all these components.

- Determine the IP address for the fail-open switch or, if you are deploying multiple switches, a range of IP addresses
- Determine a network mask and the default gateway for the fail-open switch
- 4 cables to connect the fail-open switch and the Sensor
- An RJ-11 RS232 cable to access the fail-open switch CLI
- 2 SFP, SFP+, or RJ-45 cables for NS3x00, NS5x00, NS7x00, NS9x00 Sensors
- Cables for a copper fail-open switch
  - 2 CAT5e cables (1 cross-over, 1 straight-through) for network ports
  - 2 CAT5e cables (straight-through) for monitor ports
- Cables for a fiber fail-open switch
  - 2 LC fiber cables for network ports
  - 2 LC fiber cables for monitor ports

Broadly, these are the steps you will need to follow to set up a fail-open kit.

1. Install the fail-open switch module in the chassis

Prerequisite: Identify the rack in which you plan to install the fail-open chassis.

Perform the following steps to install the fail-open switch modules 6 thru 10 in the fail-open chassis (model 11). You can install up to four fail-open switches in a single chassis. If you are installing fail-open switch model 1, refer to the section, 1. (Models 1 thru 13) Install the fail-open switch (page 659).

1. Install the ears of the chassis.

2. Slide the switch into one of the openings in the chassis, until the faceplate of the switch rests against the chassis.
3. Secure the switch to the chassis by inserting screws provided through the holes on the fail-open switch faceplate and into the panel.
4. Place the 1U chassis against the front of a standard 19-inch rack.

5. Secure the chassis by inserting screws through holes on ears of the chassis.
6. (Optional) Install up to three additional switches by following these steps:
   a. Remove screws holding each of the removable blank plates from the front of the chassis.
   b. Perform steps 2 and 3 for installing a switch in the chassis for additional fail-open switches.

2. Remove an active fail-open switch from the chassis

Prerequisite: You must make sure the fail-open switch is fully powered off before you attempt to remove it from the chassis.

Follow the steps in this section to power off and remove the fail-open switch.

1. Power off the fail-open switch using the web interface or CLI command prompt.
   - If you are using the web interface, click the **Rescue** tab and check the **Power Off** checkbox in the **System Restore** section. To access the web interface, refer Access the fail-open switch web interface (page 675).

   - If you are using the CLI command prompt, type **`power_off`** and press **Enter**. To access the CLI command prompt, refer 3. Configure fail-open switch parameters_Silicom (page 668).
2. When the fail-open switch is powered off, remove the captive screws and slide it out of the chassis.

3. Configure fail-open switch parameters

Prerequisites:

To proceed with the setup, you will require:

- One RJ-11 RS-232 cable
- One RJ-45 cable

Perform the following steps to configure the parameters of the fail-open switch.

1. Connect the applicable cables to the fail-open switch.
2. Connect the other end to a computer which runs a terminal emulation software such as HyperTerminal or PuTTY.
3. Launch the terminal emulation software, and set the communications parameters as shown below:
   - Baud rate: 9600
   - Data bits: 8
   - No parity
   - Stop bits: 1
   - No flow control
4. Turn on the fail-open switch.

   The CLI banner and login prompt are displayed.
5. At the login prompt, type the username and password, and press **Enter**.

Table 36. Username and password for both sets of fail-open switches

For fail-open switches 6 thru 10	
Username	**Trellix00**
Password	**Trellix00**

The fail-open switch CLI prompt is displayed.

6. Use these commands for fail-open switch models 6 thru 10.

Table 37. CLI commands for fail-open switch models 6 thru 10

Command	Description
set_ip xxx.xxx.xxx.xxx	Configures fail-open switch IPv4 address. Reboot the fail-open switch for the new IPv4 address to take effect.
get_ip	Displays fail-open switch IPv4 address.
set_netmask xxx.xxx.xxx.xxx	Configures fail-open switch subnet mask. Reboot the fail-open switch for the new subnet mask to take effect.
get_netmask	Displays fail-open switch subnet mask.
set_gateway xxx.xxx.xxx.xxx	Configures default gateway IPv4 address. Reboot the fail-open switch for the new gateway IPv4 address to take effect.
get_gateway	Displays default gateway address.

Command	Description
set_link <port> <on/off>	Sets the port of a 1G Copper fail-open switch to auto-negotiate. For the **<port>** use **mon0**, **mon1**, **net0**, or **net1**.
get_link <port>	Displays port status. For the **<port>** use **mon0**, **mon1**, **net0**, or **net1**.
set_link <port> off fd 100m	Sets the port to 100 Mbps full-duplex. For the **<port>**, use the syntaxes specified above.
set_link <port> <enable/disable>_autoneg	Sets the port of a 1G Fiber fail-open switch to auto-negotiate. For the **<port>** use **mon0**, **mon1**, **net0**, or **net1**. **NOTE** 10G Fiber fail-open switches do not have such a command since auto-negotiate is enabled by default.
set_ssh_state <on/off>	Enables or disables the SSH status on the fail-open switch.
get_ssh_state	Displays the SSH status, which is enabled by default.
set_web_https_state <on/off>	Enables or disables web access to the fail-open switch interface.
get_web_https_state	Displays status of web access to the fail-open switch interface.
set_snmp_srv_ip	Configures SNMP server IPv4 address. The SNMP server IPv4 address can also be set in the web interface.
get_snmp_srv_ip	Displays the SNMP server IPv4 address.
set_trap <parameter> <on/off>	Enables or disables the following SNMP traps: • **appl fail** – Application state change. • **bypass** – Bypass state change trap. • **mon link** – Monitoring port state change trap. • **net link** – Network port state change trap. • **error** – Error notification trap. • **update** – Update complete trap.
get_stat	Displays the statistics of the fail-open switch.
get_params	Displays fail-open switch parameters.
stop_all_sessions	Stops all opened sessions

4. (Optional) Configure notification by SNMP traps

Prerequisites:

- To configure SNMP traps, you will require a server that acts as an SNMP server. The SNMP server can be any Windows or Linux system installed with a MIB browser, such as iReasoning. To view requirements and download a copy of iReasoning MIB browser, follow the link:https://ireasoning.com/mibbrowser.html.
- Make sure your fail-open switch IP address can be reached within the network.
- Make sure your SNMP server and fail-open switch are able to communicate.
- In addition, you will need to obtain MIB files to decode alert codes sent by the fail-open switch. These files are specific to the fail-open switch and can be obtained by clicking this link: KB86247.
- You will require the RJ-45 cable.

1. Connect an RJ-45 cable to the Management Port at the front of the fail-open switch.
2. Connect the other end to a network device so that the SNMP server is reachable through the network.
3. Copy the fail-open switch MIB files to a suitable location on the SNMP server.

   For example, an SNMP trap is generated when one of the following events occur:

   - Bypass state changes
   - Any port link status changes
   - Either power supply state changes
4. Set up the fail-open switch IP address, network mask, and SNMP manager IP address using the commands provided in the section [Configure the fail-open switch parameters].
5. Make sure the SNMP manager and fail-open switch are able to communicate.

Configuration of SNMP traps is complete when you can see a trap appear in the MIB browser.

5. Connect the switch to an inline Sensor

After you have secured the fail-open switch in its rack, use copper or fiber connecting cables to connect the switch with the Sensor. The underlying principle in connecting these cables is to connect the Sensor and the switch such that traffic gets routed through the fail-open switch in case of a Sensor outage.

Regardless of the Sensor and fail-open kit models, the connections remain the same. The only difference between the connections for the active and the passive fail-open kits is that you must connect the switch to the Sensor control ports in a passive fail-open deployment.

If you are using a fail-open kit, you will require four cables in all.

Figure 272. Active fail-open switch connections

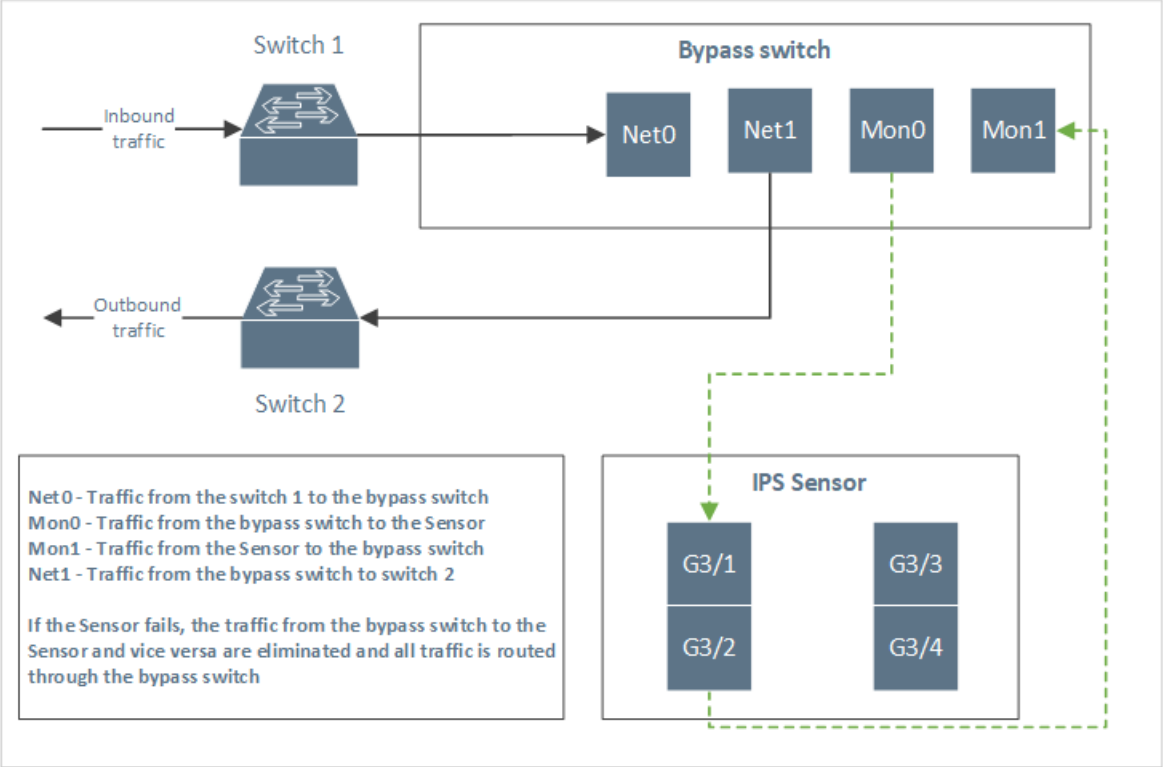
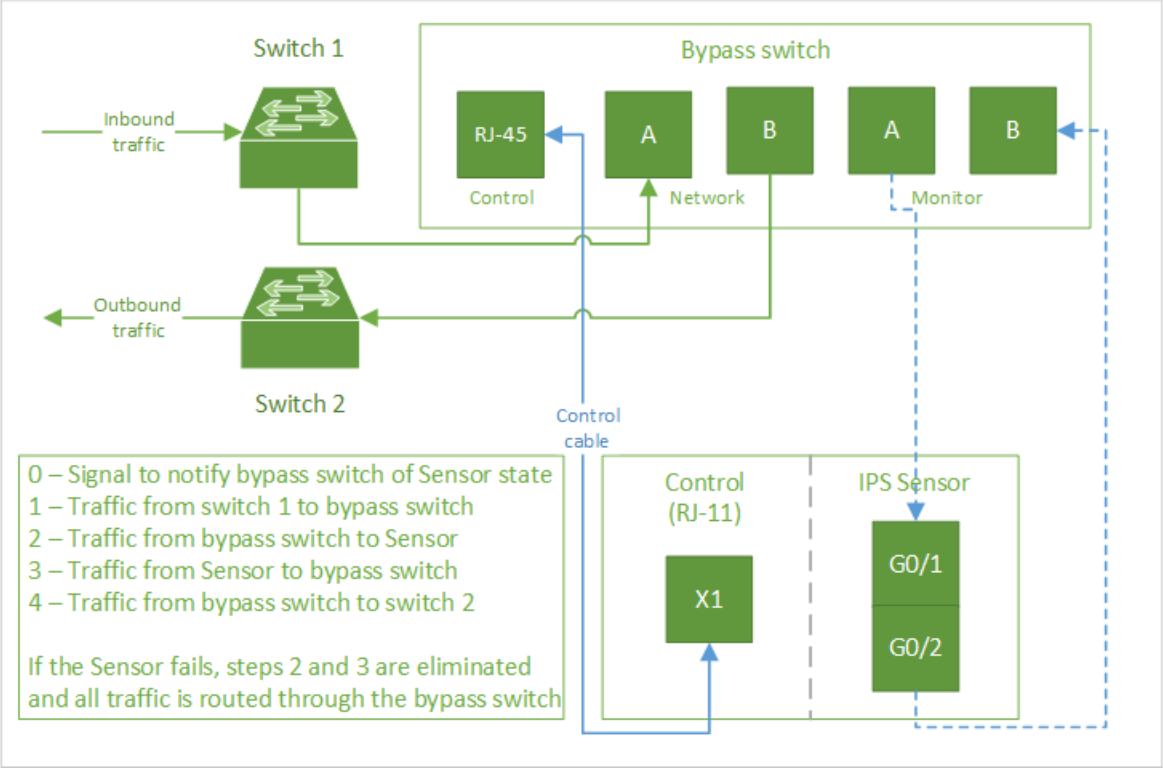


Figure 273. Passive fail-open switch connections



If you are using a passive fail-open kit, you will require five cables. One of these cables is the RJ-45 to RJ-11 cable which is used to connect the Console port in the fail-open switch with the Monitor port in the Sensor.

You require the RS-232 cable and RJ-45 cable if you plan to configure the SNMP manager.

1. If you are connecting a passive fail-open switch, connect the RJ-45 connector of the Control cable to the Control port of the fail-open switch and the RJ-11 connector of the Control cable to a Control port on the Sensor (X1 in the illustration). If you are connecting a fail-open switch, proceed to step 3.

   This cable is used to transport control signals from the Sensor to the fail-open switch. When the fail-open switch does not receive four consecutive control signals (about 4 seconds), it changes to bypass mode.

   > **NOTE**
   >
   > Each Sensor Control port is used in conjunction with a corresponding port pair.

2. Connect the GBIC port or RJ-45 port on your network device to **Network** port **A (passive)**/ **Net0 (active)** of the fail-open switch.
3. Insert SFP, SFP+, or RJ-45 (depending on your Sensor model) into each of the slots of one of the unused port pairs on your Sensor. We will use port pair G0/1-G0/2 for this illustration.
4. Connect **Monitor** port **A (passive)** / **Mon0 (active)** on the fail-open switch to port **G0/1** on the Sensor.
5. Connect **Monitor** port **B (passive)** / **Mon1 (active)** on the fail-open switch to port **G0/2** on the Sensor.
6. Connect the network device that carries traffic into the network to **Network** port **B (passive)** / **Net1 (active)** on the fail-open switch.

This completes the connections between the Sensor and fail-open switch. The link lights may not come on as yet if the Sensor has not yet been deployed inline.

6. Deploy a Sensor in inline Active Fail-Open mode

Prerequisites:

- The Sensor must be set up and have established trust with a Manager server.
- The Sensor has a free port pair which can be deployed in inline Active Fail-Open mode.
- It is assumed that you have inserted necessary transceiver modules into the Sensor if you have completed cabling the Sensor and Active Fail-Open module.

To configure a fail-open switch you must configure the port pair to operate as an inline fail-open port.

1. After cabling the Sensor and the fail-open switch, log on to your Manager.
2. Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Physical Ports**.
3. Double-click port one of the configurable ports, say **1/1** (Gx/1).

   A configuration panel appears on the right side of the window.
4. Click the **State** drop-down and select **Enabled**.

   This will impact the port 1/2 (Gx/2) as well. So, ports **1/1-1/2** (Gx/1-Gx/2) are enabled.
5. Click the **Certification** drop-down and select an option depending on your requirement.

NOTE

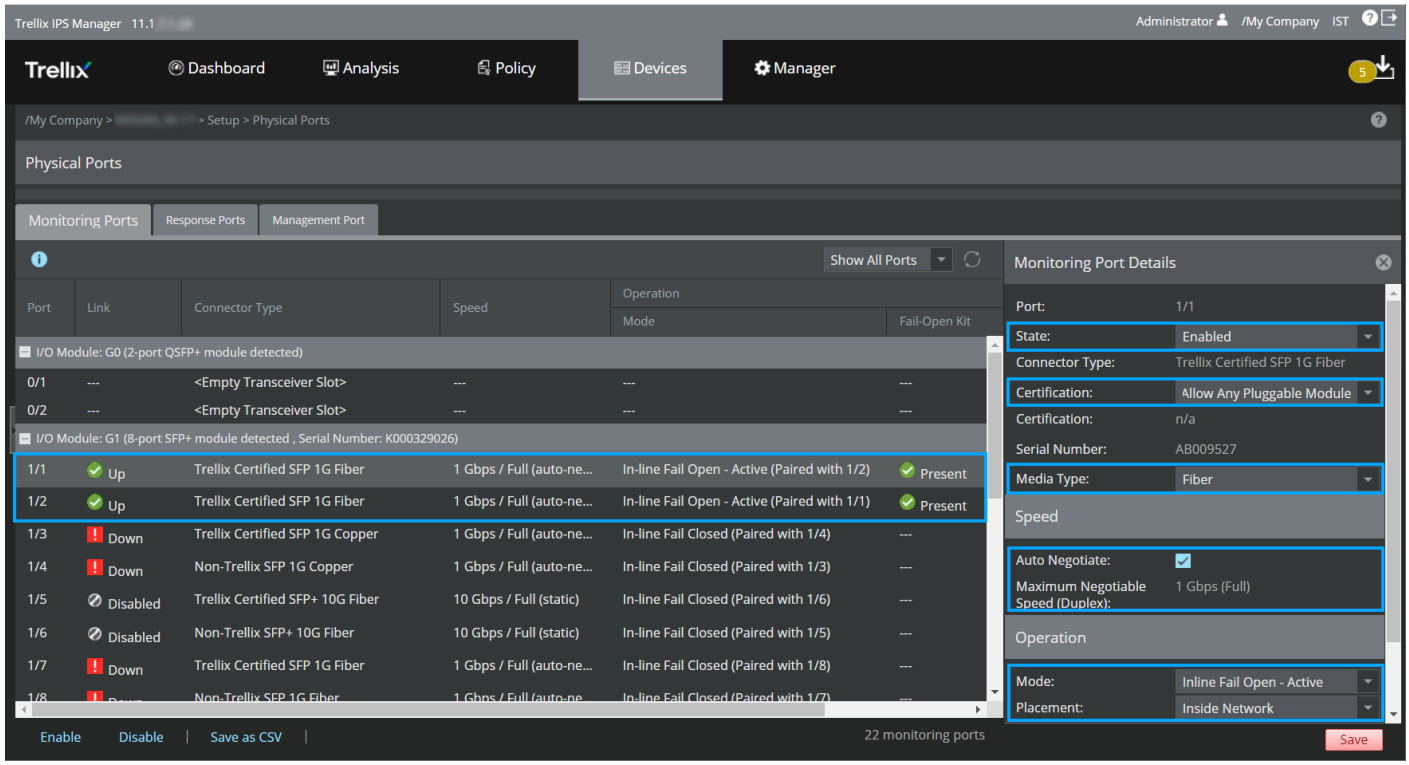
Based on the I/O module and port selected, you may be required to select the **Auto Negotiate** checkbox and set the speed under **Maximum Negotiable Speed (Duplex)**. For certain ports, the speed is automatically selected and you will not be able to edit it.

6. Click the **Media Type** drop-down and select **Copper** or **Fiber** depending on the cable type you are using.
7. Click the **Mode** drop-down and select **Inline Fail Open – Active**.

   This means port pair 1/1-1/2 is now configured for inline fail-open.
8. Under **Placement**, select **Inside Network** or **Outside Network** from the drop-down list, depending on how you want to configure your ports.

   Placement refers to the area of the network which that individual port is connected.

Figure 274. Configuration of a port pair for inline fail-open active operation



9. Click **Save**.

NOTE

An **Alert!** pop-up displays stating the changes made on port x/1 impacts x/2 as well. Click **OK**.

If traffic is passing through the ports, you will notice the port link status changes to **Up** and goes green.

7. Use the web interface to configure the fail-open switch

Besides using CLI commands, you can view and configure the fail-open switch settings for a fail-open switch through a web console.

The web interface for fail-open switch models 6 thru 10 allows you to manage the following functions:

- Configuration of general fail-open switch parameters, such as IPv4 address, subnet mask, and gateway IPv4 address
- Enabling tap mode for the fail-open switch
- Returning from tap mode to inline mode
- Configuration of notifications through SNMP traps

The next section explains the steps for each of these management options.

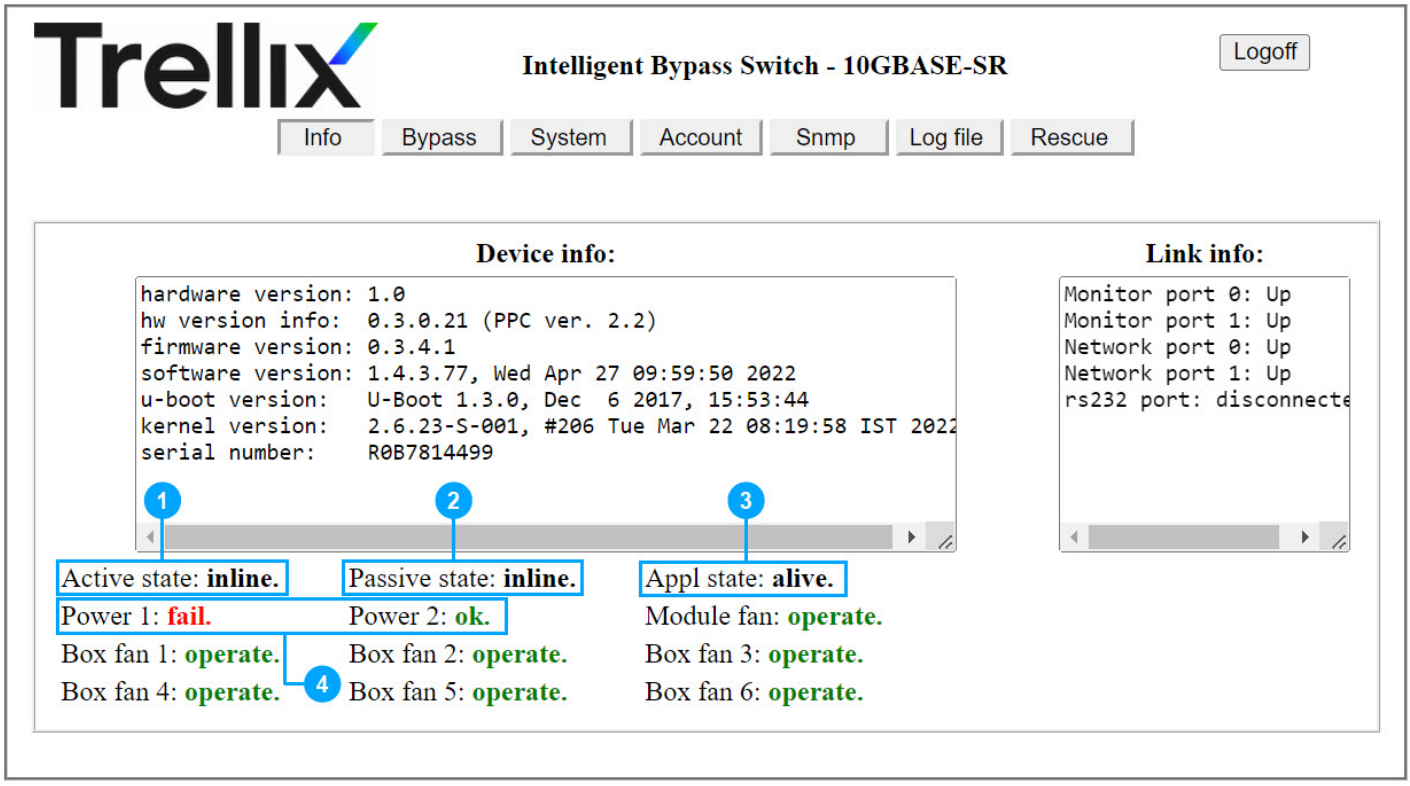
Access the fail-open switch web interface

If you have configured an IPv4 address for your fail-open switch, you have the option to manage it through a web-interface.

1. To access the fail-open switch web interface, enter the IPv4 address of the fail-open switch which you have configured.

   The fail-open switch web interface appears on the login screen.
2. To log on, enter the default username and password, **`Trellix00`** and **`Trellix00`**.

You are routed to the fail-open web interface landing page which shows you information about the present settings configured in the fail-open switch. Configuration of necessary settings is explained in the relevant sections.



Callout	Description
1	Active state of the fail-open switch: • Inline - Sensor receives traffic and the fail-open switch is operating in normal mode • Bypass - Sensor does not receive traffic and the fail-open switch is not operating in inline mode • Tap - Fail-open switch functioning like a TAP kit
2	Passive state of the fail-open switch: • Inline - Fail-open switch operating in normal mode • Bypass - Sensor does not receive traffic and the fail-open switch is not operating in inline mode
3	Appl (Application) state of the fail-open switch: • Active - Monitoring ports are up and the heartbeat packets are received • Fail - Monitoring ports are up, but the heartbeat packets are not received • Unknown - Monitoring ports are down
4	Power status of the fail-open switch: • Fail - No power provided to the power supply or faulty power supply • Ok - The power supply is normal

Enable tap mode for the fail-open switch

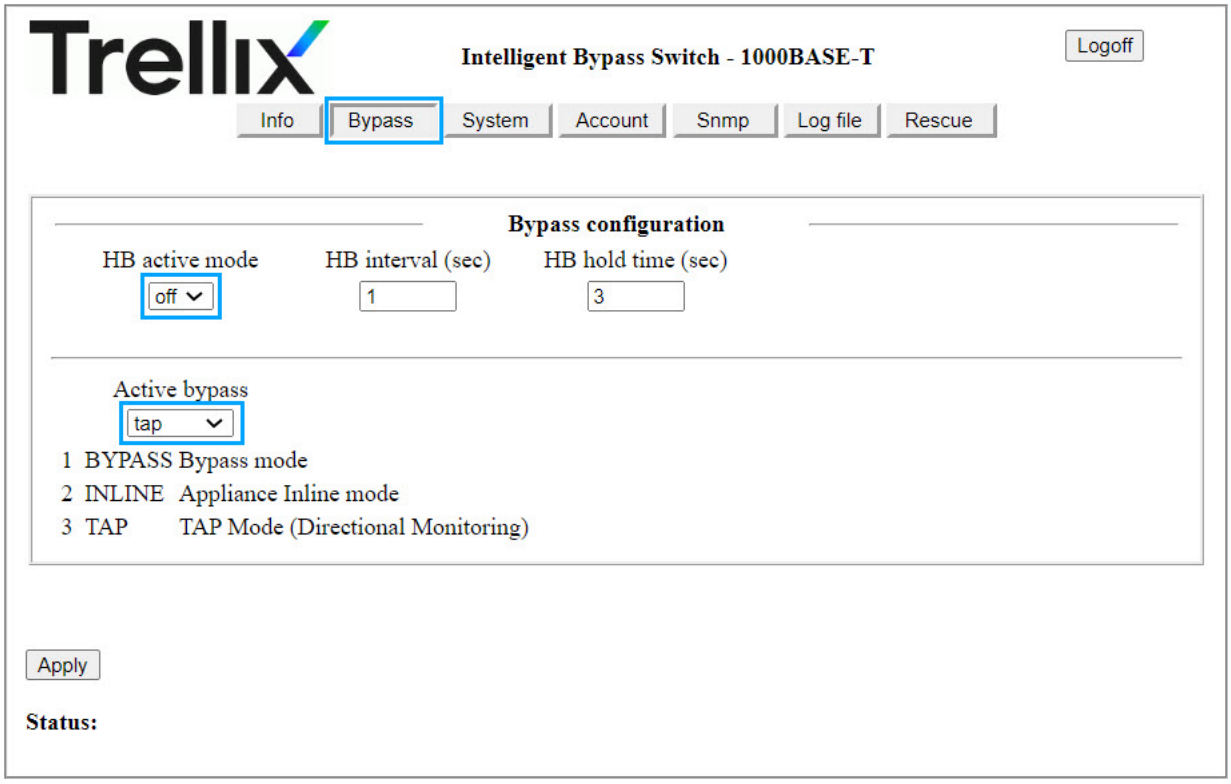
Prerequisites:

- Configure an IPv4 address for your fail-open switch.
- Make sure you are able to access the fail-open switch web-interface using a web browser.

You can enable tap mode for your fail-open switch if you use a tap to route network traffic to the Sensor monitoring ports.

1. Log on to the web interface of the fail-open switch.

   Use default credentials to access the web interface.
2. Click the **Bypass** tab to access the **Bypass** configuration page.
3. Under **HB active mode**, select **Off** from the drop-down list.
4. Under **Active bypass**, select **tap** from the drop-down list.



5. Click **Apply** to save your configuration.

You have set your fail-open switch to tap mode of operation.

Configure Active Fail-Open kits 12 thru 16

Prerequisites:

For each Active Fail-Open configuration, you will need to make sure you have all these components.

- Determine the IP address for the Active Fail-Open switch or, if you are deploying multiple switches, a range of IP addresses
- Determine a network mask and the default gateway for the Active Fail-Open switch
- 4 cables to connect the Active Fail-Open switch and the Sensor
- An RJ-45 RS232 cable to access the Active Fail-Open switch CLI
- QSFP+ for NS9x00 Sensors
- Cables for a fiber Active Fail-Open switch:
  - LC and MTP/MPO fiber cables for network ports
  - LC and MTP/MPO fiber cables for monitor ports

Broadly, these are the steps you will need to follow to set up an Active Fail-Open kit.

1. Install the Active Fail-Open module in the chassis

Prerequisite: Identify the rack in which you plan to install the Active Fail-Open chassis.

Perform the following steps to install the Active Fail-Open modules 12 thru 16 in the 40G Active Fail-Open chassis (model 29). You can install up to three Active Fail-Open modules in a single chassis.

1. Place the 1U chassis against the front of a standard 19-inch rack.
2. Slide the 10G/40G Active Fail-Open module into one of the three slots in the chassis, until the faceplate of the module rests against the chassis.
3. Secure the module to the chassis by inserting screws provided through the holes on the Active Fail-Open module faceplate and into the panel.
4. (Optional) Install up to three 10G/40G Active Fail-Open modules by following these steps:
   a. Remove screws holding each of the removable blank plates from the front of the chassis.
   b. Perform steps 2 and 3 for installing another module in the chassis.

RESULT_7CDDD16290104792B0C7060FBA1B86CC The Active Fail-Open module is ready to be connected to a Sensor.

2. Remove and replace the Active Fail-Open module from the chassis

Follow the steps in this section to remove and replace the Active Fail-Open module.

1. **To remove:** Slide the module out from any one of the two slots it is installed without shutting down the chassis.
2. **To replace:** Slide in the module into one of the three slots in the chassis while the power is on.

> **NOTE**
>
> If a new module is installed in the slot or a different type of module is installed from the previous ones, a chassis reboot is required to make the newly inserted module active.

3. Configure Active Fail-Open chassis parameters

Prerequisites:

To proceed with the setup, you require:

- One RJ-45 RS-232 cable for console connection.
- One RJ-45 cable for network management connection.

Perform the following steps to configure the parameters of an Active Fail-Open chassis.

1. Connect the applicable cable to the 40G Active Fail-Open chassis.
2. Connect the RJ-45 RS232 cable to a computer which runs a terminal emulation software such as HyperTerminal or PuTTY.
3. Launch the terminal emulation software and set the following communication parameters:
   - Baud rate: 115200
   - Data bits: 8
   - No parity
   - Stop bits: 1
   - No flow control
4. Turn on the Active Fail-Open chassis.

The CLI banner and login prompt are displayed.

5. At the login prompt, type the username and password, and press **Enter**.

Table 38. Username and password for both sets of Active Fail-Open modules

For Active Fail-Open switches 12 thru 14	
Username	**Trellix00**
Password	**Trellix00**

The Active Fail-Open chassis CLI prompt is displayed.

6. Use the following commands for the Active Fail-Open modules 12 thru 14.

Table 39. CLI commands for Active Fail-Open modules 12 thru 14

Command	Description
get_gateway	Displays default gateway address.
get_ip	Displays Active Fail-Open chassis IPv4 address.
get_netmask	Displays Active Fail-Open chassis network mask.
set_gateway xxx.xxx.xxx.xxx	Configures default gateway IPv4 address. Reboot the Active Fail-Open chassis for the new gateway IPv4 address to take effect.
set_ip xxx.xxx.xxx.xxx	Configures Active Fail-Open chassis IPv4 address. Reboot the Active Fail-Open chassis for the new IPv4 address to take effect.
set_netmask xxx.xxx.xxx.xxx	Configures Active Fail-Open chassis network mask. Reboot the Active Fail-Open chassis for the new network mask to take effect.
get_stat	Displays the device statistics
stop_all_sessions	Stops all opened sessions

For more information on the CLI commands, see [Trellix Intrusion Prevention System 10G/40G Active Fail-Open Bypass Kit Guide].

4. Configure notification by SNMP traps

Prerequisites:

- To configure SNMP traps, you require a server that acts as an SNMP server. The SNMP server can be any Windows or Linux system installed with a MIB browser such as iReasoning.

  To view the requirements and download a copy of iReasoning MIB browser, follow the link: https://ireasoning.com/mib-browser.html.
- Make sure the IP address of the 40G Active Fail-Open chassis can be reached within the network.
- Make sure the SNMP server and the 40G Active Fail-Open chassis are able to communicate.
- In addition, you need to obtain MIB files to decode alert codes sent by the 10G/40G Active Fail-Open modules. These files are specific to the 10G/40G Active Fail-Open modules and can be obtained by clicking this link: KB86247.

Steps:

1. Connect an RJ-45 cable to the Management port at the front of the 40G Active Fail-Open chassis.
2. Connect the other end to a network device so that the SNMP server is reachable through the network.
3. Copy the MIB files of an Active Fail-Open module to a suitable location on the SNMP server.

   For example, an SNMP trap is generated when one of the following events occur:

   - Bypass state changes
   - Any of the port link status changes
   - Either power supply state changes or any other trap defined under Snmp → **SNMP trap control** in the web interface.
4. Set up the 40G Active Fail-Open chassis IP address, network mask, and SNMP manager IP address using the commands provided in the section *3. Configure Active Fail-Open chassis parameters* (page 678).
5. Make sure the SNMP manager and Active Fail-Open chassis are able to communicate.

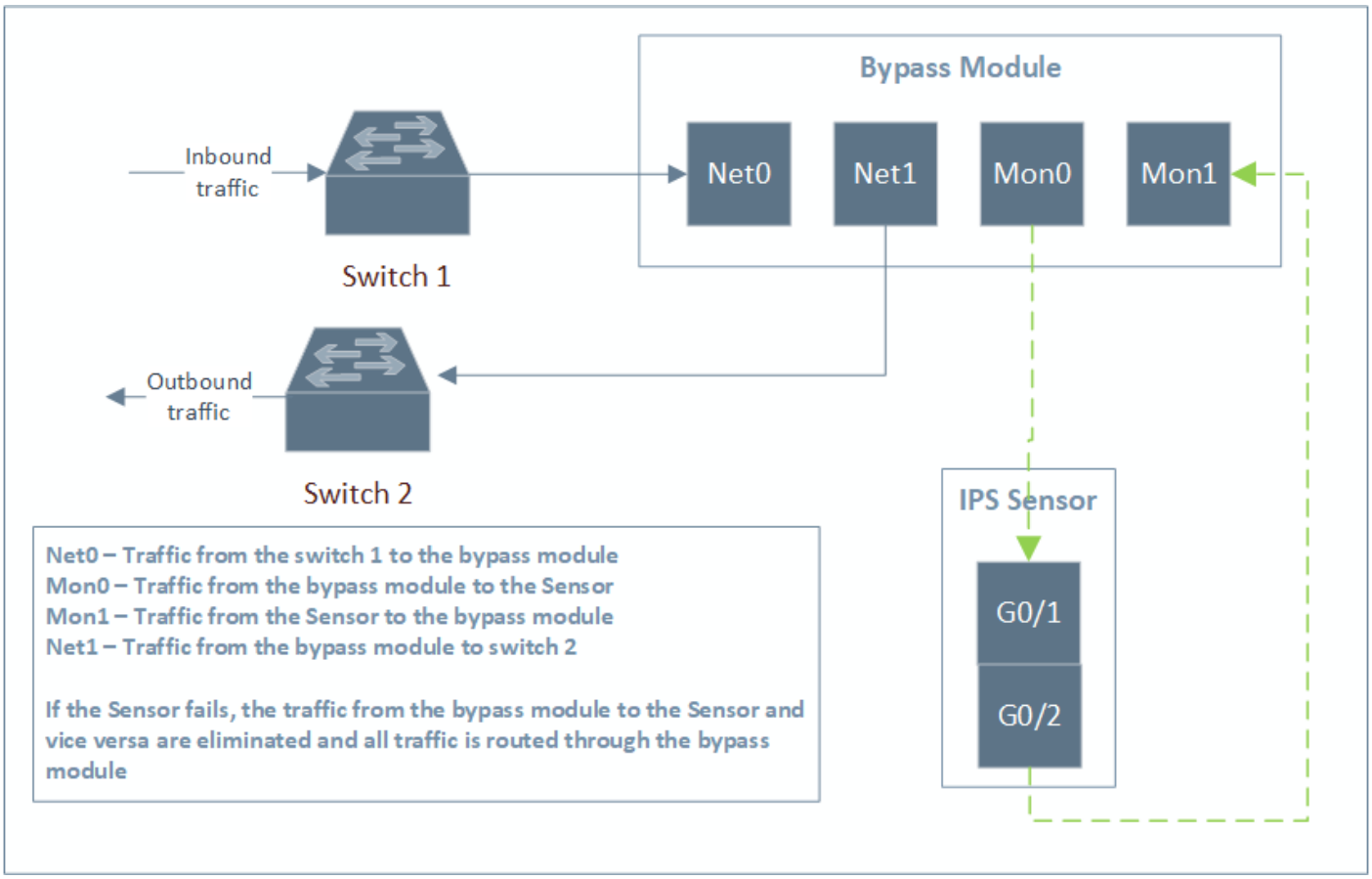
Configuration of SNMP traps is complete when a trap appears in the MIB browser.

5. Connect the module to an inline Sensor

After you have secured the Active Fail-Open module in its rack, use fiber connecting cables to connect the module with the Sensor. The underlying principle in connecting these cables is to connect the Sensor and the module so that the traffic gets routed through the Active Fail-Open module if there was a Sensor outage.

Regardless of the Sensor and Active Fail-Open module type, the connections remain the same.

Figure 275. Active Fail-Open module connections



1. Connect the port on your network device (Switch 1) to **Net0 (active)** of the Active Fail-Open module.
2. Insert a SFP+/QSFP+ into each of the slots of the unused 10G/40G port pairs on your Sensor. We use port pair G0/1-G0/2 for this illustration.
3. Connect the port **Mon0 (active)** on the Active Fail-Open module to port **G0/1** on the Sensor.
4. Connect the port **Mon1 (active)** on the Active Fail-Open module to port **G0/2** on the Sensor.
5. Connect the port **Net1 (active)** on the Active Fail-Open module to the port on the other network device (Switch 2).

This completes the connections between the Sensor and Active Fail-Open module. The link lights might not be up if the Sensor is not yet deployed in inline mode.

6. Deploy a Sensor in inline Active Fail-Open mode

Prerequisites:

- The Sensor must be set up and have established trust with a Manager server.
- The Sensor has a free port pair which can be deployed in inline Active Fail-Open mode.
- It is assumed that you have inserted necessary transceiver modules into the Sensor if you have completed cabling the Sensor and Active Fail-Open module.

When you set up a Sensor for the first time, its ports are disabled by default. The Sensor ports must be manually configured for inline Active Fail-Open operation.

1. After cabling the Sensor and the fail-open switch, log on to your Manager.
2. Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Physical Ports**.
3. Double-click port one of the configurable ports, say **2/1** (Gx/1).

   A configuration panel appears on the right side of the window.
4. Click the **State** drop-down and select **Enabled**.

   This will impact the port 2/2 (Gx/2) as well. So, ports **2/1-2/2** (Gx/1-Gx/2) are enabled.
5. Click the **Certification** drop-down and select an option depending on your requirement.

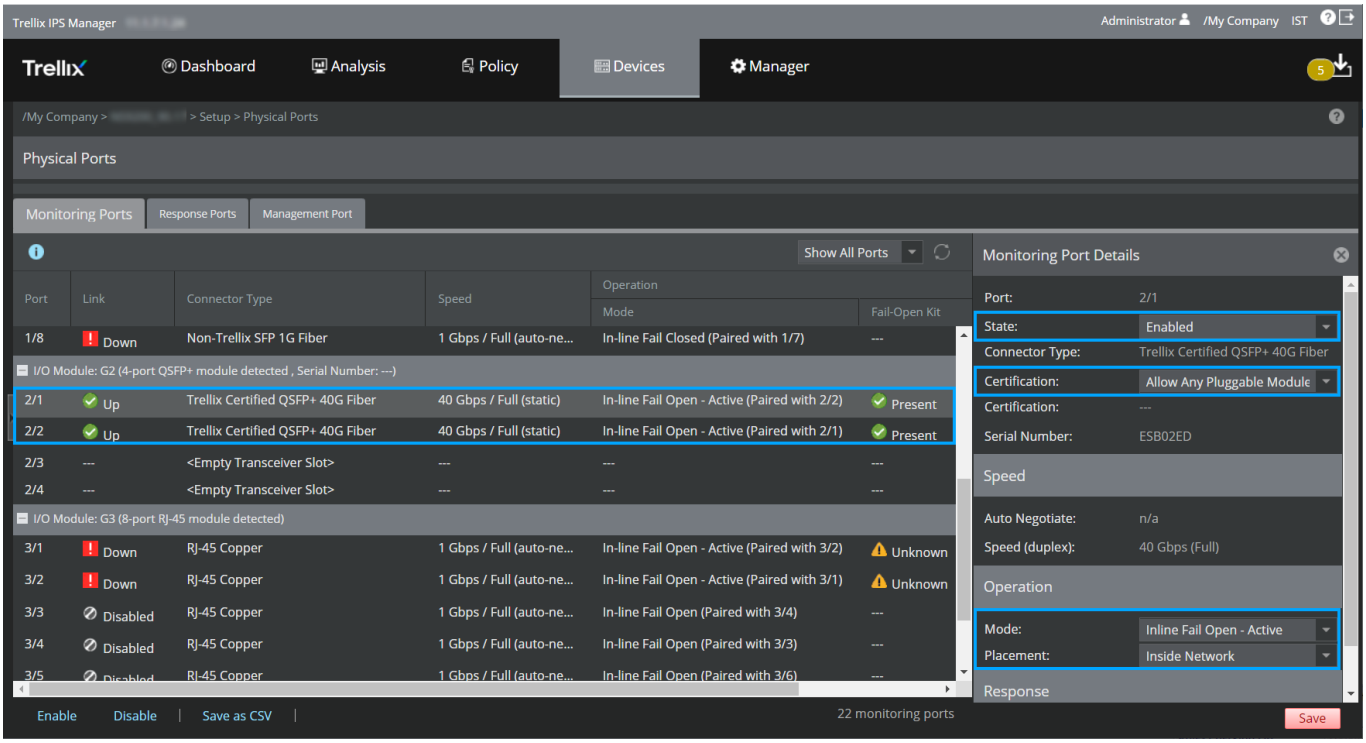
> **NOTE**
>
> Based on the I/O module and port selected, you may be required to select the **Auto Negotiate** checkbox and set the speed under **Maximum Negotiable Speed (Duplex)**. For certain ports, the speed is automatically selected and you will not be able to edit it.

6. Click the **Mode** drop-down and select **Inline Fail Open – Active**.

   This means port pair 2/1-2/2 is now configured for inline fail-open.
7. Under **Placement**, select **Inside Network** or **Outside Network** from the drop-down list, depending on how you want to configure your ports.

   Placement refers to the area of the network which that individual port is connected.

Figure 276. Configuration of a port pair for inline fail-open active operation



8. Click **Save**.

> **NOTE**
>
> An **Alert!** pop-up displays stating the changes made on port x/1 impacts x/2 as well. Click **OK**.

The Sensor and Active Fail-Open module are set up. When traffic passes through the ports, the port link status changes to **Up** and turns green.

7. Use the web interface to configure the Active Fail-Open module

Besides using CLI commands, you can view and configure Active Fail-Open module settings for the Active Fail-Open chassis through a web console.

The web interface for Active Fail-Open modules 12 thru 14 allows you to manage the following functions:

- Enabling bypass/tap mode for the Active Fail-Open module
- Returning from bypass/tap mode to inline mode
- Configuration of notifications through SNMP traps

The next section explains the steps for each of these management options.

Access the Active Fail-Open module web interface

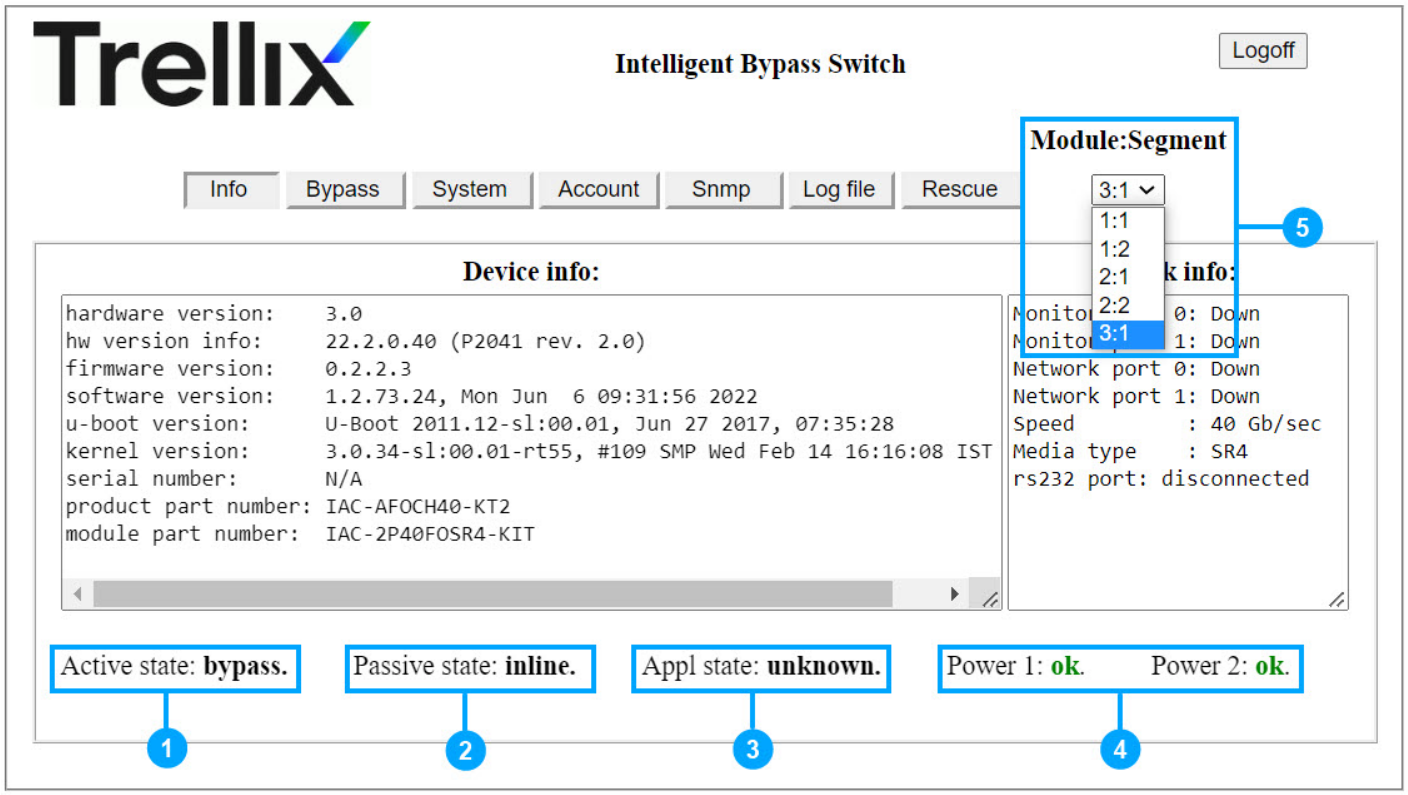
If you have configured an IPv4 address for your Active Fail-Open chassis, you have the option to manage it through a web interface.

Steps:

1. To access the Active Fail-Open module web interface, enter the IPv4 address of the Active Fail-Open chassis which you have configured through **https://x.x.x.x.**

   The Active Fail-Open module web interface appears on the login screen.
2. To log in, enter the default username and password, **`Trellix00`** and **`Trellix00`**.

You are routed to the Active Fail-Open web interface landing page which shows you information about the present settings configured in the Active Fail-Open module. Configuration of necessary settings is explained in the relevant sections.



Callout	Description
1	Active State: • Inline - Sensor receives traffic and the fail-open module is operating in normal mode • Bypass - Sensor does not receive traffic and the fail-open module is not operating in inline mode • Tap - Fail-open module functioning like a TAP kit
2	Passive State: • Inline - Fail-open module operating in normal mode • Bypass - Sensor does not receive traffic and the fail-open module is not operating in inline mode
3	Appl (Application) state: • Active - Monitoring ports are up and the heartbeat packets are received • Fail - Monitoring ports are up, but the heartbeat packets are not received • Unknown - Monitoring ports are down
4	Power status: • Fail - No power provided to the power supply • Ok - The power supply is normal
5	The 40G Active Fail-Open chassis consists of 3 modules. Select the module from the **Module: Segment** drop-down list.

Enable tap/inline mode for the Active Fail-Open module

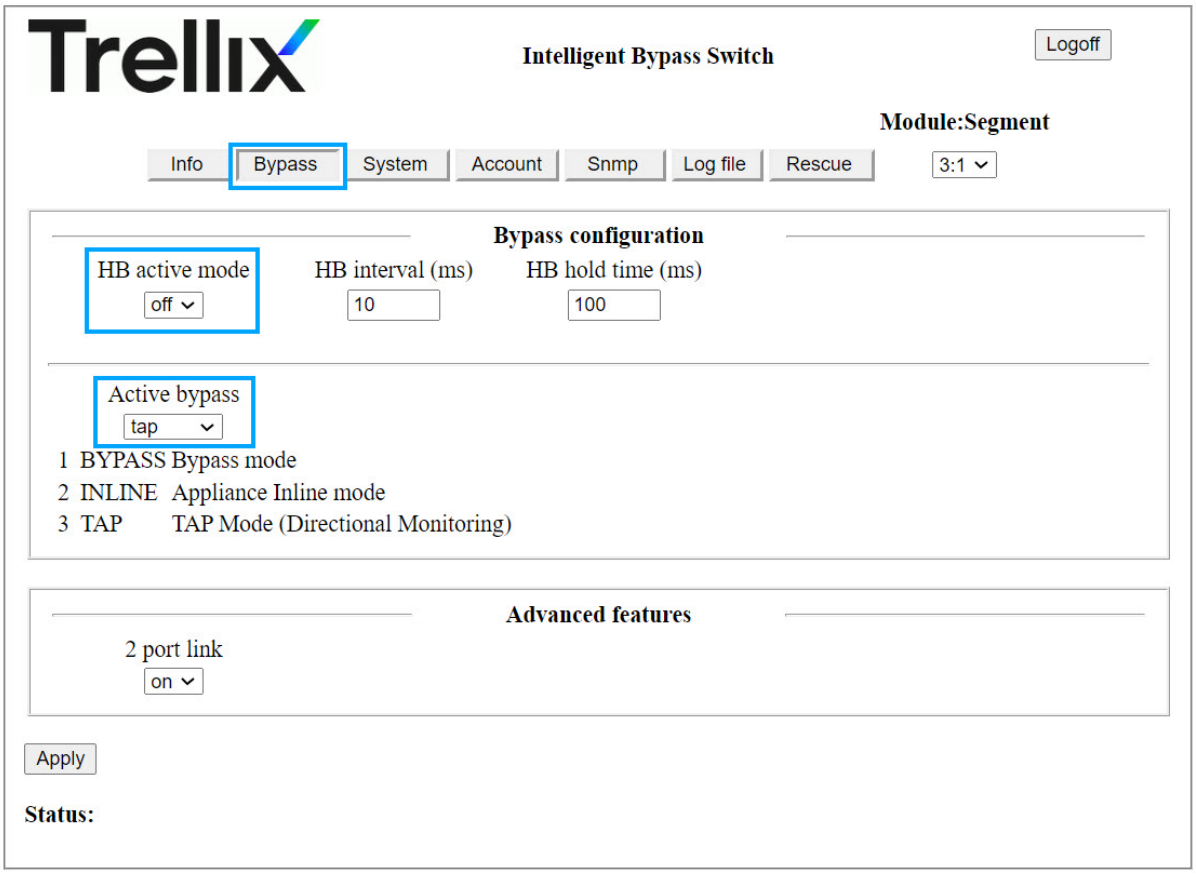
Prerequisites:

- Configure an IPv4 address for your Active Fail-Open chassis.
- Make sure you can access the Active Fail-Open web interface using a web browser.

You can enable tap mode for your Active Fail-Open module if you use a tap to route network traffic to the Sensor monitoring ports.

1. Login to the web interface of the Active Fail-Open module.

   Use default credentials to access the web interface.
2. Click the **Bypass** tab to access the **Bypass** configuration page.
3. Under **HB active mode**, select **Off** from the drop-down list.
4. Under **Active bypass**, select **tap/inline** from the drop-down list.



5. Click **Apply** to save your configuration.

You have set your Active Fail-Open to tap/inline mode of operation.

NOTE

To return to Bypass mode,

1. under **HB active mode**, select **on** from the drop-down list.
2. Click **Apply** to save your configuration.

Configure notification by SNMP traps

Prerequisites:

- To configure SNMP traps, you will require a server that will act as an SNMP server. The SNMP server can be any Windows or Linux system installed with an MIB browser, such as iReasoning.
- Make sure your Active Fail-Open chassis IP address can be reached within the network.
- Make sure your SNMP server and Active Fail-Open chassis are able to communicate.
- In addition, you will need to obtain MIB files to decode alert codes sent by the Active Fail-Open chassis. These files are specific to the Active Fail-Open chassis and can be obtained by clicking on this link: KB86247.

NOTE

The SNMP feature of your Active Fail-Open chassis can only be used to send notifications through SNMP traps.

Steps:

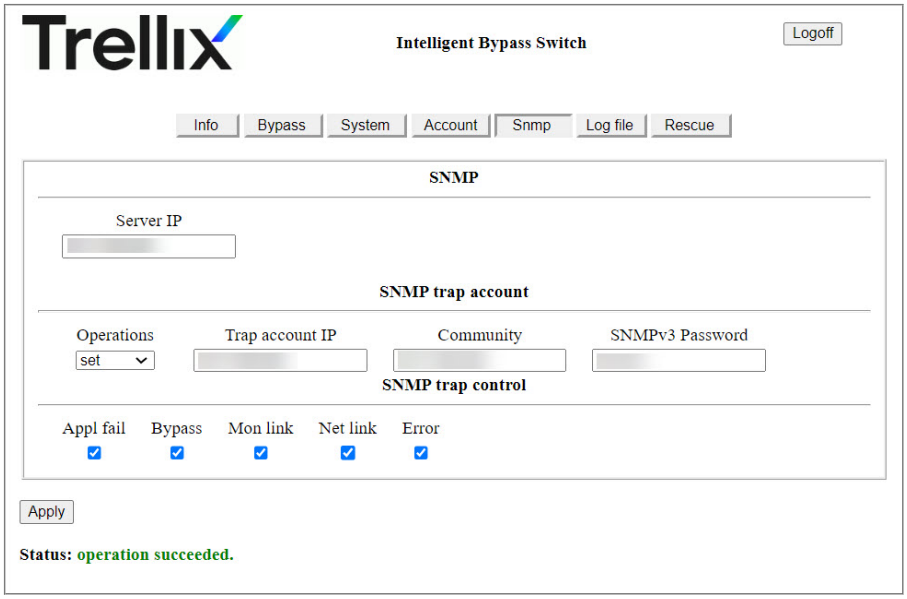
1. Connect an RJ-45 cable to the Management port at the front of the Active Fail-Open chassis.
2. Connect the other end to a network device so that the SNMP server is reachable through the network.
3. Copy the Fail-Open module MIB files to a suitable location on the SNMP server.
4. Set up the Active Fail-Open chassis IP address, network mask, and SNMP manager IP address by logging on to the web interface.

   NOTE

   You are also able to configure various other parameters specific to SNMP traps.

5. On the web interface, click the **SNMP** tab.

   The **SNMP** configuration page appears.



6. To configure the SNMP server IPv4 address, enter it in the **Server IP** field.

   The credentials used will be the default credentials for the Fail-Open module.

7. (Optional) If you want to configure multiple SNMP accounts, in the **SNMP trap account** section select **set** from the **Operations** drop-down.

> **NOTE**
>
> If you do not configure additional SNMP trap accounts, all traps will be routed to the main SNMP trap account you have set up here.

8. Enter the IPv4 address for the other account.
9. (Optional) You can specify an alternate SNMPv3 password for the additional SNMP server.

> **NOTE**
>
> SNMP **Community** strings are used only by devices that support SNMPv1 and SNMPv2 protocols. SNMPv3 uses username and password authentication, along with an encryption key. You can configure a community string if the SNMP software you use requires you to configure one regardless of the requirements in this user interface.

10. Click **Apply** to save your configuration.
11. In the SNMP server, configure these settings to enable SNMPv3 traps for the active fail-open kit.
    - USM user: **`Trellix00`**
    - Security level: **`auth, priv`**
    - Auth algorithm: **`SHA`**
    - Auth password: **`Trellix00`**
    - Privacy algorithm: **`AES`**

- Privacy password: **`Trellix00`**

12. Load the MIB file. If you do not have the appropriate MIB file, contact Trellix Support.
13. Make sure the SNMP server and Fail-Open module can communicate through the network.

Result: You have configured your active Fail-Open module to send SNMP traps to an SNMP server. You are also provided the option to configure multiple SNMP trap accounts. Access the SNMP server to view triggers.

Verify the SNMP setup

These steps show you how you test the setup for its bypass capability and SNMP traps.

1. On a Windows PC, for example, open the iReasoning MIB browser.
2. Click File → **Load MIBs**.

   A pop-up window appears.
3. Locate the MIB file for the Active Fail-Open kit and click **Open**.

   The MIB is loaded.
4. Configure the parameters for SNMPv3 traps on the server.
5. Login to the web interface of the Active Fail-Open chassis.
6. Access the **Bypass** tab by following the steps shown in *Enable tap/inline mode for the Active Fail-Open module* (page 685) to place the Active Fail-Open module into bypass condition and back to Inline.
7. snmp traps should be shown(bypass trap) in snmp trap server.

You will notice an SNMP trap appear in the list.

Configure Active Fail-Open kits 18 and 19

Prerequisites:

For each Active Fail-Open configuration, you will need to make sure you have all these components.

- Determine the IP address for the Active Fail-Open switch or, if you are deploying multiple switches, a range of IP addresses
- Determine a network mask and the default gateway for the Active Fail-Open switch
- 4 cables to connect the Active Fail-Open switch and the Sensor
- An RJ-45 RS232 cable to access the Active Fail-Open switch CLI
- QSFP28 for NS9500 Sensors
- Cables for a fiber Active Fail-Open switch:
  - LC and MTP/MPO fiber cables for network ports
  - LC and MTP/MPO fiber cables for monitor ports

Broadly, these are the steps you will need to follow to set up an Active Fail-Open kit.

NOTE

While configuring the 100G Active Fail-Open chassis, you must enable Forward Error Correction (FEC) in the AFO configuration. To enable FEC, go to AFO Configuration → Module <number> → **Advanced Features** and enable **Net 0 FEC**, **Net 1 FEC**, **Mon 0 FEC**, and **Mon 1 FEC**.

1. Install the 100G Active Fail-Open module in the chassis

Prerequisite: Identify the rack in which you plan to install the Active Fail-Open chassis.

Perform the following steps to install Active Fail-Open modules 18 and 19 in the 100G Active Fail-Open chassis (model 20). You can install up to two Active Fail-Open modules in a single chassis.

1. Place the 1U chassis against the front of a standard 19-inch rack.
2. Slide the 100G Active Fail-Open module into one of the two slots in the chassis, until the faceplate of the module rests against the chassis.
3. Secure the module to the chassis by inserting screws provided through the holes on the Active Fail-Open module faceplate and into the panel.
4. (Optional) Install up to two 100G Active Fail-Open modules by following these steps:
   a. Remove screws holding each of the removable blank plates from the front of the chassis.
   b. Perform steps 2 and 3 for installing another module in the chassis.

The Active Fail-Open module is ready to be connected to a Sensor.

2. Remove and replace the Active Fail-Open module from the chassis

perform the following steps to remove and replace the Active Fail-Open module.

1. **To remove:** Slide the module out from any one of the two slots it is installed without shutting down the chassis.
2. **To replace:** Slide in the module into one of the two slots in the chassis while the power is on.

> **NOTE**
>
> A chassis reboot is required every time a module is inserted to keep the module active.

3. Configure Active Fail-Open chassis parameters

Prerequisites:

To proceed with the setup, you will require:

- One RJ-45 RS-232 cable for console connection.
- One RJ-45 cable for network management connection.

Perform the following steps to configure the parameters of an Active Fail-Open chassis.

1. Connect the applicable cable to the Active Fail-Open chassis.
2. Connect the RJ-45 RS232 cable to a computer which runs a terminal emulation software such as HyperTerminal or PuTTY.
3. Launch the terminal emulation software and set the following communication parameters:
   - Baud rate: 115200
   - Data bits: 8
   - No parity
   - Stop bits: 1

- No flow control

4. Turn on the Active Fail-Open chassis.

   The CLI banner and login prompt are displayed.

5. At the login prompt, type the username and password, and press **Enter**.

   Table 40. Username and password for both sets of Active Fail-Open modules

For Active Fail-Open switches 16 and 17	
Username	**Trellix00**
Password	**Trellix00**

   The Active Fail-Open chassis CLI prompt is displayed.

6. Type the following commands for the Active Fail-Open modules 28 and 29.

   - **enable**
   - **configure**
   - **management eth-if ip x.x.x.x**
   - **management eth-if ip-mask y.y.y.y**
   - **management eth-if default-gateway z.z.z.z**
   - **write memory**

   > **NOTE**
   >
   > Reboot of the system is not required.

   For more information on the CLI commands, see [Trellix Intrusion Prevention System 100 Gigabit Modular Active Fail Open Bypass Kit Guide].

4. Configure notification by SNMP traps

Prerequisite:

- To configure SNMP traps, you require a server that acts as an SNMP server. The SNMP server can be any Windows or Linux system installed with a MIB browser such as iReasoning.

  To view the requirements and download a copy of iReasoning MIB browser, follow the link: https://ireasoning.com/mib-browser.html.
- Make sure the IP address of the 100G Active Fail-Open chassis can be reached within the network.
- Make sure the SNMP server and the 100G Active Fail-Open chassis are able to communicate.
- In addition, you need to obtain MIB files to decode alert codes sent by the 100G Active Fail-Open modules. This file can be obtained from the Web Interface → SNMP → **Mib File**.

1. Connect an RJ-45 cable to the management port at the front of the 100G Active Fail-Open chassis.
2. Connect the other end to a network device so that the SNMP server is reachable through the network.
3. Copy the MIB files of an Active Fail-Open module to a suitable location on the SNMP server.

For example, an SNMP trap is generated when one of the following events occur:

- Bypass state changes
- Any of the port link status changes
- Either power supply state changes or some other trap defined under SNMP → **Trap Filter** in the web interface.

4. Set up the 100G Active Fail-Open chassis IP address, network mask, and SNMP manager IP address using the commands provided in the section Active Fail-Open (page 689).
5. Make sure the SNMP manager and Active Fail-Open chassis are able to communicate.

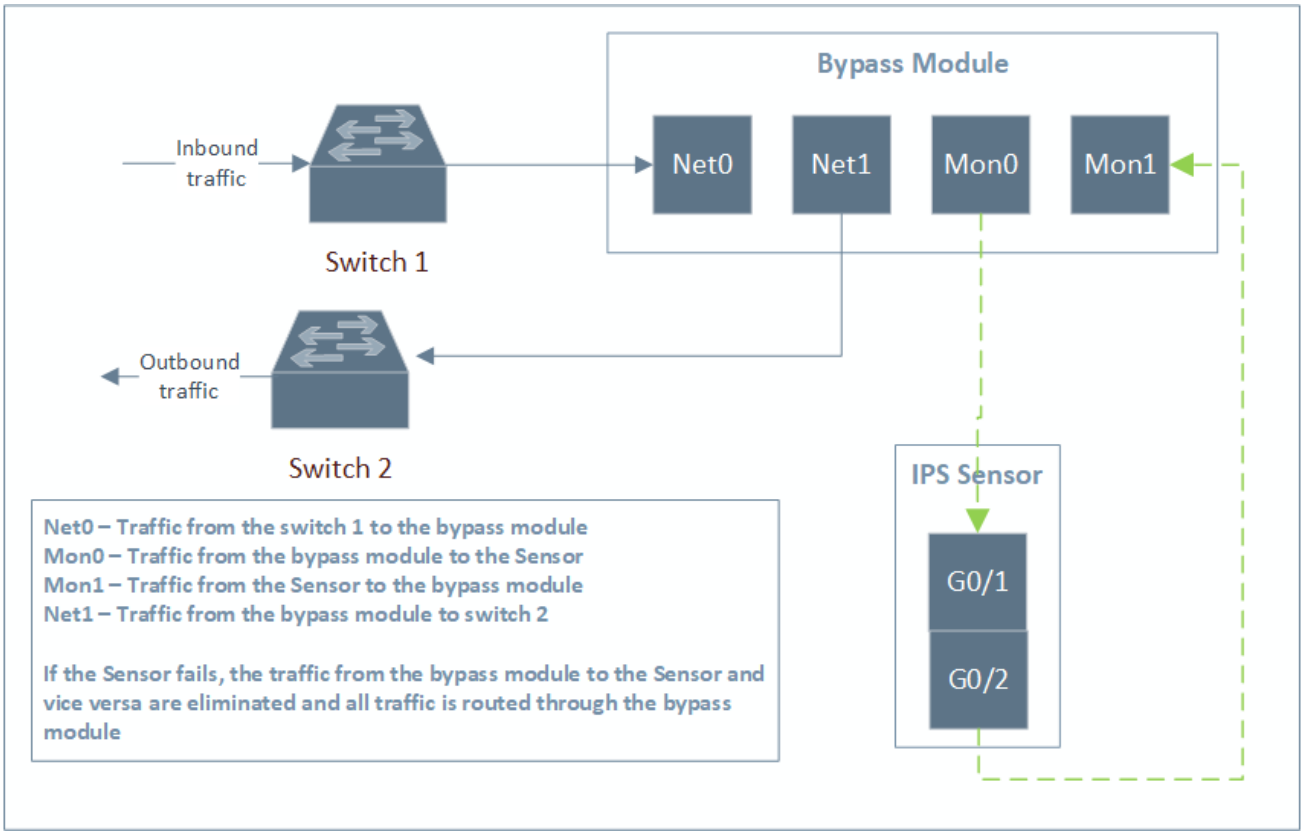
Configuration of SNMP traps is complete when a trap appears in the MIB browser.

5. Connect the module to an inline Sensor

After you have secured the Active Fail-Open module in its rack, use QSFP28 based fiber connecting cables to connect the module with the Sensor. The underlying principle in connecting these cables is to connect the Sensor and the module so that the traffic gets routed through the Active Fail-Open module if there is a Sensor outage.

Regardless of the Sensor and Active Fail-Open module type, the connections remain the same.

Figure 277. Active Fail-Open module connections



Steps:

1. Connect the port on your network device (Switch 1) to **Net0 (active)** of the Active Fail-Open module.
2. Insert a QSFP28 into each of the slots of the unused 100G port pairs on your Sensor. We use port pair G0/1-G0/2 for this illustration.

3. Connect the port **Mon0 (active)** on the Active Fail-Open module to port **G0/1** on the Sensor.
4. Connect the port **Mon1 (active)** on the Active Fail-Open module to port **G0/2** on the Sensor.
5. Connect the port **Net1 (active)** on the Active Fail-Open module to the port on the other network device (Switch 2).

RESULT_02C583722705422D98776706AC418C4C This completes the connections between the Sensor and Active Fail-Open module. The link lights might not be up if the Sensor is not yet deployed in inline mode.

6. Deploy a Sensor in inline Active Fail-Open mode

Prerequisites:

- The Sensor must be set up and have established trust with a Manager server.
- The Sensor has a free port pair which can be deployed in inline Active Fail-Open mode.
- It is assumed that you have inserted necessary transceiver modules into the Sensor if you have completed cabling the Sensor and Active Fail-Open module.

When you set up a Sensor for the first time, its ports are disabled by default. The Sensor ports must be manually configured for inline Active Fail-Open operation.

Steps:

1. In the Manager, go to Devices → <Admin_Domain_Name> → Devices → <Device_Name> → Setup → **Physical Ports**.
2. Double-click port one of the configurable ports, say **1/1** (Gx/1).

   A configuration panel appears on the right side of the window.
3. Click the **State** drop-down and select **Enabled**.

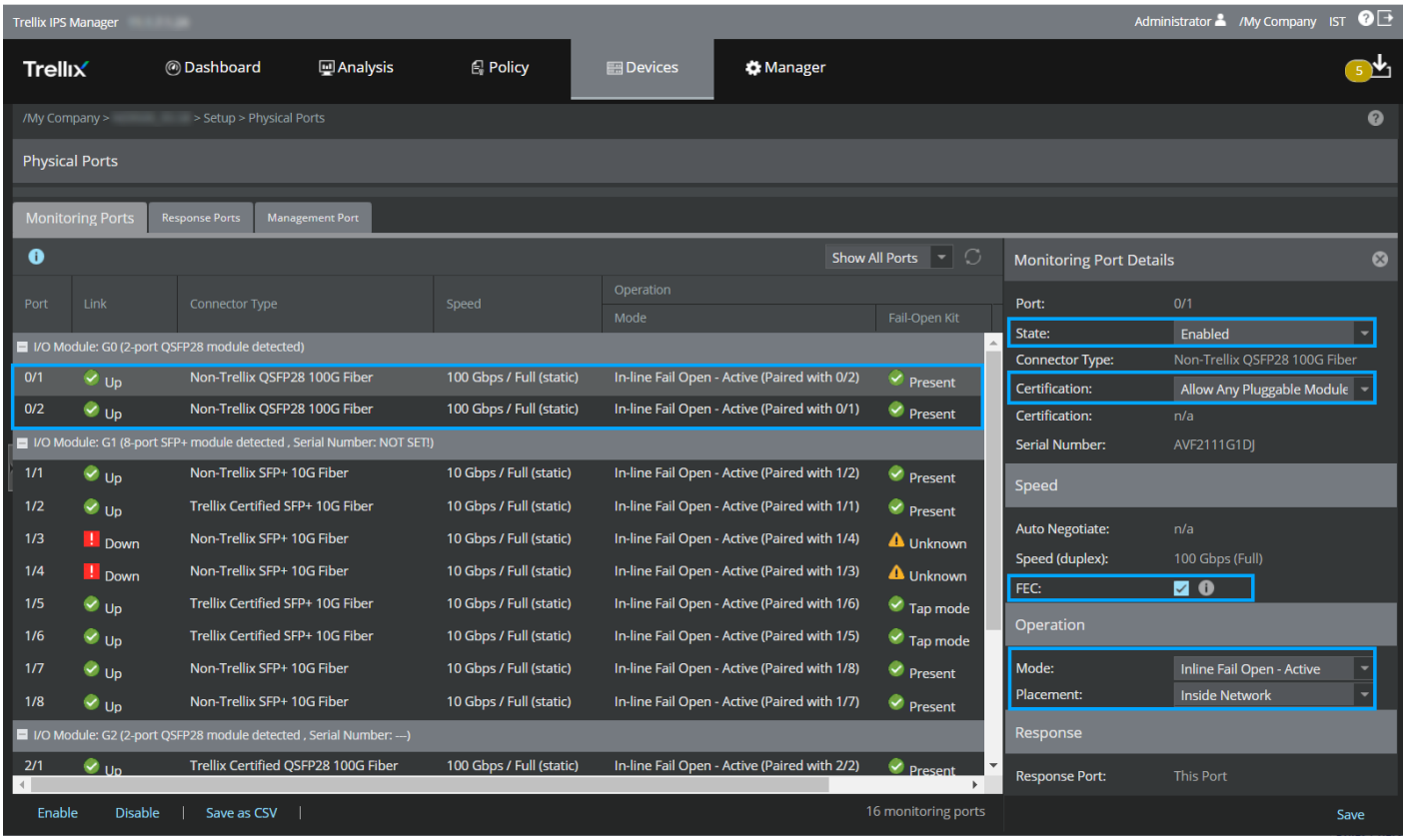
   This will impact the port 2/2 (Gx/2) as well. So, ports **2/1-2/2** (Gx/1-Gx/2) are enabled.
4. Click the **Certification** drop-down and select an option depending on your requirement.

   NOTE

   Based on the I/O module and port selected, you may be required to select the **Auto Negotiate** checkbox and set the speed under **Maximum Negotiable Speed (Duplex)**. For certain ports, the speed is automatically selected and you will not be able to edit it.
5. Select **FEC** checkbox if you want to enable Forward Error Connection.

   NOTE

   FEC should only be enabled when needed, and the device to which this port is connected must have FEC enabled too.
6. Under **Mode**, select **Inline Active Fail-Open – Active** from the drop-down list.
7. Under **Placement**, select **Inside Network** or **Outside Network** from the drop-down list, depending on how you want to configure your ports.



8. Click **Save**.

> **NOTE**
>
> An **Alert!** pop-up displays stating the changes made on port x/1 impacts x/2 as well. Click **OK**.

The Sensor and Active Fail-Open module are set up. When traffic passes through the ports, the port link status changes to **Up** and turns green.

7. Use the web interface to configure the Active Fail-Open module

Besides using CLI commands, you can view and configure Active Fail-Open module settings for the Active Fail-Open chassis through a web console.

The web interface for the Active Fail-Open modules 16 and 17 allows you to manage the following functions:

- Enabling bypass/tap mode for the Active Fail-Open module
- Returning from bypass/tap mode to inline mode
- Configuration of notifications through SNMP traps

The next section explains the steps for each of these management options.

Access the Active Fail-Open module web interface

If you have configured an IPv4 address for your Active Fail-Open chassis, you have the option to manage it through a web-interface.

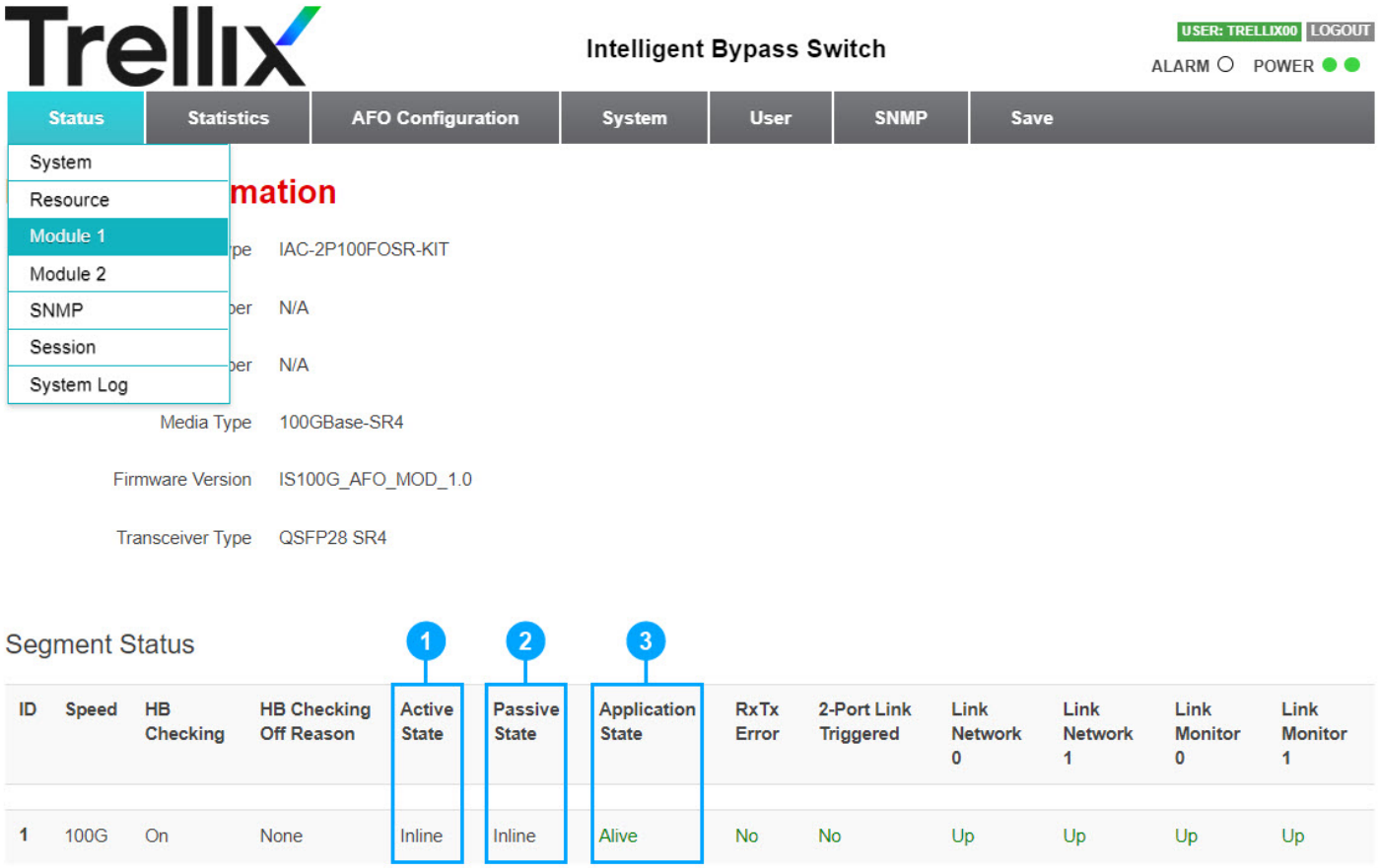
1. To access the Active Fail-Open module web interface, enter the IPv4 address of the Active Fail-Open chassis which you have configured through **https://x.x.x.x.**

   The Active Fail-Open module web interface appears on the login screen.

2. To login, enter the default username and password, **`Trellix00`** and **`Trellix00`**.

3. Go to, Status → **Module <number>**.

Under **Segment Status**, you can view the present settings configured in the Active Fail-Open module. Configuration of necessary settings is explained in the relevant sections.



Callout	Description
1	Active State: • Inline - Sensor receives traffic and the fail-open module is operating in normal mode • Bypass - Sensor does not receive traffic and the fail-open module is not operating in inline mode • Tap - Fail-open module functioning like a TAP kit
2	Passive State: • Inline - Fail-open module operating in normal mode • Bypass - Sensor does not receive traffic and the fail-open module is not operating in inline mode

Callout	Description
3	Application State: • Active - Monitoring ports are up and the heartbeat packets are received • Fail - Monitoring ports are up, but the heartbeat packets are not received • Unknown - Monitoring ports are down

Enable tap/bypass mode for the Active Fail-Open module

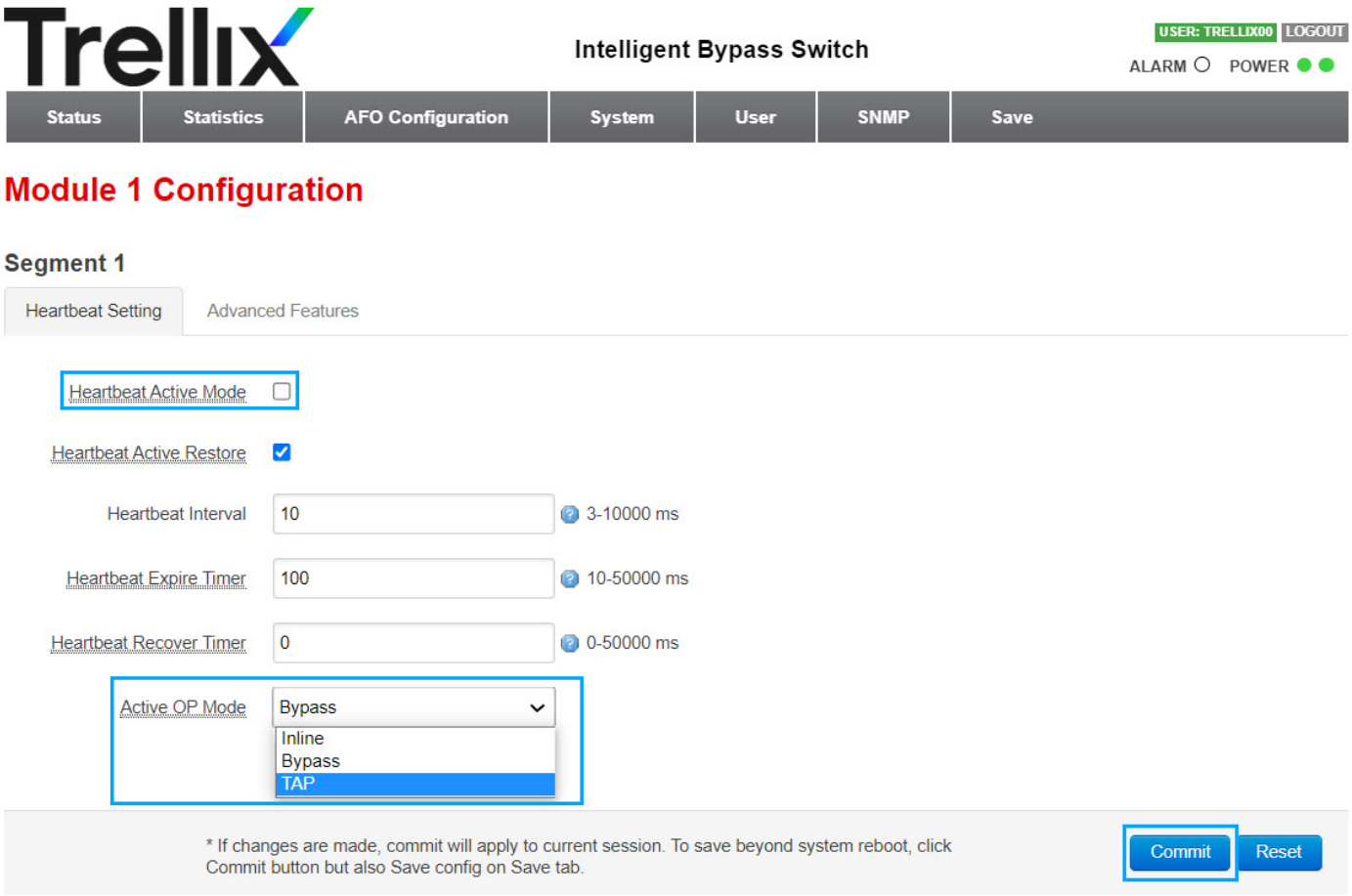
Prerequisites:

- Configure an IPv4 address for your Active Fail-Open chassis.
- Make sure you can access the Active Fail-Open web interface using a web browser.

You can enable tap mode for your Active Fail-Open module if you use a tap to route network traffic to the Sensor monitoring ports.

1. Log on to the web interface of the Active Fail-Open module.

   Use default credentials to access the web interface.
2. Go to, AFO Configuration → **Module <number>** to access the configuration page.
3. Under **Heartbeat Setting**, deselect **Heartbeat Active Mode**.
4. Under **Active OP Mode**, select **TAP/Bypass** from the drop-down list.



5. Click **Commit** to save your configuration.

You have set your Active Fail-Open to tap/bypass mode of operation.

NOTE

To return to inline mode,

1. Under **Heartbeat Setting**, select **Heartbeat Active Mode**.
2. Click **Commit** to save your configuration.
3. Click **Save** to retain the changes across active fail-open chassis reboot.

Configure notification by SNMP traps

Prerequisites:

- To configure SNMP traps, you will require a server that will act as an SNMP server. The SNMP server can be any Windows or Linux system installed with a MIB browser, such as iReasoning.
- The 100G Active Fail-Open chassis IP address should be reachable within the network.
- The SNMP server and the 100G Active Fail-Open chassis should be able to communicate.

- In addition, you will need to obtain the MIB files to decode alert codes sent by the 100G Active Fail-Open chassis. Refer to step **5** for more information.

NOTE

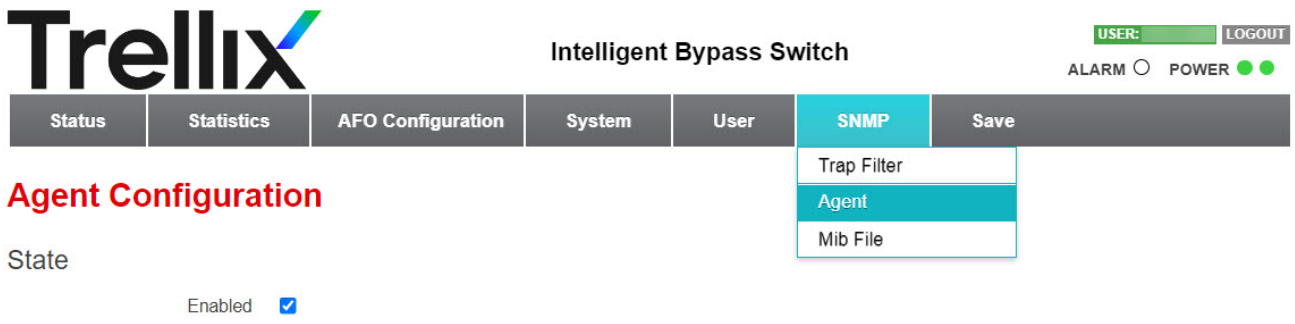
The SNMP feature of your 100G Active Fail-Open chassis can only be used to send notifications through SNMP traps.

1. Login to the web interface of the 100G Active Fail-Open chassis.

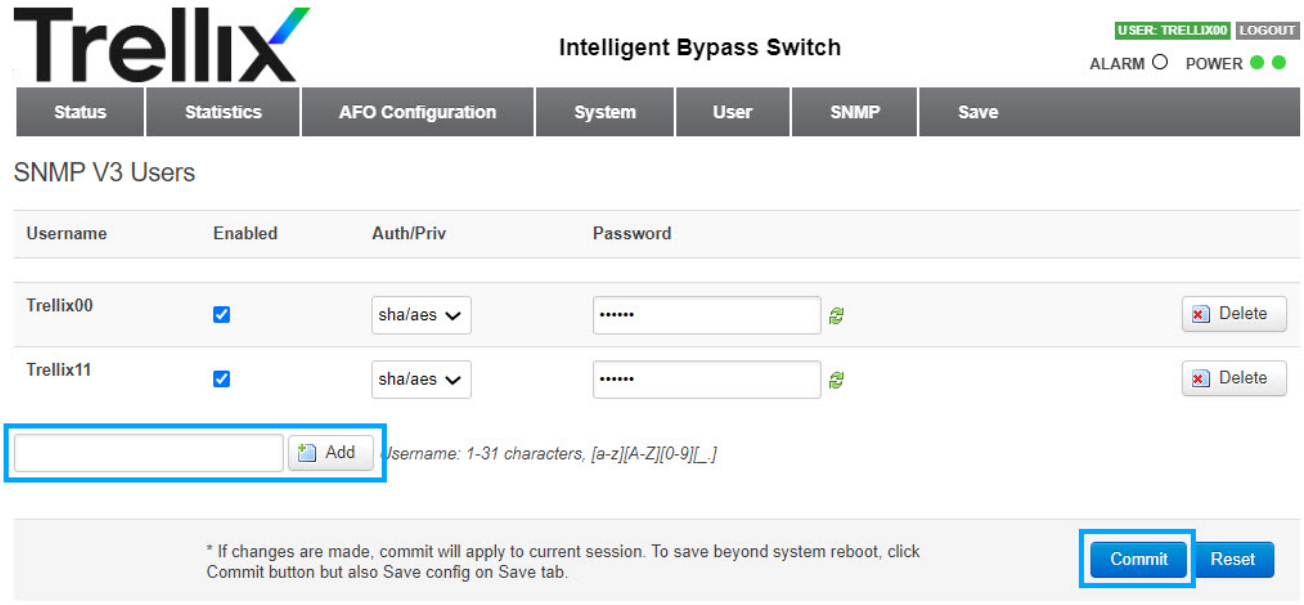
   Use default credentials to access the web interface.

2. To add an SNMP v3 user:

   a. Go to SNMP → **Agent**.



   b. Add a main SNMP v3 user and click **Commit**.



   c. To save your configuration, select the **Save** tab.

      Click **Save**.

   New user is added, type a password that is required for both **Auth**= sha and **Priv**= aes for the user.

3. To add Trap Hosts:

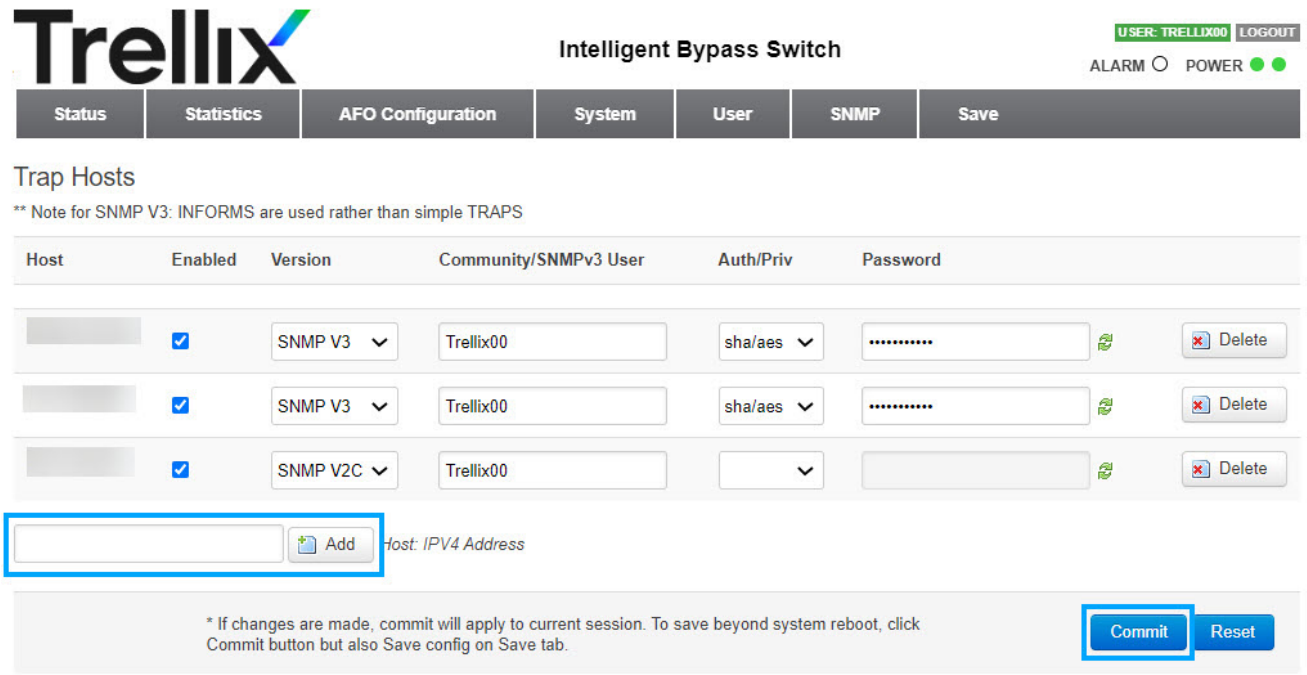
   The main SNMP v3 server can be added in this section by configuring a host with same community/SNMP v3 user/ password/auth&priv as per configured in step **b** for SNMP v3 users.

   NOTE

   The main SNMP v3 server (to be able to do GET/WALK function and receive traps from 100G Active Fail-Open module) and/or SNMP v1/v2c/v3 trap host(s) must have the same configuration as per configured here to be able to receive traps from 100G Active Fail-Open module.

   a. Go to SNMP → **Agent**.

   b. Enter an IPv4 Trap Host and click **Add**.



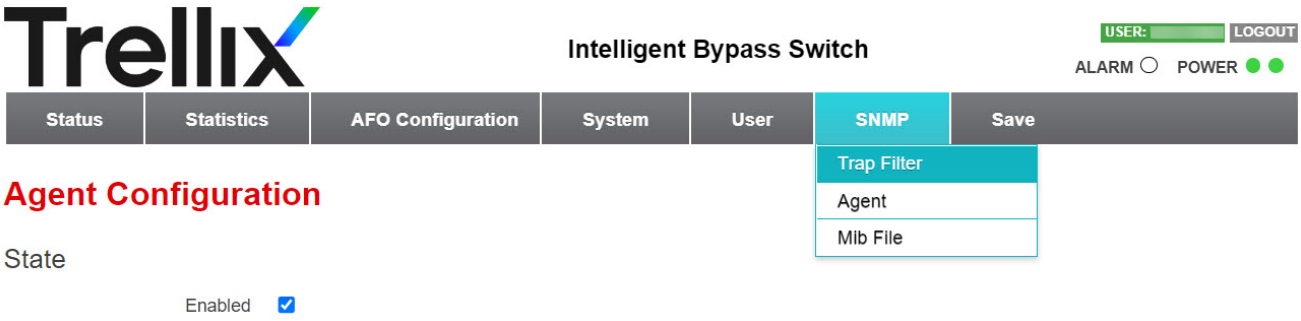
   - When configuring SNMP v1 or v2 trap user, only community string is user configurable with a minimum of 5 characters.
   - When configuring SNMP v3 trap user, **Community/SNMP v3 User**, **Auth/Priv**, and **Password** need to be configured.
     - **Community/SNMP v3 User:** Should be at least 5 characters for SNMP v3 user
     - **Auth/Priv:** Choose **sha/aes** or **md5/des** from the drop-down list
     - **Password:** Should be at least 8 characters

   c. Click **Commit**.

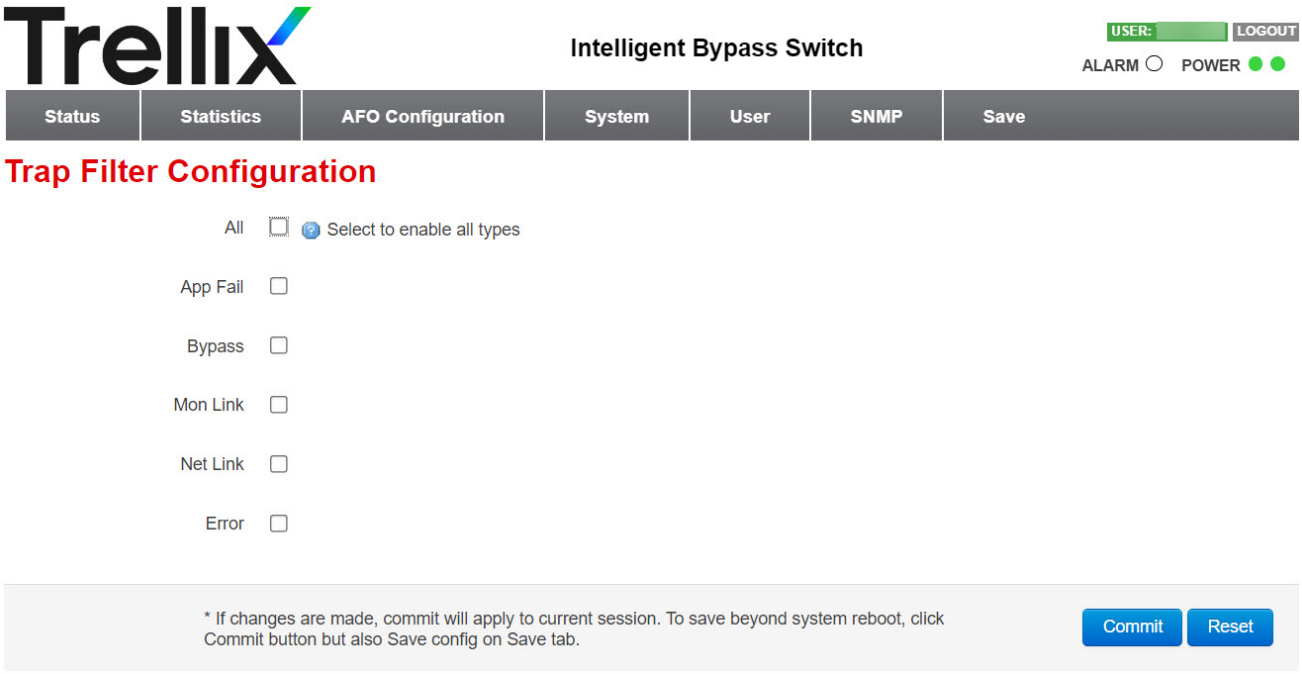
   d. To save your configuration, select the **Save** tab.

      Click **Save**.

4. To configure Trap Filter:
   a. Go to SNMP → **Trap Filter**.



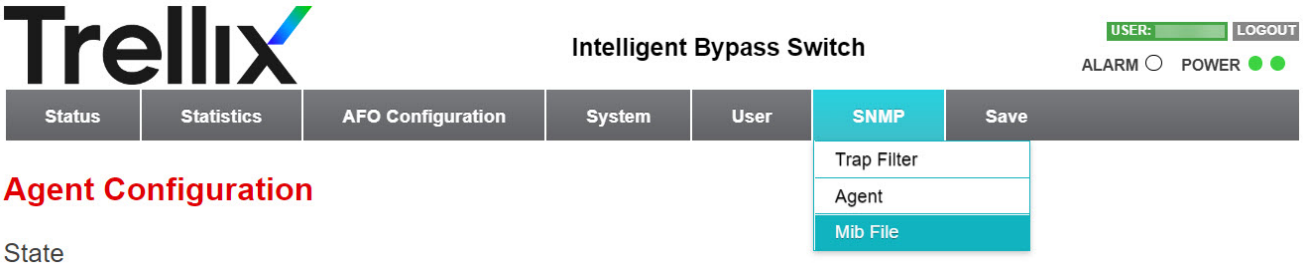
   b. Select **All** or individual traps to be generated.



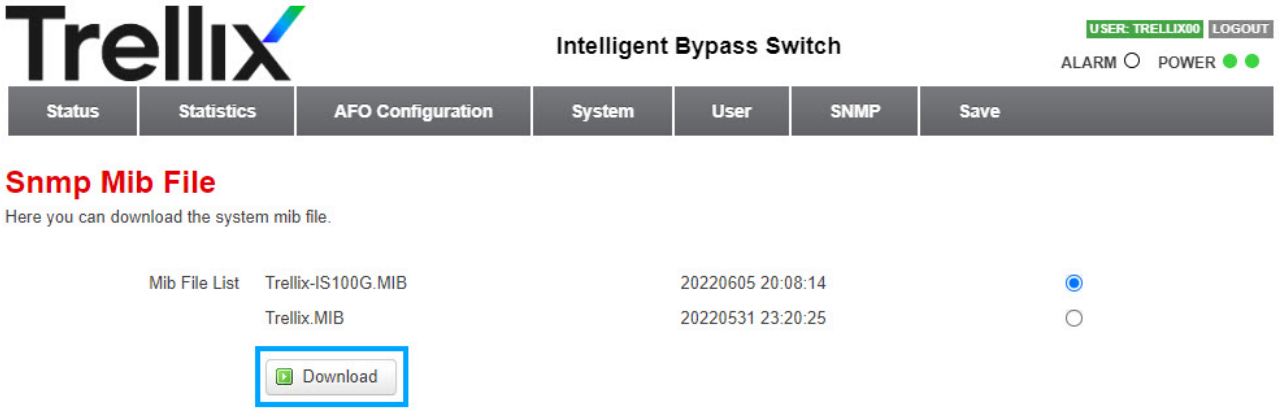
   c. Click **Commit**.
   d. To save your configuration, select the **Save** tab.

      Click **Save**.

5. To access MIB file:
   a. Go to SNMP → **Mib File**.



b. Select a MIB file from the available list and click **Download**.



It generates a MIB file.

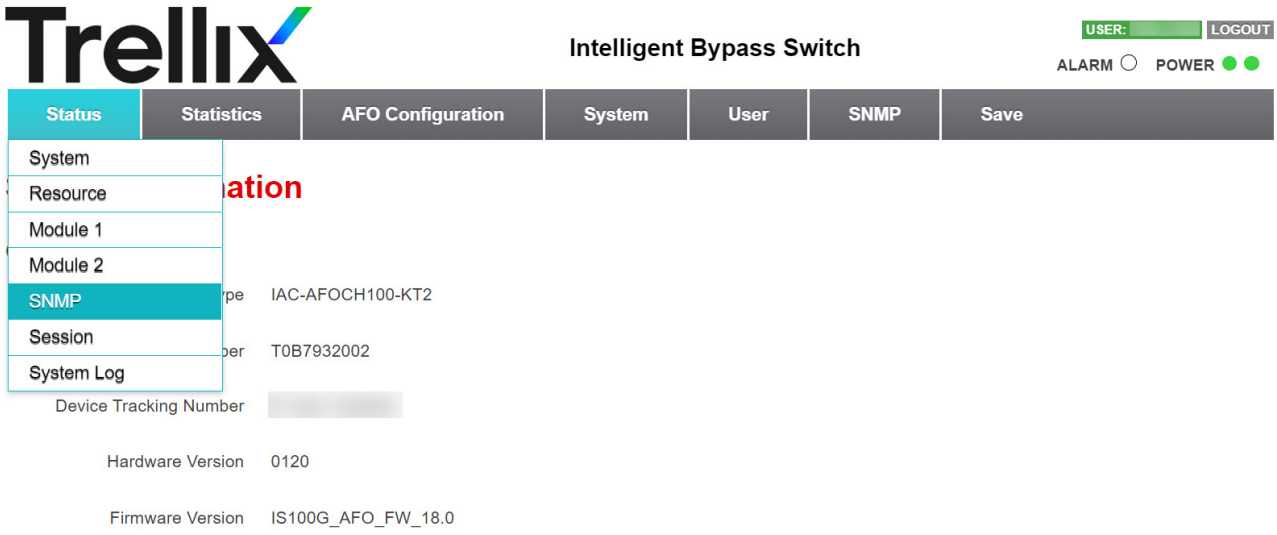
> **NOTE**
>
> Use this MIB file on your main **SNMP v3** or **Trap Host** servers to translate all MIB OIDs being generated.

c. To save your configuration, select the **Save** tab.

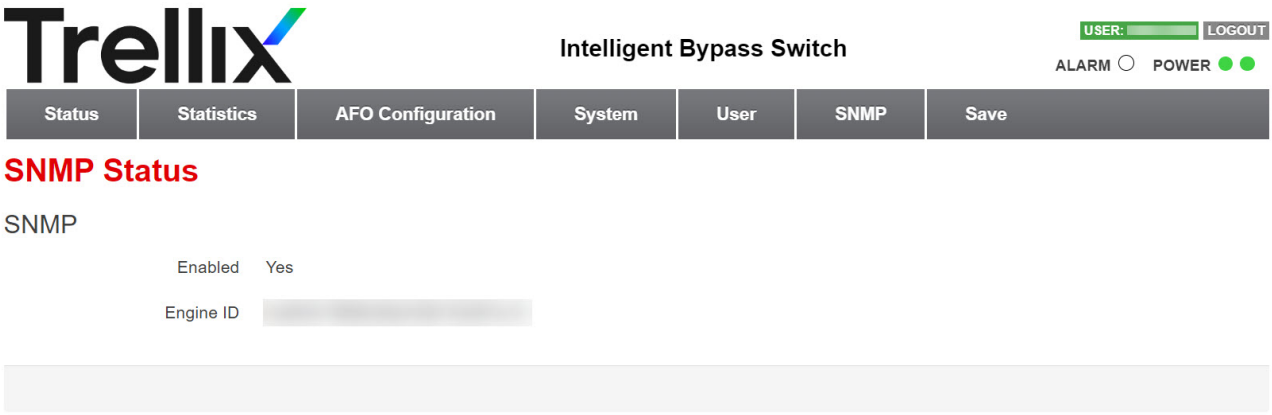
Click **Save**.

6. To view the SNMP status and Engine ID:

- Go to Status → **SNMP**.



The page displays the SNMP status and Engine ID.



Verify the SNMP setup

These steps show you how you test the setup for its bypass capability and SNMP traps.

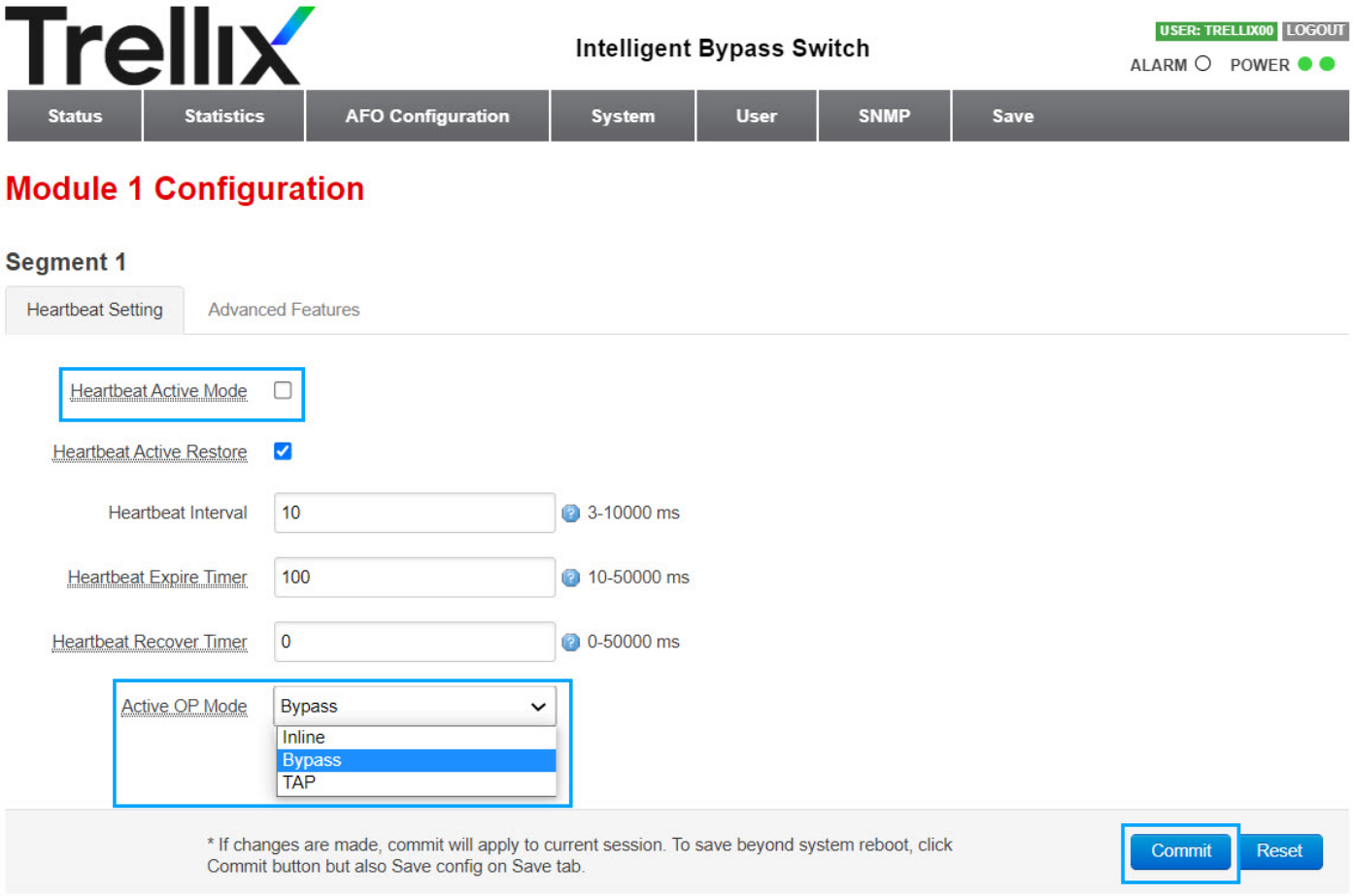
1. On a Windows PC, for example, open the iReasoning MIB browser.
2. Click File → **Load MIBs**.

   A pop-up window appears.
3. Locate the MIB file for the Active Fail-Open kit and click **Open**.

   The MIB is loaded.
4. Configure the parameters for SNMPv3 traps on the server.
5. Login to the web interface of the Active Fail-Open module.

   Use default credentials to access the web interface.
6. Go to, AFO Configuration → **Module <number>** to access the configuration page.
7. Under **Heartbeat Setting**, deselect **Heartbeat Active Mode**.

8. Under **Active OP Mode**, select **Bypass** from the drop-down list.



9. Click **Commit** to save your configuration.
10. Under **Heartbeat Setting**, deselect **Heartbeat Active Mode**.
11. Click **Commit** to save your configuration.

You will notice an SNMP trap appear in the list.

Deployment scenario

Since we have looked at the steps to set up a fail-open switch and deploy it, we'll go through a scenario to see how the setup works. We will cover configuration steps at a high level without listing each step. For more detailed steps on any section, refer to sections above.

The deployment uses the following software and hardware equipment:

- 100G - QSFP28- SR4 50 µm optical active fail-open switch
- NS9500 model with standard 100 Gigabit QSFP28 monitoring ports
- Windows or Linux system installed with a MIB browser, such as iReasoning
- Cables for connecting various devices
- Terminal emulation software such as HyperTerminal or PuTTy. We will be using PuTTy for this deployment

- Make note of these parameters that you will while setting up fail-open switch parameters.
  - Baud rate: 115200 bits per second
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow Control: XON/XOFF
  - Username and password: **`Trellix00`**
- Fail-open switch MIBs to decode SNMP traps from a 100G active fail-open switch. If you do not have MIBs with you, contact Technical Support.

Setup the fail-open switch and Sensor

Begin by configuring parameters for the fail-open switch and then connecting it to an inline Sensor. This setup does not have the provision to connect an RJ45-DB9 RS232 cable to a Windows PC after it has been installed in a rack, so the parameters for the fail-open switch will first be set up.

1. Connect one end of the cable to RJ45 port of the fail-open switch.
2. Connect the other end of the cable to DB9 port of the Windows computer.
3. Connect the power cables to the ports at the back of the fail-open switch.
4. Open PuTTy and click **Serial**.
5. Enter **Speed** as **`115200`** which is the baud rate for a fail-open switch.
6. Click **Open**.

   The fail-open switch CLI interface appears.
7. Use administrator credentials to log on to the fail-open switch.

   You are provided access to the fail-open switch command prompt.
8. To set up the fail-open switch IPv4 address, type **`management eth-if ip xxx.xxx.xxx.xxx`** and press **Enter**. For example, **`management eth-if ip 10.10.10.1`**.

   When selecting an IP address, make sure you are able to reach the SNMP server that you intend to set up.
9. To set up the fail-open switch subnet mask, type **`management eth-if ip-mask xxx.xxx.xxx.xxx`** and press **Enter**. For example, **`management eth-if ip-mask 255.255.255.0`**.
10. To set up the default gateway IPv4 address, type **`management eth-if default-gateway xxx.xxx.xxx.xxx`** and press **Enter**. For example, **`management eth-if default-gateway 10.10.10.2`**.
11. To set up the SNMP manager IP address, type **`set manager <SNMP manager IPv4 address>`** and press **Enter**.
12. After you have set up fail-open switch parameters, unplug the RS232 cable and power cables.
13. Install the fail-open switch in the rack in a way that you are able to connect it to the Sensor.
14. Gently insert the 100G-SR4 or 100G-LR4 module(s) into the slots in the front of the fail-open switch.
15. Connect the MTP/MPO Fiber cables between the fail-open switch and the Sensor if you have inserted a 100G-SR4 module. If you have inserted a 100G-LR4 module, connect the LC Fiber cables between the fail-open switch and the Sensor.
16. Connect an RJ-45 cable to the Management Port on the front of the fail-open switch.

17. Connect the power cables back to the fail-open switch.
18. Configure port pair **G0/1-G0/2** as **Inline Fail Open – Active**.
19. Click **Save**.

    The link lights on the fail-open switch and Sensor ports must come on to indicate that the fail-open switch has been set up.

Verify the SNMP setup

These steps show you how you test the setup for its bypass capability and SNMP traps.

1. On a Windows PC, for example, open the iReasoning MIB browser.
2. Click File → **Load MIBs**.

   A pop-up window appears.
3. Locate the MIB file for the active fail-open kit and click **Open**.

   The MIB is loaded.
4. Configure the parameters for SNMPv3 traps on the server.
5. Login to the web interface of the fail-open switch.
6. Access **Bypass** tab by following the steps shown in *Enable tap mode for the fail-open switch* (page 676) to place the fail -open module into bypass condition and back to inline.
7. snmp traps should be shown(bypass trap) in snmp trap server.

You will notice an SNMP trap appear in the list.

How to configure Sensors for high availability

Most networks today have some amount of in-built redundancy. However, the extent to which a network can withstand a failure varies, depending on the environment. For example, one setup might have two fully redundant paths to and from the Internet, whereas another might have Primary and Secondary firewalls, but single points of failure elsewhere.

Network devices traditionally provide redundancy at Layer 2 or 3 of the OSI model. That is, they take advantage of the existing switching or routing infrastructure to provide fault tolerance.

The principle behind hot standby router protocol (HSRP - *RFC 2281*) and virtual router redundancy protocol (VRRP - *RFC 2338*), for example, is that two or more routers share a virtual IP (VIP) address. One router takes on a primary role and "owns" the VIP; all traffic directed to the VIP routes through the primary when all is well. If the primary goes offline, a standby router is automatically promoted and takes over ownership.

Because most network devices run at Layer 2 or higher, incorporating redundancy often requires a logical topology change. As a simple example, to add the aforementioned router redundancy, you have to reconfigure all downstream routers to use with the new VIP as their default gateway.

Trellix IPS fail-over architecture

Trellix IPS was built with high availability in mind. In fact, those who initially become confused by the possibilities around Trellix IPS fail-over usually do so because the implementation is actually simpler than they assume initially.

Note the following points regarding Trellix IPS fail-over architecture:

- Sensors are invisible at layer 2 and above; the monitoring ports do not even have MAC addresses.
- Sensors configured for failover confirm a "heartbeat" once each second.
- Sensors configured for fail-over share flow information in real time.

As a result, you do not have to worry about Layer 2 and 3 topology changes when you introduce Trellix IPS fail-over into the environment; and in the unlikely event of a Sensor failure, fail-over is instantaneous and connection state is maintained.

Sensor fail-over implementation

A typical Trellix IPS failover implementation includes the following steps:

- Understanding the current network topology
- Determining optimal Sensor location
- Configuring the ports on each Sensor
- Physically installing the Sensors
- Defining Trellix IPS HA pair
- Connecting the heartbeat cables
- Verifying the failover configuration

In the sections that follow, we will consider each of these points in detail.

How to understand the current network topology

Understanding the current network topology is essential for the proper planning of Trellix IPS fail-over solution. Rather, the more you understand about the existing data flow, the less likely you run into obstacles during implementation.

The most common network topologies can be summarized as follows:

- Two paths - Active/Passive
- Two paths - Active/Active
- A single path

Two paths - Active/passive

Most redundant links today are made up of active or passive paths. There are two ways in and out of the network, but only one way will actually be available at any given time. The path passing traffic is called the active path, and the one standing by in the event of a failure is called the passive path.

HSRP, VRRP, spanning tree protocol (STP), and Dynamic Routing Protocols, such as, OSPF, EIGRP, and BGP, are arguably the most common technologies used to automate network failover. Admittedly, many of these include options to balance traffic, but they are historically configured to allow for one path to pass traffic at a time.

Two paths - Active/active

Some networks will maintain two active paths to and from the Internet. In addition to redundancy, these approaches can potentially double the available bandwidth, under normal conditions.

In most cases, the two paths are not designed to share traffic unless there is a failure. When all is well, a flow will be established on one of the paths, and all packets from that flow will traverse the same path.

In some cases, however, the network infrastructure is designed in such a way that cross both paths under normal circumstances. For example, inbound requests might come in on path A and outbound responses might go out on path B. Such traffic is said to be asymmetrically routed.

Of course, if one path becomes unavailable, all traffic will be routed across the remaining path.

A single path

Some networks do not include much or any redundancy. In this case, there is one or more single points of failure.

If one of the non-redundant devices fails, the connection to the Internet will fail as well.

Most companies that choose to invest in a redundant Trellix IPS solution also invest in redundant paths to and from their network. That is, there are numerous companies that have single points of failure, but insist on implementing Trellix IPS failover.

Optimal Sensor location determination

The previous section is mostly intended as a point of reference. The good news is that Trellix IPS fail-over process is often identical, whether the network fail-over configuration is active-active, with or without asymmetric routing, active-passive, or even made up of a single path.

The details are as follows:

- Both the Sensors in a fail-over pair are always in an active state. In this way, they are sure to protect a network on which the redundant path is active.
- However, such an approach does not preclude the Sensors from protecting a network on which the Secondary path is passive; the Sensor on the passive path will not have much or any flow information to pass to its counterpart.
- Sensors in a fail-over Pair scan independently, but use the information they share with each other during the scanning process. In this way, if a flow happens to be asymmetrically routed across both Sensors, each Sensor will end up with the full flow.

Redundant Sensors on redundant paths

Determining the optimal physical location for the Sensors on a redundant network is usually quite obvious. If you ignore the idea of Trellix IPS fail-over for a moment, the rule of thumb for Sensor placement is to install the Sensor along the same boundaries of trust that often guide firewall placement. In fact, most Sensor installations are either directly inside or directly outside the company firewall. Of course, like a firewall, a Sensor can be used deep inside an enterprise to isolate one segment of the network from the next.

The same basic rule applies to Trellix IPS fail-over. If the network currently has parallel firewalls connected to parallel switches, for example, it follows that you can introduce parallel Sensors between them. The following set of diagrams is a very simple "before and after," to help clarify the logic. (The dotted line represents a heartbeat link.):

Figure 278. Determination of optimal Sensor location — Before

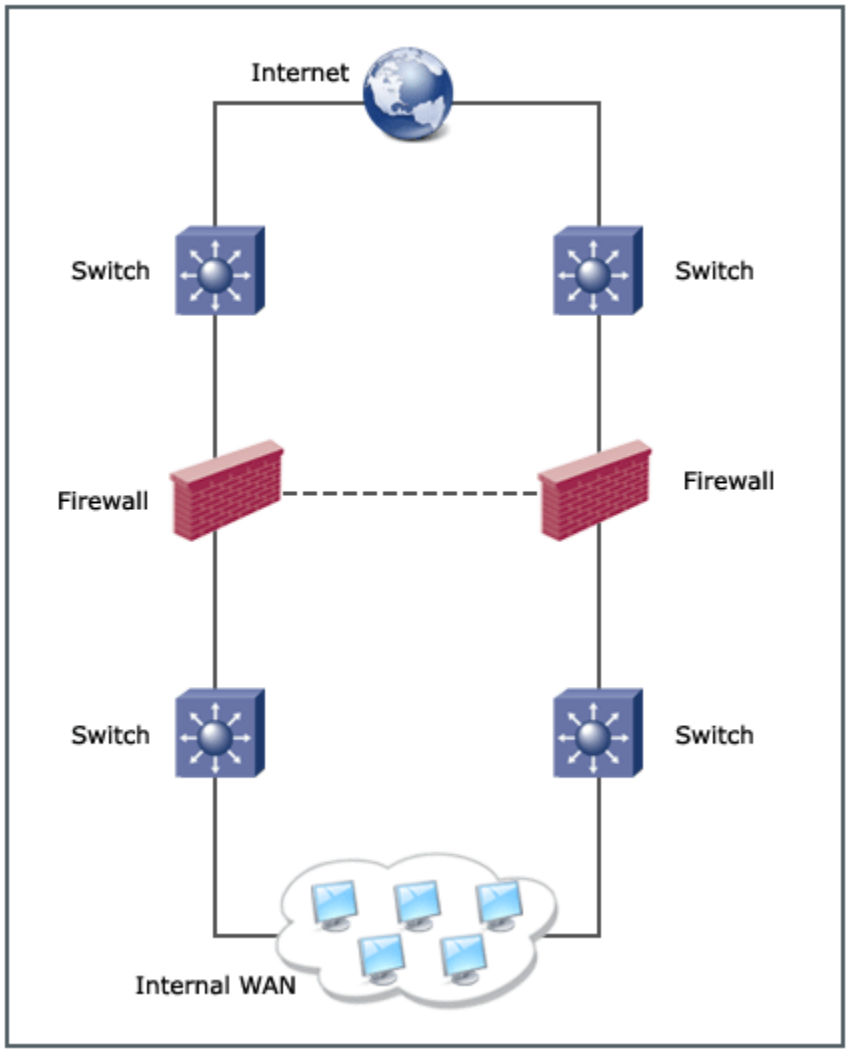
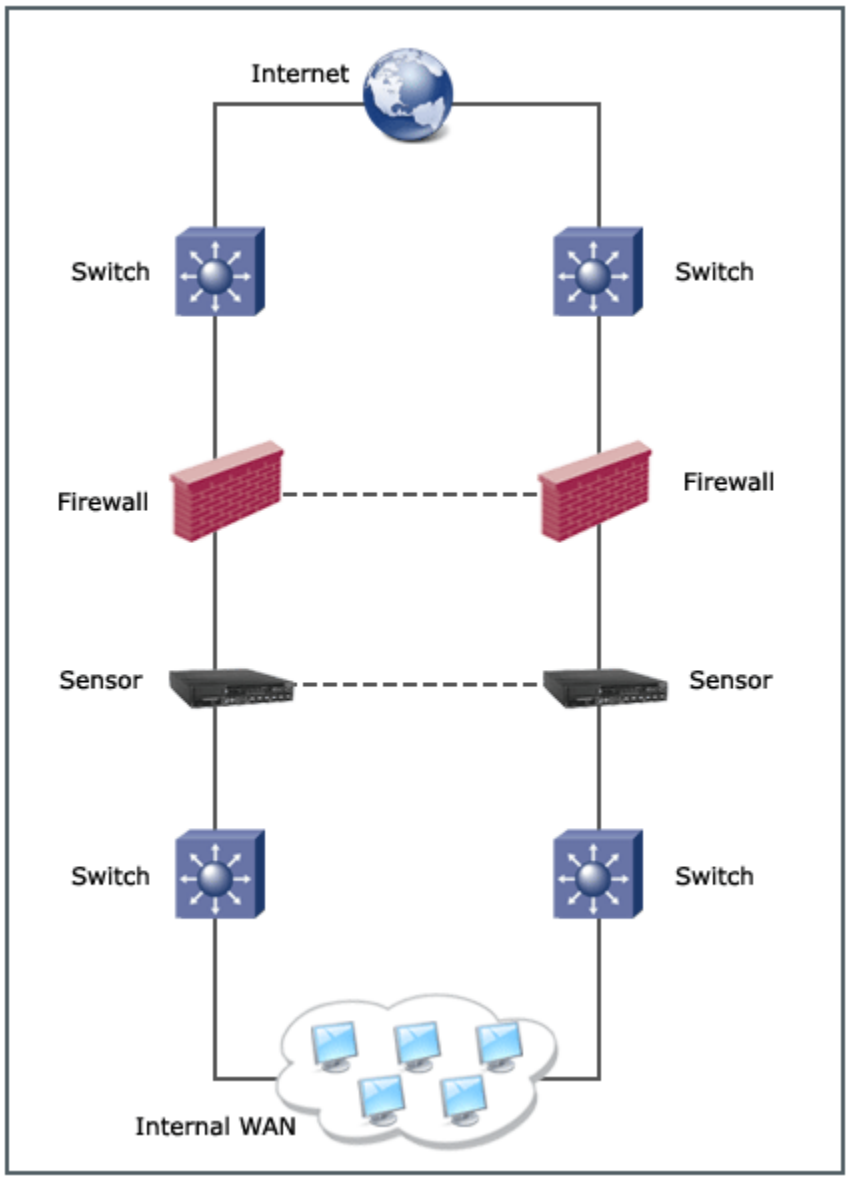


Figure 279. Determination of optimal Sensor location — After

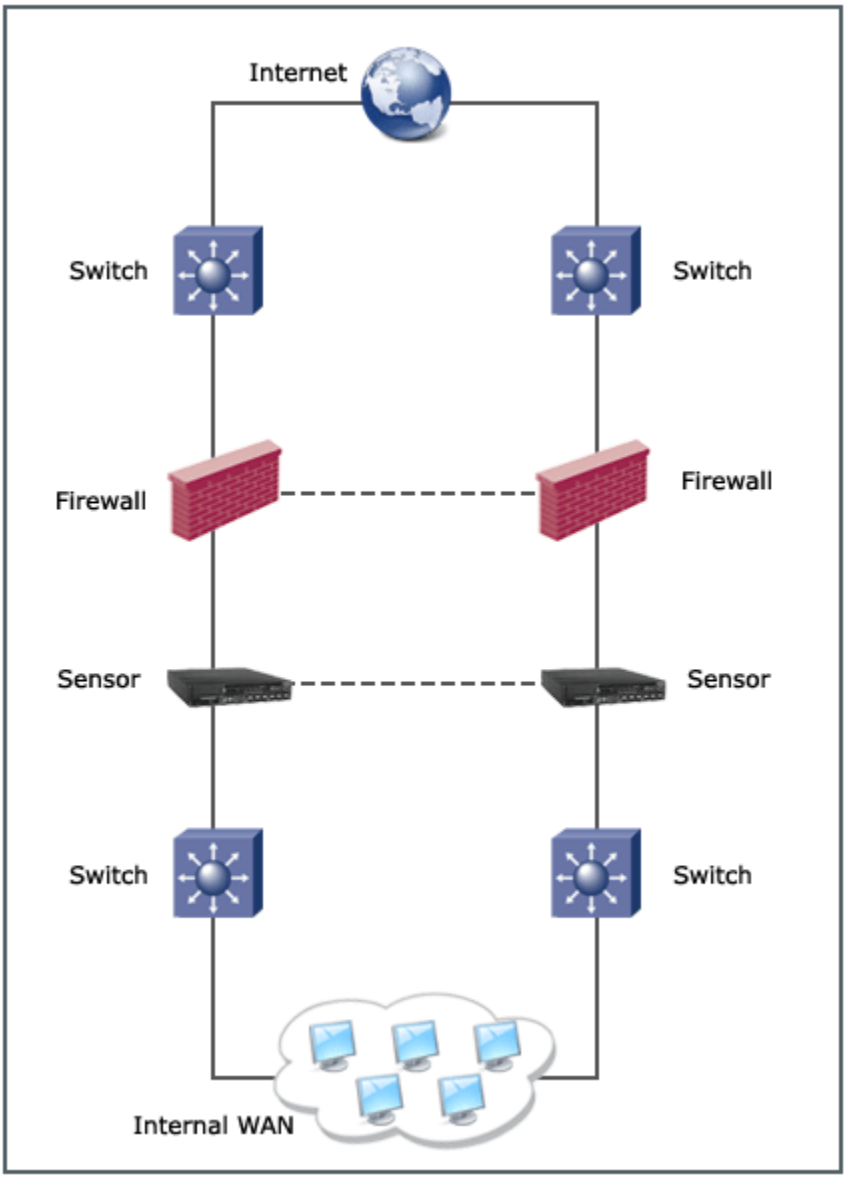


The key is to ensure the redundant Sensors will be scanning the same traffic at the same point in the network. If you were to instead place one Sensor outside the firewall on one path and the other Sensor inside the firewall on the other path, the outcome is what developers like to refer to as "undefined." That is, there is no telling what false positives and false negatives, and even instability, such a setup might produce.

Redundant Sensors on a single path

Trellix IPS is engineered to seamlessly slip onto networks within existing networks and between redundant paths. This simplifies implementing a Sensor HA pair in complicated environments. However, introducing a Sensor HA pair in a network with a single path requires additional effort.

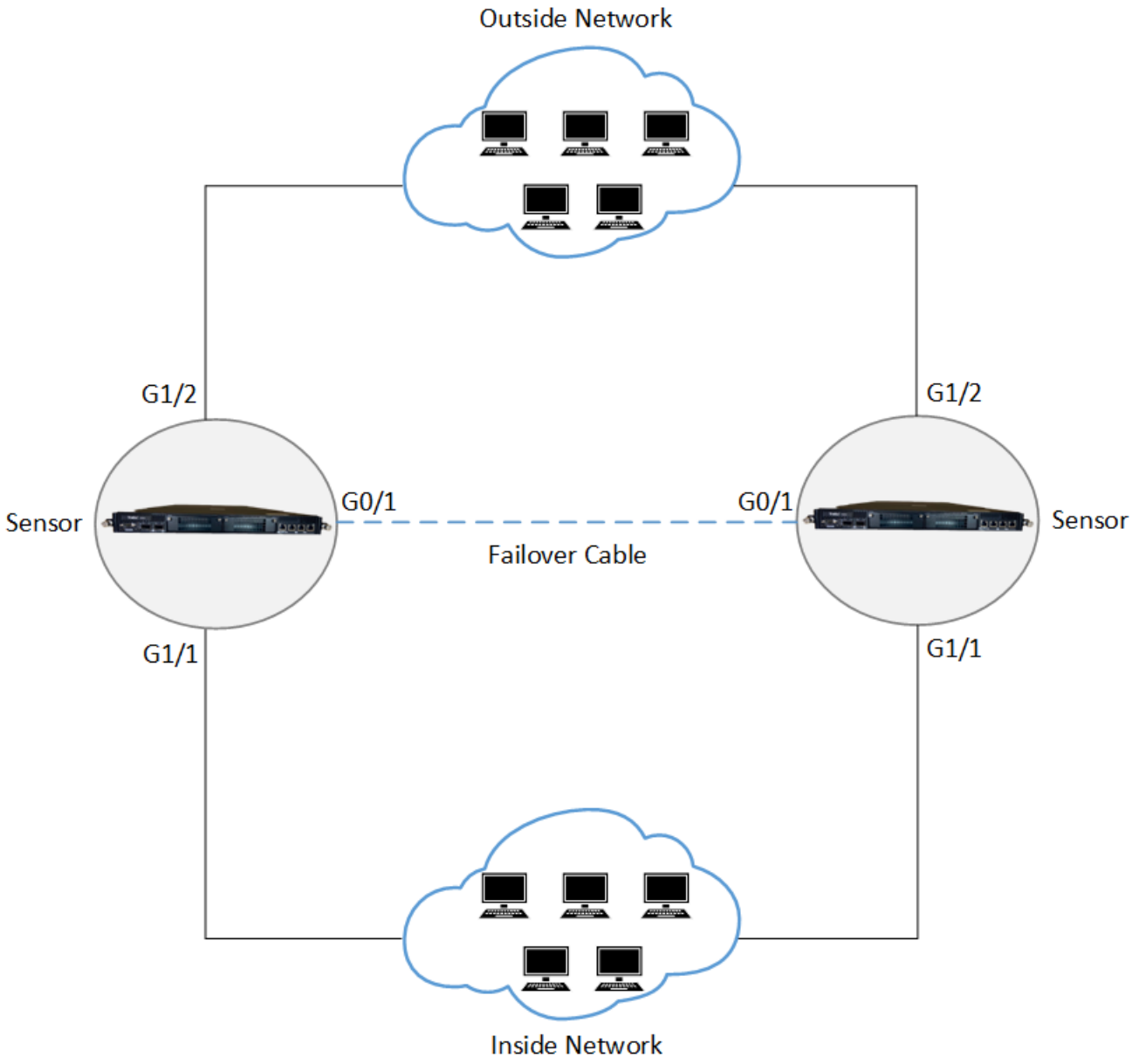
A pair of Sensors can run in parallel on a network as shown in the following figure.



Here, a pair of Sensors are "sandwiched" between a pair of switches and STP is used to control the failover process. However, this causes one Sensor to be redundant, unless a fail-over occurs. This in turn complicates the Layer 2 infrastructure and causes a latency of 12 to 50 seconds due to the STP convergence.

Instead, consider the configuration in the below figure for a single path:

Figure 280. Stack configuration



NOTE

To view the list of failover ports used for each Sensor model refer to HA pair cable connections (page 638). If you are using stacked Sensors, the failover port is G1/1.

These Sensors are configured to run inline, failopen, and function as a HA pair.

The advantages of this redundant configuration over others on a network with a single path are as follows:

- There is no dependency on Layer 2 or Layer 3 topologies for Sensor redundancy.

- If one Sensor fails, it fails open, and the other Sensor continues to scan with no interruption.
- Because they are configured as a HA pair, state will be maintained.

The disadvantages of this redundant configuration are as follows:

- Duplicate alerts are generated for UDP and ICMP attacks.
- Latency is induced as the packets traverse across two Sensors instead of one.

How to prevent duplicate alerts

To prevent the HA pair from forwarding the same alert twice, each node in the pair adheres to the following rules:

- The Sensor that received the attack packet on its monitoring port sends the signature alert to the Manager. (The Sensor that gets a copy of the attack packet from its failover peer does not send an alert.)
- The Sensor forwarding the alert also takes the configured response action, such as sending a TCP reset.
- The Sensor that has been online the longest is responsible for sending all reconnaissance and DoS alerts to the Manager.
- In the event that both Sensors have been up for exactly the same amount time, the Sensor with the higher value serial number will be responsible for sending all reconnaissance and DoS alerts.

The reality check is that because the previous "stack" configuration results in attacks arriving on the monitoring ports of both Sensors (unless blocking is enabled), this configuration will cause some duplicate alerts to be generated. The details are as follows:

- There will be no issue with reconnaissance and DoS attacks because one Sensor in a HA pair is always dedicated to send these alerts.
- There will be no issue with TCP signature attacks either, due to the stateful nature of the scanning engine. That is, even though both Sensors will get the attack packet on their monitoring ports, the second Sensor will actually get the packet on its failover port first. When it subsequently gets the packet for a second time on its monitoring port, the packet will be recognized and treated as a duplicate packet. The duplicate packet will be forwarded along, but no alert will be generated.
- However, because UDP and ICMP are not stateful, the same logic does not apply to those packets. Instead, UDP and ICMP attacks will create duplicate alerts in this configuration.

License requirement for NS9500 Sensor failover

Based on the throughput, the NS9500 Sensor requires an additional license for Sensor failover. To obtain a license, contact **Trellix Sales**.

The license is provided as a .zip or .jar file. The Manager supports both formats. The license procured contains the details of the throughput for the Sensor.

The table below shows the capacity licenses available for the NS9500 Sensor failover:

License SKUs	Throughput	Number of Sensors
FO95X10CAE-AT	10 Gbps	2 * 1 NS9500 Sensor
FO95X20CAE-AT	20 Gbps	2 * 1 NS9500 Sensor
FO95X30CAE-AT	30 Gbps	2 * 1 NS9500 Sensor

License SKUs	Throughput	Number of Sensors
FO95X40CAE-AT	40 Gbps	2 * 2 NS9500 Sensors
FO95X60CAE-AT	60 Gbps	2 * 2 NS9500 Sensors
FO95X100CAE-AT	100 Gbps	2 * 4 NS9500 Sensors

The table below shows the upgrade capacity licenses available for the NS9500 Sensor failover:

License SKUs	Throughput	Number of Sensors
NS95XF1020CAE-DT	10 to 20 Gbps	2 * 1 NS9500 Sensor
NS95XF1030CAE-DT	10 to 30 Gbps	2 * 1 NS9500 Sensor
NS95XF1040CAE-DT	10 to 40 Gbps	2 * 2 NS9500 Sensor
NS95XF1060CAE-DT	10 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF10100CAE-DT	10 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF2030CAE-DT	20 to 30 Gbps	2 * 1 NS9500 Sensor
NS95XF2040CAE-DT	20 to 40 Gbps	2 * 2 NS9500 Sensor
NS95XF2060CAE-DT	20 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF20100CAE-DT	20 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF3040CAE-DT	30 to 40 Gbps	2 * 2 NS9500 Sensor
NS95XF3060CAE-DT	30 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF30100CAE-DT	30 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF4060CAE-DT	40 to 60 Gbps	2 * 2 NS9500 Sensors
NS95XF40100CAE-DT	40 to 100 Gbps	2 * 4 NS9500 Sensors
NS95XF60100CAE-DT	60 to 100 Gbps	2 * 4 NS9500 Sensors

You can upload the license from the **Licenses** page in the Manager. In the Manager, go to Manager → <Admin Domain> → Setup → **Licenses**.

License requirement for NS7600 Sensor failover

The table below shows the capacity licenses available for the NS7600 Sensor failover:

License SKUs	Throughput	Number of Sensors
FO76X05ECE-AT MSP-NS76FO05-OT	5 Gbps	2 * 1 NS7600 Sensor
FO76X10ECE-AT MSP-NS76FO10-OT	10 Gbps	2 * 1 NS7600 Sensor
FO76X15ECE-AT MSP-NS76FO15-OT	15 Gbps	2 * 1 NS7600 Sensor

You can upload the license from the **Licenses** page in the Manager. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Licenses**.

NOTE

Upgrade capacity licenses are not available for individual NS7600 Sensor or NS7600 Sensors in failover pairs. For increasing Sensor throughput, new license can be purchased from **Trellix Sales**.

License requirement for NS7500 Sensor failover

Based on the throughput, the NS7500 Sensor requires an additional license for Sensor failover. To obtain a license, contact **Trellix Sales**.

The table below shows the capacity licenses available for the NS7500 Sensor failover:

License SKUs	Throughput	Number of Sensors
FO75X03CAE-AT	3 Gbps	2 * 1 NS7500 Sensor
FO75X05CAE-AT	5 Gbps	2 * 1 NS7500 Sensor
FO75X075CAE-AT	7.5 Gbps	2 * 1 NS7500 Sensor

The table below shows the upgrade capacity licenses available for the NS7500 Sensor failover:

License SKUs	Throughput	Number of Sensors
NS75XF35CAE-DT	3 to 5 Gbps	2 * 1 NS7500 Sensor
NS75XF375CAE-DT	3 to 7.5 Gbps	2 * 1 NS7500 Sensor
NS75XF575CAE-DT	5 to 7.5 Gbps	2 * 1 NS7500 Sensor

You can upload the license from the **Licenses** page in the Manager. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Licenses**.

License requirement for NS3600 Sensor failover

Based on the throughput, the NS3600 Sensor requires an additional license for Sensor failover. To obtain a license, contact **Trellix Sales**.

The table below shows the capacity licenses available for the NS3600 Sensor failover:

License SKUs	Throughput	Number of Sensors
FO36X01ECE-AT MSP-NS36FO01-OT	1 Gbps	2 * 1 NS3600 Sensor
FO36X03ECE-AT MSP-NS36FO03-OT	3 Gbps	2 * 1 NS3600 Sensor

License SKUs	Throughput	Number of Sensors
FO36X05ECE-AT MSP-NS36FO05-OT	5 Gbps	2 * 1 NS3600 Sensor

You can upload the license from the **Licenses** page in the Manager. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Licenses**.

NOTE

Upgrade capacity licenses are not available for individual NS3600 Sensors or NS3600 Sensors in failover pairs.

Configuration of the ports on each Sensor

To function as a HA pair, the two Trellix IPS Sensors must be the same model and have the same Sensor image (Sensor software version).

You can create Sensor fail-over pairs even if the monitoring ports are in different operating modes, that is some ports in Inline, some in SPAN, and some in Tap mode. For example, you can create an NS7100 fail-over pair with monitoring ports G0/1-G0/2, G3/1-G3/2, G3/3-G3/4 and G3/5-G3/6 deployed in Inline mode and port G3/7 deployed in SPAN mode.

In some Sensor models, a monitoring port is configured for the primary-secondary heartbeat. In such cases, the peer monitoring port is disabled. For example, in NS7200, monitoring port G0/1 is used for the heartbeat and when you create the HA pair, port G0/2 is disabled.

Note that the port deployment modes of both the primary and secondary Sensors must be the same. For example, if port G3/1 is deployed in SPAN mode in the primary then G3/1 of the secondary must be deployed in SPAN mode as well.

By design, there will always be a certain amount of independence among the Sensors. For example, the solution must be flexible enough to handle a network on which a primary path runs at 100 Mbps full duplex, but the secondary path runs at only 10 Mbps half duplex.

This is the proper time to configure each port pair to fail open or closed. In previous Trellix IPS versions, you could only configure each Sensor in a HA pair to fail closed. Now, you can configure one Sensor to fail closed and the second to fail open.

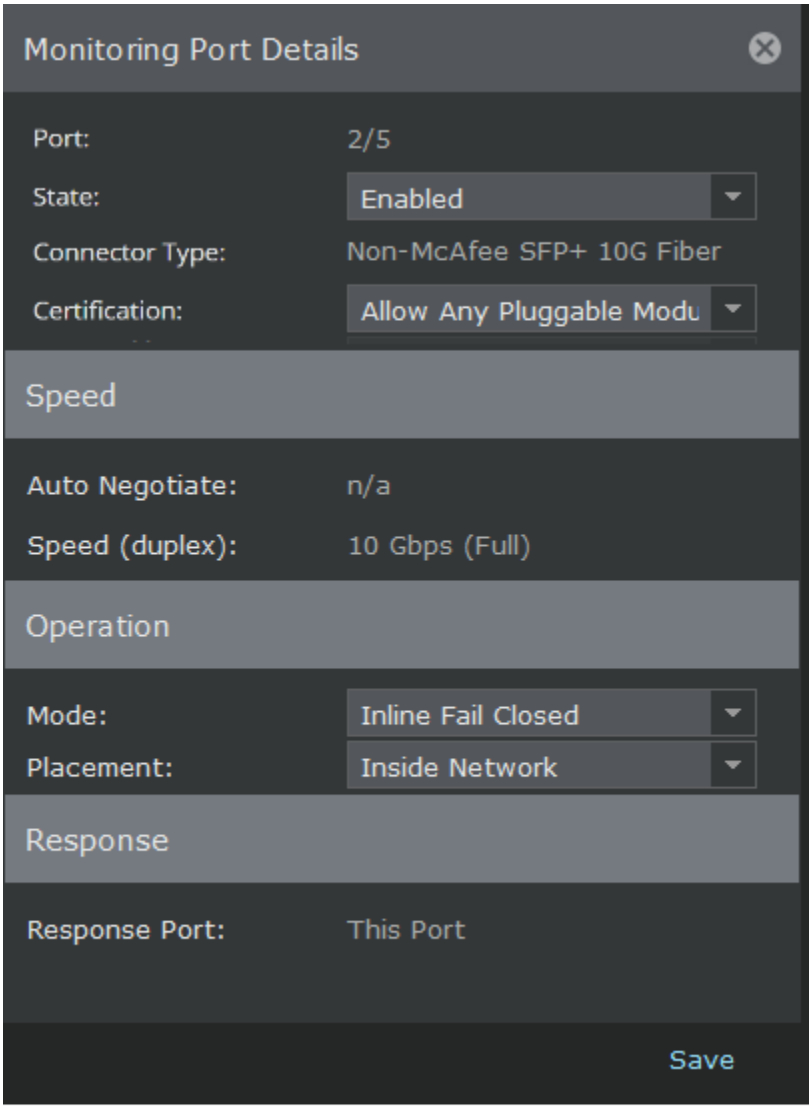
NOTE

There is no special requirement for a minimum Sensor software version to be able to configure one Sensor to fail closed and the other to fail open.

Before creating a HA pair, you have to change the **Media Type** to **Copper** in the **Physical Ports** page when using copper SFP's. A port mismatch error may be generated on the **Faults** tab in the **Logs** page as the default media type configuration is **Fiber**. If such an error is generated, you may have to delete and recreate the HA pair.

You can configure the port speed and operating mode from the **Physical Ports** page in the Manager:

Figure 281. Configure Monitoring port: 1/5 window



Potential pitfall

When you configure a HA pair, you must designate a "Primary" and "Secondary" Sensor. By design, the configuration of the Primary Sensor is copied to the Secondary Sensor, overwriting the original configuration on the Secondary.

If you intend to configure both Sensors to fail-closed or fail-open, you configure the ports on the Sensor you intend to designate as the primary during the HA pair creation process.

If you intend to have one Sensor fail-closed and the other fail-open, however, you must revisit the **Physical Ports** page of one or both Sensors after the HA pair creation and make the appropriate changes.

A note on fail open functionality for GE ports

The GE ports cannot fail open on their own. You must purchase an optical bypass kit for each port pair you wish to fail open.

If a Sensor is restarted, hangs, or fails to come up after being turned on, the optical bypass kit takes over and ensures the link remains active. When configured as a HA pair, this logic still applies, except in the case in which the Sensor port actually fails. In this case, the bypass kit does not change to bypass mode. Instead, the port pair fails closed and the redundant link takes over.

The details of optical bypass kits are beyond the scope of this document. Refer to [Trellix Intrusion Prevention System Gigabit Optical Fail-Open Bypass Kit Guide], which accompanies the Optical Fail-Open kit.

A caution about active-passive failover

The option to fail one Sensor closed and one Sensor open was intended for use with active-passive configurations. When the order in which the redundant paths will be used is known, you can safely configure the Sensor on the primary path to fail closed and the Sensor on the secondary path to fail open. The result is as follows:

- If the Sensor on the primary path fails, it will force the secondary path to take over, which will ensure the link remains protected.
- In the unlikely event that the secondary path has become active and the Sensor on it fails as well, traffic will no longer be scanned, but will continue to flow.

You might prefer to shut down the Internet connection if the traffic on the secondary path cannot be scanned for intrusions. In this case, you would configure both Sensors to fail closed.

On a network on which both paths are active, there is no way to predict the order in which the paths will fail. Configuring a Sensor to fail open in this context would at best negate the purpose of the Trellix IPS redundancy. Furthermore, if there were asymmetric flows on the paths, the remaining Sensor would not see all the packets from those flows and therefore be susceptible to false positives and false negatives.

Installation of the Sensors physically

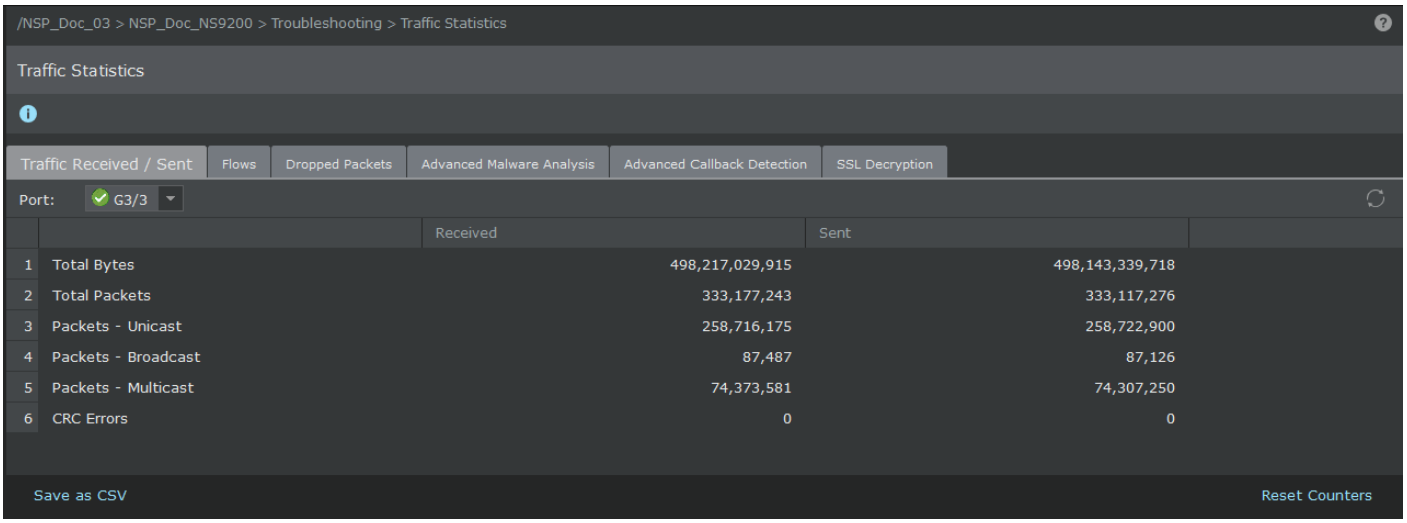
Installing Sensors at this point may seem premature. After all, you will no doubt perform tests once the HA pair has been configured. The logic here is to confirm connectivity and proper scanning with as few variables as possible. If basic connectivity and scanning prove to be fine now, but fail after configuring the HA pair, you at least know the issue is specific to the HA pair.

During Sensor boot up, there is a small time difference between when an inline fail-open port pair is enabled (port status LED is green) and actually put inline (activity LED starts blinking). This causes a minor traffic loss.

Ideally, you should test each Sensor individually. This includes, if need be, manually failing over the Primary path, so traffic will flow across the Secondary path.

You can use common utilities like **Ping** and **Traceroute** (**tracert.exe** on Windows) to test basic connectivity. You can also look at the statistics from the **Traffic Statistics** page for each Sensor port to confirm that traffic is properly flowing through it.

Figure 282. Traffic statistics



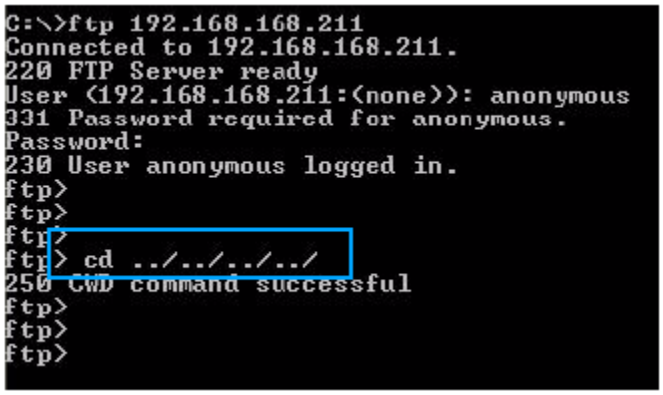
NOTE

For step-by-step procedures on verifying how to verify traffic is flowing through the Sensor, see the [Trellix Intrusion Prevention System Product Guide].

An easy and benign way to confirm that Trellix IPS is scanning for exploits is to trigger a FTP directory traversal signature.

The "attack" looks as follows:

Figure 283. FTP traversal attack



The highlighted section is the command that actually trips the signature.

If you are interested in HTTP tests, you can instead try the following URLs from your favorite browser:

http://serveraddress/inetpub/scripts/root.exe

http://serveraddress/inetpub/scripts/cmd.exe

NOTE

These exploits are specific to IIS.

CAUTION

These URLs are synonymous with Code Red and Nimda exploits, so they may trigger anti-virus software on the web server as well.

CAUTION

Use these tools for Trellix IPS testing purposes only. Trellix in no way condones use of attack traffic for any reason other than testing product connectivity and communication.

Reality check — Asymmetric routing

In the case in which the network has two active paths that route asymmetrically, these initial intrusion tests might not be successful and you may even see false positives.

In such a case, you can instead temporarily assign the Default Testing policy to the interface(s) at hand to help confirm the scanning process, or skip testing for now and hope all goes well in the steps to follow.

How to define the Trellix Intrusion Prevention System fail-over pair

After the Sensors are known to be working independently, we are ready to define a fail-over pair. It is through the fail-over pair configuration that we ensure the Sensors share flow information under normal conditions and also fail over as required.

The one important consideration is that the current configuration of "primary" Sensor will be copied over that of the "secondary" Sensor during the pair creation process.

NOTE

The creation of a fail-over pair happens in real time. There is no need to explicitly update the configuration.

When it comes to scanning roles, however, you can safely ignore the terms Primary Sensor and Secondary Sensor here. Remember that both Sensors are always scanning actively.

After completion, the display of the user interface will change to reflect the existence of the new fail-over pair:

A new fail-over pair node now exists under IPS Interfaces. That node contains icons for each interface taking part in the fail-over process. A list of its member Sensors is also found within the fail-over pair node.

Most configuration options are hereafter done at the fail-over pair node level. For example, you can now apply a policy or update the configuration at the fail-over pair node level and it will automatically propagate to each of the member Sensors. On the other hand, you still configure the port settings, view interface statistics, and upgrade the Sensor software at the Sensor node level. So,

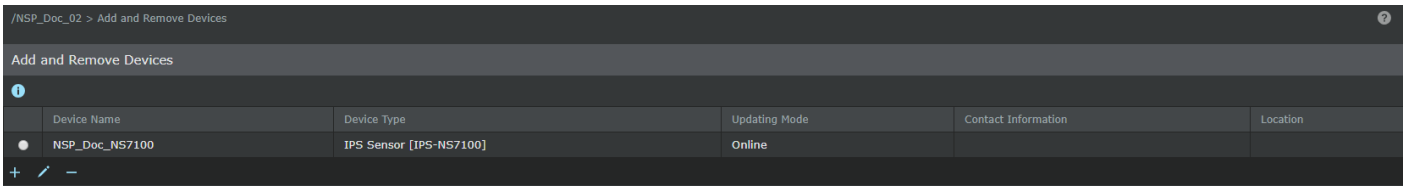
the easiest way to get a feel for the fail-over pair configuration process is to examine the user interface once the pair has been created.

NOTE

The Sensors must be running the same software version to run in a fail-over configuration. However, you upgrade software at a Sensor level, even those that are part of a fail-over pair. The recommended upgrade procedure is to, therefore, upgrade the software version on both Sensors, and then restart them sequentially. In other words, once the upgrade process is complete on both, restart the first, confirm that it has restarted without error, and restart the second.

You can view the additional details on the current fail-over status for a given interface from the **Physical Ports** page.

Figure 284. Sensor status and operational details



Connecting heartbeat cables

There is no standard heartbeat port across all Sensor models. Instead, the port or ports you use to connect the two Sensors for failover depends directly on the model at hand. The details are as follows:

NS-series Sensor model	Port used for heartbeat connection
NS9500	G0/1
NS9300	G1/1 and G1/2
NS9200	G0/1
NS9100	G0/1

NS-series Sensor model	Port used for heartbeat connection
NS7600	• G0/1 for 5 Gbps capacity • G0/1 and G0/2 for 10 and 15 Gbps capacity
NS7500	G0/1
NS7350	G0/1
NS7250	G0/1
NS7150	G0/1
NS7300	G0/1
NS7200	G0/1
NS7100	G0/1
NS5200	G1/1 and G1/2
NS5100	G1/1 and G1/2
NS3600	5
NS3200/NS3100	1

NOTE

High availability is not supported in NS3500 Sensor model.

Transceiver cable connections

All Sensor models other than the NS3200 and NS3100 use a standard Transceiver to make the heartbeat connection.

NS-series Sensors use a 10/1 GbE SFP/SFP+, 40 GbE QSFP+, or a 100 GbE QSFP28 Transceiver.

Before you attempt to connect failover cables with a Transceiver, complete the following steps:

1. Determine the appropriate Transceiver (SFP, SFP+, QSFP+, or QSFP28) for the model at hand.
2. Determine the connector type required to plug the fiber optic cable into the chosen Transceiver.
3. Determine the correct Transceiver module type and cable to support the distance between the Sensor pair.

NOTE

If you are using copper Transceivers, then use Category 6 Enhanced (Cat 6e) straight cable.

The table below addresses the first two steps. It builds off the previous table to include columns for the port type and corresponding cable connector type:

NS-series Sensor model	Port(s) used for heartbeat connection	Port type	Cable connector type
NS9500	G0/1	QSFP 28/QSFP+	Copper direct connect cable

NS-series Sensor model	Port(s) used for heartbeat connection	Port type	Cable connector type
NS9300	G1/1 and G1/2	QSFP+	Copper direct connect cable
NS9200	G0/1	QSFP+	Copper direct connect cable
NS9100	G0/1	QSFP+	Copper direct connect cable
NS7600	• G0/1 for 5 Gbps capacity • G0/1 and G0/2 for 10 Gbps and 15 Gbps capacity	SFP+	LC
NS7500	G0/1	SFP+	LC
NS7350	G0/1	SFP+	LC
NS7250	G0/1	SFP+	LC
NS7150	G0/1	SFP+	LC
NS7300	G0/1	SFP+	LC
NS7200	G0/1	SFP+	LC
NS7100	G0/1	SFP+	LC
NS5200	G1/1 and G1/2	SFP	LC
NS5100	G1/1 and G1/2	SFP	LC
NS3600	5	SFP+	LC
NS3500	1	Copper	RJ-45
NS3200/NS3100	1	Copper	RJ-45

Important notes

- The monitoring ports and failover ports use the same GBIC. (There is no special GBIC required for the heartbeat connection.)
- All GBICs and fiber optic cables are sold separately from the Sensors.

> **NOTE**
>
> Trellix officially supports GBICs purchased from Trellix price list only.

TX Transceivers

Trellix also offers a TX module type for both the standard and SFP Transceivers. The TX module type is used to connect to twisted pair (copper). With the TX module, the required cable connector type is indeed RJ45 and the maximum distance is that of standard twisted pair (100 meters).

If desired, TX modules can be used to provide the failover connection. This is not traditionally done, however, because the SX modules are less expensive and have a greater maximum distance.

NOTE

The TX module can only be used at 1000 Mbps: there is currently no option to run the TX module at 10/100 Mbps.

Cable failover through a network device

Do **not** connect the heartbeat cables through an external network device.

To keep overhead low and throughput high, the Sensors do not include layer 2 or 3 headers on the packets they pass over the heartbeat connection, and they pass data larger than the standard Ethernet maximum frame size (1518 bytes).

If you attempt to place a network device, such as a switch or router, between the heartbeat ports, the heartbeat connection will fail.

Verification of the fail-over configuration

The final steps are to:

- Confirm the Sensors are communicating over the heartbeat connection.
- Test the fail-over setup.

Sensor communication confirmation

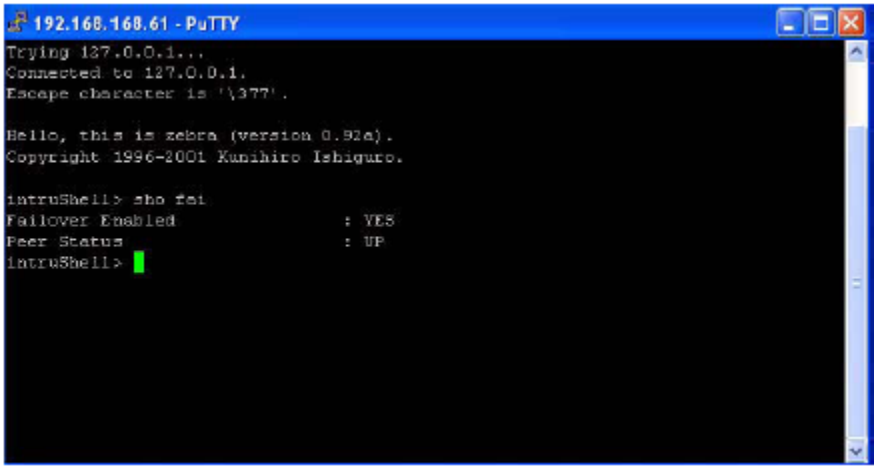
After the HA pair has been configured, failover peer status errors will appear on the **System Faults** monitor in the Manager **Dashboard** page for the selected admin domain (if enabled). You can also view this information by going to **Faults** tab under Manager → <Admin Domain Name> → Troubleshooting → **Logs**. The errors continue to appear until you connect the heartbeat cables.

The status of the communication between the Sensors can be monitored on the **Sensors** tab of **Device Manager** page of the Web-based user interface or directly from the CLI of either Sensor.

The Sensors represented by the figure *Running cables* might therefore be properly connected, but just need to be restarted.

On the CLI, you can instead run the command from either Sensor. The output includes the failover Enabled and Peer Status fields. The former indicates whether the Sensor at hand has been configured to be part of a HA pair, and the latter shows the current state of the communication between the two Sensors.

Figure 285. Sensor CLI shows failover-status window



In the figure **Sensor CLI shows failover-status window**, the Sensor is part of a HA pair, and the pair is successfully communicating over the heartbeat connection.

Test failover setup

Once communication between the Sensors has been confirmed, the failover configuration should be tested.

The way in which the configuration is best validated will vary from setup to setup, but these tests should be similar to the ones performed after the Sensors were physically installed on the network.

The key differences this time include the following:

- In the specific case in which the network at hand has two active paths that route asymmetrically, the intrusion tests that previously failed should now be successful because both Sensors are analyzing all packets from all flows.
- Existing session state should not be lost when a Sensor goes offline.

The most precise way to confirm that the session remained intact after the "failure" is to capture and analyze packets. A more rudimentary test is to open a browser and start a large download while one Sensor is taken offline. If the state is successfully kept, there will be no fatal interruption in the download process.

If the state is lost, confirm that the Sensors are indeed communicating with each other.

If the Sensors are not communicating, try the following steps in the order shown:

1. Cold start both Sensors.
2. Reconnect the cables between them. Check if the **Media Type** is selected as **Copper** when using copper SFP.
3. Recreate the HA pair.
4. If GBICs are used, confirm that Trellix supplied them.

> **⚠ CAUTION**
>
> Non-Trellix GBICs are known to create problems. If the GBICs used are not from Trellix pricelist, temporarily swap them out for those that are before spending more time on troubleshooting.

If they are communicating:

- Capture packets simultaneously on both redundant paths. This will provide a full picture of the data flow, and more insight into the problem.

How to understand virtualization

You should already be familiar with the terms *Virtual IDS* (*VIDS*), *Virtual IPS* (*VIPS*), and *sub-interfaces*.

These terms all refer to a concept more generally known as *virtualization*. The goal of virtualization is to provide scanning granularity. Virtualization enables an administrator to apply different *policies* to different groups of traffic flowing through a single Sensor port or port pair.

The terms VIDS and VIPS reinforce the idea that virtualization allows you to tailor a single Sensor solution as if it was a multiple-Sensor solution. Trellix IPS user interface uses the term sub-interface, however, and this term better describes the process by which virtualization is implemented. For this reason, we will use the term sub-interface here.

The easiest way to cover the implementation and benefits of virtualization is to start with a non-virtual Sensor implementation and work our way to multiple sub-interfaces.

All eight ports inherit and use the policy applied to the Sensor. You can apply a unique policy to each port, and many people do. This notion of hierarchy is important to remember at the outset of the discussion because, as you will soon see, sub-interfaces also take advantage of the power of the hierarchical Trellix IPS management design.

NOTE

This chapter discusses the concepts and procedures related to virtualization of Sensor monitoring ports. These virtualization concepts and procedures explained in this chapter apply to both physical and Virtual IPS Sensors. However, for information on how to deploy Virtual IPS Sensors, see [Virtual IPS Sensor deployment .]

Network scenario without virtualization

Imagine a network on which Windows and Linux hosts are interspersed. The best approach here is to apply a policy that includes attacks for both Windows and Linux hosts on all the ports through which their traffic will flow.

If this network happens to be controlled in such a way that the traffic from all the Windows hosts is flowing through one segment of the network and the traffic from all Linux hosts is flowing through a different segment, you could connect these different segments to different Sensor monitoring ports. You could then apply Windows-specific and Linux-specific policies to the respective ports. In doing so, you would minimize the chance of false positives and reduce the quantity of scanning required on each port.

When you consider that many IDS and IPS offerings only allow for a single policy per Sensor, the option to apply a unique policy to each port is much more impressive. But what happens if a Sensor doesn't have enough physical ports to cover the different ways in which traffic may be controlled on a given network? Or more realistically, what happens if the Sensor is placed at an aggregation point on the network, such as on a trunked uplink, or an administrator wants a unique policy applied to a single host or two? This is when virtualization becomes relevant.

Virtual IPS

Most Sensor-based IPS products permit you to apply only one security policy for the entire Sensor. Typically these one-policy Sensors also have only one port which cannot be segmented for more granular policy application. However, if you have multiple segments to monitor or you need to monitor aggregated traffic — like on Gigabit uplinks — a multi-port box and more granularity in the inspection process makes for a much more cost-effective and efficient security solution. Sensor appliances have multiple ports coupled with multiple policy application options. Thus, Trellix IPS offers Virtual IDS (VIDS) and Virtual IPS (VIPS).

To make use of virtualization, consider that a Sensor is made of the following resources:

- Sensor itself as a whole
- Sensor monitoring ports
- Interfaces
- Sub-interfaces

The VIPS feature enables you to configure multiple policies for multiple unique environments and traffic directions all monitored with a single Sensor. The goal of virtualization is scanning granularity. Virtualization allows you to apply multiple policies to traffic flowing through a single interface. In this way, a unique scanning policy can be applied to a single host or group of hosts, when their traffic will not travel through a unique Sensor port.

For example, suppose port G3/1 of an NS9500 Sensor is connected to the SPAN port on a switch. Port G3/1 is configured with a specific environment detection policy. The rest of the ports on the Sensor can have policies completely different than the policy on G3/1, or they can use the same policy. In this case, each monitoring port of the Sensor is an interface. The other option is to segment each monitoring port by multiple VLAN tags or CIDR addresses, each customized with its own security policy. In this case, each monitoring port is segmented into virtual sub-interfaces.

Sensors

A security policy can be applied at the Sensor level; however, this policy application is intended to be inherited by those interfaces of a Sensor whose custom-applied policy has been deleted. For example, you have created a custom IPS policy called Custom1. You apply it to interfaces G2/3, G3/1, and G3/4 on a single NS7200 Sensor. After some time, you determine Custom1 does not work effectively, and you want to delete it. You can apply a different policy to the Sensor that will allow you to delete the custom policy without having to change the policy at each interface where it has been applied. When you delete the custom policy, all of the interfaces (G2/3, G3/1, and G3/4) enforcing the policy will inherit the policy applied to the Sensor.

Interfaces

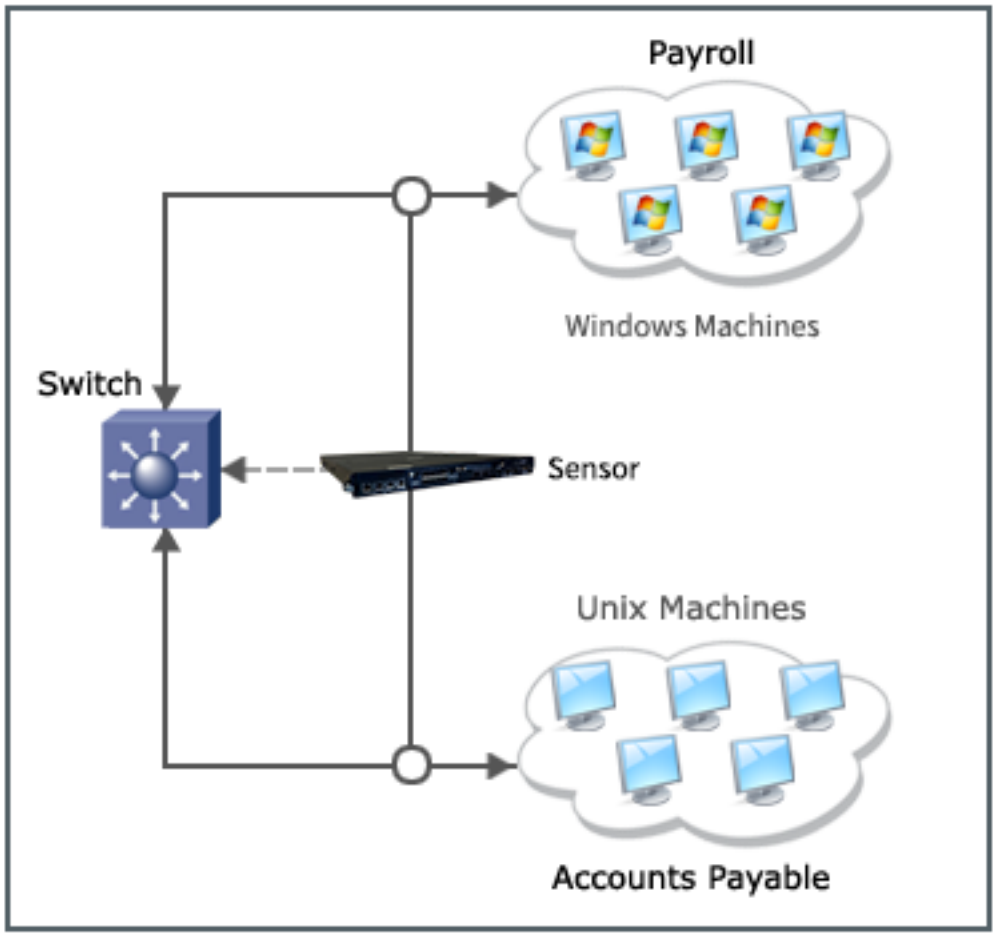
Networking professionals often interchange the terms *port* and *interface*. In the Trellix IPS context, however, there is an important distinction to be made; a port actually represents the physical component, whereas an *interface* represents the logical abstraction of one or more physical monitoring ports on a Sensor and all traffic flowing through the port(s). All Sensor interfaces are represented by FE or GE monitoring ports connected directly or through an external tap, hub, or SPAN port to network segments.

A simple, yet effective example of the difference between port and interface is with regard to a "port pair." When you configure a Sensor to run inline, you combine and manage the two physical *ports* as a single logical *interface*.

To use an example, assume that you have a Finance parent domain, and it has two child domains—Payroll and Accounts Payable. The Payroll department network is comprised entirely of Windows machines, and Accounts Payable is predominantly

Solaris. You have a single Sensor that is running in internal tap mode with two peer ports, port pair G1/1 and G1/2, monitoring traffic in the Payroll department and port pair G1/3 and G1/4 monitoring Accounts Payable. You can use a **Windows Server IPS** policy and apply it to the Payroll interface and a **Solaris Server IPS** policy to apply to the Accounts Payable interface.

Figure 286. Deploying security policies

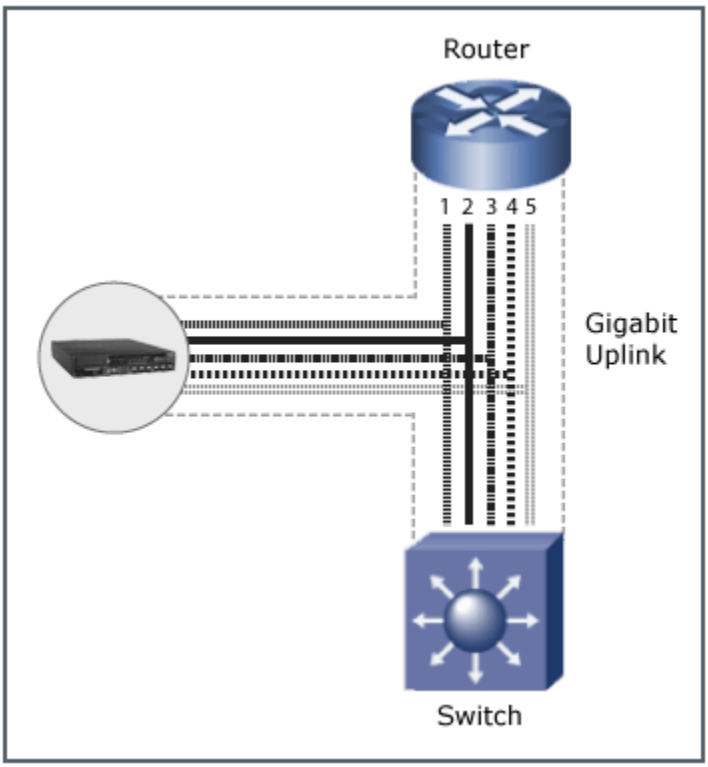


Sub-interfaces

The terms VIDS and VIPS reinforce the idea that virtualization allows you to tailor a single Sensor solution as if it were a multiple-Sensor solution. The Trellix IPS user interface uses the term *sub-interface*, and this term better describes the process by which virtualization is implemented.

Sensors take port monitoring deeper than the interface-level: you can segment the security management of an interface and apply policies at a traffic *sub-flow* level within the interface. A sub-flow, or *sub-interface*, is a segment of data within a traffic flow. This sub-interface is also a VIPS. A VIPS can be defined based one or more blocks of CIDR-based IP addresses or one or more VLAN tags. Sensors can process these data segments and apply multiple traffic policies for the multiple subnets transmitting across a single wire, right down to policies protecting individual hosts.

Figure 287. Sub-interfaces



In the above figure, a gigabit uplink between a router and a switch is monitored in external tap mode by an NS9300. Behind the switch is a corporate network with five departments: HR, Sales, Payroll, Engineering, and Marketing. The traffic for each of these departments has been segmented using VLANs with each department's traffic tagged with a distinct VLAN ID, represented by the numbers 1-5 in the illustration.

Using peer ports G0/1 and G0/2 to tap the full-duplex uplink, the NS9300 can analyze and process the VLAN IDs in the traffic transmitted between the router and switch. The security administrator can configure unique policies for each VLAN ID (representing traffic from the different departments) within the uplink, rather than apply a single policy across the entire interface. In this scenario, each of the five VLAN IDs from each of the five departments can have a distinct policy assigned to it, or different combinations of the VLAN IDs within the uplink can have the same policy applied. Policy application simply depends on assigning a policy to an interface or sub-interface resource as you see fit.

Policy inheritance

A security policy defined at the admin domain level is inherited by its child admin domains, and the resources—Sensor interfaces and sub-interfaces—within the child domains unless the policy is explicitly set during resource configuration. If you want to set another policy for a specific resource, you can select or create a different policy.

The policy inheritance order is shown below.

When you allocate Sensor interfaces to an admin domain (a process that is part of child admin domain creation), all of the interfaces automatically inherit the admin domain's policy. So, as part of the process of creating an admin domain, you assign the policy to be inherited by the allocated interfaces. If you want, you can then go into each allocated interface and assign a different policy.

Changing policies at higher levels (for example, admin domain level) once they have been applied at a lower level has no effect on the lower levels (for example, interface level).

NOTE

A custom policy defined at a child admin domain level can't be applied to a resource at the parent admin domain level.

DoS policies

It is also worth noting that each interface and sub-interface maintains a unique *Denial-of-Service (DoS) profile*. DoS policies can be applied to subsets of a sub-interface for even more granular security monitoring. These DoS profile instances are known as *DoS IDs*. You can monitor DoS attacks to the granularity of individual hosts. Any deviation from the established normal traffic behavior flags a DoS condition, even a situation wherein a single host/subnet downstream to a gigabit network link comes under attack—with even a couple of Mbps of traffic. The Sensor's granular DoS detection can spot the attack.

Another reason to consider creating a sub-interface for a single host is when that host tends to have traffic patterns that are significantly different from the rest of the hosts sharing the interface. An example is an e-commerce Web server as compared to internal file and print servers; the Web server will no doubt have a different traffic pattern than the file and print servers. If not isolated from the file and print servers, that one Web server is potentially skewing the calculations for the entire interface and therefore creating false positives, or even false negatives, in the DoS analysis process. By isolating that one host, you allow the Sensor to analyze the traffic destined to and originating from the file and print servers independently of the traffic to and from the Web server, and therefore increase the likelihood the analysis will be accurate.

Port versus interface

Networking professionals often interchange the terms **port** and **interface**, and we have purposely done so to this point. In the Trellix IPS context, however, there is an important distinction to be made; a port actually represents the physical component, whereas an interface represents the logical abstraction of one or more ports.

A simple example of the difference between port and interface is with regard to a "port pair." When you configure a Sensor to run inline, you combine and manage two physical ports as a single logical interface.

A sub-interface is a further abstraction of an interface. It allows an administrator to apply different scanning policies to different types of traffic flowing through the same interface.

Network scenario with virtualization

Assume there is a single uplink to and from the Internet for all internal hosts, and that this uplink sends traffic through a Sensor running inline. That is, the Sensor does indeed reside at an aggregation point for this network.

If the Windows and Linux hosts are scattered across the network, creating a sub-interface will be of little value; the best approach here is to again use a single policy that will account for both types of traffic.

If these hosts have been given different ranges of IP addresses or reside on different VLANs, however, you can create a sub-interface for each block of addresses or VLAN, and achieve the same result across a single interface as you did previously when each group of traffic traversed a unique port.

Additionally, if there is a requirement to apply a unique policy to a specific host, you can do so by creating a sub-interface to represent that one host. For example, if your DMZ is comprised entirely of Windows servers, with the exception of a single Solaris server, it makes good sense to apply a Windows-specific policy to the interface and a Solaris-specific policy to a sub-interface representing that one host.

It is also worth noting that each interface and sub-interface maintains a unique denial-of-service (DoS) profile. So another reason to consider creating a sub-interface for a single host is when that host tends to have traffic patterns that are significantly different from the rest of the hosts sharing the interface. An example is an e-commerce Web server as compared to internal file and print servers; the Web server will no doubt have a different traffic pattern than the file and print servers. If not isolated from the file and print servers, that one Web server is potentially skewing the calculations for the entire interface and therefore creating false positives, or even false negatives, in the DoS analysis process. By isolating that one host, you allow the Sensor to analyze the traffic destined to and originating from the file and print servers independently of the traffic to and from the Web server, and therefore increase the likelihood the analysis will be accurate.

This may appear similar to the option of creating unique DoS IDs at the interface level, and it is. The difference is that interface-level DoS IDs are limited to a single layer of CIDR addressing, whereas DoS IDs at the sub-interface level allow you to create DoS profiles by VLAN ID and have two layers of CIDR addressing. For example, you can create a DoS profile for an entire CIDR range at the interface level, and then create a unique DoS profile for an individual host on that same network at the sub-interface level.

Interface types

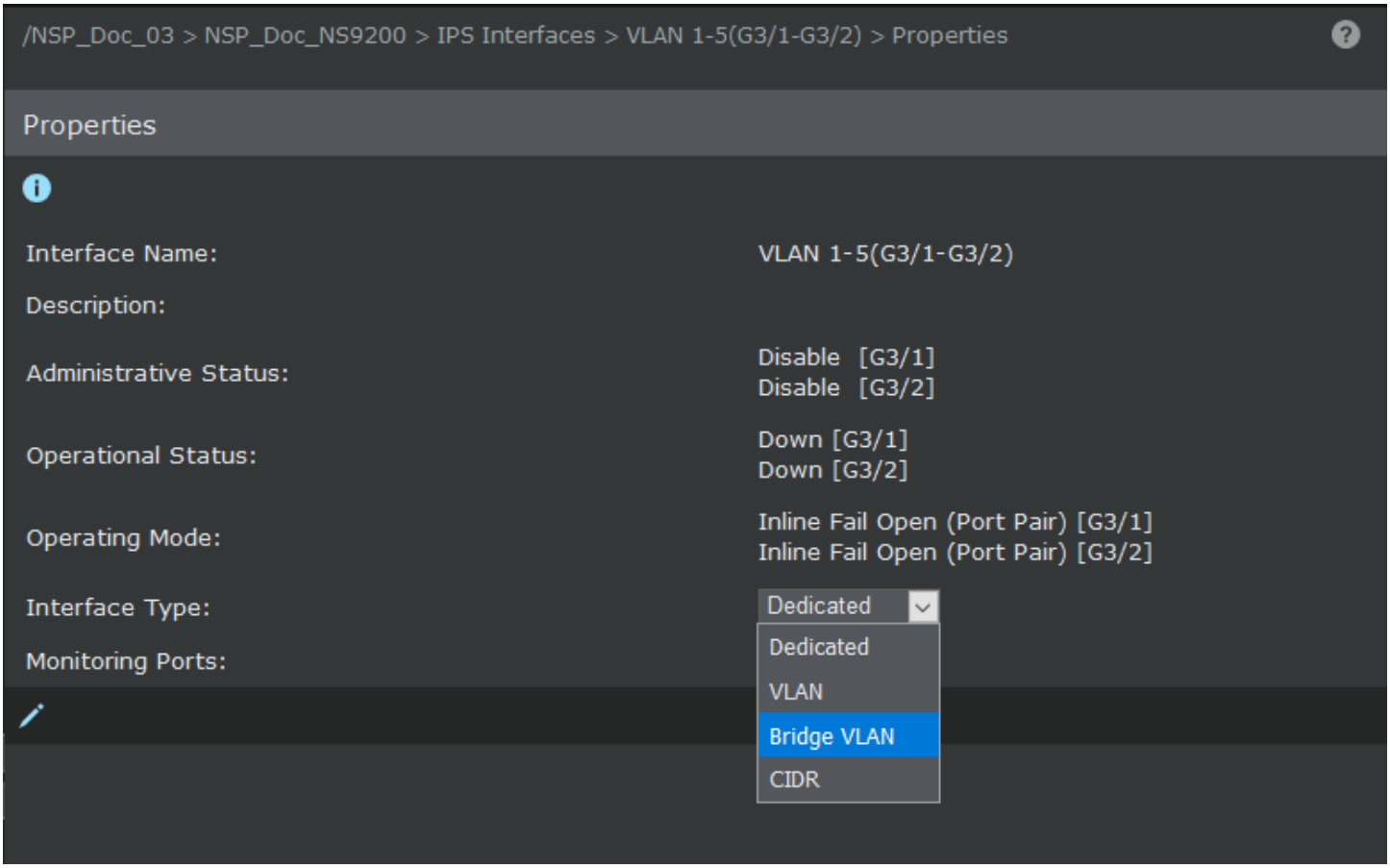
Valid interface types include:

- **Dedicated**
- **VLAN**
- **Bridge VLAN**
- **CIDR**

Dedicated interfaces

The **Interface Type** option in the **Edit** window has the default **Dedicated** interface.

Figure 288. Interface Type option



When the default interface supports a sub-interfaces, Virtualization is effectively disabled.

VLAN interfaces

When you choose an interface type of VLAN, you instruct the Sensor to apply policies according to VLAN tags.

Background

Imagine you have two hosts residing on the same VLAN and connected to two different switches, but you want them to communicate as if they were directly connected to the same switch, this includes sharing Layer 2 multicasts and broadcasts. The way to achieve this goal is to set up a trunk between the two switches.

When you enable trunking on both switches, they will pass extra information in each frame to identify the VLAN to which that frame belongs.

As a frame travels across a trunk, the receiving switch checks the VLAN ID and copies the frame to local ports in the same VLAN as if that frame had originated locally.

A switch that meets the industry-standard, IEEE 802.1Q specification for trunking will include an additional 32 bits in each frame, of which 12 of the bits are used to indicate the VLAN ID for that frame. Valid VLAN ID values are therefore between 0 and 4095 (2^12).

The actual supported VLAN ID values will vary by switch implementation. For example, VLAN 0 is generally not used, VLAN 1 is the default VLAN is used for management on Cisco switches, and many switches do not support all the way up to VLAN ID 4095 unless you use an enhanced version of software. Trellix IPS will accept values between 1 and 4095.

NOTE

Trellix IPS will initially accept a value of 0 in the GUI, but then discard it. For example, if you enter a range of 0 - 2, Trellix IPS will accept it, but only include VLAN IDs 1 and 2 in its configuration.

CAUTION

If you send trunked traffic across a device that does not specifically support trunking, that device will typically discard tagged frames as bad (too large) and communication will fail.

NOTE

Trellix IPS supports (passes and scans) frames meeting the 802.1Q standard. It does not, however, support Cisco's proprietary, legacy Inter-Switch Link (ISL) protocol. ISL traffic sent through a Sensor will be forwarded and would not be dropped.

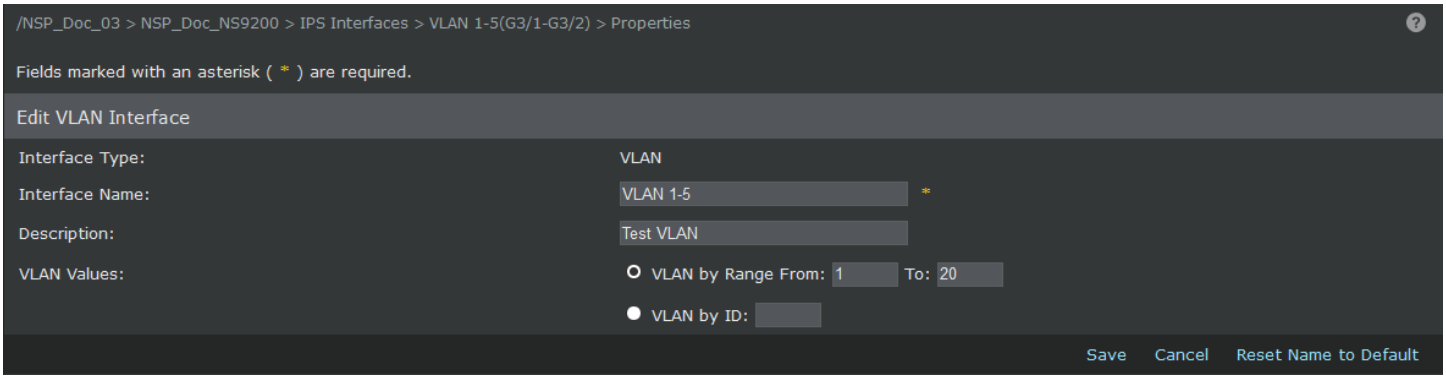
Defining VLAN interfaces definition

After you have configured an interface to be of type VLAN, the next step is to edit it and associate VLAN IDs with it. You will want to define here all the VLANs whose traffic you anticipate will traverse this interface.

The expectation is that you will see traffic from multiple VLANs. (If not, it would be simpler to leave the interface as type Dedicated and apply a single policy, or consider a CIDR sub-interface instead).

You can specify VLAN values by Range from or by IDs.

Figure 289. Edit VLAN Interface window

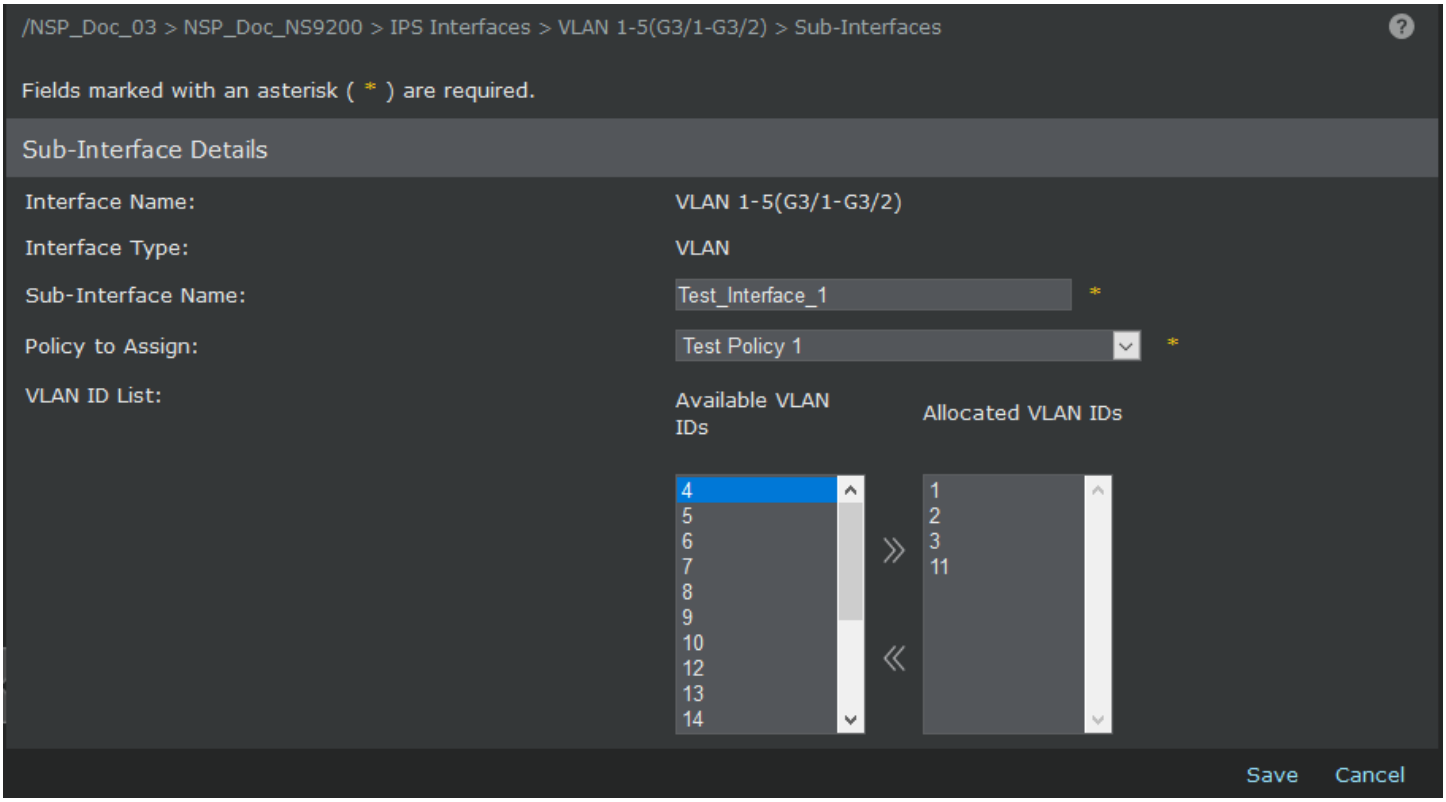


VLAN sub-interfaces definition

The next step is to allocate one or more of those VLANs to a sub-interface to further refine the scanning process.

In the figure, we are adding a sub-interface called "WindowsServers", assigning it the **Default Prevention** policy, and allocating VLANs 2 and 5 to it:

Figure 290. Sub-Interface



We highly recommend you give the sub-interface a name that indicates its contents. The name could have been as obvious as VLANS_1_2. It is more common, however, to name the sub-interface after the user community or hosts it protects, for example, Accounting_VLANs or, as is the case here, WindowsServers.

When we now look back at the details of the interface, a few things have changed:

The IPS interfaces now includes an icon representing the new sub-interface.

The details of the final configuration are as follows:

- Traffic with a VLAN tag ID of 2 and 5 will have the **Default Prevention** policy applied to it.
- Traffic with a VLAN tag ID of 1,3,and 4 will have the **Default Detection** policy applied to it.

We could of course create another sub-interface for Linux servers and allocate VLAN 7-9 to it, for example. At that point, all VLANs defined on the VLAN 7-9 interface would be allocated to sub-interfaces.

If we subsequently wanted to allocate yet another VLAN to a sub-interface, we would first have to de-allocate an existing VLAN ID from an existing sub-interface or add another VLAN ID to the G3/3-G3/4 interface.

Bridge VLAN interfaces

A Bridge VLAN interface is similar to that of a VLAN interface except for that post traffic inspection, the Sensor changes the VLAN tag of the traffic to the one that you specify.

Thus the Sensor bridges the traffic between these two VLANs. This feature can enable effective utilization of the IPS capacity of your Sensors.

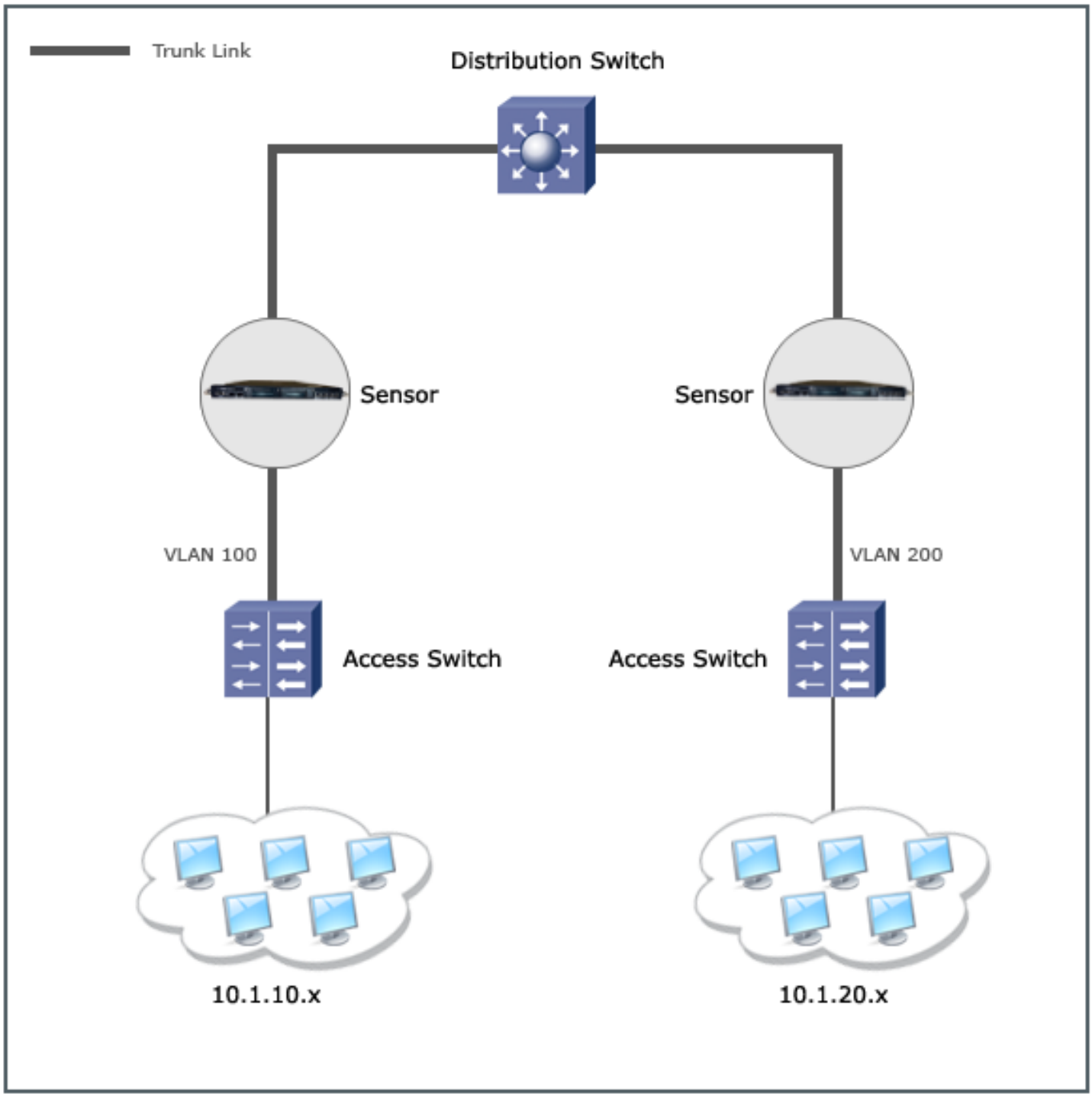
NOTE

This is applicable only for NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, and NS3600 Sensors deployed inline fail-closed. However, ports that have built-in fail-open, support VLAN bridging even when the ports are configured for fail-closed. VLAN bridging is not supported on NS5200, NS5100, NS3500, NS3200, and NS3100 Sensors.

Background

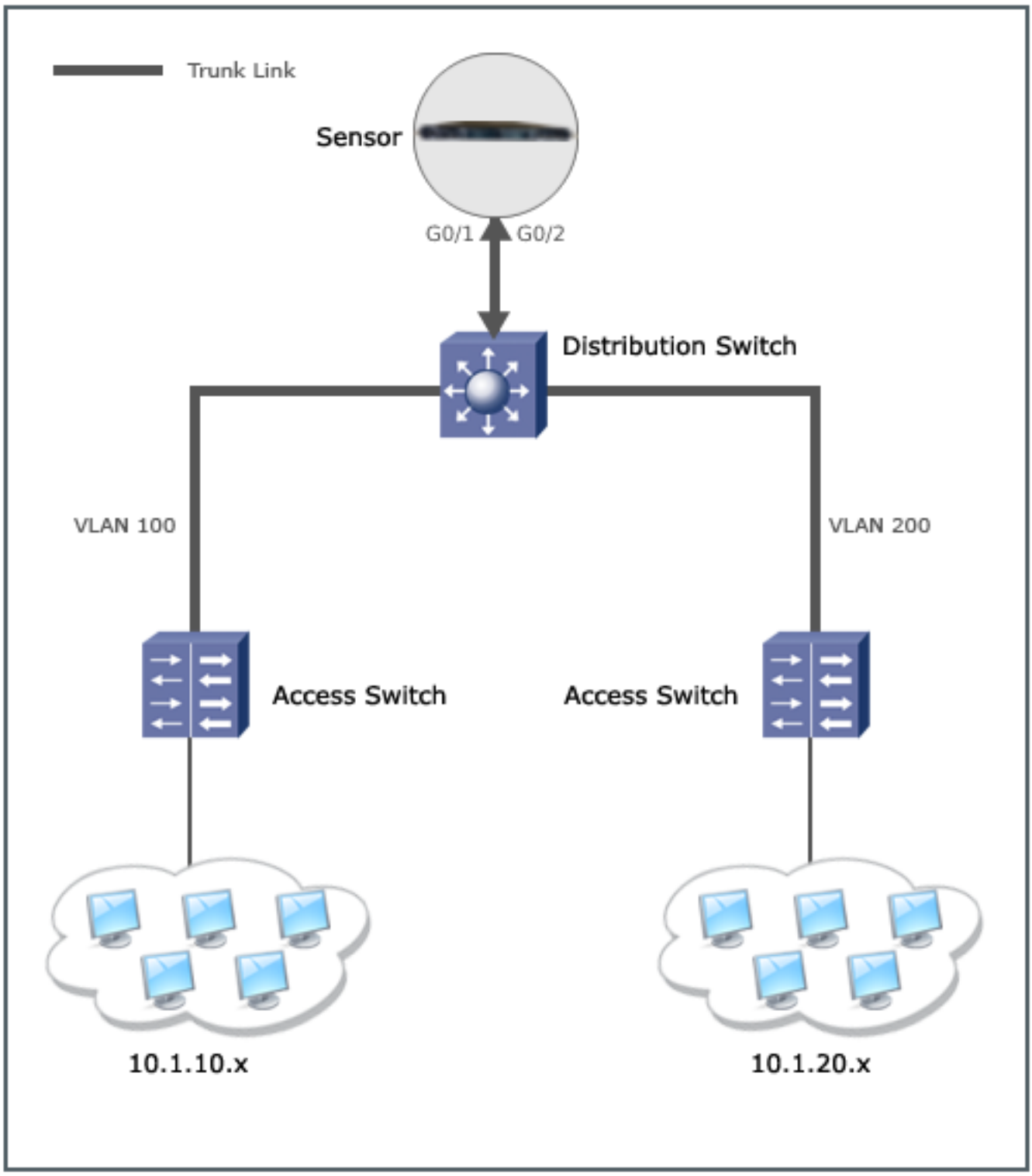
Consider a typical network where many access switches connect to a few distribution switches as shown partly in the figure below. To monitor inter-VLAN traffic, you can place a Sensor inline for every trunk link between the access switches and the distribution switch. However, this would mean deploying a large number of Sensor port pairs (one for every trunk link between the access and distribution switches) and hence, may require a large number of Sensors.

Figure 291. A simple scenario without VLAN bridging



An alternative and cost-effective solution for this scenario would be to monitor the aggregated traffic at the distribution switch as shown in the figure below.

Figure 292. A simple scenario with VLAN bridging



With this method, the same volume of traffic can be monitored with less number of Sensors, provided that the aggregate traffic at the Distribution switch monitored by the Sensor does not exceed the Sensor throughput. This solution requires the following:

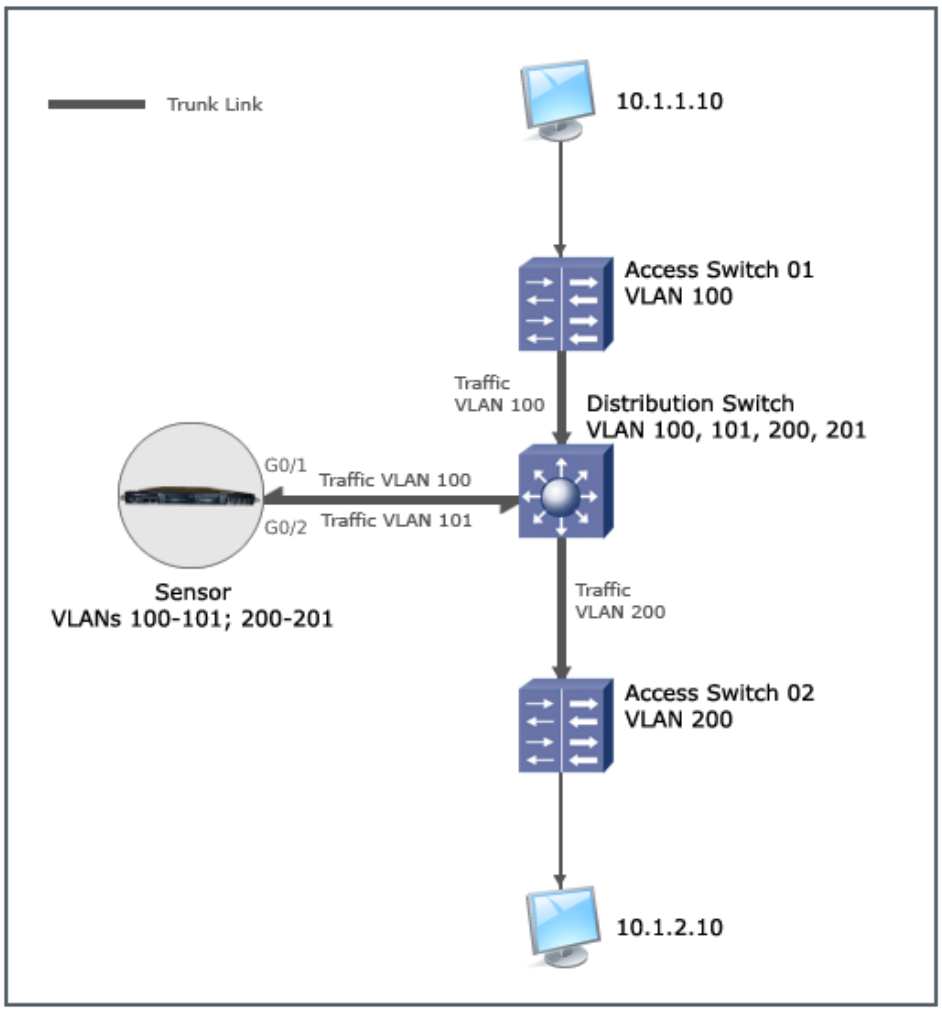
the VLANs on the access switches and the distribution switch must be configured in such a way that all traffic that is to be subjected to IPS is forwarded to the Sensor before being switched or routed. Then the Sensor inspects and bridges the traffic using VLAN Bridging. Effectively, traffic from the access switches is switched or routed only after VLAN bridging by the Sensor.

Additionally, if you have multiple Sensors (or Sensor interfaces) connected to the distribution switch, then you can configure Ether Channel Load Balancing (ECLB) on the switch so that the traffic is split across the Sensors or Sensor ports for optimal utilization of your IPS infrastructure. This section does not have information on how to configure your switches for ECLB. Refer to the documentation provided with your switch.

A simple VLAN bridging scenario

Consider this scenario to understand the advantages of VLAN Bridging:

Figure 293. VLAN bridging scenario



1. Host 10.1.1.10 in VLAN 100 tries to communicate with a host 10.1.2.10 in VLAN 200.
2. Access Switch 01 tags the packet with VLAN 100 and forwards it to the Distribution Switch. The Distribution Switch is an L3 switch, which has trunk links to the Sensor.

3. In the distribution switch, only the ports connected to G0/1 of the Sensor and Access Switch 01 are configured for VLAN 100. No other ports are configured for 100. This is a very critical configuration for enforcing IPS. When the Distribution Switch receives VLAN 100 traffic, the only network path available is to the Sensor.
4. In the distribution switch, only the ports connected to G0/2 are configured for VLAN 101.
5. The Sensor is configured to bridge VLANs. This is done by specifying the VLANs to be bridged as a pair at the interface level.
6. For this scenario, let us assume that you have configured VLANs 100 and 101 as a VLAN pair. Assuming the traffic is clean, the Sensor changes the VLAN tag to 101 and forwards it to the Distribution Switch through the corresponding peer port. Conversely, traffic tagged 101 is changed to tag 100 and sent through the corresponding peer port. Thus, the Sensor bridges VLANs 100 and 101.
7. The Distribution Switch receives the traffic tagged 101. Based on ARP, ARP replies, and the destination subnet, the switch forwards the traffic to the appropriate port so that it reaches host 10.1.2.10.

Note the following before you configure VLAN Bridging:

- You can configure VLAN Bridging only on Sensors that are deployed inline fail-closed, unless you are attempting this on ports that have in-built fail-open.
- Note that the distribution switch configuration has to keep the traffic separation of inbound/outbound on one Sensor's two links: the switch must restrict traffic from the outside net VLAN to only one link, and the inside net VLAN to only the other link. This switch configuration should be consistent with the Sensor's port designations of inbound/outbound.
- If the traffic has a VLAN tag that is not configured on the Sensor, then post-IPS the traffic comes out from the Sensor to the switch with the same VLAN tag. Because both G0/1 and G0/2 are connected to the same switch, it will detect a loop and attempt to bring down the ports. For this reason, it is important that you disable Spanning Tree Protocol on the switch.
- VLAN bridging will not work when Sensor enters L2 mode or when Sensor ports fail-open. This may result in traffic drop.

Define bridge VLAN interfaces

Configuring a Sensor to act as a VLAN Bridge.

1. Defining Bridge VLAN Interfaces: You need to change the Interface Type to Bridge VLAN.
   a. Go to Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Interface_Name> → **Properties**.

      The **Properties** page displays.

   b. In the **Properties** page, change the **Interface Type** to **Bridge VLAN** and click **OK** to confirm.

      > ⚠ **CAUTION**
      >
      > When you change the Interface Type, the configurations relevant to the earlier Interface Type is lost. For example, if the Interface was of type VLAN earlier with VLAN ID list configured, the list is lost when you change this interface to Bridge VLAN.

2. Specifying the VLAN pairs: At the Interface level, you need to specify the VLANs that are to be bridged as a pair. For example, if you want to bridge VLANs 10 and 11, you need to specify them as a pair. Then, the Sensor tags VLAN 10 traffic as VLAN 11 before forwarding it through the peer port. Similarly, it tags VLAN 11 traffic as VLAN 10.

You can define all the VLANs that you want the Sensor to bridge now. Then, you can assign all or some of them to the Sub-Interfaces.

For each VLAN pair that you want to specify:

a. From the **Properties** page, click .

   The **Properties** page appears.

b. Enter the **VLAN ID** and **Peer VLAN ID** in the corresponding fields and click **Save**.

c. Repeat the steps a and b to add more VLAN pairs.

> **NOTE**
>
> To delete a VLAN pair, select it in the **Properties** page and click .

> **NOTE**
>
> At a given point in time, up to 127 pairs of VLANs can be defined per VIDS. When you reach 127 VLAN pairs at the interface level, you can assign some or all of them to a Sub-Interface to be able to define more at the interface level.

> **NOTE**
>
> The VLANs should be unique within an Interface. For example, you cannot configure 20-21 and 22-21 as two VLAN pairs for one Interface.

> **NOTE**
>
> The VLAN pairs are symmetric; the VLANs are mapped with their peer IDs regardless of the Sensor port in which they are seen. The switch port connecting to the Sensor port must be configured to receive the corresponding VLAN traffic.

3. Updating the Sensor: After you define the Bridge VLAN interface, you must update the Sensor about this configuration change.

Define bridge VLAN sub-interfaces

You can allocate one or more VLAN pairs defined at the interface to a sub-interface to further refine the process.

1. Select Devices → <Admin Domain Name> → Devices → <Device_Name> → IPS Interfaces → <Interface_Name> → **Sub-Interfaces**.

   The sub-interface list appears.

2. To allocate VLAN pairs to an existing sub-interface, click ; else click .
3. If you are creating the sub-interface, specify the sub-interface name and policy to be applied.
4. Select the required VLAN pairs from the **Available VLAN IDs** list and move them to the **Allocated VLAN IDs** list.

   The Available VLAN ID list contains the VLAN pairs defined at the interface.

5. For the configuration shown above, if the Sensor sees traffic tagged with VLANs 10, 11, 12, or 13, it applies the corresponding policy of Finance_VLAN sub-interface. After applying this policy, if the Sensor finds traffic to be clean, it changes the VLAN tag to that of the peer VLAN and forwards it through the peer port. For example, if the traffic is tagged 12 and seen at G0/1, then tags it as VLAN 13 and forwards it through G0/2.

   If the traffic seen at an interface is tagged with a VLAN defined at the Interface level but not allocated to a Sub-Interface, then the Sensor applies the policy specified for the Interface and also changes the VLAN tag to that of its peer.

6. Updating the Sensor: After you allocate VLAN pairs to sub-interfaces, you must update the Sensor about this configuration change.

VLAN bridging details

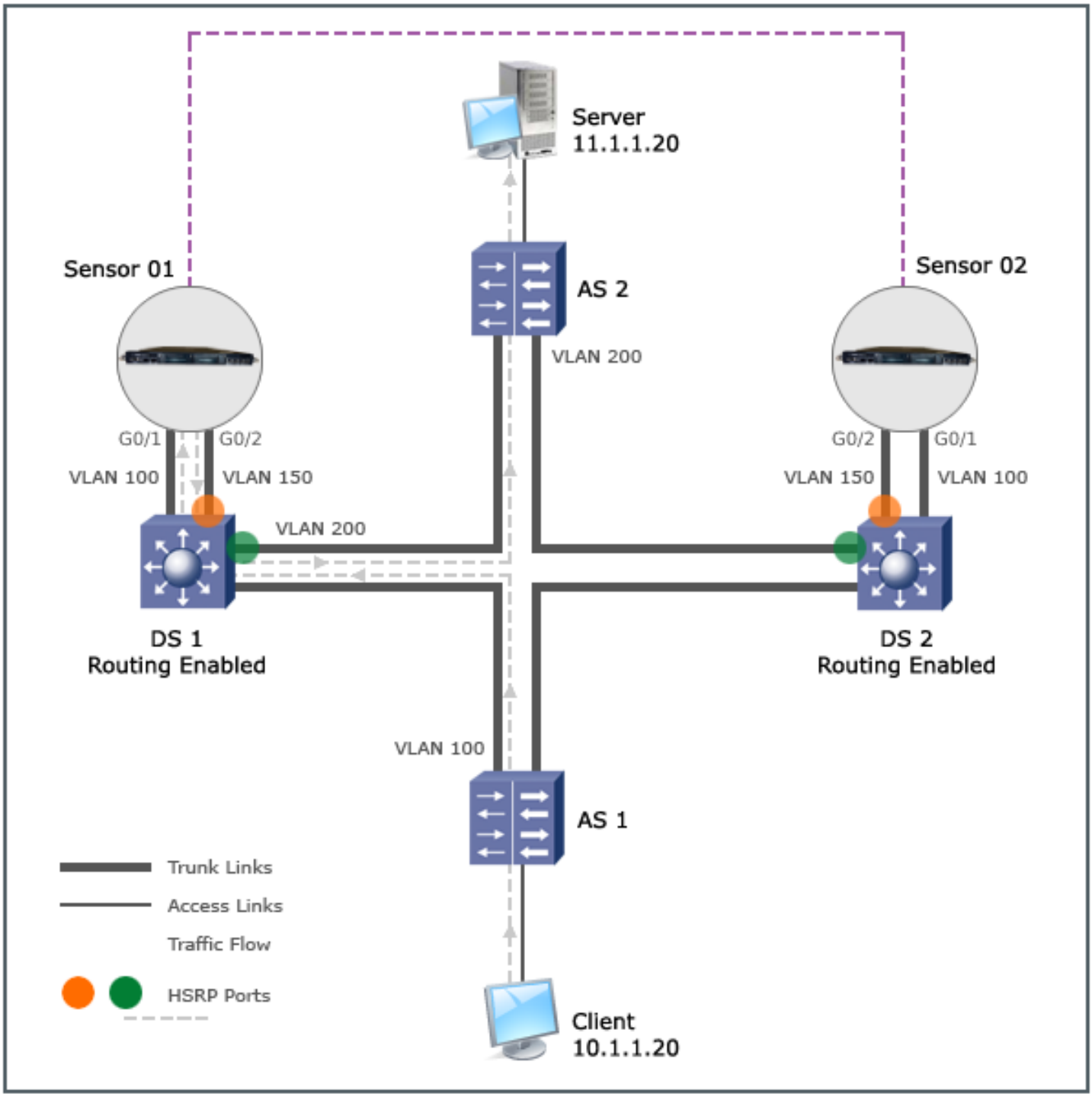
VLAN Bridging details in reports

Selecting the Port Configuration and Interface Configuration in the Sensor Configuration Report, displays the Bridge VLAN type interfaces and the corresponding VLAN pairs. For information on reports, see Report Generation (page 239).

VLAN bridging for Sensors in fail-over mode

This section explains a sample scenario in which Sensors in fail-over mode are configured for VLAN Bridging.

Figure 294. Sensors in fail-over mode



The network design in the diagram above is as follows:

- This scenario represents an active/standby network path.
- Client 10.1.1.20 is in VLAN 100 and the server 11.1.1.20 is in VLAN 200.

- The client is connected to an access switch AS 1 and the server is connected to the access switch AS 2.
- The access switches, AS 1 and AS 2 are connected to two L3 switches (DS 1 and DS 2) for redundancy.
- Spanning Tree Protocol is disabled in both DS 1 and DS 2.
- DS1 is connected to Sensor 01 and DS 2 is connected to Sensor 02. These Sensors are in fail-over mode.
- Sensor ports G0/1 and G0/2 are configured to bridge VLANs 100 and 150.
- In DS 1 and DS 2 only the ports connecting to G0/1 and AS 1 are configured for VLAN 100.
- Only the switch ports connected to port G0/2 are configured for VLAN 150.
- The ports of DS 1 and DS 2 connecting to G0/2 are configured as one Hot Standby Routing Protocol (HSRP) group. This provides an active/standby network path.
- The ports of DS 1 and DS 2 that connect to AS 2 are configured as one HSRP group to provide the active/standby network path for the response traffic.
- It is critical that the HSRP Hello multicasts from HSRP group members reach all the participating HSRP group members to trigger a HSRP switchover.

The flow of traffic when the client tries to access the server is as follows:

- Traffic from the client is tagged VLAN 100 by AS 1 and then sent to either DS 1 or DS 2 based on which path is active. Let us assume that currently DS 1 is active and DS 2 is in standby.
- From DS 1, the only path available for the VLAN 100 traffic is it to port G0/1 of Sensor 01.
- If the traffic is clean, the Sensor changes the VLAN tag to 150 and sends it out through G0/2.
- DS 1 does inter-VLAN routing accordingly and the traffic reaches the server through AS 2.
- If Sensor 01 is down, then HSRP failover is triggered and DS 2 becomes the active path. As a result, IPS and VLAN bridging are performed by Sensor 02. All the flows that were processed by Sensor 01 are intact since Sensor 02 has the updated state information for all those flows and it takes over seamlessly.

CIDR interfaces

When you choose an interface type of CIDR, you are instructing the Sensor to apply policies according to the IP address of one or more hosts.

Background

The strategy for classless inter-domain routing (CIDR) was originally submitted to the networking community as *RFC 1519* in 1993.

RFC 1519 aimed to address two of the principal networking problems of its day:

- The exhaustion of the class B network address space.
- The unmanageable growth of routing tables in Internet routers.

In so many words, CIDR introduced the concept of "subnetting."

Before RFC 1519, networks were "classful." That is, an explicit network mask was not used to determine the quantity of hosts a network could maintain. Instead, a class was determined based on the value of the first octet in the IP address.

Class	Value of First Octet	Assumed Network Mask
A	1 - 126	255.0.0.0
B	128 - 191	255.255.0.0
C	192 - 223	255.255.255.0

For example, an IP address of 32.x.x.x was assumed to have an 24-bit network mask (class A), an address of 155.x.x.x was assumed to have a 16-bit mask (class B), and an address of 210.x.x.x was assumed to have a 8-bit mask (class C).

According to RFC 1519, the fundamental cause of the exhaustion of the class B network address space was the lack of an appropriate class for mid-sized organizations. Specifically, a class C network allows for a maximum of 254 usable hosts (2^8) - 2, which is typically too small, whereas, a class B network provides 65534 usable hosts (2^16) - 2, which is overkill in most cases.

NOTE

You subtract 2 from the quantity of usable hosts to account for the network address and the broadcast address for each segment.

The overwhelming growth of routing tables is also a product of this shortcoming. Imagine your network has 1000 hosts. It would not be in the interest of your ISP to allocate your company a full class B network, yet a class C network would not suffice. Instead, the ISP would likely allocate you four class C networks. Unfortunately, the ISP would then have to include a new route for each of those four networks in its routing tables and propagate them across the Internet.

In this case, four routes would be added to the Internet routing space when a single route could have ideally achieved the same end.

CIDR deprecates the notion of network class and introduces the requirement that all networks and hosts be represented by a combination of IP address and explicit network mask. In this way, CIDR resolves both the aforementioned problems. Specifically, CIDR allows for:

- The straightforward division of class B networks into blocks of class C networks.
- Aggregation of those blocks into a single Internet route.

CIDR arithmetic

When you calculate subnets, it is helpful to remember that:

- There is a finite amount of bits with which to work (32 bits, assuming IPv4).
- Bits can either represent a network or a host, but not both. So each time a bit is allocated to one, that implicitly means it has been de-allocated from the other.

The calculations are in binary, so each time you allocate an additional bit to networks, for example, you double the quantity of available networks, but cut the quantity of hosts per network in half. (If you instead allocate an additional bit to hosts per network, the opposite is true.)

Consider a traditional class B network of 155.49.0.0. Its traditional network mask is 255.255.0.0. That is, out of the 32 bits available for a network mask, 16 of those bits are representing networks and 16 are representing hosts per network. This leaves us with 65534 usable hosts per network (2^16) - 2.

An ISP will likely reallocate this network with a longer network mask (more bits allocated to networks) to get a greater quantity of blocks of networks from that range. The ISP might allocate the 155.49.0.0 range using a 21-bit mask (255.255.248.0) instead, for example. In doing so, the ISP can find a happy medium between traditional class B and class C networks.

In the specific case of a 21-bit network mask, the ISP can reallocate the 155.49.0.0 range in 32 blocks of (8) class C networks and use a single route to represent each block. How is that achieved?

If we do not subnet the 155.49.0.0 network at all, we are left with a single network containing 2^16 - 2 or 65,534 hosts.

If we now allocate another bit to the networks (17 bits) and therefore take one away from the hosts (15), the quantity of subnets doubles to 2, and the quantity of hosts per subnet is cut to 2^15 - 2 or 32,766.

Again, each time we add a bit to the network mask, we double the quantity of subnets available, but split the quantity of hosts per network in (almost) half.

If we follow the same arithmetic for our 21-bit network mask, that yields 32 subnets. It also leaves 11 bits for the hosts or 2046 (2^11 - 2) hosts per subnet.

Calculation of the quantity of subnet blocks

To quickly determine the quantity of subnets a given mask will yield, you subtract the number of bits in the traditional, "classful" mask from the mask you aim to use, and then use the difference to find the binary exponent.

In our example, a traditional class B network mask uses 16 bits, whereas we aim to use a 21-bit mask. So the equation is:

21 - 16 = 5

The binary exponent is then 2^5 or 32 available subnets.

Calculation of the quantity of networks per block

To determine the quantity of class C networks each of those 32 subnets will contain, you subtract the number of bits you aim to use from the traditional, "classful" mask, and then use the difference to find the binary exponent.

This time, we are interested in (blocks of) traditional class C networks, each of which uses a mask of 24 bits, and we still aim to use a 21-bit mask. So the equation is:

24 - 21 = 3

The binary exponent is 2^3 or 8 class C subnets per block.

Sample class C blocks

The following are the first three class C network blocks resulting from the combination of the 155.49.0.0 network and a 21-bit mask, as well as the corresponding Internet route required for each block

Block #1

Allocated customer class C networks:

155.49.0.0 / 24

155.49.1.0 / 24

155.49.2.0 / 24

155.49.3.0 / 24

155.49.4.0 / 24

155.49.5.0 / 24

155.49.6.0 / 24

155.49.7.0 / 24

Corresponding Internet route: 155.49.0.0 / 21

Block #2

Allocated customer class C networks:

155.49.8.0 / 24

155.49.9.0 / 24

155.49.10.0 / 24

155.49.11.0 / 24

155.49.12.0 / 24

155.49.13.0 / 24

155.49.14.0 / 24

155.49.15.0 / 24

Corresponding Internet route: 155.49.8.0 / 21

Block #3

Allocated customer class C networks:

155.49.16.0 / 24

155.49.17.0 / 24

155.49.18.0 / 24

155.49.19.0 / 24

155.49.20.0 / 24

155.49.21.0 / 24

155.49.22.0 / 24

155.49.23.0 / 24

Corresponding Internet route: 155.49.16.0 / 21

Summary

The ISP can take the traditional class B network (16 bits) it was assigned and subnet it is using, in this case, a 21-bit mask (255.255.248.0) to allocate blocks of class C networks (24 bits) to its customers as needed, and also minimize the amount of new routes required to reach each customer's network.

Of course, the ISP could follow similar logic to further subnet one or more of these networks blocks to accommodate even smaller customers.

TIP

Consider using one of the many subnet calculators freely available on the Internet. They often simplify the creation of a CIDR addressing scheme, and can at least serve to check your work.

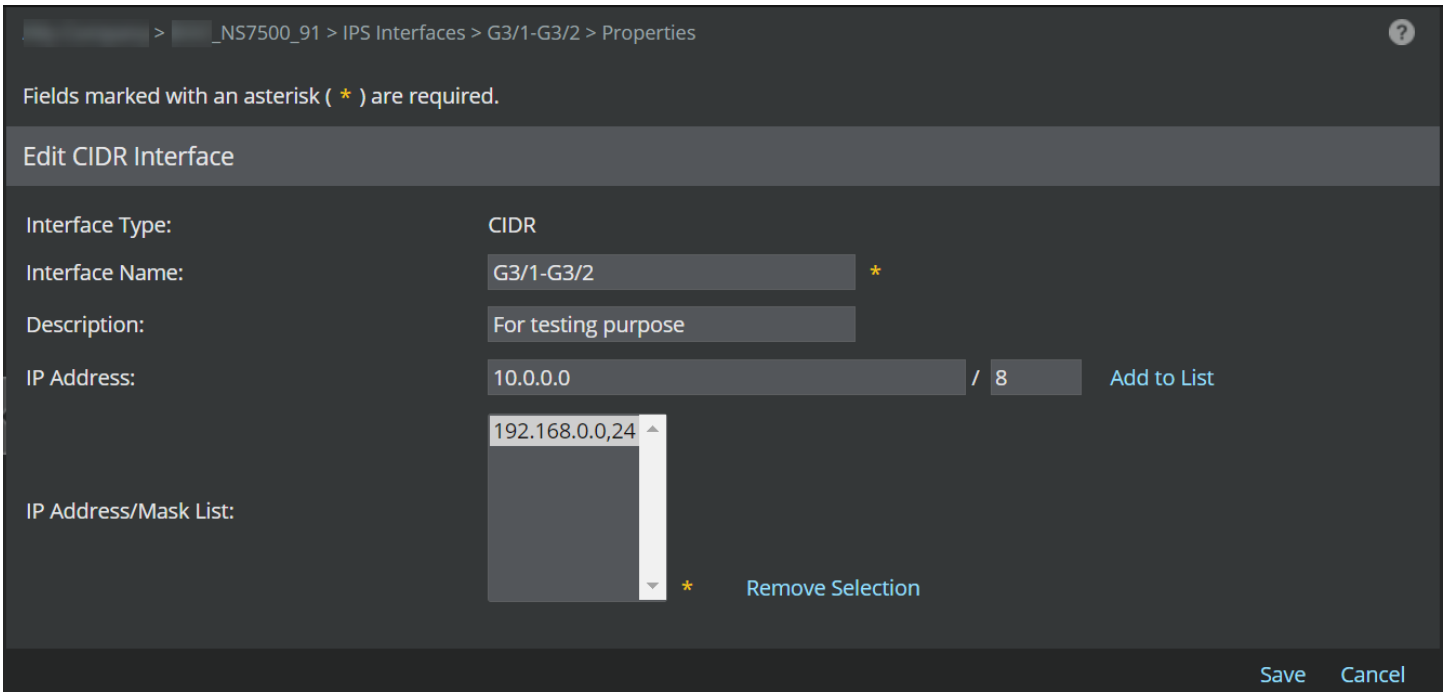
CIDR interfaces definition

The first step to using a **CIDR** interface is to change the interface type from **Dedicated** to **CIDR**.

The next step is to edit the interface and associate CIDR ranges with it. You'll want to define here all the internal CIDR ranges whose traffic you anticipate traversing this interface.

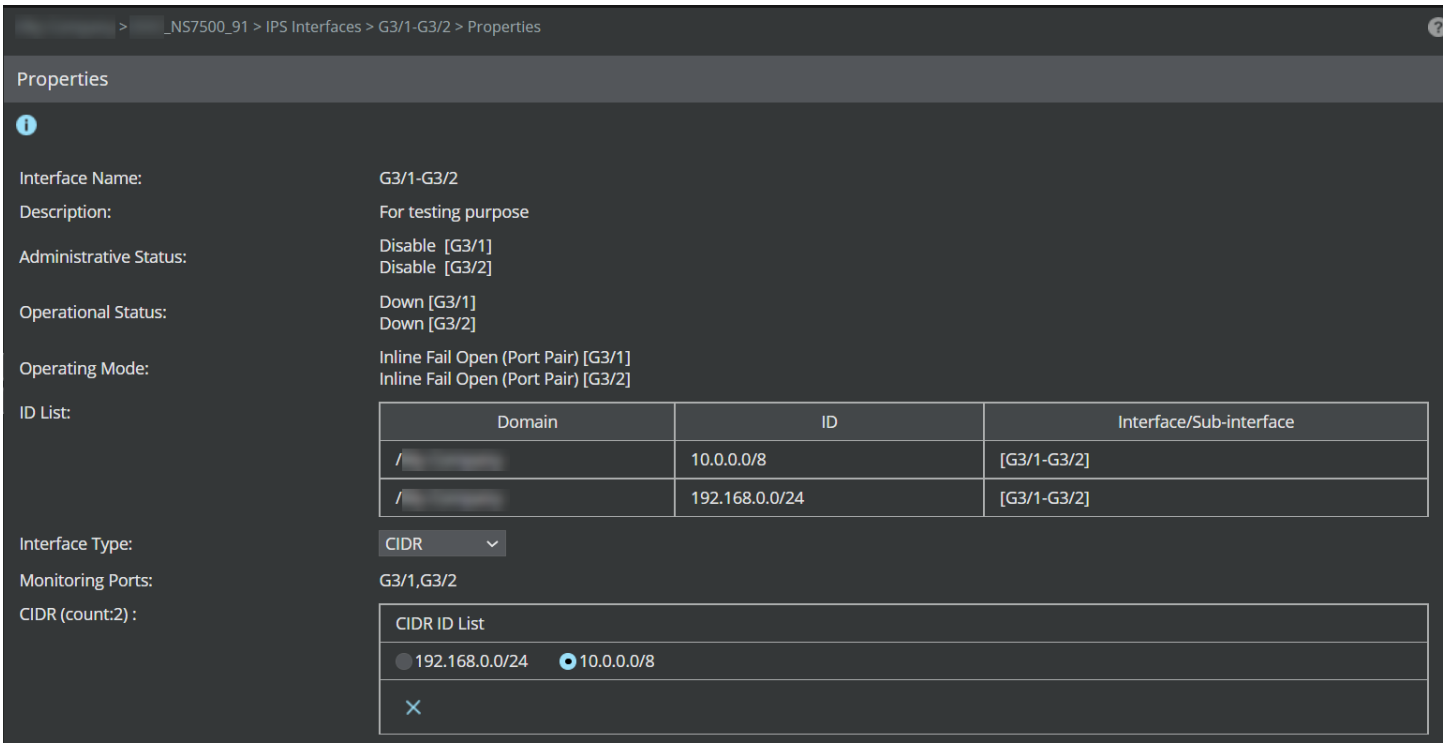
The user interface expects CIDR ranges as a combination of IP network (or address) and mask length (in bits). In the figure below, the 192.168.0.0/24 network has already been added to the list and the 10.0.0.0/8 network is about to be added.

Figure 295. CIDR Interface window



The figure below shows the results of the last step:

Figure 296. Current CIDR range



If we look at the Devices → <Admin Domain Name> → Devices → <Device Name> → IPS Interfaces → <Interface_Name> → **Properties**, the interfaces and their corresponding policies, the **CIDR** interface will appear no different than the **Dedicated** interface it replaced.

However, if we look back at the details of interface G3/1-G3/2, we can confirm at a glance that it is now associated with CIDR ranges 192.168.0.0/24 or 10.0.0.0/8.

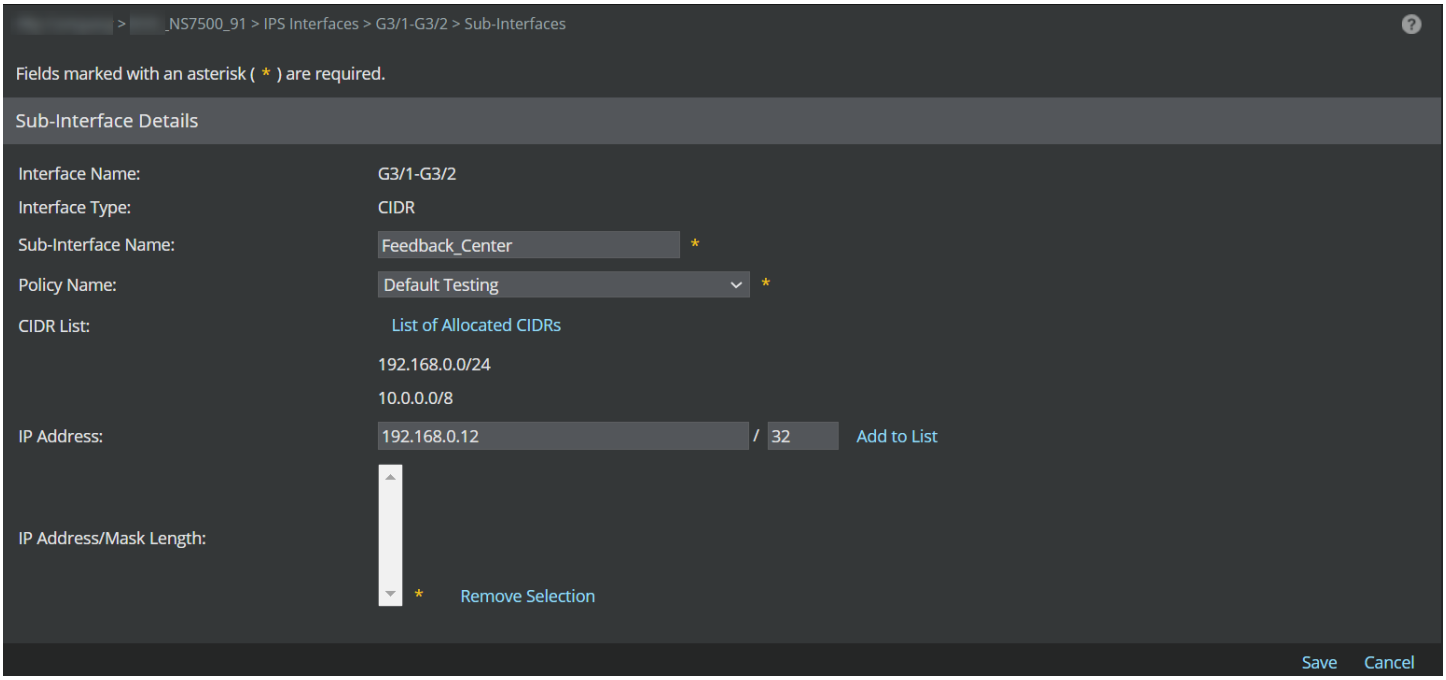
If traffic flows through interface G3/1-G3/2, with no source address on the 192.168.0.0/24 or 10.0.0.0/8 networks, the Default Prevention policy will no longer be applied. Instead, the traffic applied will be that of the parent (physical interface) and **not** the Sensor policies.

Defining CIDR sub-interfaces definition

The next step is to allocate all or part of those CIDR ranges to a sub-interface to further refine the scanning process.

In the figure below, we are adding a sub-interface called Feedback_Center, assigning it the **Default Testing**, and allocating only the IP address of the Feedback Center to it. To specify a single host, you use a 32-bit network mask:

Figure 297. Sub-Interface Details window - 1



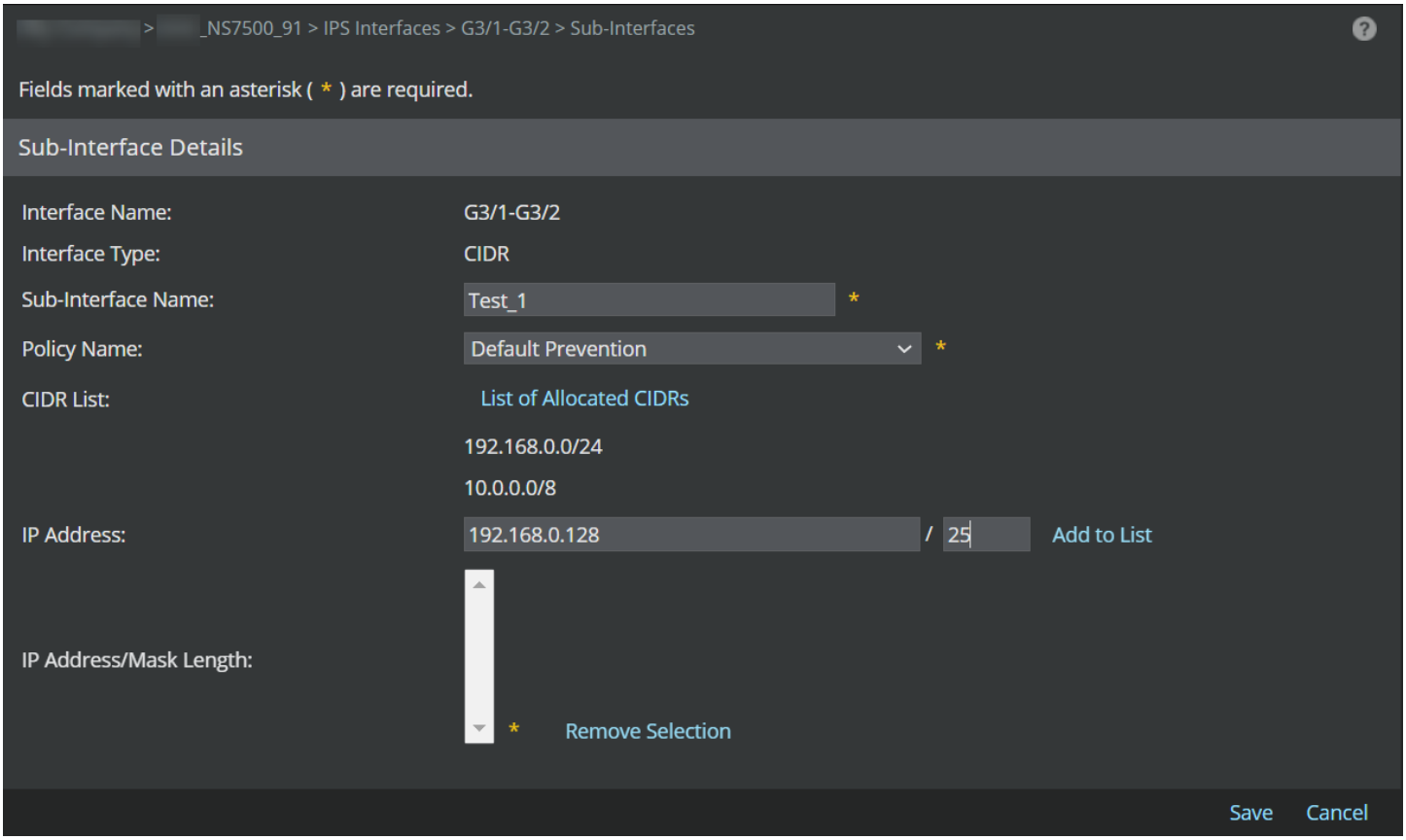
The key to successfully allocating multiple subnets from a single CIDR range is that the corresponding sub-interfaces cannot overlap. As obvious as it might sound that you cannot allocate all or part of a CIDR range multiple times, the flexibility of CIDR addressing can sometimes also make the calculations confusing.

If you attempt to use a CIDR range multiple times, the user interface will return an error. Let's step through an example to produce such an error.

At this point in the configuration process, the entire 192.168.0.0/24 CIDR range is available for sub-interfaces, except the 192.168.0.12 IP address (which is the IP address of the Feedback Center).

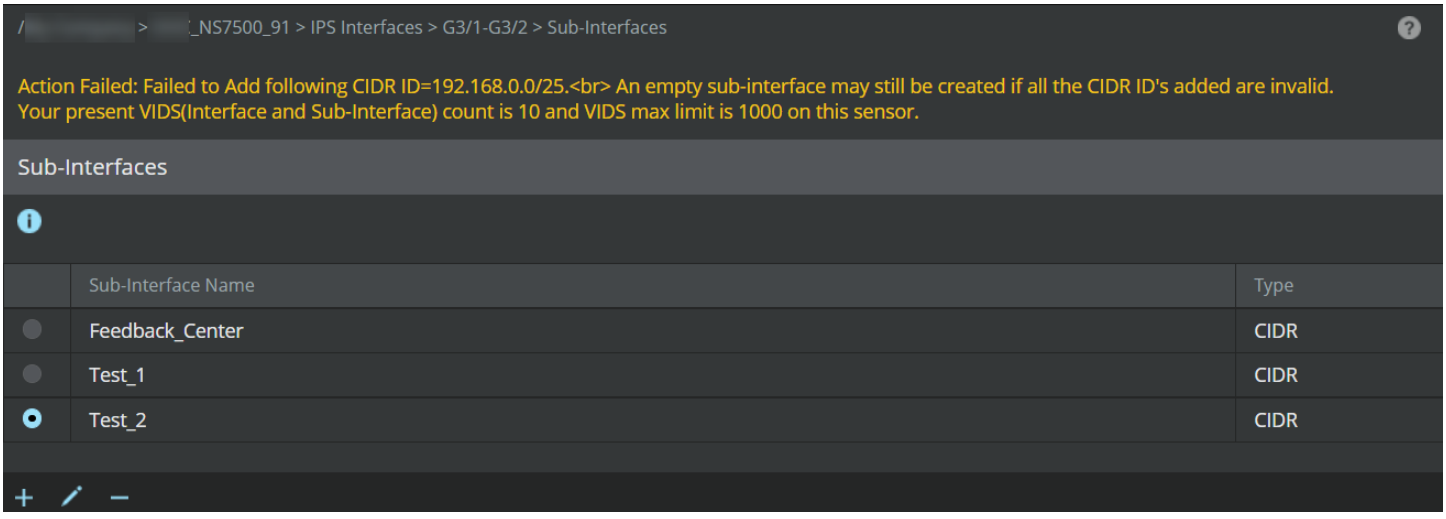
In the figure below, we are allocating the 192.168.0.128/25 range as well via a sub-interface called Test_1 and assigning the **Default Prevention** policy to it. Otherwise put, this will allocate the IP range from 192.168.0.128 to 192.168.0.255.

Figure 298. Sub-Interface details window - 2



If we next attempt to allocate 192.168.0.1/25, we will receive the following error:

Figure 299. CIDR block allocation error



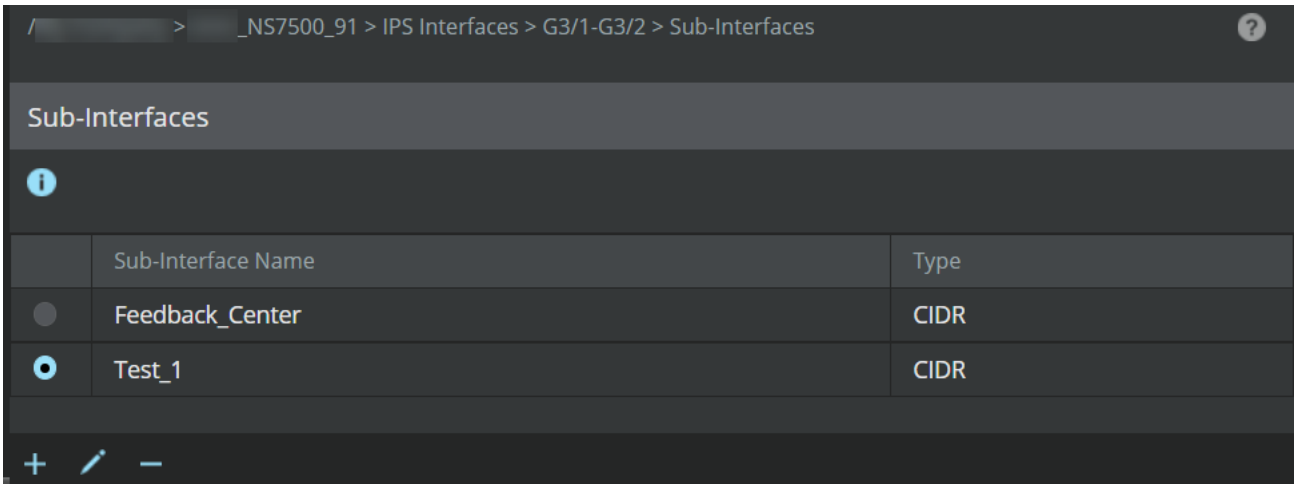
The reason for the failure is that 192.168.0.0/25 allocates the IP range from 192.168.0.0 to 192.168.0.127, which includes the previously allocated IP address of the Feedback Center 192.168.0.12, so this is an overlap. The error is explaining that the sub-interface was created, but no CIDR range was actually allocated to it.

If you need a reality check while in the process of creating or editing a sub-interface, you can always view the list of currently allocated CIDR ranges.

If we discard the third sub-interface (the one that returned an error, i.e., Test_2) and look back at the details of the interface, a few things have changed.

The output for the network will look as follows:

Figure 300. Sub-interface details



The **IPS Interfaces** includes an icon for each new sub-interface.

Parts of the 192.168.0.0/24 CIDR range are now shown in the **Properties** page to be associated with the new sub-interfaces (and, therefore, their policies).

The details of the final configuration are as follows:

- Traffic from or to IP addresses ranging from 192.168.0.128 - 192.168.0.255 will have the **Default Prevention** policy applied to it.
- Traffic from or to the Feedback Center (192.168.0.12) will have the **Default Testing** policy applied to it.
- Traffic from or to any other IP in the 192.168.0.0/24 CIDR range or the 10.0.0.0/8 CIDR range will have the DMZ policy applied to it.
- Traffic not containing any of those IP addresses will have the default policy applied to it (the policy assigned to the Sensor).

We could, for example, create another sub-interface for all or part of the 10.0.0.0/8 CIDR range. If we subsequently wanted to allocate yet another CIDR range to a sub-interface, we would first have to add that range to the G3/1-G3/2 interface.

How policies are applied

When you add a VLAN or CIDR block to a subinterface, Trellix Intrusion Prevention System treats the corresponding hosts as internal and builds a "protection domain" around them. All inbound traffic to and outbound traffic from those hosts is scanned using the policy associated with the sub-interface.

Background

Each interface and subinterface has a unique ID called its "VIDS ID," and each VIDS ID is associated with the IPS policy that you apply to the corresponding interface or subinterface. Each IPS policy in turn, is associated with inbound and outbound attack set profiles, and each attack set profile contains a list of rules that determine whether attack definitions are to be included or excluded in your IPS policies. The Sensor must therefore track the VIDS ID and direction of each flow to eventually know which attacks (signatures, Reconnaissance, or DoS) to use when scanning it.

NOTE

Similar to IPS policy, a VIDS ID is associated with the other security policies that you have applied to the interface or subinterface.

Every time a new flow is established through a Sensor, information about the flow is added to the Sensor's state table. The state table includes standard connection tracking information, such as source and destination IP address/port, protocol ID, and TCP state and sequence numbers. Each state table entry also includes the VIDS ID and direction of the flow in question.

The VIDS ID and direction are determined at the outset of the connection, for example, by the SYN packet. The Sensor scans the entire flow using the attack signatures corresponding to the stored VIDS ID and direction. It does **not** apply the inbound attack set profile in one direction and the outbound attack set profile in the other.

The determination of VIDS ID and direction depends directly on the operational mode and interface type in question.

Inline mode and dedicated interface

The simplest scenario is the one in which a SYN packet arrives on a port that is operating in inline mode and configured as a dedicated interface.

As a dedicated interface, there is a single VIDS ID associated with the entire interface, so it is straightforward to identify.

To determine direction, the Sensor considers the physical port on which the SYN packet arrives:

- If the SYN packet arrives on the port connected to the inside network, the entire flow is considered outbound.
- If the SYN packet arrives on the port connected to the outside network, the entire flow is considered inbound.

NOTE

A port is defined as inside versus outside from the **Physical Ports** page of the Manager.

For example, if a client connects to a server through the G0/1-G0/2 monitoring ports, and the client's SYN packet arrives on the outside port, all traffic in the flow is scanned using the signatures associated with the inbound attack set profile and VIDS ID for the G0/1-G0/2 interface; this includes return traffic from the server.

Sub-interfaces

If the same port on which the SYN packet arrives is instead associated with a **VLAN** or **CIDR** interface, the Sensor applies the same logic to determine the direction of the flow, but must do additional work to determine the VIDS ID.

If the interface type is **VLAN**, the Sensor compares the VLAN tag in the SYN packet against all previously defined VLAN IDs to determine the sub-interface to which the flow belongs.

- If the Sensor matches the VLAN in the SYN tag packet with one of its VLAN IDs, it stores the VIDS ID of the matching sub-interface in its state table.
- If the Sensor does not match the VLAN tag in the SYN packet with one of its VLAN IDs, it stores the VIDS ID associated with the parent interface instead.

If the interface type is **CIDR**, the Sensor uses the direction of the flow to determine the sub-interface to which the flow belongs.

- If the flow is inbound, the Sensor compares the destination IP address of the SYN packet against its CIDR sub-interfaces.
- If there is a match, the Sensor stores the VIDS ID associated with the matched CIDR sub-interface.
- Otherwise, it stores the VIDS ID associated with the parent interface.
- If the flow is outbound, the Sensor compares the source IP address of the SYN packet against its CIDR sub-interfaces.
- If there is a match, the Sensor stores the VIDS ID associated with the matched CIDR sub-interface.
- Otherwise, it stores the VIDS ID associated with the parent interface.

SPAN or tap mode

Ports in SPAN mode do not provide a Sensor with the same physical means to determine direction. In the case of SPAN mode, for example, traffic is mirrored from a switch to a single Sensor monitoring port, so a Sensor cannot easily differentiate inbound traffic from outbound.

How the Sensor determines direction and VIDS ID in SPAN mode depends on the interface type in question.

Dedicated interface

When running a dedicated interface in SPAN mode, no direction information is available; the Sensor considers all traffic as inbound traffic. Further, the Sensor stores the VIDS ID of this interface.

VLAN interface

When running a VLAN interface in SPAN or tap mode, no direction information is available; the Sensor considers all traffic as inbound traffic. Further, the Sensor stores the VIDS ID of this interface.

CIDR interface

When running a CIDR interface in SPAN mode, the Sensor uses the following logic to determine direction and VIDS ID:

- When a SYN packet arrives on a SPAN port, the Sensor compares its CIDR sub-interfaces against the destination IP address in the SYN packet.
- If there is a match, the entire flow is considered inbound and the Sensor stores the VIDS ID of the matched CIDR sub-interface.
- If there is no match, the Sensor compares its CIDR sub-interfaces against the source IP address in the SYN packet.

- If there is a match, the entire flow is considered outbound and the Sensor stores the VIDS ID of the matched CIDR sub-interface.
- If there is no match, the entire flow is considered inbound and the Sensor stores the VIDS ID of the parent interface.

Common use of VLAN, bridge VLAN, and CIDR interfaces

There is no rule governing when to use one approach over the other. Instead, consider the most common uses of each:

- **VLAN** sub-interfaces are most common when the customer has grouped like systems by VLANs and the Sensor resides at an aggregation point on the network. You can obviously only take advantage of VLAN sub-interfaces when the traffic in question is trunked VLAN tagged.
- **Bridge VLAN** sub-interfaces, however, have a specific use. This is applicable only for NS-series Sensors deployed in in-line mode. You use this feature to subject all inter-VLAN traffic to IPS using the minimal number of Sensors.
- **CIDR** sub-interfaces have a specific use. You can create sub-interfaces and then allocate policies to them.

Interface, VLAN, and CIDR limits

The following is a list of limits to consider when using sub-interfaces:

- It is perfectly acceptable to use both VLAN and CIDR sub-interfaces on a single Sensor. As we have seen, however, you cannot mix VLAN and CIDR sub-interfaces on a single interface.
- Trellix IPS supports VLAN IDs 1 through 4095.

Troubleshooting

This section contains information that may help you solve problems you may experience with your inline mode deployment.

Traffic statistics

Device health mainly depends on its performance capabilities. A Sensor indicates good health when there is no traffic overload. The traffic flowing can be controlled by monitoring different parameters. The Manager offers viewing these parameters to help maintain the Sensor health which is critical for functioning efficiently without any downtime. To view the traffic statistics for a standalone Sensor, navigate to Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Traffic Statistics**.

To view the traffic statistics for Sensors in a stack, navigate to Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Traffic Statistics**.

You can refresh the data displayed by clicking the  icon. **Reset Counters** resets all the data counters. There is flexibility to customize the columns based on what you want to view. You can rearrange the columns based on priority, or hide columns, or sort in ascending/descending order. The **Save as CSV** option exports information as a .csv file which you can use for further analysis.

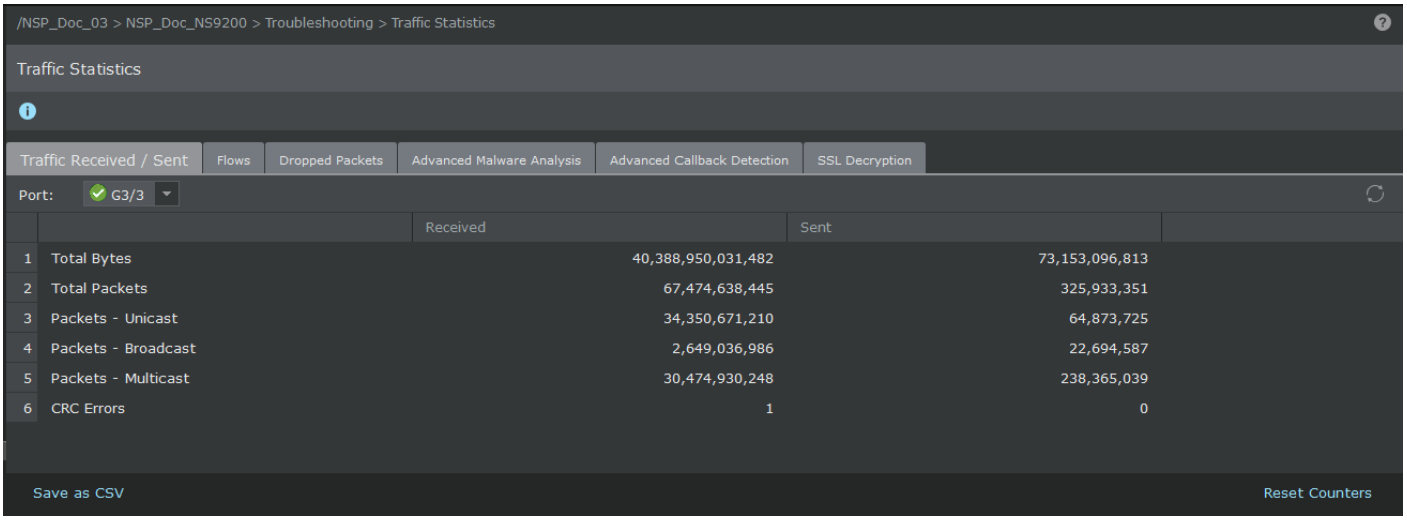
Device performance statistics

View traffic sent/received data

You can view the statistics of the total number of packets received (Rx) and transmitted (Tx) for a given device per port. You can select the port from the **Port** drop-down list for which you want to view the sent/received data. The **All Ports** option is selected by default and displays information for all the ports. When you hover the mouse over a port in the **Port** drop-down list, a tooltip displays the status of the port as **Link Up**, **Link Down**, or **Disabled**. This tab displays the following information:

- **Total Bytes** - Total number of bytes received and sent through the selected interface port
- **Total Packets** - Total number of Unicast, Broadcast, and Multicast packets received and sent through the selected interface port
- **Packets - Unicast** - Total number of Unicast packets received and sent through the selected interface port
- **Packets - Broadcast** - Total number of Broadcast packets received and sent through selected interface port
- **Packets - Multicast** - Total number of Multicast packets received and sent through the selected interface port
- **CRC Errors** - Total number packets with CRC errors received and sent through the selected interface port

Figure 301. Traffic Received / Sent



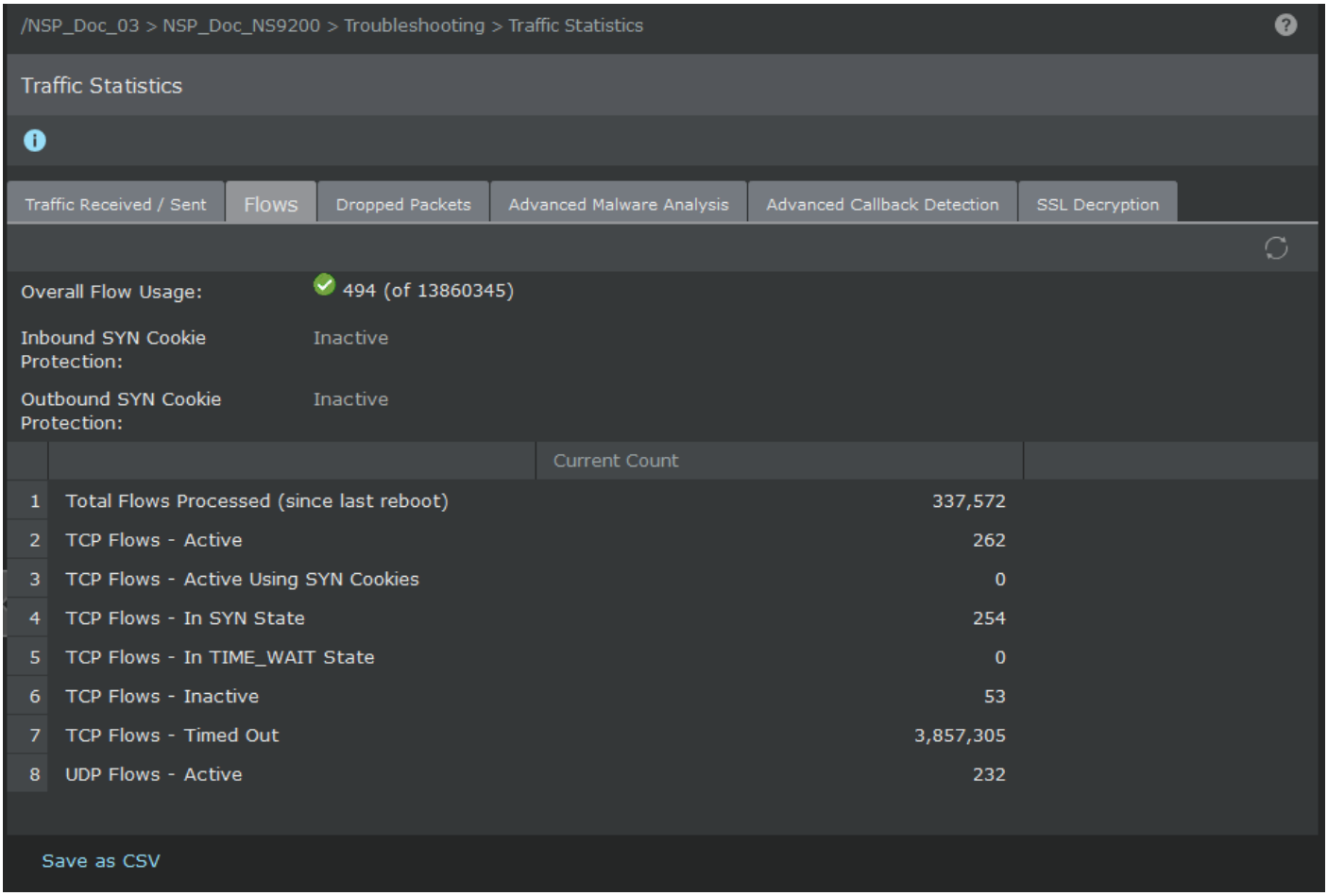
View traffic flows

You can view the statistical TCP and UDP flow data processed by a device. Checking your flow rates can help you determine if your device is processing traffic normally. This also provides you with a view of statistics such as the available flows supported, as well as the number of active TCP and UDP flows. This tab displays the following information:

- **Total Flows Processed (since last reboot)** - Total number of flows processed by the Sensor since the last Sensor reboot
- **TCP Flows - Active** - Total number of TCP flows that are currently active
- **TCP Flows - Active Using SYN Cookies** - Total number of active TCP flows that are using SYN cookies
- **TCP Flows - In SYN State** - Total number of TCP flows that are currently in SYN state
- **TCP Flows - In TIME_WAIT State** - Total number of TCP flows that are currently in TIME_WAIT state

- **TCP Flows - Inactive** - Total number of TCP flows that are currently inactive
- **TCP Flows - Timed Out** - Total number of unsuccessful TCP connection completions
- **UDP Flows - Active** - Total number of UDP flows that are currently active

Figure 302. Traffic Flows



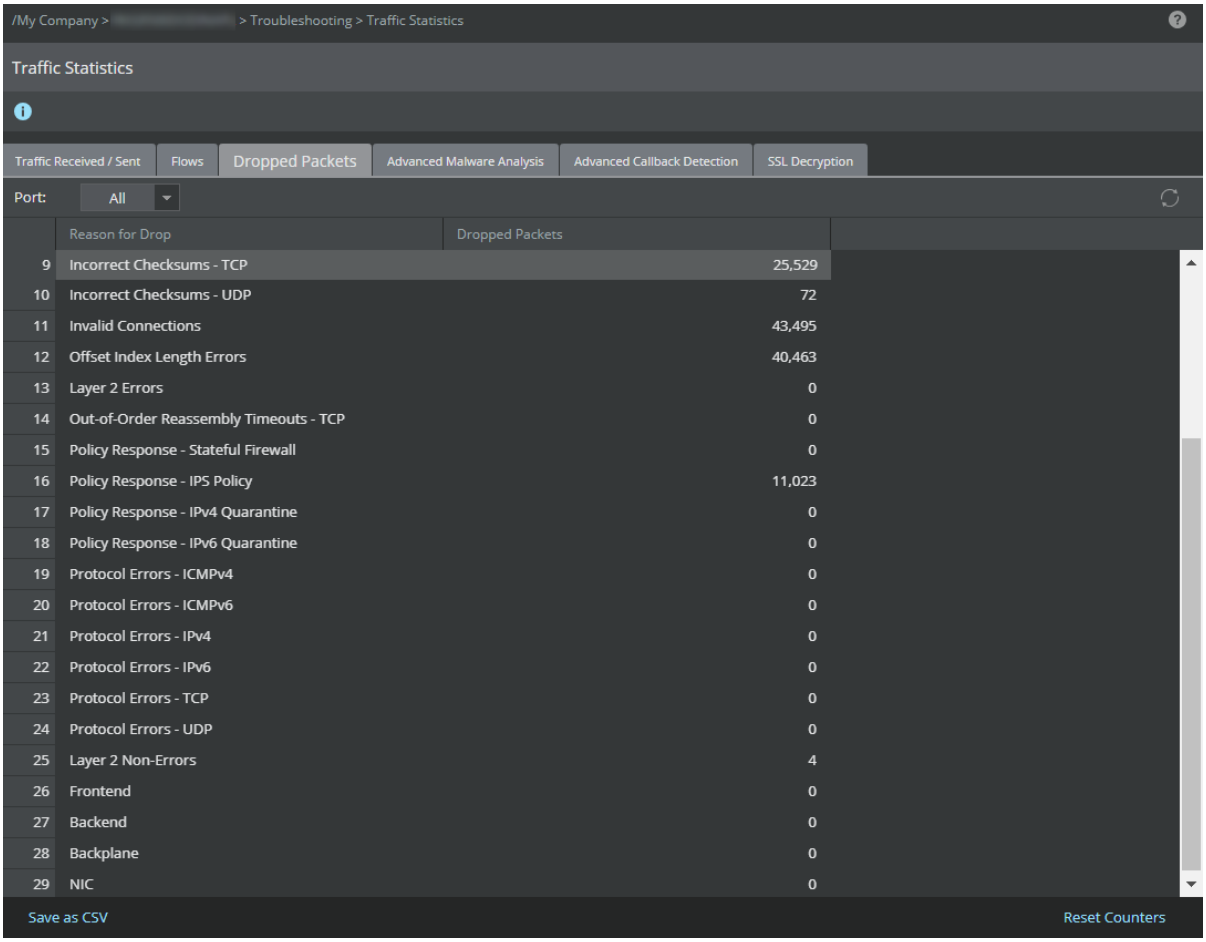
View the dropped packets data

Using this tab, you can view the reason and the packet drop rate on a port for a device. The **All** option is selected by default and displays information for all the ports. This tab displays the following information:

- **Backend** - Total number of miscellaneous packets dropped at back-end
- **Backplane** - Total number of miscellaneous packets dropped at BMC switch
- **CRC Failures** - Total number of packets dropped due to CRC errors
- **Device Power Up** - Total number of packets dropped during cold start
- **Device Resource Exhaustion** - Total number of packets dropped by the Sensor because of non availability of resources
- **Fragment Reassembly Timeouts - IPv4** - Total number of packets dropped due to IPV4 fragment reassembly timeout
- **Fragment Reassembly Timeouts - IPv6** - Total number of packets dropped due to IPV6 fragment reassembly timeout

- **Frontend** - Total number of miscellaneous packets dropped at front-end
- **Incorrect Checksums - ICMPv4** - Total number of packets dropped due to incorrect ICMP v4 checksum
- **Incorrect Checksums - ICMPv6** - Total number of packets dropped due to incorrect ICMP v6 checksum
- **Incorrect Checksums - IP** - Total number of packets dropped due to incorrect IP checksum
- **Incorrect Checksums - TCP** - Total number of packets dropped due to incorrect TCP checksum
- **Incorrect Checksums - UDP** - Total number of packets dropped due to incorrect UDP checksum
- **Invalid Connections** - Total number of packets dropped due to of invalid connection
- **Layer 2 Errors** - Total number of packets dropped due to Layer 2 errors
- **Layer 2 Non-Errors** - Total number of Layer-2 packets dropped due to other reasons
- **NIC** - Total number of miscellaneous packets dropped at NIC
- **Offset Index Length Errors** - Total number of packets dropped due to offset index length errors
- **Out-of-Order Reassembly Timeouts - TCP** - Total number of packets dropped due to TCP out-of-order reassembly timeout
- **Policy Response - Stateful Firewall** - Total number of packets dropped due to the configured firewall policy
- **Policy Response - IPS Attack** - Total number of packets dropped due to the configured IPS policy
- **Policy Response - IPv4 Quarantine** - Total number of packets dropped due to the configured IPv4 Quarantine policy
- **Policy Response - IPv6 Quarantine** - Total number of packets dropped due to the configured IPv6 Quarantine policy
- **Protocol Errors - ICMPv4** - Total number of packets dropped due to ICMPv4 protocol errors
- **Protocol Errors - ICMPv6** - Total number of packets dropped due to ICMPv6 protocol errors
- **Protocol Errors - IPv4** - Total number of packets dropped due to IPv4 protocol errors
- **Protocol Errors - IPv6** - Total number of packets dropped due to IPv6 protocol errors
- **Protocol Errors - TCP** - Total number of packets dropped due to TCP protocol errors
- **Protocol Errors - UDP** - Total number of packets dropped due to UDP protocol errors

Figure 303. Dropped packets



NOTE

The following counters are displayed only when you select the **All** option in the **Port** drop-down:

- **Frontend**
- **Backend**
- **Backplane**
- **Layer 2 Non-Errors**
- **NIC**

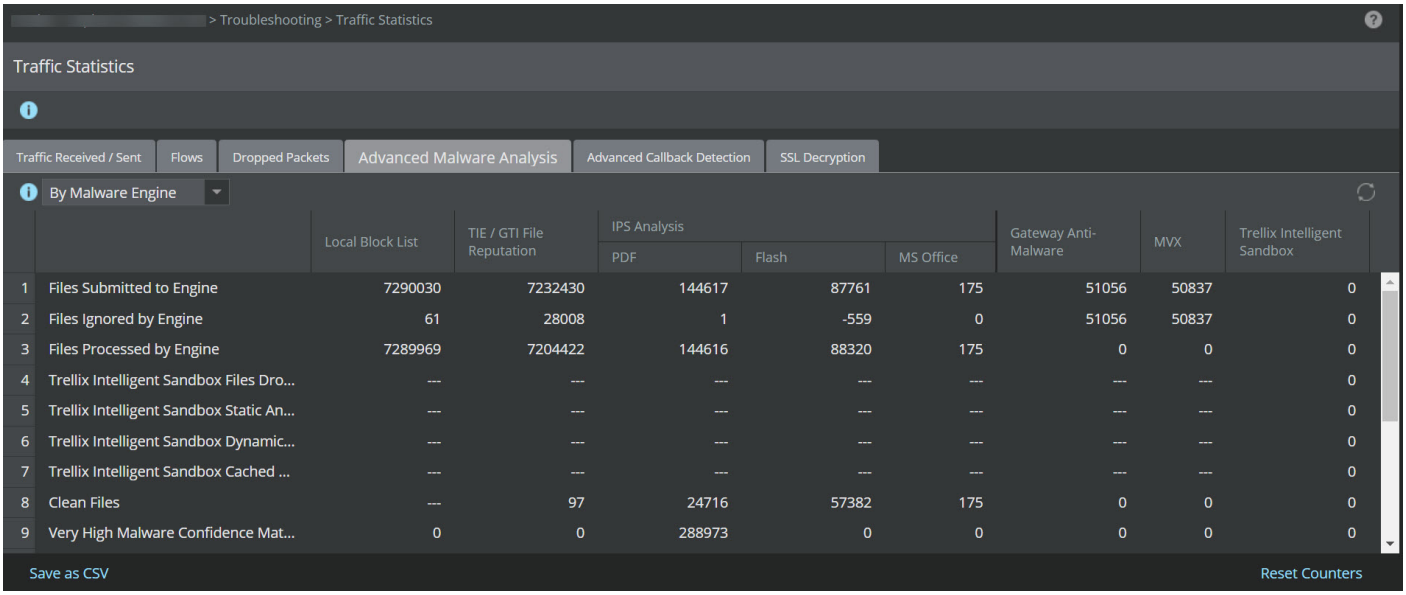
View the malware analysis data for a device

You can view the statistics of the malware detected for a given device. The **By Malware Engine** option displays the malware detected data based on the malware engines configured for the device. The **By File type** option displays data based on the file type analyzed. This tab displays the following information:

- **Files Submitted to Engine** - Number of malware files submitted to specific malware engine
- **Files Ignored by Engine** - Number of malware files ignored by the specific malware engine

- **Files Processed by Engine** - Number of malware files processed by the specific malware engine
- **Trellix Intelligent Sandbox Files Dropped Under Load** - Number of malware files dropped by the Trellix Intelligent Sandbox engine due to excessive load
- **Trellix Intelligent Sandbox Static Analyses** - Number of malware files processed by the Trellix Intelligent Sandbox engine based on static analysis using Block list and Allow list, GTI File Reputation, and Gateway Anti-Malware (GAM)
- **Trellix Intelligent Sandbox Dynamic Analyses** - Number of malware files processed by the Trellix Intelligent Sandbox engine based on dynamic analysis using Sanbox and Machine Learning
- **Trellix Intelligent Sandbox Cache Response Matches** - Number of malware results obtained from the Trellix Intelligent Sandbox cache
- **Clean Files** - Number of clean files processed by the specific malware engine
- **Very High Malware Confidence Matches** - Number of malware alerts generated by the specific malware engine and having malware score as very high
- **High Malware Confidence Matches** - Number of malware alerts generated by the specific malware engine and having malware score as high
- **Medium Malware Confidence Matches** - Number of malware alerts generated by the specific malware engine and having malware score as medium
- **Low Malware Confidence Matches** - Number of malware alerts generated by the specific malware engine and having malware score as low
- **Very Low Malware Confidence Matches** - Number of malware alerts generated by the specific malware engine and having malware score as very low
- **Unknown Malware Confidence Matches** - Number of files for which the malware confidence level is not known
- **Alerts Generated** - Number of malware alerts sent to the Manager by the Sensor for the specific malware engine
- **Files Blocked** - Number of malware attacks blocked by the Sensor for the specific malware engine
- **Connections Reset** - Number of malware TCP Resets sent by the Sensor for the specific malware engine

Figure 304. Malware analysis

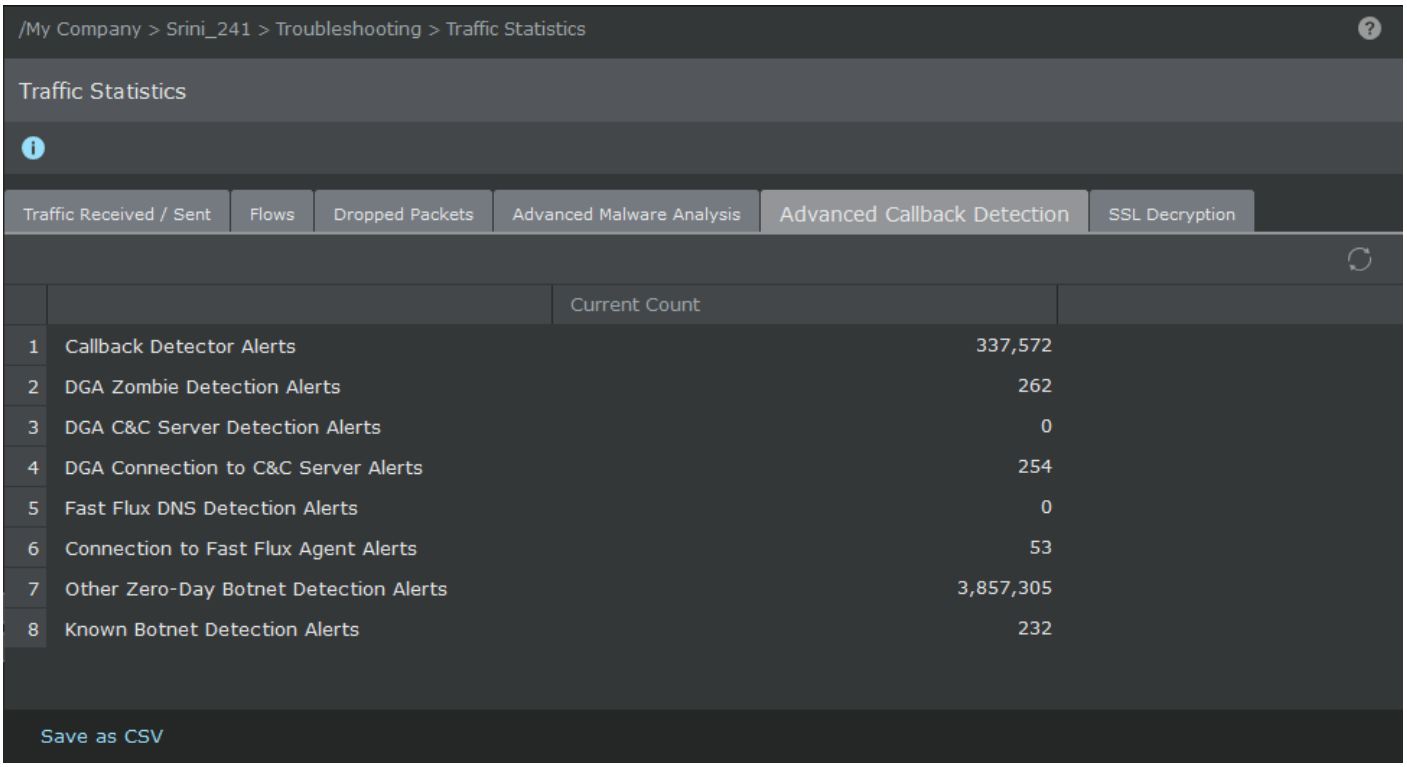


View Advanced Callback Detection

You can view the count for number of alerts generated for various bot activities. This provides information on the amount of callback activity and also communication attempts to the C&C servers. This tab displays the following information:

- **Callback Detector Alerts** - Total number of alerts pertaining to a callback detector match
- **DGA Zombie Detection Alerts** - Total number of alerts for DGA zombies
- **DGA C&C Server Detection Alerts** - Total number of alerts for C&C server suspects
- **DGA Connection to C&C Server Alerts** - Total number of alerts for DGA zombie callback and C&C server
- **Fast Flux DNS Detection Alerts** - Total number of alerts for IP flux botnet activity
- **Connection to Fast Flux Agent Alerts** - Total number of alerts for IP flux agent call back activity
- **Other Zero-Day Botnet Detection Alerts** - Total number of alerts for other Zero-Day botnets
- **Known Botnet Detection Alerts** - Total number of alerts for known botnets

Figure 305. Advanced Callback Detection



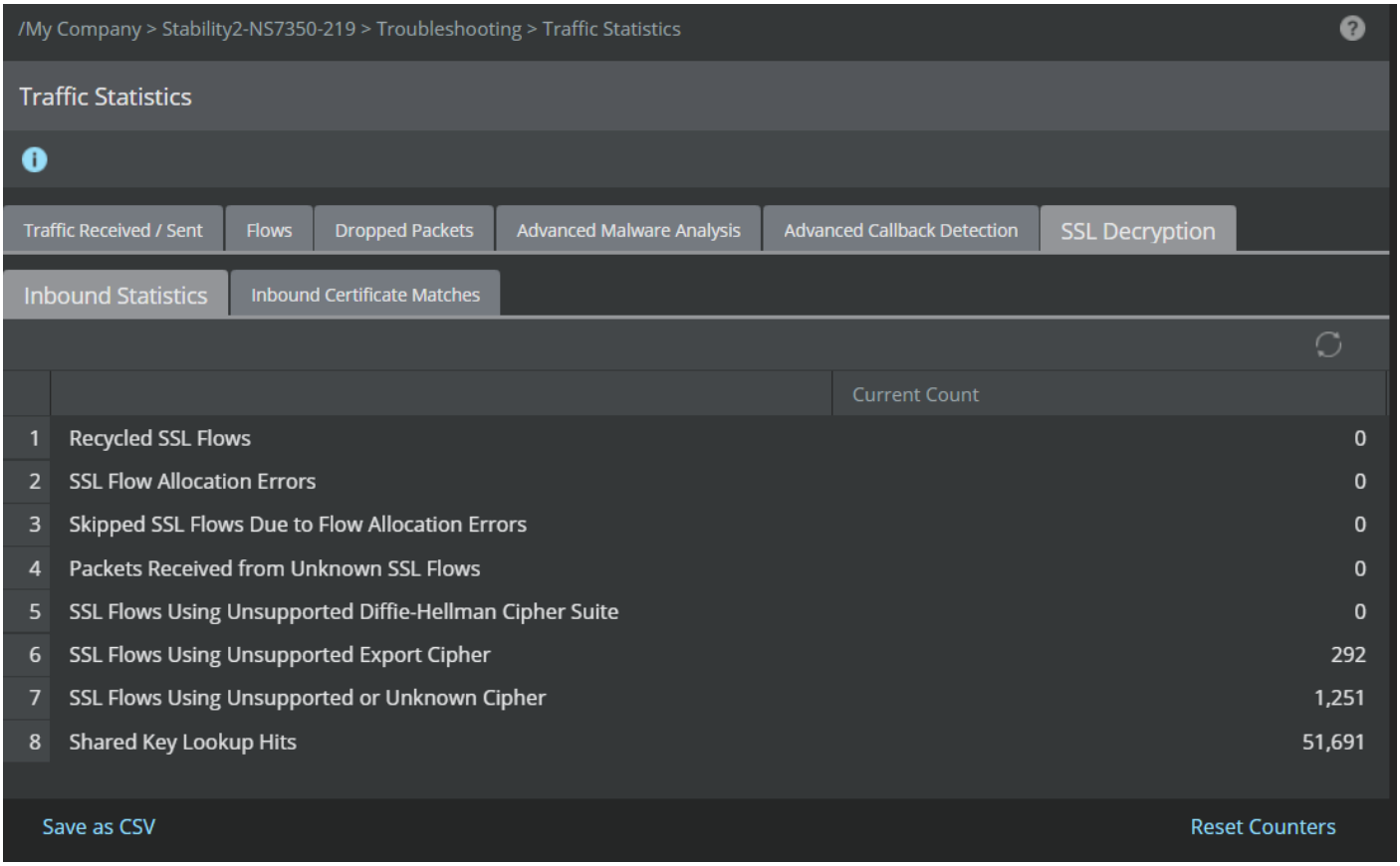
View SSL Decryption statistics

Using this tab, you can view traffic statistics for inbound and outbound SSL decryption:

- **Inbound Statistics**: Using this tab, you can view traffic statistics for inbound SSL decryption.
  - **Recycled SSL Flows** - Total number of SSL flows that are not used recently and freed by the Sensor
  - **SSL Flow Allocation Errors** - Total number of SSL flows the Sensor could not allocate due to resource unavailability

- **Skipped SSL Flows Due to Flow Allocation Errors** - Indicates total SSL flows that were skipped as the Sensor could not process them due to resource unavailability
- **Packets Received from Unknown SSL Flows** - Total number of SSL packets received that did not have a corresponding SSL flow
- **SSL Flows Using Unsupported Diffie-Hellman Cipher Suite** - SSL flows that are negotiated and not decrypted by the Sensor due to unsupported ciphers DH cipher suite in the traffic
- **SSL Flows Using Unsupported Export Cipher** - Total flows with SSLv3/TLS export cipher that are negotiated and not decrypted by the Sensor due to unsupported RSA cipher suite
- **SSL Flows Using Unsupported or Unknown Cipher** - Total flows with unsupported or unknown ciphers
- **Shared Key Lookup Hits** – Displays the number of times the Sensor uses the session key table provided by the Agent to decrypt inbound traffic using Diffie-Hellman cipher suite

Figure 306. SSL Decryption - Inbound Statistics

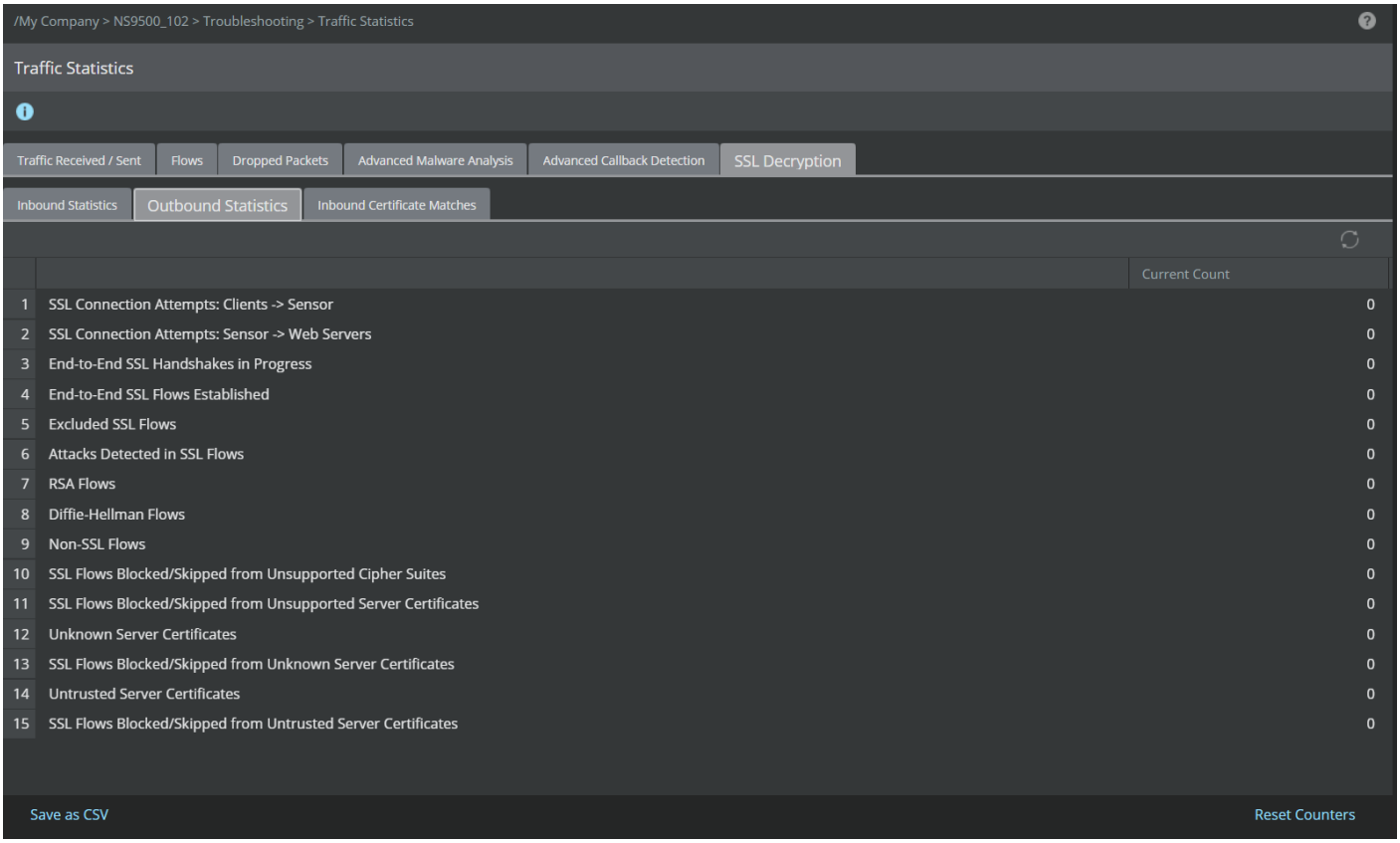


- **Outbound Statistics**: Using this tab, you can view traffic statistics for outbound SSL decryption.

> **NOTE**
>
> Outbound SSL decryption uses **Proxy method** for traffic decryption and is supported by specific NS-series Sensor models. So, you will be able to see outbound statistics tab being populated only when you add these Sensor models to the Manager. List of NS-series Sensor models supported — NS7200, NS7300, NS7500, NS9100, NS9200, and NS9500 Standalone.

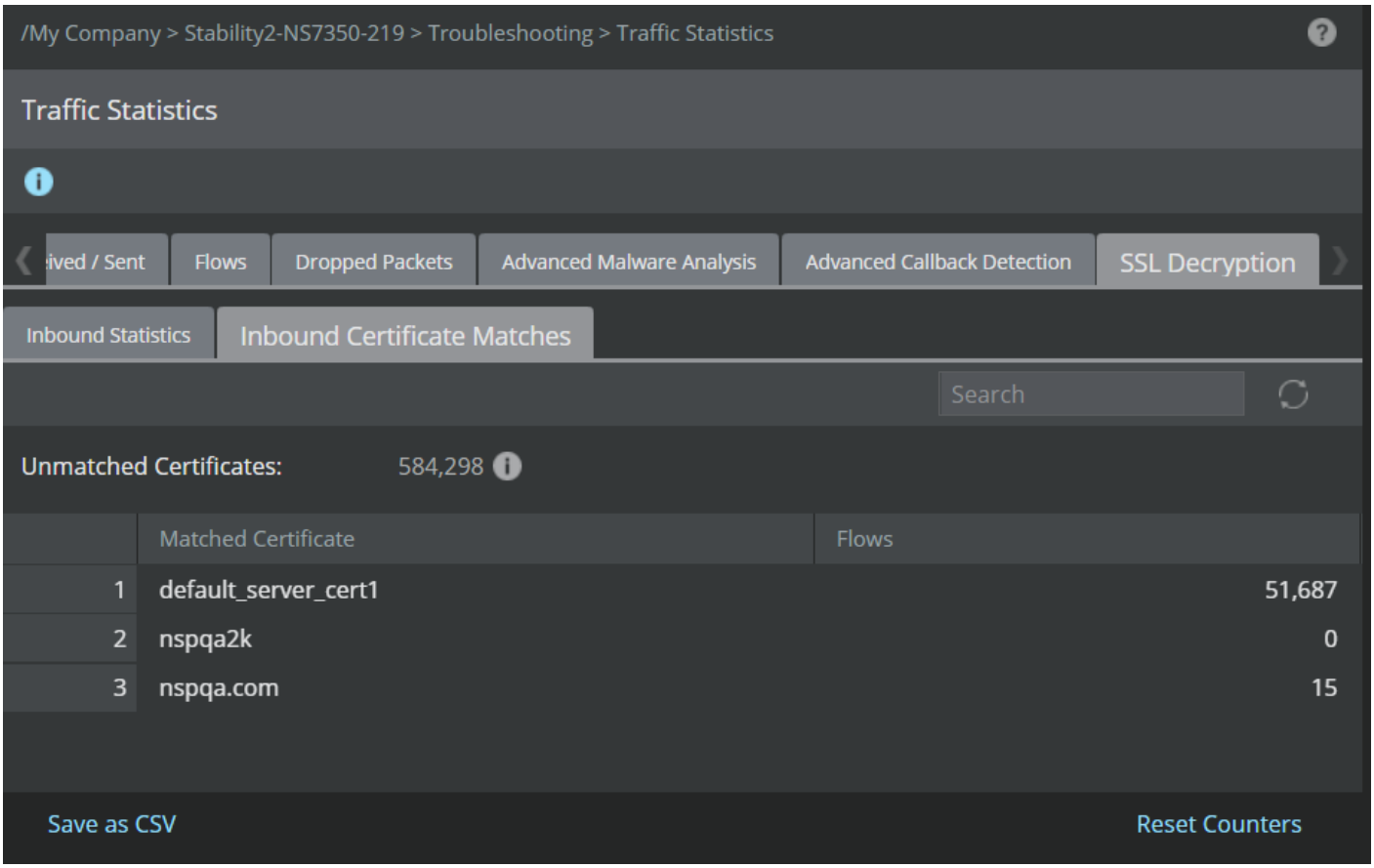
- **SSL Connection Attempts: Clients -> Sensor** - Total number of SSL flow attempts from client to Sensor in outbound direction
- **SSL Connection Attempts: Sensor -> Web Servers** - Total number of SSL flow attempts from Sensor to external server in outbound direction
- **End-to-End SSL Handshakes in Progress** - Total number of SSL handshakes in progress in the outbound direction
- **End-to-End SSL Flows Established** - Total number of SSL flows established in the outbound direction
- **Excluded SSL Flows** - Total number of SSL flows in outbound direction that are excluded from getting blocked
- **Attacks Detected in SSL Flows** - Total number of attacks detected in the outbound SSL flows
- **RSA Flows** - Total number of flows seen with RSA key exchange in outbound direction
- **Diffie-Hellman Flows** - Total number of flows seen with Diffie-Hellman key exchange in the outbound direction
- **Non-SSL Flows** - Total number of non-ssl flows seen in the outbound direction
- **SSL Flows Blocked/Skipped from Unsupported Cipher Suites** - Total number of SSL flows blocked or skipped due to unsupported cipher suites found in them
- **SSL Flows Blocked/Skipped from Unsupported Server Certificates** - Total number of SSL flows blocked or skipped due to unsupported certificates found in them
- **Unknown Server Certificates** - Total number of unknown certificates seen in the outbound SSL flows
- **SSL Flows Blocked/Skipped from Unknown Server Certificates** - Total number of outbound SSL flows blocked or skipped due to unknown certificates
- **Untrusted Server Certificates** - Total number of untrusted certificates seen in the outbound SSL flows
- **SSL Flows Blocked/Skipped from Untrusted Server Certificates** - Total number of outbound SSL flows blocked or skipped due to untrusted certificates

Figure 307. SSL Decryption - Outbound Statistics



- **Inbound Certificate Matches**: This tab displays the count for unmatched and matched certificates found in inbound SSL traffic.

Figure 308. SSL Decryption - Inbound Certificate Matches



Performance charts

The **Performance Charts** consist of the core Sensor performance metrics like the device/port throughput usage, flow usage, and the CPU usage. Monitoring these core metrics helps you monitor threshold limit and maintain efficient performance of the Sensor. The metrics for all the devices configured to the Manager can be monitored from the **Performance Charts** page. For a standalone Sensor, you can view and enable the device usage metrics in Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Performance Charts**.

For Sensors in a stack, you can view and enable the device usage metrics in Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Performance Charts**.

The performance data is available in the Manager dashboard as **Throughput Usage**, **Memory Usage**, and **CPU Usage** monitors. You can navigate to the respective performance charts by clicking on the parameter in the dashboard monitor.

CPU and port throughput metric collection are disabled by default and device throughput and memory metric collection are enabled by default. To enable performance monitoring for data collection, navigate to the **Performance Monitoring** page from the respective performance charts metric by clicking **Performance Monitoring Settings**. For more information, see Enable device performance monitoring (page 1647).

The time filter drop-down list in the **Performance Charts** page allows you to set your time preference by selecting any of the available options. This selection persists across tabs/windows in the GUI. There are two ways to view performance data:

- **Summarized** – selected by default and displays performance data in an hourly view. Data can be further viewed based on maximum, average, and minimum data usage.
- **Raw** – displays the average value for 3-minute intervals. The drop-down list of maximum, average, and minimum does not apply for this selection.

> **NOTE**
>
> For the same time period, there are approximately 20x more raw data points than summarized data points.

The charts also allow zoom in and zoom out, that is, you can select a portion of the existing charts and that portion will be zoomed in. To undo the zoom in action, click **Zoom Out**. The refresh button allows you to pull the latest data points for the selected time range.

Performance metrics

View Throughput Usage

View Device Throughput Usage

You can view the Sensor throughput usage for the selected device. The unit used for plotting the charts is percentage. Each Sensor is rated for an official maximum throughput, and the throughput usage data displayed in the charts is a percentage of that maximum throughput. Sensors can max out above that maximum rating depending on the type of traffic.

> **NOTE**
>
> The maximum number of records displayed for a selected device is 10,000.

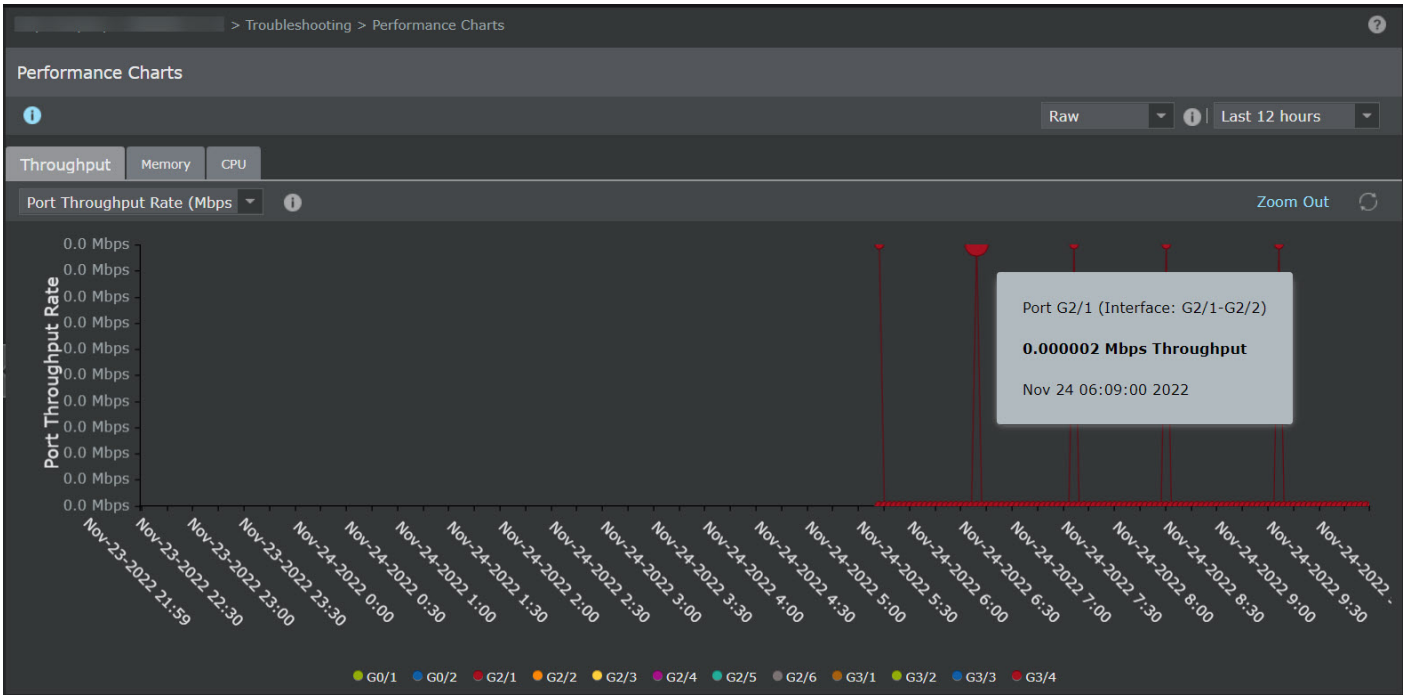
Figure 309. Device Throughput Usage

View Port Throughput Usage

You can view the port throughput usage for a specific interface depending on the device selected. The unit used for plotting the charts is Mbps. Device throughput data is displayed by default. To view data for port throughput, select **Port Throughput Usage** from the drop-down list.

To view the port throughput for a particular or multiple interfaces, select the interfaces displayed at the bottom of the charts. To hide the throughput for an interface, deselect that specific interface. For any selected interface, you can view the details of **Port <port number> (Interface: <interface name>)**, **Port throughput rate in Mbps** and time in **MMM DD HH:MM:SS YYYY**.

Figure 310. Port Throughput Usage

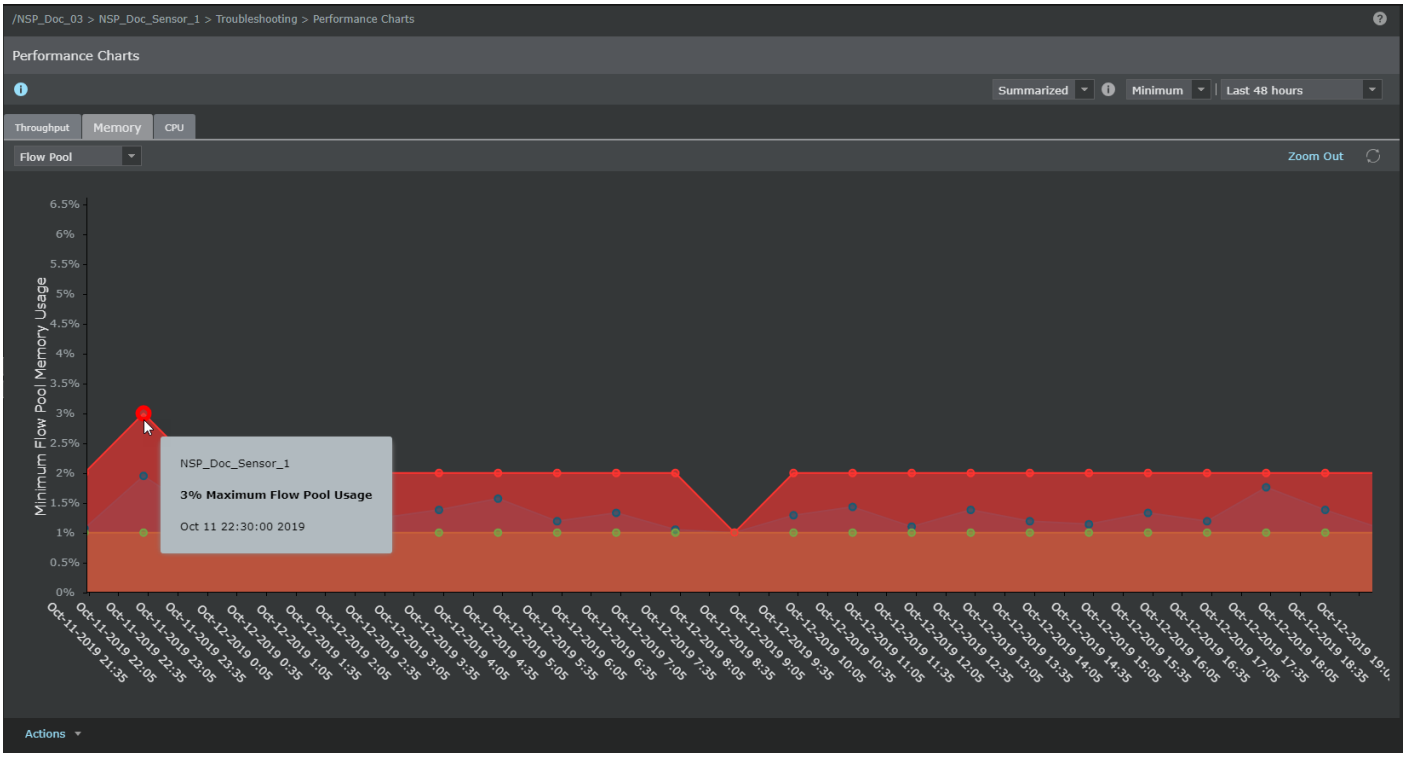


View the Memory usage

You can view the memory usage which helps monitor the usage before reaching the threshold limit. The unit used for plotting the charts is percentage. The following metrics are displayed:

- **Flow pool** — The percentage of memory allocated to inspect all flows. This is the default metric.
- **Decrypted Flow Pool** — The percentage of memory allocated to inspect decrypted SSL flows
- **Packet Buffers** — The percentage of the packet buffer used by the Sensor
- **System Memory** — The percentage of the system memory used by the Sensor

Figure 311. Memory



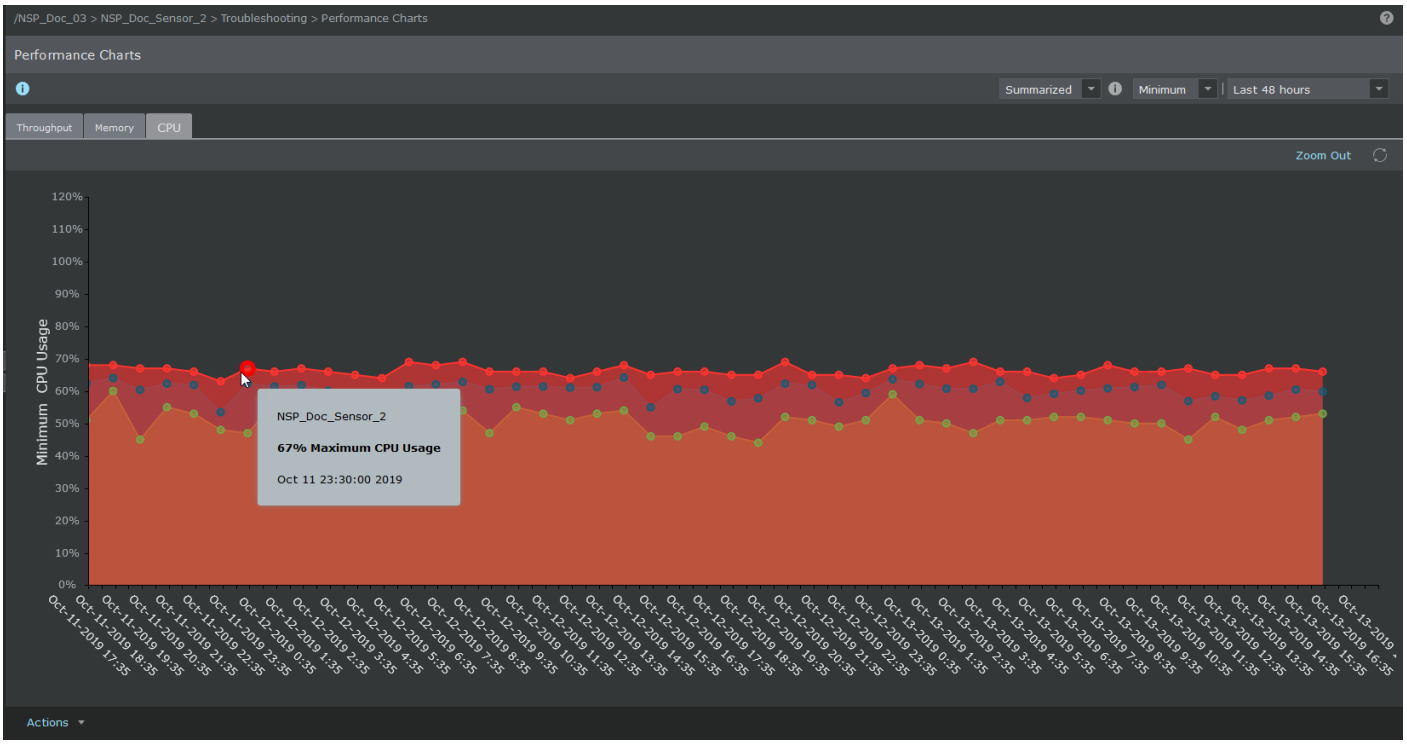
View the CPU Usage

CPU usage is the usage that represents the combined usage of software processing in the datapath along with the throughput usage in the Sensor. You can view the device CPU usage which helps monitor the CPU usage before it reaches the threshold limit. The unit used for plotting the charts is in percentage.

NOTE

By default, a fault message will be generated if the CPU usage goes beyond 90%.

Figure 312. CPU Usage



The **Actions** menu at the bottom of the page allows you to perform the following actions:

- **Save as Image File (PNG)** - This allows you to save the charts as an image file in `SENSORNAME-METRIC_Performance-YYYYMMDD_hhmm.PNG` format.
- **Manage Performance Metric Collection** - This opens the Devices → Setup → Performance Monitoring → **Summary page**.
- **Manage Performance Data Storage** - This opens the Manager → Maintenance → Database Pruning → **File and Database Pruning page**.

NOTE

This option is available only if you have access to the **Manager** menu.

Upload diagnostics trace

The **Diagnostics Trace** action uploads a device diagnostics log from a Sensor to your Manager server. The diagnostics file includes debug, log, and other information that can be used to determine device malfunctions or other performance issues. Once uploaded to your Manager, this file can be sent through email to Trellix Technical Support for analysis and troubleshooting advice.

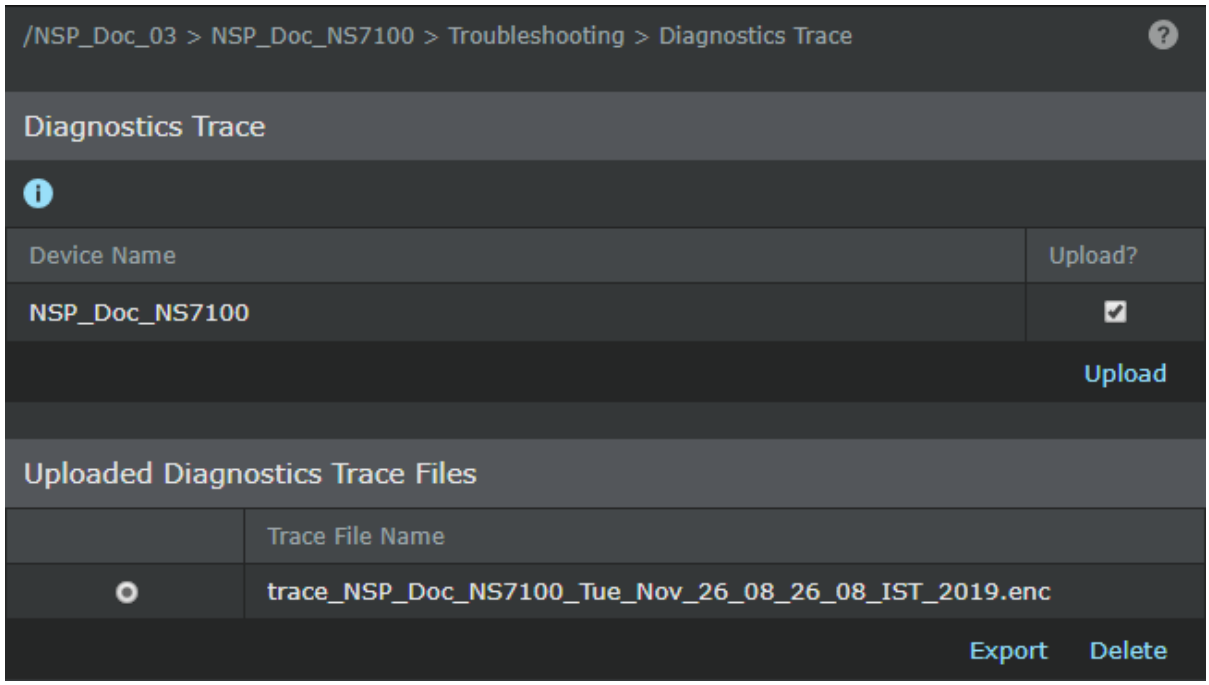
1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Diagnostics Trace**.

For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Diagnostics Trace**.

> **NOTE**
>
> The <Device Name> refers to a Sensor.

The **Diagnostics Trace** page is displayed.

Figure 313. Diagnostics Trace page



2. Select the **Upload?** checkbox if it is not already selected.
3. Click **Upload**.

   The status appears in the **Upload Diagnostics Status** pop-up window.
4. Click **Close Window** when the message DOWNLOAD COMPLETE appears. The trace file is saved to your Manager server at **`<Install_Dir>\temp\tftpin\<Device Name>\trace\`**. Once downloaded, the file also appears in the **Uploaded Diagnostics Trace Files** dialog box under this action.
5. [Optional] Export a diagnostics file to a client machine by selecting the file from the **Uploaded Diagnostics Files** listed and clicking **Export**. Save this file to your client machine. Saving the file is particularly useful if you are logged in remotely, need to perform a diagnostics trace, and send the file to technical support.

How to verify if traffic is flowing through the Sensor

For any inline Sensor, you can look at the statistics for each Sensor port to confirm if traffic is properly flowing through it, by monitoring the traffic statistics of the ports.

NOTE

For more information on traffic flowing through the Sensor, see Traffic Statistics (page 752).

Verification to check whether HA pair creation is successful

If you have configured a HA pair before connecting the heartbeat cables, you will notice Failover peer status errors appearing on the **System Faults** monitor until you connect the heartbeat cable. These messages will not appear if the two communicate properly. Errors also appear when the **Media Type** is not selected as **Copper** when using copper SFPs.

The status of the communication between the standalone Sensors can be monitored on the Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <HA Pair Node> → **Summary** page of the Manager interface or directly from the CLI of either Sensor.

The status of the communication between the Sensors in a stack can be monitored on the Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → **Summary** page of the Manager interface or directly from the CLI of either Sensor.

The Sensor command line interface (CLI) is a valuable tool for verifying correct configuration as well as diagnosing possible problems.

NOTE

For more information, see the [CLI commands] section.

show

This command shows all of the current configuration settings on the Sensor. You can use the **show** command to verify information, such as the Sensor's management port IP address, the version of software currently running, Manager's IP address, and the gateway IP address that connects the Sensor to the Manager.

status

It shows Sensor system status, such as System Faults, total number of alerts detected, and total number of alerts sent to the Manager. The **status** command is useful for verifying that trust has been established between the Sensor and the Manager, and for verifying the Sensor is detecting attacks and sending alerts to the Manager.

- If trust is not established, check the Sensor name and shared secret on both the Sensor and the Manager.
- If the Sensor is not seeing attacks for a significant period of time, check status for Sensor health and established trust. Also, check your port configuration and cabling setup.

show failover-status

This command shows whether failover is enabled on the Sensor and the status of the peer Sensor. You can run the command from either Sensor. The output includes the fields Failover Enabled (must be YES) and Peer Status (must be UP). The former

indicates whether the Sensor on which the command is issued has been configured to be part of a HA pair, and the latter shows the current state of the communication between the two Sensors.

downloadstatus

This command displays the status of various download/upload operations: signature, software image, and DoS profile downloads (from Manager to Sensor) and DoS profile and debug trace uploads (from Sensor to Manager).

Lists the number of times you have performed the operation, status of your previous attempt to perform the operation (including-if the operation failed-the cause of failure), and the time the command was executed.

How to replace a Sensor

This section describes how to replace a physical Sensor that is not functioning with a new physical Sensor.

How to replace a failed Sensor

If a Sensor has failed and is no longer operational, you must replace it with a new Sensor.

NOTE

You cannot swap out one Sensor model with another without reconfiguring the trust arrangement between the Sensor and the Manager. If you want to, for example, replace an NS3200 Sensor with an NS5200 Sensor, you must treat the installation and configuration as if you were installing a new Sensor.

NOTE

You also cannot replace a regular Sensor with a failover-only (FO) Sensor model. These Sensors are for use only in a failover configuration and cannot be used as a standalone Sensor.

Replace a failed Sensor with the same model Sensor

If you replace a failed Sensor with the same model Sensor (for example, replace an NS5100 with another NS5100), you need only install the new Sensor and configure it with the same information as the failed Sensor.

1. Remove the failed Sensor. You must turn it off, unplug it from its electrical source, unplug its cables, and remove it from its rack mounting.
2. Mount the new Sensor in the rack.
3. Follow the entire configuration process. See the section [Configuring the Sensor] in [Trellix Intrusion Prevention System Intstallation Guide]. Make sure to configure the Sensor with the same name and shared key as the failed Sensor. (You can reuse the name of the failed Sensor; however, the name must be unique to the Sensor. The Manager will not recognize two active Sensors with the same name.)

NOTE

The new Sensor does not need to have the same IP address and can reside on a different network. (If the Sensor is on a different network from the Manager, you must set the gateway IP address, and you may need to configure the Management port's speed and determine whether it is full-duplex or half-duplex.) See the [Manager Administration] section for more details.

4. For a standalone Sensor, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → **Reboot**.

   For Sensors in a stack, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Maintenance → **Reboot**.

5. Click **Reboot Now**.

NOTE

You can also perform Sensor reboot from Devices → <Admin Domain Name> → Global → **Device Manager**. Select the required Sensor and click **Reboot** from **Other Actions** drop-down.

The Sensor restarts and is ready for operations once it comes up.

Maintenance of Sensor certificate information when replacing a Sensor

NOTE

Import or export of SSL certificate data is not supported on NS3500, NS3200, NS3100, IPS-VM600, and IPS-VM5000 Sensors.

We recommend saving the Sensor certificate information to an external flash and then using that flash to re-establish all Sensor certificate data if the Sensor fails and needs to be replaced. These commands export/import the Sensor certificates, which establishes trust between the Sensor and the Manager. These certificates include the Manager public key, Sensor private key, and Sensor public key.

CAUTION

The compact flash should be physically secured at all times, since certificate data exported to flash is used to validate Sensor certificate information.

Export SSL certificate data to an external flash

You can export SSL certificate data to an external flash.

1. If the Sensor is up and running, type **`shutdown`** from the Sensor CLI.
2. Answer **Y** to the confirmation question.

3. Wait a minute, and then turn off the Sensor.
4. Insert the compact flash into the external flash receptacle on the Sensor (see the corresponding [Trellix Intrusion Prevention System Sensor Product Guide] for an illustration of the location of the external flash port).
5. Turn on the system.
6. Log on to the Manager.
7. Once the connection and trust to the Manager is established, type

   `exportSensorcerts` from the Sensor CLI. This exports all certificate data to the external flash.
8. Once done, repeat the shutdown procedure as described in **Step 1** through **Step 3**.
9. Remove the external compact flash.

> **CAUTION**
>
> Never remove or insert the compact flash when the Sensor is turned on.

Import SSL certificate data from an external flash

You can import SSL certificate data from an external flash.

1. If the Sensor is up and running, type **`shutdown`** from the Sensor CLI.
2. Answer **`Y`** to the confirmation question.
3. Wait a minute, and then turn off the Sensor.
4. Insert the compact flash into the external flash receptacle on the Sensor (see the Sensor's [Trellix Intrusion Prevention System Product Guide] for an illustration of the location of the external flash port).
5. Turn on the system.
6. Once the system comes up, type **`importsensorcerts`** from the Sensor CLI.
7. Once done, repeat the shutdown procedure as described in **Step 1** through **Step 3**.
8. Remove the external compact flash.
9. Turn on the system and when it comes up it will establish trust with the Manager automatically.

> **NOTE**
>
> Never remove or insert the compact flash when the Sensor is turned on.

Delete a Sensor from the Manager

You can delete a previously added Sensor from the Manager.

1. Delete the Sensor from the Manager:
   a. Start the Sensor software.

b. Log on to the Manager.

c. Go to Devices → <Admin Domain Name> → Global → **Add or Remove Devices**.

d. Select the Sensor from the **Add or Remove Devices** page.

e. Click .

f. Confirm the deletion.

2. Clear the configuration information on the Sensor:

a. In the Sensor command prompt window, type **`deinstall`**.

This removes the trust relationship between the Sensor and the Manager.

b. (Optional) Type **`resetconfig`**.

This clears the configuration values on the Sensor and restarts the Sensor.

> **NOTE**
>
> **`resetconfig`** does not clear values such as Sensor name, and Sensor IP. You must reset those values manually.

c. Type **`show`** to view the configuration settings.

d. To exit the session, type **`exit`**.

Add a deleted Sensor back to the Manager

If you deleted a Sensor from the Manager and want to re-add it, you must reset the shared key value on the Sensor to re-establish secure communication between the Sensor and Manager.

1. Connect a terminal to the Sensor Console port. (For instructions on connecting to the Console port, see the corresponding [Trellix Intrusion Prevention System Sensor Product Guide].)
2. At the login prompt, log on to the Sensor.
3. Clear the certificates used for communication with the Sensor. At the prompt, type **`deinstall`**.
4. Type **`show`** to see the current configuration information for the Sensor.

   Modify it as needed.
5. Re-enter the shared key information for the Sensor.

   At the command prompt, type **`set sensor sharedsecretkey <WORD>`**.

   This value is used to establish a trust relationship between the Sensor and the Manager. The secret key value can consist of up to 25 characters of any ASCII text. The shared key value is case-sensitive.

   Example: **`set sensor sharedsecretkey IPSkey123`**.
6. To exit the session, type **`exit`**.
7. Re-add the Sensor to the Manager as described in [Adding a Sensor to the Manager].

Trellix IPS policies

In Trellix IPS, all the major features, including IPS, are policy based. For example, for IDS/IPS, you use IPS policies and recon policies. Similarly, for the Firewall feature, you use the Firewall policies. This chapter introduces the security policies in Trellix IPS and provides the conceptual details for IPS policies. Other security policies such as the Firewall policies and Advanced Malware policies are discussed in their respective sections.

Generally, a security policy in Trellix IPS is a set of rules defining the activity you want the Sensors to detect and how you want to respond if that activity is detected. The activity that a rule is to detect need not be a malicious one always. For example, you can define a Firewall rule to always allow all types of traffic from your CEO's laptop. Creating a policy enables you to define a set of rules that define the different services, protocols, and/or product implementations in your network.

The following are the type of security policies in Trellix IPS:

- IPS policies
- Reconnaissance policies
- Advanced Malware policies
- Inspection Options policies
- Firewall policies
- QoS policies
- Connection Limiting policies

The best practice for protecting against misuse is not to apply a one-size-fits-all policy to the entire network, but to create multiple specific policies which focus on the specific needs of unique segments of your network. Except for some policies, Trellix IPS enables rule-based policies for your network resources, right down to individual sub-flows of network traffic. For certain policy types, several pre-configured policies are supplied for immediate application.

Imagine a network that has Windows and Linux hosts interspersed across it. The best approach for IPS here is to apply a policy that includes attacks for both Windows and Linux on all ports through which their traffic flows. If this network happens to be controlled in such a way that the traffic from all Windows hosts is flowing through one segment of the network and the traffic from all Linux hosts is flowing through a different segment, you could connect these different segments to different monitoring ports. You could then apply Windows-specific and Linux-specific policies to the respective ports. In doing so, you would minimize the chance of false positives and reduce the quantity of scanning required on each port.

How policies are applied

When you add a VLAN or CIDR block to a subinterface, Trellix Intrusion Prevention System treats the corresponding hosts as internal and builds a "protection domain" around them. All inbound traffic to and outbound traffic from those hosts is scanned using the policy associated with the sub-interface.

Inline mode and dedicated interface

The simplest scenario is the one in which a SYN packet arrives on a port that is operating in inline mode and configured as a dedicated interface.

As a dedicated interface, there is a single VIDS ID associated with the entire interface, so it is straightforward to identify.

To determine direction, the Sensor considers the physical port on which the SYN packet arrives:

- If the SYN packet arrives on the port connected to the inside network, the entire flow is considered outbound.
- If the SYN packet arrives on the port connected to the outside network, the entire flow is considered inbound.

> **NOTE**
>
> A port is defined as inside versus outside from the **Physical Ports** page of the Manager.

For example, if a client connects to a server through the G0/1-G0/2 monitoring ports, and the client's SYN packet arrives on the outside port, all traffic in the flow is scanned using the signatures associated with the inbound attack set profile and VIDS ID for the G0/1-G0/2 interface; this includes return traffic from the server.

SPAN or tap mode

Ports in SPAN mode do not provide a Sensor with the same physical means to determine direction. In the case of SPAN mode, for example, traffic is mirrored from a switch to a single Sensor monitoring port, so a Sensor cannot easily differentiate inbound traffic from outbound.

How the Sensor determines direction and VIDS ID in SPAN mode depends on the interface type in question.

Dedicated interface

When running a dedicated interface in SPAN mode, no direction information is available; the Sensor considers all traffic as inbound traffic. Further, the Sensor stores the VIDS ID of this interface.

VLAN interface

When running a VLAN interface in SPAN or tap mode, no direction information is available; the Sensor considers all traffic as inbound traffic. Further, the Sensor stores the VIDS ID of this interface.

CIDR interface

When running a CIDR interface in SPAN mode, the Sensor uses the following logic to determine direction and VIDS ID:

- When a SYN packet arrives on a SPAN port, the Sensor compares its CIDR sub-interfaces against the destination IP address in the SYN packet.
- If there is a match, the entire flow is considered inbound and the Sensor stores the VIDS ID of the matched CIDR sub-interface.
- If there is no match, the Sensor compares its CIDR sub-interfaces against the source IP address in the SYN packet.
- If there is a match, the entire flow is considered outbound and the Sensor stores the VIDS ID of the matched CIDR sub-interface.
- If there is no match, the entire flow is considered inbound and the Sensor stores the VIDS ID of the parent interface.

Sub-interfaces

If the same port on which the SYN packet arrives is instead associated with a **VLAN** or **CIDR** interface, the Sensor applies the same logic to determine the direction of the flow, but must do additional work to determine the VIDS ID.

If the interface type is **VLAN**, the Sensor compares the VLAN tag in the SYN packet against all previously defined VLAN IDs to determine the sub-interface to which the flow belongs.

- If the Sensor matches the VLAN in the SYN tag packet with one of its VLAN IDs, it stores the VIDS ID of the matching sub-interface in its state table.
- If the Sensor does not match the VLAN tag in the SYN packet with one of its VLAN IDs, it stores the VIDS ID associated with the parent interface instead.

If the interface type is **CIDR**, the Sensor uses the direction of the flow to determine the sub-interface to which the flow belongs.

- If the flow is inbound, the Sensor compares the destination IP address of the SYN packet against its CIDR sub-interfaces.
- If there is a match, the Sensor stores the VIDS ID associated with the matched CIDR sub-interface.
- Otherwise, it stores the VIDS ID associated with the parent interface.
- If the flow is outbound, the Sensor compares the source IP address of the SYN packet against its CIDR sub-interfaces.
- If there is a match, the Sensor stores the VIDS ID associated with the matched CIDR sub-interface.
- Otherwise, it stores the VIDS ID associated with the parent interface.

Configuration of policies

Your policy determines what traffic analysis your Sensor will perform. Trellix IPS provides a number of policy templates to get you started toward your ultimate goal: prevent attacks from damaging your network, and limit the alerts displayed in the Attack Log to those which are valid and useful for your analysis.

There are two stages to this process: initial *policy configuration* and *policy tuning*. Policy tuning is renowned to be a tedious task. However, because networks and attacks constantly evolve, the policy tuning process is never truly complete. Instead, you might equate it to a disk defragmentation; the more often you do it, the less time each check takes. The ultimate goal of policy tuning is to eliminate **false positives** and noise and avoid overwhelming quantities of legitimate, but anticipated alerts.

Tune your policies

This central point of this section is the IPS policy, but conceptually it is relevant to some of the other security policies of Trellix IPS as well.

The pre-defined IPS policies are provided as a generic starting point; you will want to customize one of these policies for your needs. So, the first step in tuning is to clone the most appropriate policy for your network and your goals, and then customize it. (You can also edit the policy directly.) Some things to remember when tuning your policies:

- We ask that you set your expectations appropriately regarding the elimination of false positives and noise. A proper Trellix IPS implementation includes multiple tuning phases. False positives and excess noise are routine for the first 3 to 4 weeks. Once properly tuned, however, they can be reduced to a rare occurrence.
- When initially deployed, Trellix IPS frequently exposes unexpected conditions in the existing network and application configuration. What may at first seem like a false positive might actually be the manifestation of a misconfigured router or Web application, for example.

- Before you begin, be aware of the network topology and the hosts in your network, so you can enable the policy to detect the correct set of attacks for your environment.
- Take steps to reduce false positives and noise from the start. If you allow a large number of "noisy" alerts to continue to sound on a very busy network, parsing and pruning the database can quickly become cumbersome tasks. It is preferable to all parties involved to put energy into preventing false positives than into working around them. One method may be is to disable all alerts that are obviously not applicable to the hosts you will protect. For example, if you use only Apache Web servers, you may want to disable IIS-related attacks.

For more information on IPS policy tuning best practices, refer to Effective policy tuning practices (page 2291).

Attack Definitions

Attack Definitions are essentially a 'shortcut' to customizing a particular attack's response across all policies containing that attack. Responses configured at the Attack Definitions level are then available for that attack at the attack set profile and policy level.

We've discussed policy inheritance and response actions. To fully understand Attack Definitions, consider a concept that we will loosely call *response inheritance*.

A new signature set straight from the Update Server contains some default actions associated with particular attacks. For example, certain attacks are configured to log packets, and others are configured not to log packets.

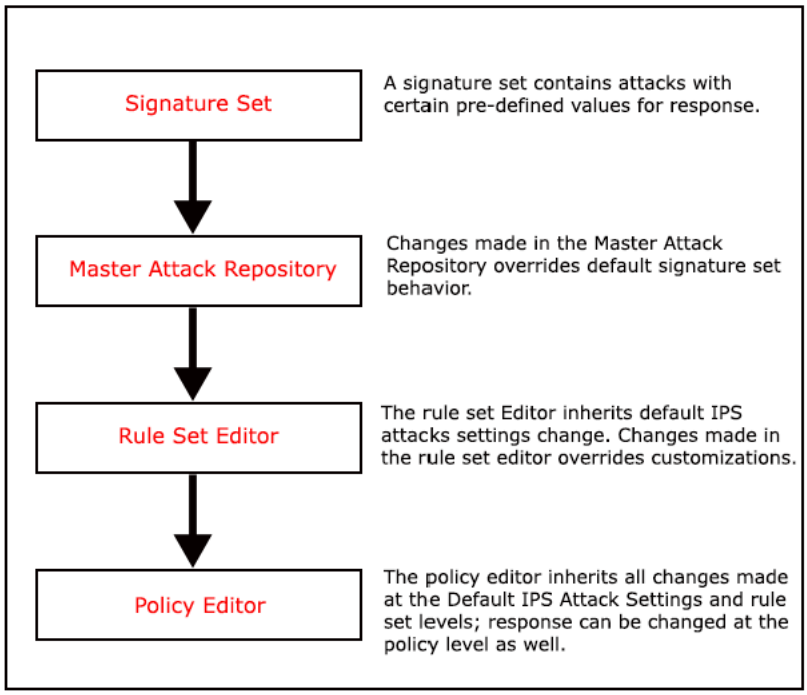
When you open an attack in the Attack Definitions editor, Attack Definitions displays the default attack values specified by the signature set. Attack Definitions thus "inherits" the response actions from the signature set. Customizing these values in the Attack Definitions overrides the signature set's values. Regardless of what the signature set suggested as the attack's response, the attack now has a custom response as specified in Attack Definitions.

Attack Definitions values are then available for customization at the attack set profile level. For example, at the attack set profile level, you inherit all the customization from the Attack Definitions level, but can set a response action of "blocking" for certain attacks. Now the attack can have the Attack Definitions customization plus the attack set profile customization.

Finally, you have the Policy level. All the customization made at the attack set profile level or at the Attack Definitions level are inherited at the Policy level.

As shown in the following figure, each level *inherits* response attribute values from previous level. At each level you can either retain the inherited value for an attack or customize it by explicitly setting or removing a value.

Figure 314. Attack set profile



The policy editor now displays labels showing at what level an attack was customized:

D – Default Trellix IPS-supplied

D – Master Attack Repository

R – Attack set profile Editor (only blocking action)

P – IPS Policy Editor

For example, suppose you want to create 3 policies that detect the attack "FTP: Attack Example," which happens to be a Recommended For Blocking (RFSB) attack.

Your requirements are as follows:

- Policy1: block FTP: Attack Example and log packets
- Policy2: do not block FTP: Attack Example; log packets.
- Policy3: block FTP: Attack Example; do not log packets
- For all three policies, you want to be notified by email if FTP: Attack Example is discovered.

How to accomplish this?

1. At the Master Attack Repository level for FTP: Attack Example, configure packet logging and email notification.
2. At the attack set profile level, enable blocking for RFSB attacks.
3. At the PS Policies level, create your three policies. When you choose FTP: Attack Example for Policy2, disable blocking. For Policy3, disable packet logging.

NOTE

Master Attack Repository customization can be imported/exported using the Policy Import/Export feature.

False positives and noise

The mere mention of false positives always causes concern in the mind of any security analyst. However, false positives may mean quite differently things to different people. To better manage the security risks using any IDS/IPS devices, it's very important to understand the exact meanings of different types of alerts so that appropriate response can be applied.

With Trellix IPS, there are three types of alerts that are often taken as "false positives":

- Incorrectly identified events
- Correctly identified events subject to interpretation by usage policy
- Correctly identified events uninteresting to the user.

Incorrect identification

These alerts typically result from overly aggressive signature design, special characteristics of the user environment, or system bugs. For example, typical users will never use nested file folders with a path more than 256 characters long; however, a particular user may push the Windows' free-style naming to the extreme and create files with path names more than 1024 characters. Issues in this category are rare. They can be fixed by signature modifications or software bug fixes.

Correct identification — significance subject to usage policy

Events of this type include those alerting on activities associated with instant messaging (IM), internet relay chat (IRC), and peer-to-peer programs (P2P). Some security policies forbid such traffic on their network; for example, within a corporate common operation environment (COE); others may allow them to various degrees. Universities, for example, typically have a totally open policy for running these applications. Trellix IPS provides two means to tune out such events if your policies deem these events uninteresting. First, you can define a customized policy in which these events are disabled. In doing so, the Sensor will not even look for these events in the traffic stream to which the policy is applied. If these events are of interest for most of the hosts except a few, creating ignore rules to suppress alerts for the few hosts is an alternative approach.

Correct identification — significance subject to user sensitivity (also known as noise)

There is another type of event that you may not be interested in, due to the perceived severity of the event. For example, Trellix IPS will detect a UDP-based host sweep when a given host sends UDP packets to a certain number of distinct destinations within a given time interval. Although you can tune this detection by configuring the threshold and the interval according to their sensitivity, it's still possible that some or all of the host IPs being scanned are actually not live. Some users will consider these alerts as *noise*, others will take notice because it indicates possible reconnaissance activity. Another example of noise would be if someone attempted an IIS-based attack against your Apache Web server. This is a hostile act, but it will not actually harm anything except wasting some network bandwidth. Again, a would-be attacker learns something he can use against your network: the fact that the attack failed can help him zero in on the type of Web server you use. Users can also better manage this type of events through policy customization or installing ignore rules.

The noise-to-incorrect-identification ratio can be fairly high, particularly in the following conditions:

- The configured policy includes many Informational alerts, or scan alerts which are based on request activities (such as the Default Testing and Default Exclude Informational)
- Deployment links where there is much hostile traffic, such as in front of a firewall
- Overly coarse traffic VIDS definition that contains disparate applications. For example, a highly aggregated link in dedicated interface mode

Users can effectively manage the noise level by defining appropriate VIDS and customize the policy accordingly. For dealing with exceptional hosts, such as a dedicated pen test machine, ignore rules can also be used.

Components of an IPS policy

An IPS policy is one of the many types of security policies used in Trellix IPS. A Sensor uses the assigned IPS policy to determine if the detected traffic is free of attacks according to that policy. An IPS policy is for detecting exploit attacks, policy violations, and DoS attacks. Also, the IPS policy determines how a Sensor responds when it detects traffic that violates an IPS policy.

The main components of an IPS policy are the attack set profiles and the Attack definitions. An IPS policy is essentially a set of attack definitions for various protocols (HTTP, UDP), operating systems (Windows, NT, Solaris), and other types of information transmitted across your network. In addition to other anomalies in the detected traffic, the Sensor also checks if that traffic matches with what is defined in an attack. If a match is found, that means the corresponding attack was attempted.

In an IPS policy, an attack set profile for inbound and an attack set profile for outbound is specified. It can be the same attack set profile for both inbound and outbound or different ones. The attack set profiles specified in the IPS policy determine the attack definitions to be included in the IPS policy.

NOTE

There are quite a few predefined IPS policies provided for you to deploy Trellix IPS out-of-the box. You can use them or create your own.

To create and use IPS policies, familiarize yourself with the terminologies discussed here.

Attack Set Profile— The best practice is to create multiple, specific IPS policies that focus on the specific needs of unique zones in your network, rather than a one-size-fits-all policy for the entire network. Therefore, the attack definitions are internally classified based on:

- Whether they are exploits, malwares, policy violation, and so on
- The relevant protocols, such as FTP, HTTP, RADIUS, and so on
- The relevant operating systems
- The applications such as Skype and Google Search that attacks are relevant for
- The chances of attacks being false-positives

In an attack set profile, you can specify the categories of attacks that must be included and the categories that must be excluded. Then when you specify this attack set profile in the IPS Policy, the Manager processes the Signature Set and identifies the attack definitions according to what you specified in the attack set profile. Only these attack definitions are included in the IPS policy. You can also create rules to choose attacks to be explicitly blocked by the Sensor as per your network requirements while creating an attack set profile. The configuration options on the **Attacks to Block** tab enables you to select minimum severity, categories, and subcategories of attacks which should be explicitly blocked by the Sensors. It works on the subset of data that comes in the form of **Include** rule(s) set on the **Attacks to Include/Exclude** tab. In other words, rules created on

the **Attacks to Block** tab determine the attack definitions that are automatically set to be blocked in the corresponding IPS policy. For more formation, refer to the section Defining and using user-customizable blocking strategy to make self-adaptable IPS policies (page 876).

In the Manager, there are several provided attack set profiles which match the preconfigured policies. You can view, clone (copy), and customize these attack set profiles for your own use.

Rules— You specify the categories of attacks to be included and excluded, along with categories and/or subcategories of attacks to be blocked in an attack set profile. To do so, you define rules in an attack set profile. Each rule in a set is either an include rule, exclude rule, or a rule to block specific attacks.

An include rule which should always start an attack set profile is a set of parameters that encompasses a broad range of well-known attacks for detection. An exclude rule removes elements from the include rule to focus the policy's attack set profile. By broadening (includes) and narrowing (excludes) the rules, you can enable detection for the attacks that affect the intended environment.

If you have an exclude rule, an include rule added afterward might negate the exclusion For example, if you specify an exclude rule for the DNS protocol, then later include multiple protocols including DNS, the exclusion rule is negated.

You can also define rules of blocking during attack set profile configuration, that include one or more categories and subcategories of attacks and the minimum severity level, as per your own blocking strategy. These rules determine the attack definitions that are automatically set to be blocked in the corresponding IPS policy.

Signature Set— This is the complete set of attack definitions developed and provided by Trellix Advanced Research Center. The Signature Set enables Trellix IPS to properly detect and protect against malicious activity. The Manager and the Sensors must be frequently updated with the latest signatures and software patches made available to you via the Update Server.

Attack definitions and signatures— Note that as you interact with Trellix IPS policies, you encounter the term attack, not signature. Trellix IPS defines an attack as being comprised of one or more signatures, thresholds, anomaly profiles, or correlation rules, where each method is used to detect an attempt to exploit a particular vulnerability in a system. These signatures and checks might contain specific means for identifying a specific known exploit of the vulnerability, or more generic detection methods that aid in detecting unknown exploits for the vulnerability. Combined in an attack, the signatures provide for maximum accuracy and coverage in attack detection.

Custom Attacks— There could be unique security requirements that would not be possible to be covered in the Trellix-supplied signature set. For such cases, you have the option of developing your own attack definitions. Such user-defined attacks are referred to as custom attack definitions or custom attacks. The Manager factors in the Custom Attacks as well when it calculates the attack definitions to be included according to an attack set profile. Custom Attacks are exclusively covered in the Custom attacks (page 1676).

Classification of attack definitions

As mentioned earlier, the attack definitions are classified based on multiple factors. This classification is to enable you to include only the relevant attacks in your IPS policies. Factors such as protocols, operating systems, and applications are straight-forward. Factors that require some explanation are discussed in the following sections.

Attack categories

When a system vulnerability has been discovered, an attacker can threaten the system with an attack that affects the system. The attack categories, also known as *attack type*, detail the general types of attacks that can be performed to a system.

Attack category	Description
Exploit	This category covers most attack activities that actively seek to compromise systems, gain unauthorized access to system or services, or tamper normal system operations by exploiting known or potential system vulnerabilities.
Malware	Malware is the short form for malicious software. It can be defined as a piece of harmful software code created and spread with a malicious intent. Examples are virus programs, Trojan horses, computer worms, spyware, and botnets. In general, the objective of the attacks in this category is to steal system or user confidential information and send it back to the server controlled by the attacker. Targeted information includes user name, host name, user passwords, and license keys. Some other common characteristics of the attacks in this category include spamming, launching DoS attacks, downloading additional malicious code, and downloading updates to the malicious code.
Policy violation	An attacker performed an action that goes against the organizational or system policy, possibly by attempting to gain access they are not authorized to have. This includes all activities for which the underlying traffic content might not be malicious by itself, but are explicitly forbidden by the usage policies of the administrative domain. This includes application protocol behaviors that violate common usage practices.
Reconnaissance	This type of activities is for intelligence gathering to prepare for further attacks; for example, a port scan or probe conducted to enumerate or identify services and possible vulnerabilities.
DoS and DDoS	A denial of service (DoS) or distributed denial of service (DDoS) attack is performed, possibly harming the ability of the network or system to respond or continue providing services.
Multi Sensor correlation	Manager correlates the attack detection information from multiple intrusion detection systems (Sensors) to identify different phrases of the attack behaviors.
Protocol discovery	Sensor determines protocol anomaly on well-known ports, such as P2P software running on a well-known port.
Multi method correlation	Multiple detection methods are used to correlate the attacking traffic to identify different phrases of the attack behaviors. Examples of such correlation are attack signature, Trellix IPS shellcode detection, and statistical correlation.
Flow correlation	Sensor correlates the bi-directional traffic of each session to increase the accuracy of the attack detection as well as impact of the attack.
Application anomaly	This type of attack is caused when a large number of bytes comes from an HTTP browser than that are actually going onto it. An example of such an attack is Buffer Overflow.
Volume DoS	Large volume of traffic, which could be perfectly valid from the perspective of application content, that can overwhelm processing element along the path to the target including switches, routers, firewalls, target servers, and so on; this will cause a DoS effect on other legitimate traffic.

Attack subcategories

Attack subcategories are the specific, inherent system flaws that can be exploited by attackers familiar with a vulnerability or malware. A known vulnerability poses a threat to the system; the attacking party exploits this threat with an attack that is designed to affect some part of the vulnerable system. The following table captures some of the Attack subcategories:

Category	Description
Trellix Intelligent Sandbox	This kind of alert indicates that a malicious file transfer is detected on network by Trellix Intelligent Sandbox Engine.
Arbitrary Command execution	An attacker can execute system commands and scripts, like getting a directory listing on a system, thus stealing and destroying data. The attacker who is able to access a user's system can exploit the vulnerability and install malicious software and use the system to launch attacks on other systems.
Audit	Any networking event deemed to be of interest to the security analyst. Examples include invocation of particular applications or use of particular commands in certain applications.
Backdoor	Depending on the confidence level of the triggers, this can either be some attempts at contacting a backdoor process or the occurrence of actual backdoor two-way conversation. If the latter has occurred, it means that a backdoor process exists in your network, the backdoor user is in your network, or both are inside your network, depending on the locations of the communication endpoints.
Bot	It refers to a group of computers running or executing a program that allows an attacker to control the system remotely and make users execute commands like DOS. These commands are taken place in the IRC channel. A 'bot' is a type of malware which allows an attacker to gain complete control over the affected computer. Computers that are infected with a 'bot' are generally referred to as 'zombies'. Attackers are able to access lists of 'zombie' PC's and activate them to help execute DoS (Denial of Service) attacks against Web sites, host phishing attack Websites or send out thousands of spam email messages. A bot worm is a self-replicating malware program that resides in current memory (RAM), turns infected computers into zombies (or bots) and transmits itself to other computers. A bot worm may be created with the ultimate intention of creating a botnet that functions as a vehicle for the spread of viruses, Trojans and spam.
Botnet	It refers to a group of computers that has been infected by Bots in a network.
Brute Force	Brute force attacks are performed using programs, such as password crackers, to try different sets of passwords so as to guess the right one.
Buffer Overflow	This kind of alerts indicates attempts at exploiting software vulnerabilities where manipulation of buffer spaces can result in overwriting of unintended memory areas. Such overwriting can have different consequences depending on if the areas are executable or not. If not, it can cause malfunction of the software, thus denial of service; if yes, it can lead to execution of arbitrary machine code within the context of the current process which can lead to much more severe security breach.
Code/Script Execution	It refers to a vulnerability which can be exploited by malicious people to compromise a user's system. An attacker can execute malicious programs or code on a user's system. Successful exploitation allows execution of arbitrary code and possibly takes complete control of the affected system. Attacker can run code with elevated permissions. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Category	Description
Command Shell	Traffic activities indicating interactive shells under Unix or Windows operating systems, and so forth
Covert Channel	Any communication activities that are deemed unintended by the communication channel being monitored
Custom Fingerprinting	It refers to the detection of malicious files using known hashes (MD5 or SHA256). MD5 and SHA256 hashes can be added to the Manager based on requirements.
DDoS Agent Activity	Known DDoS attack tools use various patterns of communication among attackers or handlers, and attacking agents or zombies. Detection of these activities is a good sign that either someone is attempting to contact DDoS agents, or there may be real attackers or agent processes in the monitored networks.
DoS	Well-crafted packets, for example, with invalid/inconsistent TCP/UDP/IP header values, aiming at crashing the target TCP/IP stack or causing high resource consumption.
Endpoint Intelligence Agent	This kind of alert indicates that a malicious file transfer is detected on network by McAfee Endpoint Intelligence Agent.
Evasion Attempt	This kind of alert indicates a sequence of packets or bytes in the traffic signifying a specific attempt at evading an IDS. For example, FTP attacks are known to use escape control character sequences to hide attack payload and TCP-based RPC attacks may use record format to split up attack payload.
File Mismatch	It refers to a file that has been given an extension which does not match its actual file type and/or content type. For example, a file with .exe extension (executable) downloaded with a text/plain content type.
OS Fingerprinting	Well-defined sequence of packets, each of which is typically a probe attempt itself, launched against a given destination IP address, typically aiming at identifying the target operating system or host type.
Gateway Anti-Malware	It refers to a malware that has been detected in a file analyzed by the Gateway Anti-Malware (GAM) advanced malware engine, which is the same Anti-Malware Engine found in Trellix Endpoint products, but it is optimized for network analysis.
GTI File Reputation	It refers to a malware that has been detected in a file analyzed by the Trellix Global Threat Intelligence.
Host Sweep	Well-defined sequence of packets sweeping through a range of destination IP addresses, typically aiming at identifying live hosts
Malicious Flash Analysis Engine	This kind of alert indicates that a malicious file transfer is detected by Flash Analysis Engine.
Malware Being Redownloaded	This kind of alert indicates that an action to redownload a known malware that has been blocked.
Multi-Attack Correlation	It refers to the categories of attacks which use Multiple Attack Correlation mechanism. Multi-AID attacks can correlate attacks to identify zero-day, DoS, and Bot behavior.
Multi-Attack Known Bot	Multiple attack correlation used for known Bots
Multi-Attack Heuristic Bot	Multiple attack correlation used for zero day attack detection

Category	Description
Non-standard Port	Any traffic activities suggesting that a standard protocol running over non-standard ports according to specifications.
Trellix IPS Analysis	This kind of alert indicates that a malicious file transfer is detected by Trellix Advanced Malware engine.
Over Threshold	Any of the well-defined traffic thresholds has been crossed. Examples include ICMP packet rate, IP fragment rate, and so forth.
PDF Emulation	This kind of alert indicates that a malicious file transfer is detected by JavaScript Emulation engine.
Phishing	It is an email-fraud method in which the perpetrators send out legitimate looking email in attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy websites. Websites that are frequently spoofed by phishers include oBey, MSG, Yahoo, etc. "Phishing" is a form of Internet fraud that aims to steal valuable information, such as credit cards, social security numbers, user IDs, and passwords. A fake website is created that is similar to that of a legitimate organization, typically a financial institution such as a bank or insurance company. An email is sent requesting that the recipient access the fake website (which is usually a replica of a trusted site) and enter their personal details, including security access codes.
Port Scan	Well-defined sequence of packets sweeping through a range of destination ports on a given IP, typically aiming at identifying open ports on the target host.
Privileged Access	Privileged access indicates the most serious type of successful exploitation, where unauthorized access to privileged accounts has been obtained. For example, a successful buffer overflow on a Unix server may open a root shell for the attacker. Alternatively, the attacker may have achieved successful permission elevation from a legitimate user account, or from a remote access compromise. Privileged access allows the attacker to potentially take complete control of the compromised system.
Probe	Probes of specific service or host, typically based on specially constructed packets, for example unusual flag settings
Protocol Violation	Unusual application protocol behaviors, including invalid field values or invalid command sequences, and so forth
Potentially Unwanted Program	A Potentially Unwanted Program (PUP) is a program that may be unwanted, despite the possibility that users consented to download it. PUBs include spyware, adhere, and dialers, and are often downloaded in conjunction with a program that the user wants. Trellix differentiates PUPs from other types of malware, such as viruses, Trojans, and worms, which can be safely assumed to be unwanted by the user.
Read Exposure	With a successful attack, this suggests that a breach of confidentiality has occurred. Examples include directory traversal, dump of file content such as CGI script, or read of other sensitive data files such as password and database records.
Remote Access	Remote access indicates a potentially successful exploitation in which unauthorized access has been obtained. For example, a successful buffer overflow on a Windows server may open a Windows command shell for the attacker. The remote access does not have to be for a privileged user to begin with, but an attacker may be able to perform further attacks to achieve permission elevation once remote access is obtained.

Category	Description
Restricted Access	Any activities related to using any network resources that are explicitly forbidden, for example, emails to/from particular addresses and browsing of specific URLs.
Restricted Application	Any activities related to running network applications that are forbidden by policy. Examples include running an IRC or music share server on the corporate network without authorization.
Sensitive Content	Any content keyword matches that are deemed to indicate transmission of sensitive information, for example, document with "Company Confidential" marking.
Service Sweep	An alert indicates that a client scans for services on your network or sub network, thus leading to increased bandwidth corruption and increase in network traffic. It is usually generated by a P2P client. A Service Sweep is an attempt to determine if a service is running on a range of machines. The hacker will pick one port (usually 25-SMTP, 80-HTTP, or 139-NetBIOS SSN) and a range of IP addresses. A Ping Sweep is an attempt to see which machines in a network are on and responding. The easiest way to detect these in a trace is to look for ARP packets. So, create a filter looking for ARP requests.
Shellcode Execution	This kind of alert indicates the most severe form of buffer overflow attacks, that is, a buffer overflow attack carrying shellcode payload. Shellcode is a general term used for a piece of executable code that, upon successful execution on the target system, modifies the target's configuration or behavior for malicious purposes.
Statistical Deviation	Indicates that a significant change was detected in the packet rate for a particular traffic measure. For example, if in your normal flow of traffic, TCP SYN packets make up between 23–28% of the traffic, a short-term measure of TCP SYN traffic at 40% may indicate a DoS attack.
TIE File Reputation	This kind of alert indicates that a malicious file transfer is detected by Trellix Threat Intelligence Exchange (TIE), which takes advantage of Trellix Data Exchange Layer to consolidate threat information, including malware confidence, infection timelines, and prevalence. TIE data sources include Global Threat Intelligence (GTI), Trellix Intelligent Sandbox, and ePolicy Orchestrator (ePO).
Trojan	Refers to a malicious program that works in the background and perform malicious actions. For example, the Trojan could allow full access of the affected system to the creator. Trojans are usually packaged in innocuous file downloads or links.
Unassigned	This category is for attacks that fall outside the scope of the known subcategories in the Trellix IPS environment. For example, if an attacker comes along a Van Eck device and starts conducting Tempest attacks, "unassigned" would be the description.
Unauthorized IP	Any traffic activities suggesting existence of IP addresses that are not known to be authorized for the protected network.
Virus	Any network event or payload specifically related to a virus. Virus can inflict many different types of damage to its target, ranging from stealing or destroying information to installing backdoor processes. However, a virus relies on other carriers, for example, email, to propagate through the network.
Worm	Any network event or payload specifically related to worm activities. A worm can inflict many different types of damages to its target, ranging from stealing or destroying information to installing backdoor processes. The worm differs from a virus in that it can propagate itself through the network.

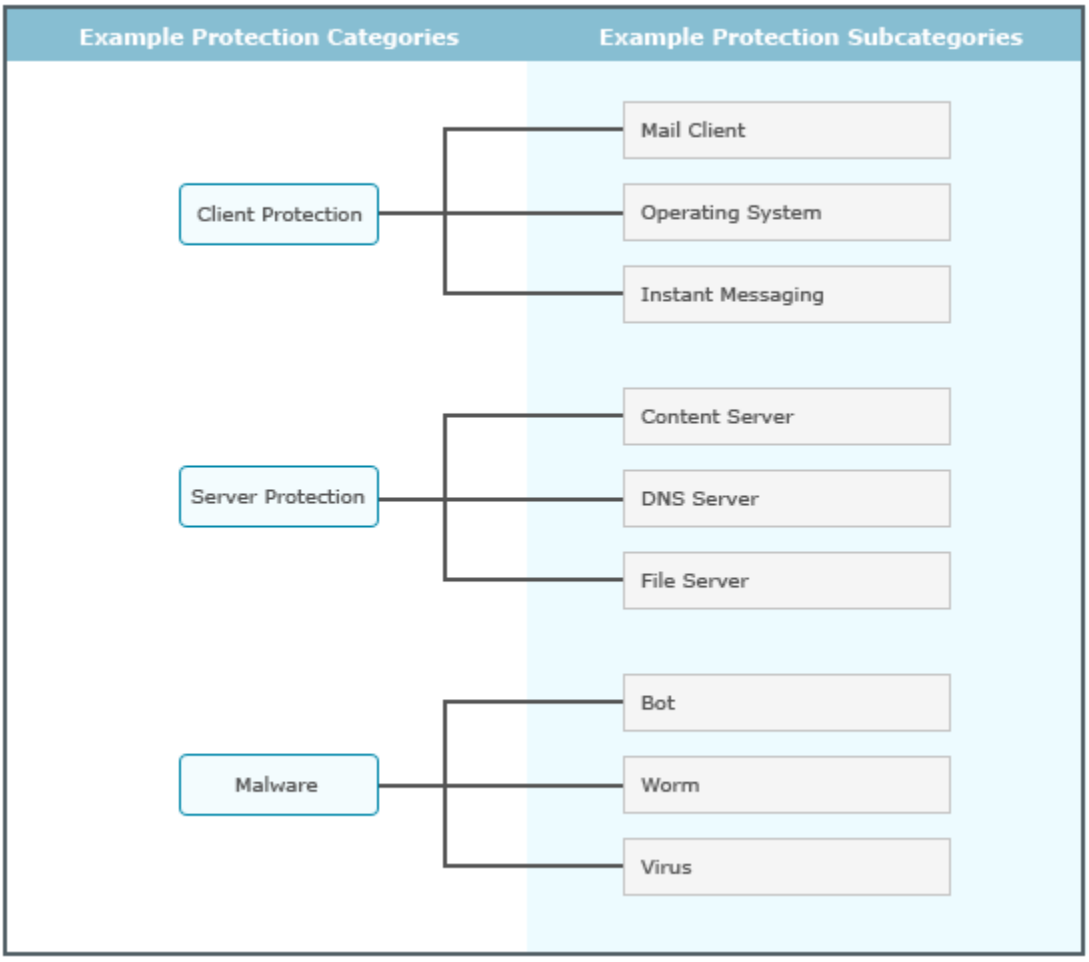
Category	Description
Write Exposure	With a successful attack, this suggests that a breach of integrity and/or authenticity of data has occurred. Examples include creation/removal of files and modification of files for system configuration or user passwords. With write exposures, there is often more severe indirect impact, for example, breach of access control by adding an illegal user account records.

Protection categories

In Trellix IPS, attacks are traditionally classified based on their type. For example, an attack can be an exploit attack, reconnaissance attack, DoS attack, or a policy violation. These categories are referred to as attack categories. Attacks are also classified based on the intent of the attack and the intended target. For example, an attack targeting vulnerabilities in client operating systems is classified under Client Protection/Operating System. These are referred to as protection categories.

There are two levels in protection categories. The first-level classification is at a broader level and can indicate whether an attack is a malware or whether it is targeted at clients or servers. Each of these categories has subcategories that can indicate the specifics of an attack. See the examples shown in the following diagram.

Figure 315. Examples of protection categories and protection subcategories



For Trellix-defined attacks, Trellix ARC classifies the attacks into one or more protection categories. In case of Trellix custom attacks, you can specify a relevant protection category for each attack definition.

Protection categories help you to relate attacks better. For example, an attack classified as an exploit that targets client operating systems is more informative than just being classified as an exploit attack. You can also view the attack definitions related to a specific category in a policy. For example, you can check what are the attack definitions you have in your policy to protect your DNS servers. Thus, you can map attack definitions to the network resources you want to protect.

In the Attack Log, the protection category feature facilitates analysis that is more granular. For, example you can analyze whether it is the clients or servers that are being attacked. Similarly, you can generate reports based on protection categories.

Notes:

- Currently you can only filter based on protection categories when you view exploit attack definitions. This display filter is only available in the **IPS** page and not in the **Master Attack Repository** page (formerly **Global Attack Response Editor** or GARE).
- In the **Recon Policy Editor**, you cannot filter attack definitions based on protection categories. However, in the Attack Log, protection category detail is displayed for recon attacks as well.
- In the **Custom Attack Editor**, when you create an exploit or recon Trellix custom attack, you can specify the protection category. This is not relevant for Snort Custom Attacks.

Protection category details in the Attack Log and reports

In the Attack Log, the protection category is available for every alert in the alert details panel, if available. The number of protection categories, to which the corresponding attack belongs, is displayed. For example, if the displayed number is 2, it means the attack belongs to two protection categories. For information regarding the Attack Log, see the topic [Attack Log].

When you create a Next Generation User Defined report based on Alert Data, you can include protection category as one of the columns in the report. You can also use it as a **Data Filter** for the report. For information on Next Generation User Defined Reports, see the topic [Generate Next Generation user defined reports].

Severity level calculation of attacks

Trellix IPS assigns a default severity (high, medium, or low) to every attack in its attack database. *Severity* is based on the immediate effect, or impact, on the target system.

Severity numbering scheme

Trellix IPS uses a numeric mapping scheme to indicate Informational, Low, Medium, and High severity for a more intuitive display. The numbering scheme is as follows:

INFORMATIONAL	LOW	MEDIUM	HIGH
0	1-3	4-6	7-9

The guidelines in assigning severity levels are very similar to those used in many open security forums. You can customize these severity levels to meet the needs of your system based on the worth of your protected assets—an attack whose severity might be considered Low to one company might be High to another.

Attack categories and severity range

Trellix IPS categorizes attacks into four groups: Reconnaissance, Exploits, Volume DoS, and Policy Violation. The following table illustrates how severity levels are assigned for attacks in different categories.

Category	Threat type	Severity Level	Attack Description
Reconnaissance	Host sweep	4-4	A well-defined sequence of packets covering a range of destination IP addresses or ports, that aims to identify live hosts or open ports on the target host.
	Port scan	4-4	Traffic activities that indicate interactive shells under operating systems like Unix or Windows.
	Brute force	4-6	Alerts that indicate that someone is making repeated attempts at an authorization or information query service like POP3 and IMAP logins and invocation of SMTP VRFY commands. Such events suggest possible reconnaissance activities for targeted attacks. Activities related to running network applications that are forbidden by policy such as running an IRC or music share server on the corporate network without authorization. Activities suggesting that a standard protocol is run over non-standard ports.
	Service sweep	6-6	A well-defined sequence of packets, each of which is a probe attempt itself, launched against a given destination IP address that aims at identifying the target operating system or host type. A well-defined traffic that crossed the thresholds like ICMP packet rate, IP fragment rate, etc. A well-defined sequence of packets covering a range of destination IP addresses, and aims at identifying hosts with a particular service.
	OS Fingerprinting	6-6	
Exploits	Probe	2-2	Alerts that probe on a specific service or host, based on specially constructed packets, for example, unusual flag settings.
	Protocol Violation	3-5	Unusual application protocol behaviors that includes invalid field values or invalid command sequences etc.
	DoS	3-5	Packets that are well crafted, for example, with invalid or inconsistent TCP/UDP/IP header values, aiming to crash the target TCP/IP stack or to cause high resource consumption. Any network event or payload that is specifically related to virus. A malicious virus can inflict many different types of damages to its target, ranging from stealing or destroying information to installing backdoor processes. However, a virus relies on other carriers like e-mail, to gain access the network. A successful attack, that suggests that a breach of confidentiality has occurred. Examples include directory traversal, dump of file content such as CGI script, or reading other sensitive data files such as password and database records.
	Virus	3-5	
	Read Exposure	3-5	

Category	Threat type	Severity Level	Attack Description
	Trojan	3-9	Alerts that indicate Trojan activities like communication, installing, downloading, and the alerts that indicate malware detected through GTI File Reputation and/or custom fingerprinting.
	Write Exposure	5-7	A breach of integrity or authenticity of data like the creation or removal of files and modification of files for system configuration or user passwords. There is often a severe indirect impact, for example, a breach of access control by adding an illegal user account. These are content keyword matches that are deemed to indicate transmission of sensitive information such as a document with the marking "Company Confidential".
	Remote Access	5-9	Remote access that potentially indicates a successful exploitation where unauthorized access is obtained. For example, a successful buffer overflow on a Windows server may open a windows command shell for the attacker. An attacker may be able to perform further attacks to achieve privilege elevation once remote access is obtained. The attempts can be either contacting backdoor process or occurrence of actual backdoor 2-way conversation.
	Evasion Attempt	7-7	Alerts that indicate a sequence of packets or bytes in the traffic, signifying specific attempt at evading IDS.
	Code/ Script Execution	7-7	Large volume of traffic, that is valid from the perspective of an application content that can overwhelm processing element along the target path including switches, routers, firewalls, target servers etc.; this will cause an effect of DoS on other legitimate traffic.
	Bot	7-9	These kinds of alerts indicate attempts to exploit software vulnerabilities where manipulation of buffer spaces can result in overwriting of unintended memory areas. Such overwriting can have different consequences depending on whether the areas are executable or not. If not, it can cause malfunction of the software. These kinds of alerts indicate the most severe form of buffer overflow attacks that is, a buffer overflow attack carrying shellcode payload. Shellcode is a general term used for a piece of executable code that, upon successful execution on the target system, will modify the target's configuration or behavior for malicious purposes. Depending on the confidence level of the triggers, it can either be some attempts at contacting backdoor process or occurrence of actual backdoor 2-way conversation.
	Shellcode Execution	7-9	
	DDoS Agent Activity	7-9	
	Backdoor	7-9	
	Buffer Overflow	7-9	
	Worm	6-9	Any network event or payload related to worm activities. A malicious worm can inflict many different types of damage on its target, ranging from stealing or destroying information to installing backdoor processes.

Category	Threat type	Severity Level	Attack Description
	Privileged Access	8-9	An unauthorized access to privileged accounts is obtained such as a successful buffer overflow on a UNIX server may open a root shell for the attacker. Alternatively, the attacker may have achieved successful privilege elevation from a legitimate user account, or from a remote access compromise. Privileged access allows the attacker to take complete control of the compromised system.
	Arbitrary Command Execution	8-8	Alerts that indicate attempts to execute arbitrary commands on the target machine. For example, an IIS vulnerability may allow remote invocation of cmd.exe to execute any other Windows commands.
Volume DoS	Statistical Deviation	7-7	Alerts that indicate a sequence of packets or bytes in the traffic, signifying specific attempt at evading IDS. Large volume of traffic, that is valid from the perspective of an application content that can overwhelm processing element along the target path including switches, routers, firewalls, target servers etc.; this will cause an effect of DoS on other legitimate traffic.
	Over Threshold	6-6	A well-defined sequence of packets, each of which is a probe attempt itself, launched against a given destination IP address that aims at identifying the target operating system or host type.
Policy Violation	Audit	0-0	It is reserved for those attacks and conditions that is not determined to fit accurately into any of the specific categories currently defined. Any networking event deemed to be of interest to the security analyst such as invocation of particular applications or use of a particular command in certain applications.
	Restricted Access	4-5	Any activity related to usage of network resources that are explicitly forbidden. For example, emails sent to or received from a particular address.
	Restricted Application	4-5	
	Unauthorized IP	5-5	Any traffic activity that suggests an existence of IP address that is not authorized for the protected network.
	Covert Channel	5-5	Communication activities that are deemed unintended but the communication channel being monitored.
	Sensitive Content	5-7	A breach of integrity or authenticity of data like the creation or removal of files and modification of files for system configuration or user passwords. There is often a severe indirect impact, for example, a breach of access control by adding an illegal user account. These are content keyword matches that are deemed to indicate transmission of sensitive information such as a document with the marking "Company Confidential".

Category	Threat type	Severity Level	Attack Description
	Command Shell	4-4	A well-defined sequence of packets covering a range of destination IP addresses or ports, that aims to identify live hosts or open ports on the target host.
	Non-standard Port	4-4	Traffic activities that indicate interactive shells under operating systems like Unix or Windows.
	Phishing	1-3	Potentially an unwanted program that may include a malware, adware or any other program.
	Potentially Unwanted Program		
Malware	Malware	4-9	Alerts that indicate a malicious file transfer is detected on network by Trellix ARC.

How to block attacks

The ability to drop and deny traffic is available only with a Sensor running in inline mode. The most efficient way to block exploits is to customize one or more of the pre-defined IPS policies to pro-actively drop malicious traffic. One of the pre-configured policies includes this functionality by default. The **Default Prevention policy** is automatically applied to Sensor interfaces when the Sensor is first added to the Manager. This policy contains a number of attacks that Trellix IPS has categorized as "recommended for smart blocking" (RFSB), and which are pre-configured with the drop attack packets response.

With other provided policies, the default Sensor response is to send alerts and log packets.

The first step towards prevention is typically to block attacks that have not caused false positives, have a high severity level, and have a low benign trigger probability. When you know which attacks you want to block, you can configure your policy to perform the drop attack packets response for those attacks.

From 11.1 Update 3 version and above, Trellix IPS Manager enables users to choose attacks that they want to be automatically blocked by the IPS Sensor. Users can define and store one or more customizable rules for blocking attacks as per their network requirements during attack set profile configuration. When the same attack set profile is used in the IPS policy, the Manager automatically correlates the blocking criteria set by the user with the new and existing attack signatures. As the attack set profile mapped to the IPS policy stores the user-defined blocking criteria for attacks, it is automatically applied to any new/modified attack definitions included in any signature set update that match the set criteria. This eliminates the requirement of repeated manual intervention and provides user-customizable and automated attack blocking mechanism that further enhances network security. For more information, refer to the section How to automate blocking of attacks based on user-defined blocking strategy (page 877).

Methods for blocking attacks

The Trellix Intrusion Prevention System IPS offers a variety of ways to block malicious traffic. These options include the following:

- Block exploit traffic (based on IPS policy configuration)

- Block DoS traffic (behavior-based detection)
- Block malware download (based on Malware policies)
- Block using Firewall policies (based on ACLs in the Firewall policies)
- Use Trellix IPS's traffic normalization feature—block based on configured TCP flow violation (out-of-order packets, deny...)
- Block IP-spoofed packets (configured)

> **TIP**
>
> Ignore rules can be configured to override the blocking criteria—to permit particular source IPs, for example.

The Malware, Firewall, and DoS are detailed in their respective chapters of this Guide.

How to block exploit traffic

Exploit refers to attacks that are discovered through a set of parameters, or rules, and matched against data within a packet. *Signatures* — specific strings used to match data in offending packets — are the key method in discovering an exploit. An attack can have multiple signatures; thus, enabling more than one chance at attack detection.

Using the Policy Editor, you can enable the blocking option for the required attacks.

The blocking of traffic for exploit works as follows:

- The Sensor applies the configured inbound or outbound policy depending on the traffic direction, which is determined via the Sensor cabling and port configuration.
- The Sensor analyzes the traffic and, based on the policy, determines whether the traffic is "good" (does not match an attack configured in the policy) or "bad" (matches an attack configured in the policy). If the traffic is bad, the Sensor then applies the configured "drop packets" action. When Trellix IPS identifies a malicious flow, it blocks only the flow; not all the traffic from the source IP address (Sensor behavior is unlike that of a firewall).
- For UDP and ICMP traffic, only the attack packet is blocked. With TCP traffic, the entire attack flow is blocked; we recommend that you also configure a TCP Reset action in the policy to reset the flow.

> **NOTE**
>
> When inline, the TCP resets always go out the inline ports. Response ports are used when the device is configured for tap or span mode.

Use of traffic normalization

Traffic normalization — available when the system is operating in inline mode — removes any traffic protocol ambiguities, protecting the end systems by cleaning up potentially harmful traffic in real time. Traffic normalization consists of two Sensor techniques: cleaning up malformed packets, and dropping illegal packets, for example, packets where the IP header is smaller than 20 bytes, IP fragments are smaller than 64KB, and so on. Traffic normalization also thwarts any attempts to evade the system while boosting attack detection accuracy. This feature, also known as *protocol scrubbing* or *packet scrubbing*, allows Trellix IPS systems to prevent hackers from *fingerprinting* a host system. Attackers often send abnormal traffic in the hope that the end

system responds in a way that allows them to determine what environments and technologies are deployed at a particular site. This makes it easier to launch subsequent attacks against known vulnerabilities in host network hardware or software resources.

Specifically, when enabled, normalization does the following:

- When the TCP Timestamp option is not negotiated in the SYN/SYN_ACK packet for a connection, but appears in any of the packets for the rest of the connection, the TCP Timestamp is removed from the headers of these packets.
- The MSS option is permitted only in the SYN/SYN_ACK packets for a TCP connection. If any other packets in the flow contain the MSS option, the Sensor removes it.

In both cases, Trellix IPS performs an incremental checksum of the TCP header and regenerates the CRC integrity check value.

NOTE

Packet scrubbing must be manually enabled. On the **Devices** tab, select the **Domain**, click **Devices** tab, and select the Sensor. Then, go to Setup → Advanced → **Protocol Settings** and enable Normalization On/Off Option; dropping of illegal packets is a default Sensor behavior.

How to block based on configured TCP/IP settings

Sensors have the intelligence to keep a number of TCP/IP connection parameters, as well as complete state information. The Devices → <Domain name> → Devices → <Device Name> → Setup → Advanced → **Protocol Settings** and Devices → <Domain name> → Devices → <Device Name> → Setup → Advanced → **IP Settings** action enables you to configure 16 TCP/IP parameters, such as the number of supported UDP flows, the TCB inactivity timer length, and accepting old data or new data for TCP or IP overlaps. All of the TCP/IP Settings parameters relate to the handling of monitored transmissions while in inline mode. You can use these settings to deny or drop certain traffic.

Two of the more notable parameters are as follows:

- **Cold Start Drop Action** — When starting a Sensor for the first time, you can decide to allow (forward) or drop all packets that do not have a flow control block recognized by the Sensor. You have the choice to Forward Flows or Drop Flows.
- **TCP Flow Violation** — This helps you determine to handle a packet received for a connection that does not exist, such as an ACK packet when no SYN for a connection has been received. Choices are as follows:
  - **Permit** — Reassembles out-of-order packets and processes them. It forwards traffic if strict TCP protocol violations and if State Not Established on Sensor fails.
  - **Permit out-of-order** — Allows out of order packets to continue to transmit without processing
  - **Deny** — Checks the flow for strict TCP protocol violations; if it discovers violations, it drops the packet and reassembles out-of-order packets.
  - **Deny no TCB** — (Deny if state is not established) drops the session only if the state has not been established. It forwards traffic only if strict TCP protocol violations fails.
  - **Stateless Inspection** — Does not consider the flow for inspection

NOTE

- If malware analysis is configured, select **Permit** as the malware analysis requires all packets to construct the file.
- If asymmetric routing is configured in your environment, select **Stateless Inspection** or **Permit out-of-order**. Using **Permit** can cause the packets to be held for TCP segment reassembly and subsequent timeouts which might result in higher latency.

For more information about standalone and HA pair of Sensors with asymmetric traffic, refer to *Asymmetric traffic handling* (page 1558).

How to block IP-spoofed packets

When enabled, the anti-spoofing option drops packets containing invalid source IP addresses. Trellix IPS determines the validity of a source IP address by comparing it against a configured list of internal networks. Thus, as a pre-requisite, you must define CIDR blocks for every internal network that will send traffic through the Sensor interface in question. Without a comprehensive set of CIDR blocks defined, especially if outbound anti-spoofing is enabled, Trellix IPS may block valid packets.

Anti-spoofing is available only for Sensors in inline mode.

How Trellix IPS determines the validity of a packet depends directly on the direction of that packet:

- **Inbound** — When a packet arrives on the outside interface, its source IP address is compared to the CIDR blocks associated with the interface. If the source IP address of the inbound packet matches one of the CIDR blocks, the packet is considered spoofed and dropped.
- **Outbound** — When a packet arrives on the inside interface, its source IP address is compared to the CIDR blocks associated with the interface. If the source IP address of the outbound packet does not match one of the CIDR blocks, the packet is considered spoofed and dropped.

Working with IPS policies

To be able to work with IPS Policies of Trellix IPS, you must be familiar with the concepts related to IPS Policies as well with the Manager user interfaces related to IPS Policies. You can modify the various specifications in an attack description according to your requirement. Each default IPS policy is matched with preconfigured attack set profiles. You can clone and customize preconfigured attack set profiles. While creating a new IPS policy, an attack set profile must be created first and then it should be configured to the new IPS policy.

This chapter begins with the description of user interfaces related to attack set profiles and then proceeds to IPS Policy. Review this chapter to familiarize yourself with these user interfaces and to know how to use the options available in them.

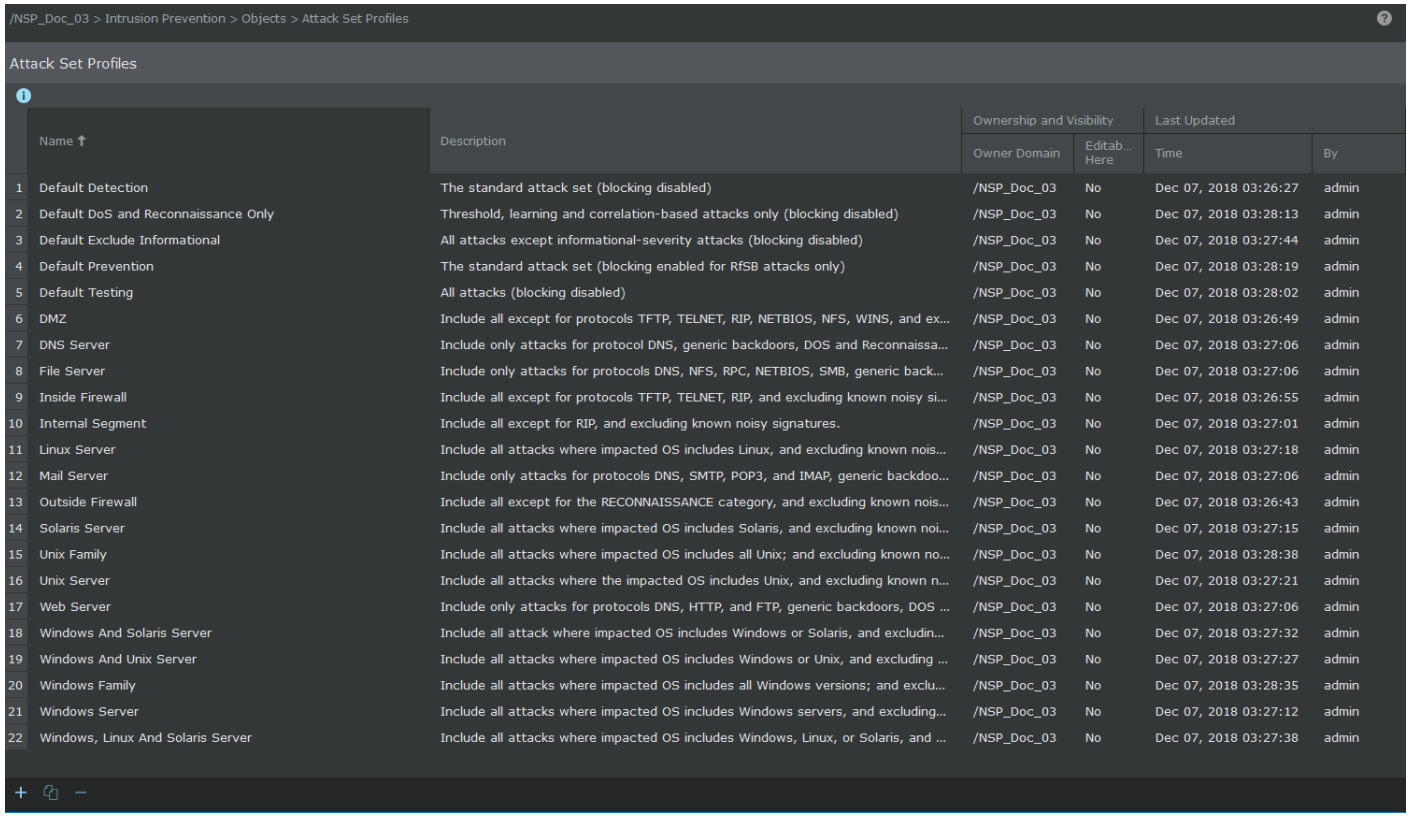
View attack set profiles

You can view the pre-defined attack set profiles and the user-defined attack set profiles available for the selected admin domain.

1. In the Manager, click **Policy** and select the required **Domain.**
2. Select Intrusion Prevention → Objects → **Attack Set Profiles.**

   The **Attack Set Profiles** page is displayed.

Figure 316. Attack Set Profiles page



	Name	Description	Ownership and Visibility		Last Updated	
			Owner Domain	Editab... Here	Time	By
1	Default Detection	The standard attack set (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:26:27	admin
2	Default DoS and Reconnaissance Only	Threshold, learning and correlation-based attacks only (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:28:13	admin
3	Default Exclude Informational	All attacks except informational-severity attacks (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:27:44	admin
4	Default Prevention	The standard attack set (blocking enabled for RfSB attacks only)	/NSP_Doc_03	No	Dec 07, 2018 03:28:19	admin
5	Default Testing	All attacks (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:28:02	admin
6	DMZ	Include all except for protocols TFTP, TELNET, RIP, NETBIOS, NFS, WINS, and ex...	/NSP_Doc_03	No	Dec 07, 2018 03:26:49	admin
7	DNS Server	Include only attacks for protocol DNS, generic backdoors, DOS and Reconnaissa...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
8	File Server	Include only attacks for protocols DNS, NFS, RPC, NETBIOS, SMB, generic back...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
9	Inside Firewall	Include all except for protocols TFTP, TELNET, RIP, and excluding known noisy si...	/NSP_Doc_03	No	Dec 07, 2018 03:26:55	admin
10	Internal Segment	Include all except for RIP, and excluding known noisy signatures.	/NSP_Doc_03	No	Dec 07, 2018 03:27:01	admin
11	Linux Server	Include all attacks where impacted OS includes Linux, and excluding known nois...	/NSP_Doc_03	No	Dec 07, 2018 03:27:18	admin
12	Mail Server	Include only attacks for protocols DNS, SMTP, POP3, and IMAP, generic backdoo...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
13	Outside Firewall	Include all except for the RECONNAISSANCE category, and excluding known nois...	/NSP_Doc_03	No	Dec 07, 2018 03:26:43	admin
14	Solaris Server	Include all attacks where impacted OS includes Solaris, and excluding known noi...	/NSP_Doc_03	No	Dec 07, 2018 03:27:15	admin
15	Unix Family	Include all attacks where impacted OS includes all Unix; and excluding known no...	/NSP_Doc_03	No	Dec 07, 2018 03:28:38	admin
16	Unix Server	Include all attacks where the impacted OS includes Unix, and excluding known n...	/NSP_Doc_03	No	Dec 07, 2018 03:27:21	admin
17	Web Server	Include only attacks for protocols DNS, HTTP, and FTP, generic backdoors, DOS ...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
18	Windows And Solaris Server	Include all attack where impacted OS includes Windows or Solaris, and excludin...	/NSP_Doc_03	No	Dec 07, 2018 03:27:32	admin
19	Windows And Unix Server	Include all attacks where impacted OS includes Windows or Unix, and excluding ...	/NSP_Doc_03	No	Dec 07, 2018 03:27:27	admin
20	Windows Family	Include all attacks where impacted OS includes all Windows versions; and exclu...	/NSP_Doc_03	No	Dec 07, 2018 03:28:35	admin
21	Windows Server	Include all attacks where impacted OS includes Windows servers, and excluding...	/NSP_Doc_03	No	Dec 07, 2018 03:27:12	admin
22	Windows, Linux And Solaris Server	Include all attacks where impacted OS includes Windows, Linux, or Solaris, and ...	/NSP_Doc_03	No	Dec 07, 2018 03:27:38	admin

The fields displayed in this page are as follows:

Option	Definition
Name	Displays the name of the attack set profile.
Description	Displays the description of the attack set profile.
Ownership and Visibility	**Owner Domain —** Indicates the admin domain to which an attack set profile belongs. **Editable here —** Indicates whether you can edit or delete an attack set profile from the current admin domain. You can edit but not delete the pre-defined attack set profile. You can edit or delete a user-defined attack set profile only from the admin domain from which it was created.**Yes** indicates that the attack set profile belongs to the current admin domain. If it is **No**, you cannot edit the attack set profile because it is defined at a parent admin domain.
Last Updated	**Time —** Displays the time when the attack set profile was last updated **By —** Displays the user who modified the attack set profile.
+	Click + to create an attack set profile. The **Properties**, **Attack to Include/Exclude**, and **Attack to Block**tabs are explained in the sections that follow.
	Select an attack set profile and click to copy it. This is helpful especially if you want to use a non-editable attack set profile with slight changes.

Option	Definition
	Select any of the listed attack set profile and click to edit or view the details. To edit in bulk, select more than one attack set profile and click to effect the same changes in all the selected attack set profiles.
	Select an eligible attack set profile and click to delete.

Preconfigured attack set profiles

Trellix supplies a set of preconfigured attack set profiles that correspond to the preconfigured IPS policies as well. You can use these attack set profiles to create specific IPS policies according to your requirements. That is, you can clone these attack set profiles and modify them to create custom IPS Policies. These pre-defined attack set profiles are available in the **Attack Set Profiles** page, which you can access from the **Policy** tab.

Attack set profiles	Designed to Protect Against:
Default Detection	All attacks.
Default DoS and Reconnaissance Only	All signatures are disabled by default. This policy is provided for the scenario where a sub-stream of traffic needs to be ignored by the IPS.
Default Exclude Informational	All attacks, including those with known noisy signatures, but omitting Informational severity attacks. This policy differs from Default as it alerts for every attack in the Trellix IPS database, including those with noisy signatures. This enables expert security personnel to fully analyze their network traffic. Informational "attacks" are not enabled.
Default Prevention	All attacks and Trellix-recommended blocking of selected attacks
Default Testing	Similar to above, with the exception that Informational-level alerts are included.
DMZ	All attack types except for those exploits using TFTP, Telnet, RIP, NETBIOS, NFS, and WINS.
DNS Server	All Reconnaissance and DoS attacks, generic backdoors, and exploits using the DNS protocol.
File Server	All Reconnaissance and DoS attacks, generic backdoors, and exploits using DNS, NFS/RPC, and NETBIOS/SMB protocols.
Inside Firewall	All attack types except for those exploits using TFTP, Telnet, and RIP.
Internal Segment	All attacks except for exploits using RIP and routing protocol attacks.
Linux Server	All attacks where the impacted operating system includes Linux.
Mail Server	All Reconnaissance and DoS attacks, generic backdoors, and exploits using DNS, SMTP, POP3, and IMAP protocols.
Outside Firewall	All attacks except for Reconnaissance category.
Solaris Server	All attacks where the impacted operating system includes Solaris.
UNIX Family	
UNIX Server	All attacks where the impacted operating system includes UNIX.
Web Server	All Reconnaissance and DoS attacks, generic backdoors, and exploits using DNS, HTTP, and FTP protocols.
Windows and Solaris Server	All attacks where the impacted operating system includes Windows or Solaris.

Attack set profiles	Designed to Protect Against:
Windows and UNIX Server	All attacks where the impacted operating system includes Windows or UNIX.
Windows Family	
Windows Server	All attacks where the impacted operating system includes Windows.
Windows, Linux, and Solaris Server	All attacks where the impacted operating system includes Windows, Linux, or Solaris.

Manage attack set profiles

Attack Set Profiles enable the use of a powerful tool for defining the exact environment resources you want to protect. To recap, an attack set profile consists of select attacks specific to a network environment, such as the operating systems you employ, the installed applications (email, chat), and the transport and application protocols (HTTP, FTP) used for data delivery. The protocol field includes all of the attacks detected by Trellix IPS for specific selection by attack name, severity, and the chance a signature may trigger a false positive. Each rule you configure narrows the detection focus of your Sensor interfaces (where policy is applied) to provide the highest degree of detection accuracy and performance.

The **Attack Set Profiles** page provides the following functions:

- Viewing an attack set profile
- Adding an attack set profile
- Cloning an attack set profile: Cloning duplicates an existing attack set profile, and is similar to a "save as" function. You can clone any attack set profile to further refine the parameters for the characteristics of a new environment. You can clone a provided attack set profile, save it under a new name, and customize it to meet the needs of your unique environment.

  Cloning a provided attack set profile specifically enables you to add/subtract from the default settings of an attack set profile. For example, you may not want to see alerts for Low severity attacks, thus you would clone and customize an attack set profile to reflect a minimum severity of 4 (Medium) for all attacks.
- Editing an attack set profile: Editing an attack set profile allows you to make the changes necessary to better define the environment you will be monitoring. You can edit only the attack set profiles you have created; the preconfigured policies cannot be edited. Editing a user-created attack set profile permanently changes that attack set profile.
- Deleting an attack set profile: You cannot delete currently applied attack set profiles and non-editable attack set profiles.

Create an attack set profile

Sensors support both normal blocking and SmartBlocking. SmartBlocking is the blocking of attacks based on the Benign Trigger Probability (BTP) value of the attack signatures which trigger the attack. Trellix recommends certain attacks for SmartBlocking, and these are referred to as Recommended for SmartBlocking (RFSB) attacks. While creating an attack set profile, you can enable SmartBlocking for those exploit, recon, or policy violation attacks for which Trellix has recommended SmartBlocking.

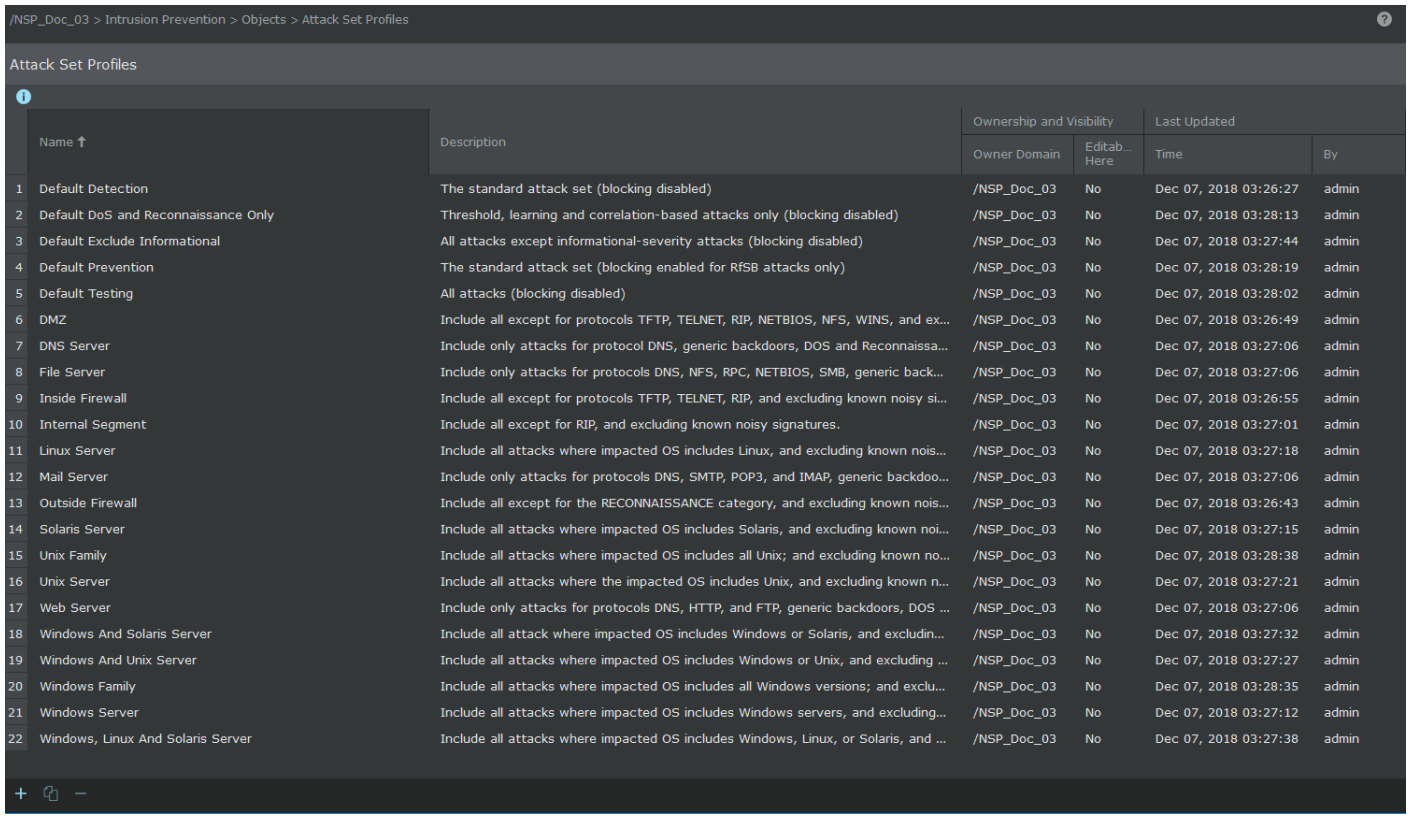
You can also create rules to choose attacks to be explicitly blocked by the Sensor as per your network requirements while creating an attack set profile. The configuration options on the **Attacks to Block** tab enables you to select minimum severity, categories, and subcategories of attacks which should be explicitly blocked by the Sensors. It works on the subset of data that comes in the form of **Include** rule(s) set on the **Attacks to Include/Exclude** tab. In other words, rules created on the **Attacks to Block** tab determine the attack definitions that are automatically set to be blocked in the corresponding IPS policy.

For more formation, refer to the section Defining and using user-customizable blocking strategy to make self-adaptable IPS policies (page 876).

1. In the Manager, click **Policy** and select the required **Domain**.
2. Select Intrusion Prevention → Objects → **Attack Set Profiles.**

   The **Attack Set Profiles** page is displayed.

Figure 317. Attack Set Profiles page

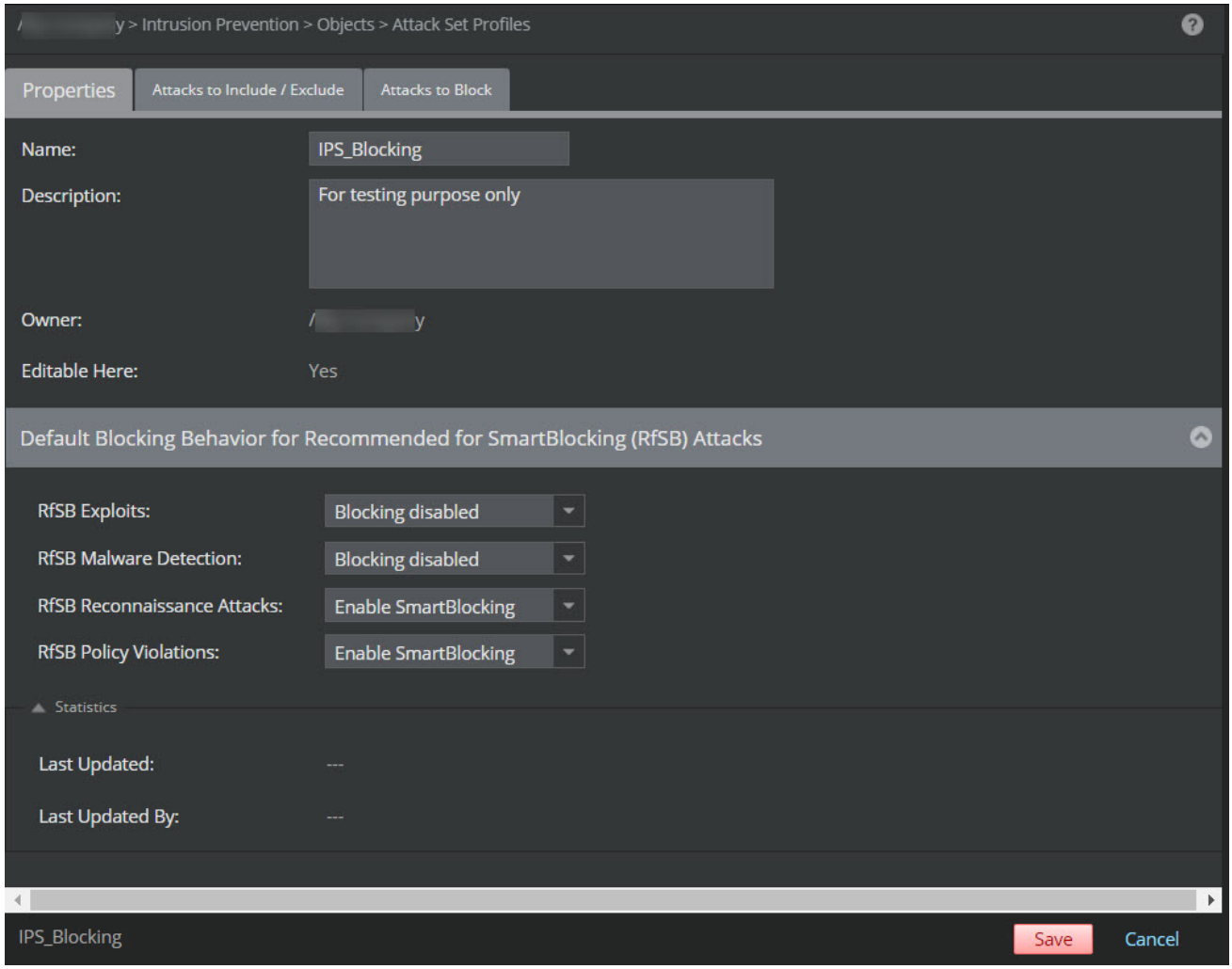


	Name	Description	Ownership and Visibility		Last Updated	
			Owner Domain	Editab... Here	Time	By
1	Default Detection	The standard attack set (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:26:27	admin
2	Default DoS and Reconnaissance Only	Threshold, learning and correlation-based attacks only (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:28:13	admin
3	Default Exclude Informational	All attacks except informational-severity attacks (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:27:44	admin
4	Default Prevention	The standard attack set (blocking enabled for RfSB attacks only)	/NSP_Doc_03	No	Dec 07, 2018 03:28:19	admin
5	Default Testing	All attacks (blocking disabled)	/NSP_Doc_03	No	Dec 07, 2018 03:28:02	admin
6	DMZ	Include all except for protocols TFTP, TELNET, RIP, NETBIOS, NFS, WINS, and ex...	/NSP_Doc_03	No	Dec 07, 2018 03:26:49	admin
7	DNS Server	Include only attacks for protocol DNS, generic backdoors, DOS and Reconnaissa...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
8	File Server	Include only attacks for protocols DNS, NFS, RPC, NETBIOS, SMB, generic back...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
9	Inside Firewall	Include all except for protocols TFTP, TELNET, RIP, and excluding known noisy si...	/NSP_Doc_03	No	Dec 07, 2018 03:26:55	admin
10	Internal Segment	Include all except for RIP, and excluding known noisy signatures.	/NSP_Doc_03	No	Dec 07, 2018 03:27:01	admin
11	Linux Server	Include all attacks where impacted OS includes Linux, and excluding known nois...	/NSP_Doc_03	No	Dec 07, 2018 03:27:18	admin
12	Mail Server	Include only attacks for protocols DNS, SMTP, POP3, and IMAP, generic backdoo...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
13	Outside Firewall	Include all except for the RECONNAISSANCE category, and excluding known nois...	/NSP_Doc_03	No	Dec 07, 2018 03:26:43	admin
14	Solaris Server	Include all attacks where impacted OS includes Solaris, and excluding known noi...	/NSP_Doc_03	No	Dec 07, 2018 03:27:15	admin
15	Unix Family	Include all attacks where impacted OS includes all Unix; and excluding known no...	/NSP_Doc_03	No	Dec 07, 2018 03:28:38	admin
16	Unix Server	Include all attacks where the impacted OS includes Unix, and excluding known n...	/NSP_Doc_03	No	Dec 07, 2018 03:27:21	admin
17	Web Server	Include only attacks for protocols DNS, HTTP, and FTP, generic backdoors, DOS ...	/NSP_Doc_03	No	Dec 07, 2018 03:27:06	admin
18	Windows And Solaris Server	Include all attack where impacted OS includes Windows or Solaris, and excludin...	/NSP_Doc_03	No	Dec 07, 2018 03:27:32	admin
19	Windows And Unix Server	Include all attacks where impacted OS includes Windows or Unix, and excluding ...	/NSP_Doc_03	No	Dec 07, 2018 03:27:27	admin
20	Windows Family	Include all attacks where impacted OS includes all Windows versions; and exclu...	/NSP_Doc_03	No	Dec 07, 2018 03:28:35	admin
21	Windows Server	Include all attacks where impacted OS includes Windows servers, and excluding...	/NSP_Doc_03	No	Dec 07, 2018 03:27:12	admin
22	Windows, Linux And Solaris Server	Include all attacks where impacted OS includes Windows, Linux, or Solaris, and ...	/NSP_Doc_03	No	Dec 07, 2018 03:27:38	admin

3. Click +.

   The new page with **Properties** tab is displayed.

Figure 318. Properties tab



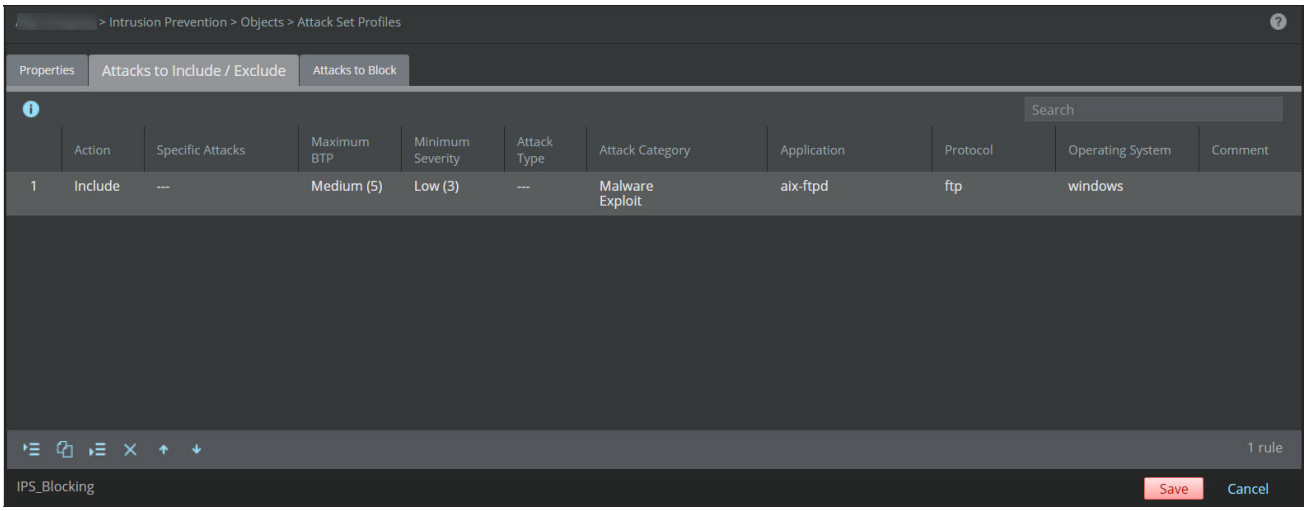
The following fields are displayed on the **Properties** tab:

Option	Definition
Name	Type the name of the attack set profile being created. The name should contain only letters, numbers, spaces, commas, hyphens and underscores. **NOTE** The name field should not be left blank and no special character should be entered while typing the name.
Description	Type the description of the attack set profile.
Owner	Displays the domain to which the IPS Policy belongs

Option	Definition
Editable here	Indicates whether you can edit or delete the selected attack set profile from the current admin domain
Default Blocking Behavior for Recommended for SmartBlocking (RfSB) Attacks	To enable SmartBlocking, select the options from the drop-down list of the following categories: **RfSB Exploits** **RfSB Malware Detections** **RfSB Reconnaissance Attacks** **RfSB Policy Violations** The available options for the above mentioned categories are **Blocking disabled** and **Enable SmartBlocking**.

4. Click **Next** to save the changes made on the **Properties** tab and go to the next tab. The **Attacks to Include/Exclude** tab is displayed.

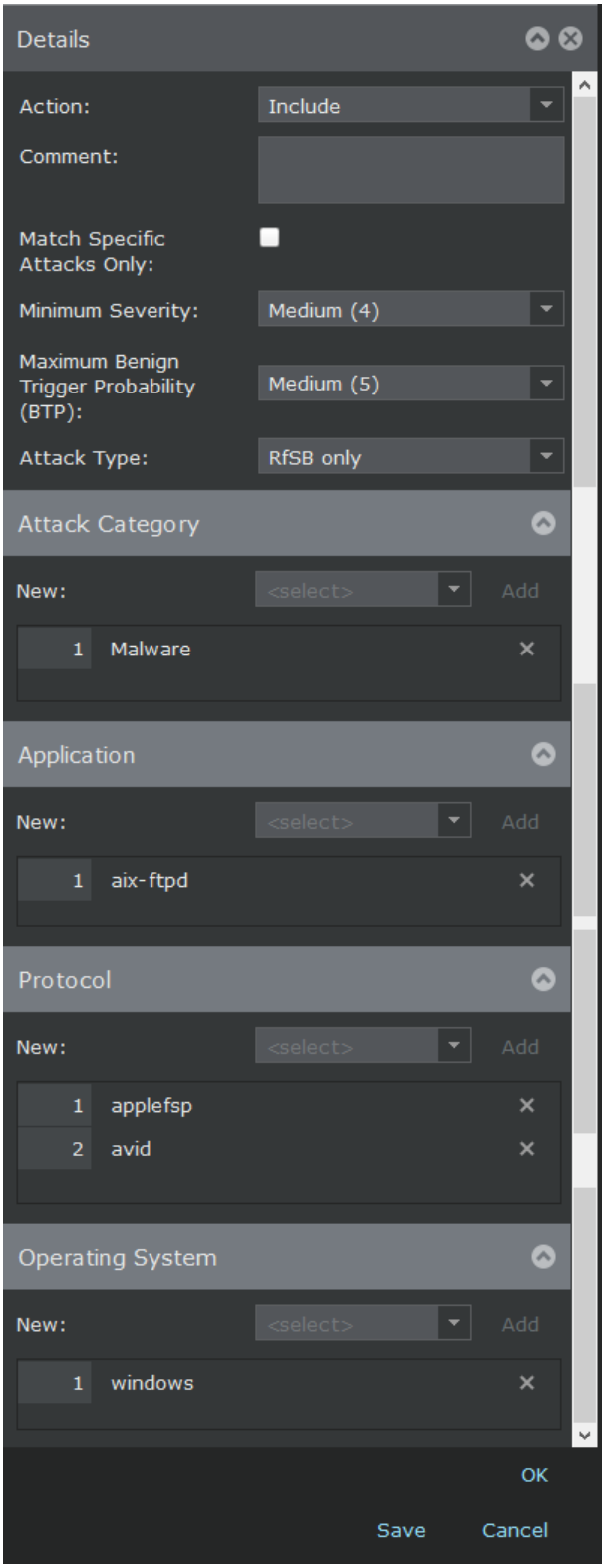
Figure 319. Attacks to Include/Exclude tab



5. On the **Attacks to Include/Exclude** tab, click the appropriate button to insert a new rule.

   You can insert a new rule by clicking either or icon. The **Details** panel is displayed.

Figure 320. Details panel on Attacks to Include/Exclude tab



6. In the **Details** panel, select the appropriate options.

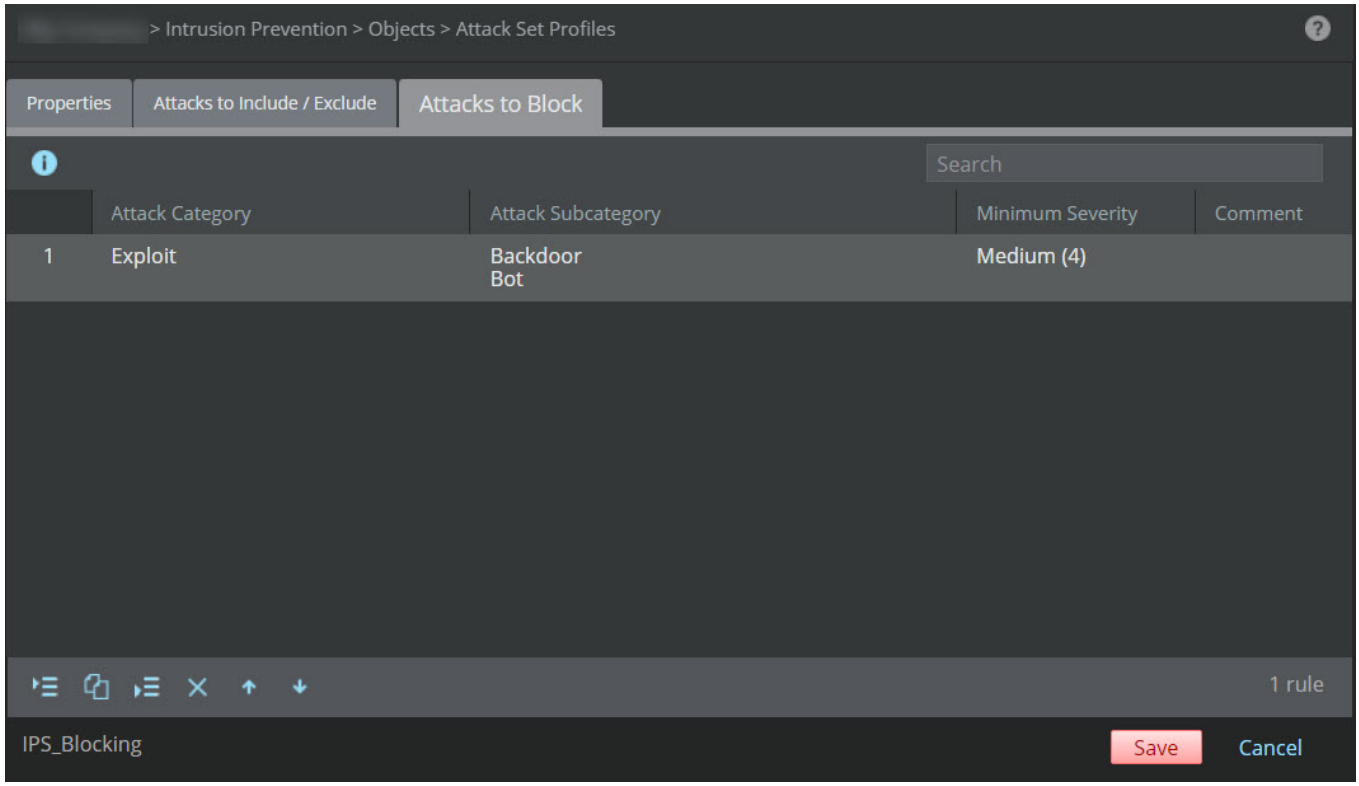
Option	Definition
Action	Select the action as **Include** or **Exclude**.
Comment	Enter additional comments, if any.
Match Specific Attacks Only	Select the checkbox if you want to mark the rule for a specific attack.
Minimum Severity	Select the minimum severity level from the drop-down list. The following are the available options: • **None** • **Informational (0)** • **Low (1)** • **Low (2)** • **Low (3)** • **Medium (4)** • **Medium (5)** • **Medium (6)** • **High (7)** • **High (8)** • **High (9)**
Maximum Benign Trigger Probability (BTP)	Specify the maximum probability of the search for this attack that will return a false positive. The following are the available options: • **None (0)** • **Low (1)** • **Low (2)** • **Medium (3)** • **Medium (4)** • **Medium (5)** • **High (6)** • **High (7)**
Attack Type	From the drop-down list, select the attack type as **Any** or **RfSB only**

Option	Definition
Attack Category	1. Select the attack category from the drop-down-list. The attack categories are: • **Exploit** • **Malware** • **Policy Violation** • **Reconnaissance** 2. Click the **Add** button to add the attack category to the list. Click ✕ to remove the item from the list.
Application	1. Select the applications from the drop-down-list. 2. Click the **Add** button to add the applications to the list. Click ✕ to remove the application from the list.
Protocol	1. Select the protocol from the drop-down-list. 2. Click the **Add** button to add the protocol to the list. Click ✕ to remove the protocol from the list.
Operating System	1. Select the operating system from the drop-down-list. 2. Click the **Add** button to add the operating system to the list. Click ✕ to remove the operating system from the list.
Specific Attacks	This section is displayed only if you select the **Match Specific Attacks Only** option. 1. Type and search for a specific attack by typing the first few letters of the attack in the text field. The list of attacks matching with the letters are displayed. 2. Select the required attack from the drop-down list. 3. Click on the **Add** button to add the attack to the list. Click ✕ to remove the attack from the list.

7. Click **OK** to confirm the configuration changes.
8. Repeat the relevant steps to add more rules to the attack set profile being created. Click **Next** to save the changes made on the **Attacks to Include/Exclude** tab and go to the next tab.

   The **Attacks to Block** tab is displayed.

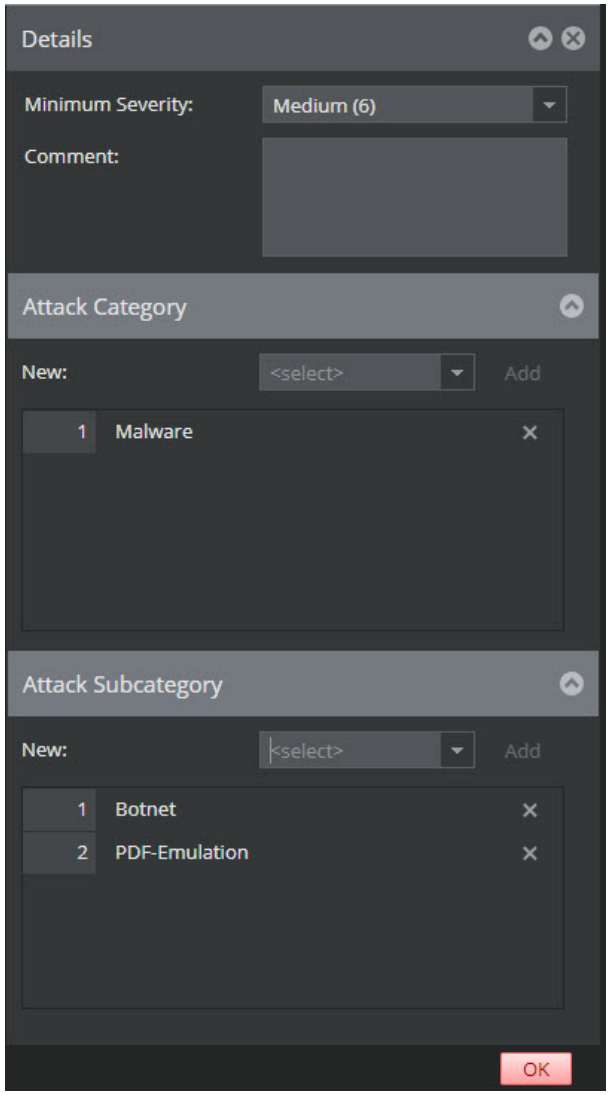
Figure 321. Attacks to Block tab



9. On the **Attacks to Block** tab, click the appropriate button to insert a new rule.

   You can insert a new rule by clicking either or icons. The **Details** panel is displayed.

Figure 322. Details panel on Attacks to Block tab



NOTE

You can create rule for blocking in custom attack set profiles only, as the default or preconfigured attack set profiles are read-only.

10. In the **Details** panel, select the appropriate options.

Option	Definition
Minimum Severity	Select the minimum severity level from the drop-down list. The following are the available options: • **Medium (4)** • **Medium (5)** • **Medium (6)** • **High (7)** • **High (8)** • **High (9)** **NOTE** The default value selected while creating a rule is **High (9)**. **IMPORTANT** **Informational** and **Low** severity attacks cannot be set for automatic blocking.
Comment	Enter additional comments, if any.
Attack Category	Select one or more attack categories as per your requirement from the drop-down-list. The attack categories available are the following: • **Exploit** • **Malware** • **Policy Violation** • **Reconnaissance** Click the **Add** button to add the attack category to the list. Click ✕ to remove the item from the list.
Attack Subcate-gory	Select one or more attack subcategories for the attack category selected. Click the **Add** button to add any subcategory to the list. Click ✕ to remove the item from the list. **IMPORTANT** • Attack subcategories are available only when you add an attack category. • You cannot select any attack subcategory if you have added two or more attack categories in a single rule. For example, if you want to block exploits and malware of severity 8 and backdoors and botnets of severity level 9, you need to create two separate rules - one with minimum severity level chosen as **High (8)**, **Attack Category** selected as **Exploit** and **Attack Subcategory** selected as **Backdoor**, and another with minimum severity level chosen as **High (8)**, **Attack Category** selected as **Malware** and **Attack Subcategory** selected as **Botnet**.

11. Click **OK** to confirm the configuration changes.

On the **Attacks to Include/Exclude** and **Attacks to Block** tabs, you can perform the following actions:

Option	Definition
	Inserts a new rule above the currently selected rule
	Inserts a new rule below the currently selected rule
	Clones the currently selected rule
	Deletes the currently selected rule
	Moves the currently selected rule one row up
	Moves the currently selected rule one row down

NOTE

Rules are cumulative on the **Attacks to Include/Exclude** and **Attacks to Block** tabs and the option to make changes in the rule order is solely to optimize viewing.

12. Click **Save** to save the Attack set profile configuration.

    Your new attack set profile is listed in the **Attack set Profiles** page.

Manage IPS policies

The Manager provides an ultimate refining tool for IPS policy management, by bringing together ignore rules and attack set profiles for final customization before deployment. Using IPS policies, you can select the exact Exploit and Denial of Service (DoS) attacks you want to protect against, the types of automatic responses you need to block current or further impacts, and the methods of notification that will help your team respond to malicious use of your network in the most expeditious time.

The **IPS** page provides the following actions:

- Launch the Custom Attack Editor. See [Custom Attack Definitions] section.

  For more information on types of custom attacks, see Types of custom attacks (page 1677).
- Adding an IPS policy
- Copying an IPS policy: Copying duplicates an existing policy, and is similar to a "save as" function. You can edit a Trellix IPS-provided policy. However, if you want to copy a policy, you can copy an existing policy to further refine the policy for application in a new environment. You can copy a predefined policy, save it under a new name, and customize it for your unique environment.

  Copying a provided policy specifically enables you to add or subtract from the default settings of a policy. For example, you might find a signature is generating false positives, and you might want to disable the alerting of the signature's attack. Also,

you might receive attacks uncommon to a network environment that are affecting your system and you want to add specific attacks to a policy for added security.

- Viewing/editing an IPS policy: Editing an IPS policy allows you to make the changes necessary to match the policy with the traffic you are monitoring. Editing a policy permanently changes that policy. However, every time you edit a policy, a new version is created. This enables you to revert the changes by going back to an older version. To make modifications or updates to a policy, try the following:
  - If you intend to make slight changes to a policy but want to save it under a different name, try cloning an IPS policy.
  - If you edit a predefined policy and later want to recreate that policy as it was when provided by Trellix, simply revert to the earlier version of the policy. If you had deleted the earlier versions, add a policy and apply the inbound and outbound attack set profile that matches the original policy you want to recreate.

> **NOTE**
>
> In the **IPS** page, the **Last Updated** column displays the time stamp of when a policy was last modified. The **Last Updated-By** column displays the logon name of the user who modified it. For policies defined in the Central Manager, the **Last Updated-By** column shows *NSCM Defined Policy* as the value.

- Deleting an IPS policy.

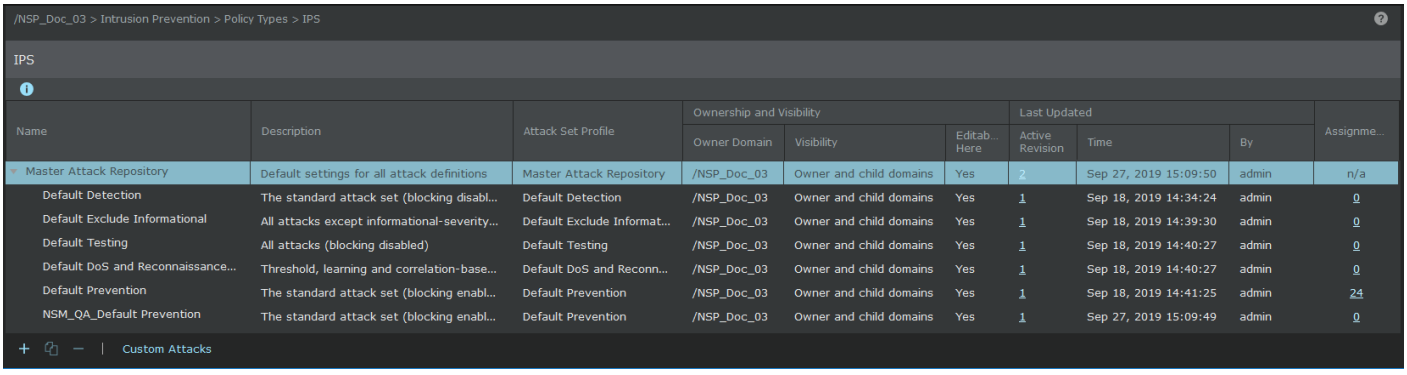
View IPS Policies

Recall that Trellix IPS provides some pre-defined IPS Policies. The **IPS** page displays the pre-defined IPS Policies and the user-defined IPS Policies available for the selected admin domain.

1. In the Manager, click **Policy** and then select the required **Domain**.
2. Go to Intrusion Prevention → Policy Types → **IPS**.

   The **IPS** page is displayed.

Figure 323. IPS page



The options on this page are as follows:

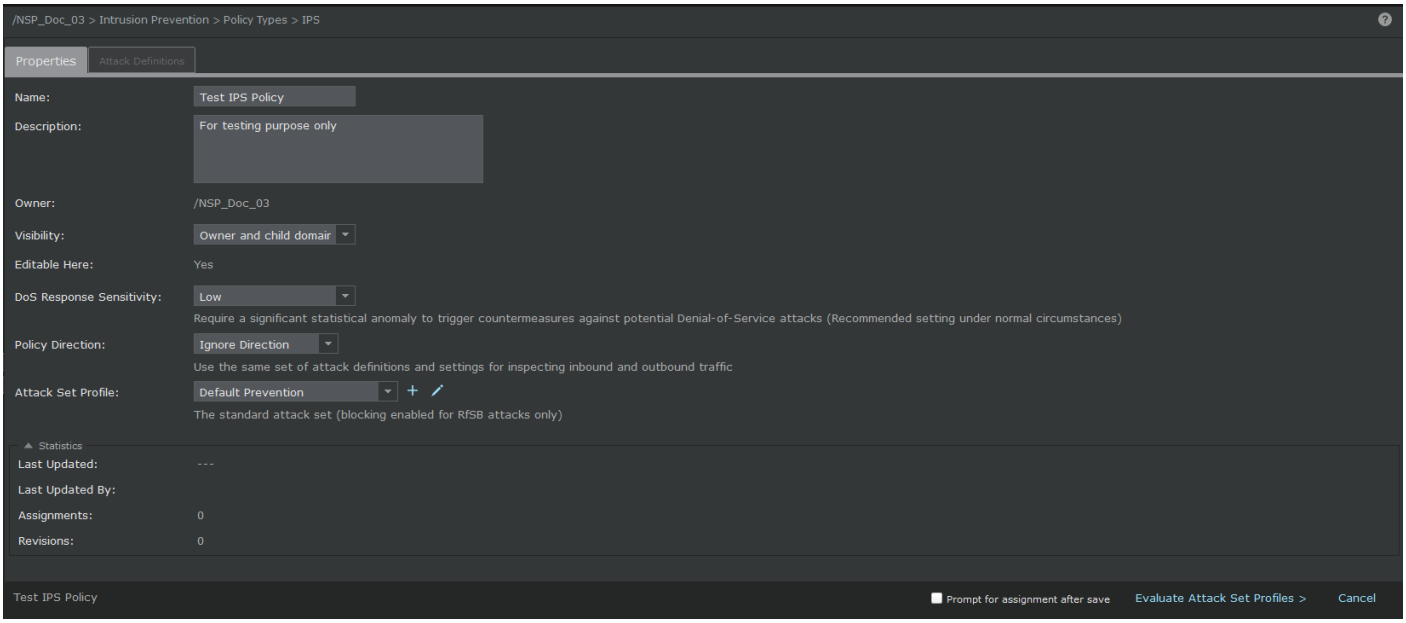
Option	Definition
Name	Displays the name of the policy.
Description	Displays the description of the policy.

Option	Definition
Attack Set Profile	
Ownership and Visibility	**Owner Domain** — Indicates the admin domain to which an attack set profile belongs. **Visibility** — Displays the admin domains to which the policy is visible. **Editable here** — Indicates whether you can edit or delete an attack set profile from the current admin domain. You can edit but not delete the pre-defined attack set profile. You can edit or delete a user-defined attack set profile only from the admin domain from which it was created.**Yes** indicates that the attack set profile belongs to the current admin domain. If it is **No**, you cannot edit the attack set profile because it is defined at a parent admin domain.
Last Updated	**Active Revision** — Revision number of the policy that is currently applied. **Time** — Displays the time when the attack set profile was last updated. **By** — Displays the user who modified the attack set profile.
Assignments	Number of interfaces to which the policy is assigned.
	Click  to create an attack set profile. The **Properties** and **Attack Definitions** tabs are explained in the sections that follow.
	Select an attack set profile and click  to copy it. This is helpful especially if you want to use a non-editable attack set profile with slight changes.
	Select any of the listed attack set profile and click  to edit or view the details. To edit in bulk, select more than one attack set profile and click to effect the same changes in all the selected attack set profiles.
	Select an eligible attack set profile and click  to delete.

Properties tab

The **Properties** tab is to manage the basic properties such as name, description, the attack set profile for inbound and outbound, and DoS response.

Figure 324. Properties tab



Attack Definitions tab

The **Attack Definitions** tab lists the inbound and outbound attack definitions included in the IPS Policy. An IPS Policy typically contains thousands of attack definitions. So, the **Attack Definitions** tab has some useful filtering options to locate attack definitions.

To set the display of attack definitions click on the column header and then select or type in the **Filters** options. There are two options to filter the displayed attack definitions: **List based filter** and **String based filter**.

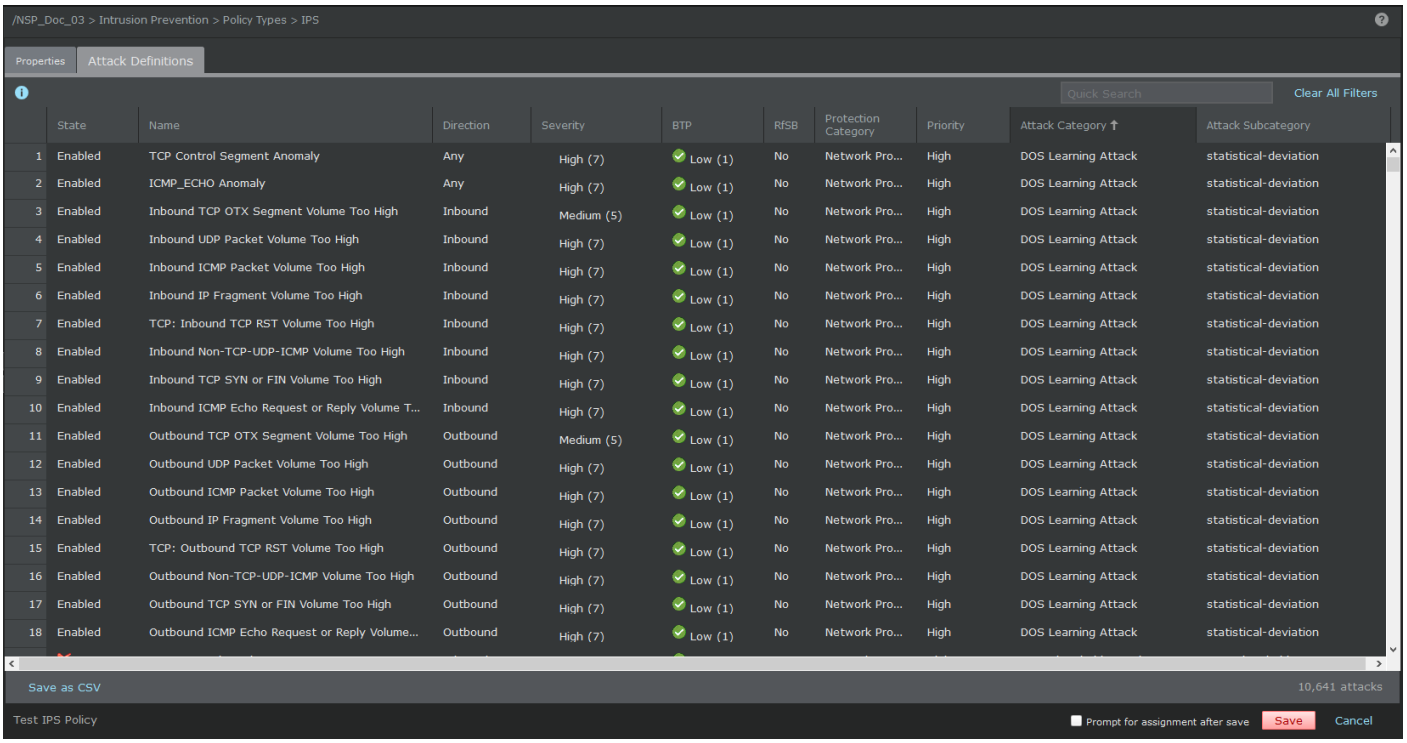
List based filter is available for those columns where the display of attack definitions is based on selecting a specific criteria listed in the column.

String based filter is available for those columns where the display of attack definitions is based on the criteria typed in the text field of the **Filters** option. By typing the first few characters in the text field, the policy assignments matching the typed characters are displayed on the page.

NOTE

When the attack definitions are displayed by using the **Filters** option, the header of column by which the policy assignments are filtered is highlighted in orange color. By clicking the **Clear All Filters** button, the filter is removed and all the attack definitions are displayed on the page.

Figure 325. Attack Definitions tab



Click a column header and select the option to sort based on ascending or descending order. The options are **Sort Ascending** and **Sort Descending**.The column based on which the list is sorted is indicated in the column header by an up arrow icon for ascending order and down arrow icon for descending order.

Figure 326. Sorting and Grouping options

For a consolidated view of a group of the attack definitions, click on the column header of the field (Example : **Severity**) by which it should be grouped and click **Group by this field**.

NOTE

To remove the display of attack definitions by groups unselect the **Show in groups** check-box option from the column header. The **Show in Groups** option is enabled only if the **Groups by this field** option is selected.

All fields can be sorted, except the following:

- **Industry IDs(All)**
- **Protocols**
- **Sensor Actions**
- **Manager Actions**

All fields can be grouped, except the following:

- **Industry IDs(All)**
- **Protocols**
- **Name**
- **Protection Category**

You can search for an attack based on the criteria typed in the text field of the **Quick Search** option. By typing the first few characters in the **Quick Search** text field, the attacks matching the typed characters are displayed on the page. By clicking the **Clear All Filters** button, the filter is removed and all the attacks are displayed on the page.

Preconfigured policies

Trellix supplies a set of preconfigured policies for immediate application in a number of different network environments. These policies are available under **IPS** in the Manager.

These policies are "starting points," designed to help you get your system up and running quickly. You can use any of the default scenarios initially, or you can clone and modify these and apply your new policies. In fact, the **Default Prevention** policy, applied by default when you add your first Sensor, enables you to begin monitoring your network immediately, and actually begin blocking attacks right out of the box (if you deployed your Sensor in inline mode). As you tune your IPS, you will modify these policies to best suit your particular environment.

Each preconfigured policy is designed to address the most common attacks targeting specific network environments. To provide the most efficient attack detection options, these policies take into account distinct factors such as protocols (HTTP, SMTP), services (email, FTP, Web), and implementations (Apache, IIS).

Attacks are classified into four general categories:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS)** — All of the conditions indicative of activities that lead to service disruption, including the slowing down or crashing of applications, servers, or networks.
- **Exploit** — All malicious activities, other than DoS and Reconnaissance, carried out through specific traffic content. This includes buffer overflows, viruses, and worms.
- **Reconnaissance** — All of the conditions indicative of probing, scanning, and OS fingerprinting activities. These activities are generally in preparation for more targeted attacks.
- **Policy Violation** — All activities for which the underlying traffic content may not be malicious by itself, but are explicitly forbidden by the usage policies of the administrative domain. This includes application protocol behaviors that violate common usage practices.

The following are pre-formatted policies and their descriptions.

NOTE

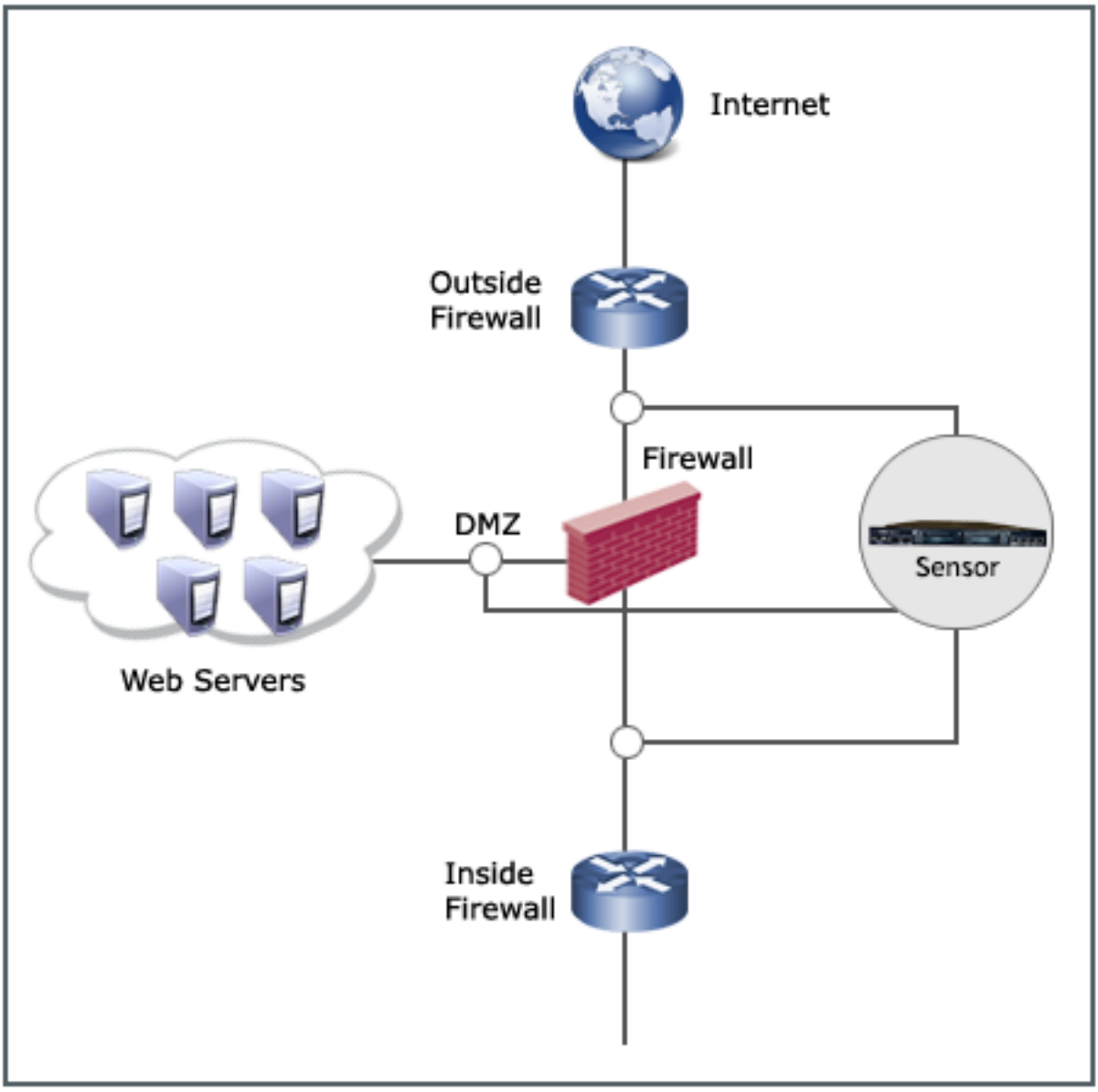
All provided policies, except the **Default Testing** and **Default Exclude Informational** policies, enable attacks with a minimum Severity of 2 (Low) and a maximum Benign Trigger Probability of 4 (Medium). The Severity and Benign Trigger Probability settings exclude known noisy signatures in an effort to limit spurious alerts.

Policy	Designed to Protect Against
Default Prevention	All attacks of Low severity or greater, below a Medium benign trigger probability, with a blocking Sensor action enabled for all Trellix Recommended for Blocking (RFB) attacks.
Default Detection	All attacks of Low severity or greater, below a Medium benign trigger probability.
Outside Firewall	All attacks except for Reconnaissance category.
DMZ	All attack types except for those Exploits using TFTP, Telnet, RIP, NETBIOS, NFS, and WINS.
Inside Firewall	All attack types except for those Exploits using TFTP, Telnet, and RIP.
Internal Segment	All attacks except for Exploits using RIP and routing protocol attacks.
Web Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using DNS, HTTP, and FTP protocols.
Mail Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using DNS, SMTP, POP3, and IMAP protocols.
DNS Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using the DNS protocol.
File Server	All Reconnaissance and DoS attacks, generic backdoors, and Exploits using DNS, NFS/RPC, and NETBIOS/SMB protocols.
Windows Server	All attacks where the impacted OS includes Windows.
Solaris Server	All attacks where the impacted OS includes Solaris.
UNIX Server	All attacks where the impacted OS includes UNIX.
Linux Server	All attacks where the impacted OS includes Linux.
Windows and UNIX Server	All attacks where the impacted OS includes Windows or UNIX.
Windows and Solaris Server	All attacks where the impacted OS includes Windows or Solaris.
Windows, Linux, and Solaris Server	All attacks where the impacted OS includes Windows, Linux, or Solaris.
Default Exclude Informational	All attacks, including those with known noisy signatures, but omitting Informational severity attacks. This policy differs from Default as it alerts for every attack in the Trellix IPS database, including those with noisy signatures. This enables expert security personnel to fully analyze their network traffic. Informational "attacks" are not enabled.
Default Testing	Similar to Default Exclude Informational, with the exception that Informational-level alerts are included.
Default DoS and Reconnaissance Only	All signatures are disabled by default. This policy is provided for the scenario where a substream of traffic needs to be ignored by the IPS. Alternatively, you can use Firewall Access Rules to exempt this traffic from IPS.

For example, in the following figure, an NS-series Sensor protects three network areas: outside the firewall, inside the firewall, and the DMZ. You can enforce a single policy across all three areas, or you can configure individual policies specifically for each zone.

In this example, the area outside the firewall is best protected by the default **Outside Firewall** policy (or one similar to it created by an admin) provided with Trellix IPS. For the DMZ area, the provided **DMZ** policy is the most efficient for that segment. Similarly, for the area inside the firewall, the provided **Inside Firewall** policy is best suited for the traffic in that zone.

Figure 327. Deploy security policies



Add an IPS policy

Make sure that attack set profiles that you intend to use in the IPS Policy are available.

Adding a policy in IPS policy takes you through the process of refining the parameters for securing your network. The following procedure explains the essential elements of a complete policy configuration.

Inbound and *outbound* refer to the direction that traffic is flowing with regard to the network. Inbound refers to traffic destined for the internal network, and outbound refers to traffic destined for the external network. Trellix recommends applying different attack set profiles for inbound and outbound traffic for the following reason: traffic coming into a network area, such as the DMZ, might only require the DMZ attack set profile, while traffic leaving the DMZ might be headed for external networks. Thus, a more generic attack set profile, such as the default attack set profile, better protects the outbound traffic.

NOTE

Separate attack set profiles for inbound and outbound can be applied to Sensors in SPAN or tap mode. If the Sensor is unable to determine the direction of the traffic, it enforces the inbound attack set profiles.

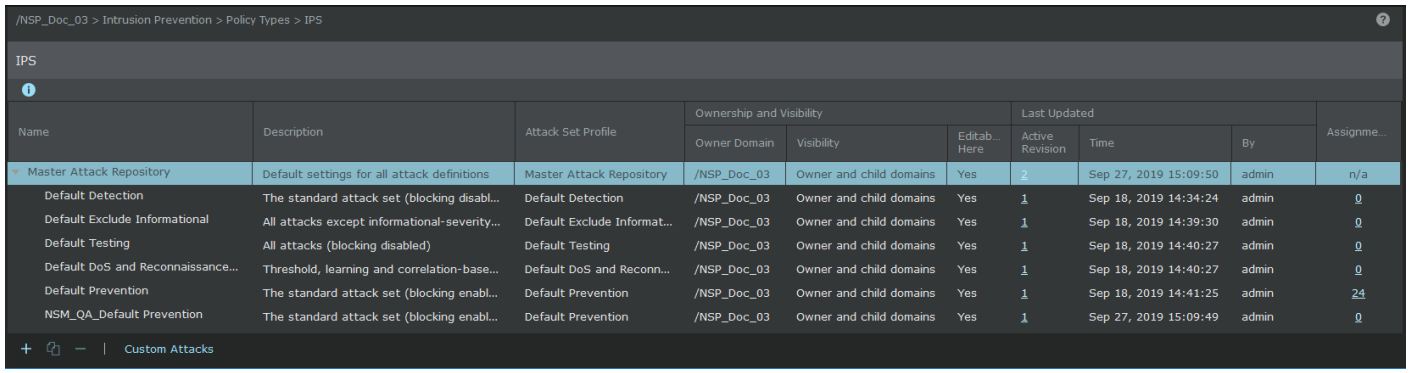
NOTE

While working within IPS policies, the task of creating or modifying settings opens up to four separate Java windows. Each window has either a **Save** or **OK** button as well as a **Cancel** button. Clicking **Save** saves the information to the database *and* closes all policy configuration actions. Clicking **OK** closes the subwindow that has been opened from within policy configuration, saving any changes made in that subwindow. Clicking **Cancel** ends any operation and closes the window. If you want to continue creating or modifying a policy, do not click either **Save** or **OK** until you have completed every tab, step, or action available in a window.

1. In the Manager, click **Policy** and select the required **Domain.**
2. Select Intrusion Prevention → Policy Types → **IPS.**

   The **IPS** page is displayed.

Figure 328. IPS page



3. Click +.

   The **New Policy** window opens with the **Properties** tab selected.
4. Update the following fields:

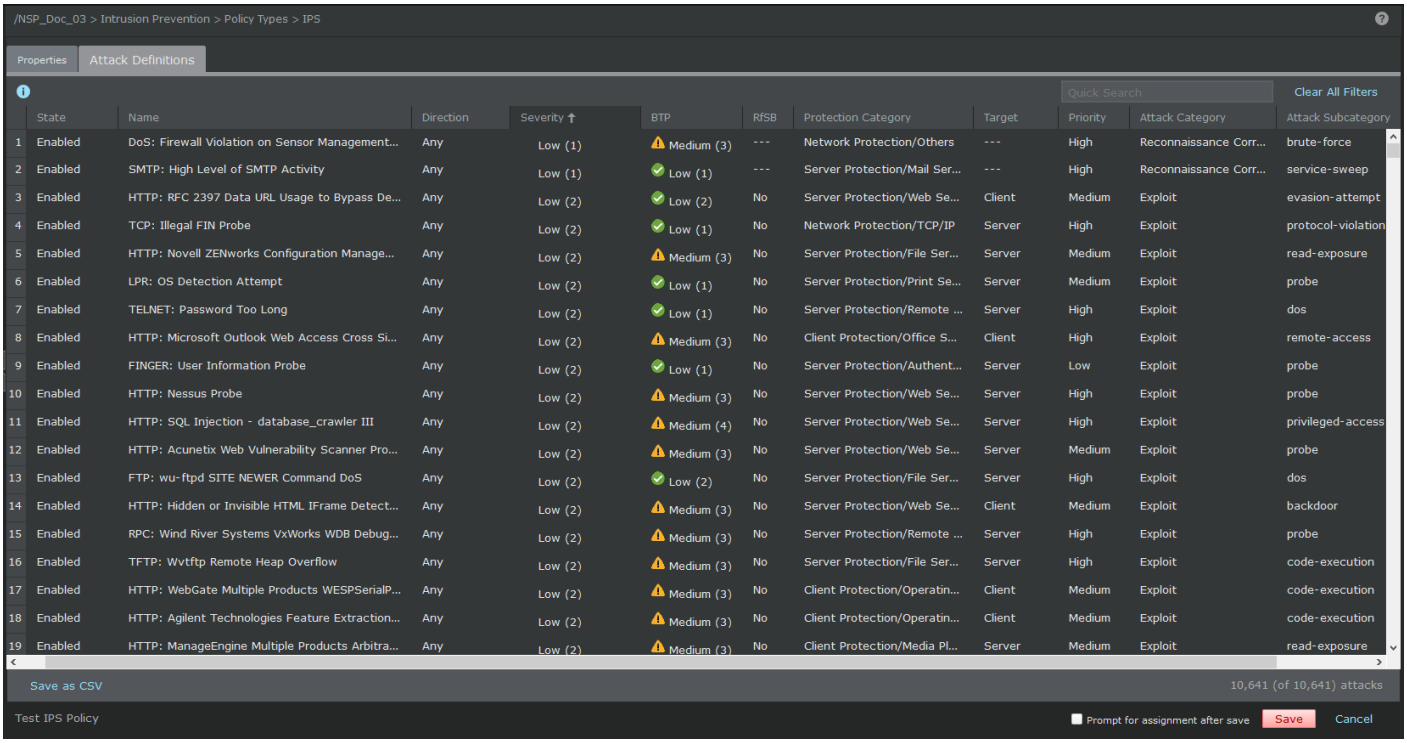
Option	Definition
Name	Enter a unique name to easily identify the policy. The name should contain only letters, numericals, spaces, commas, hyphens and underscores. **NOTE** The name field should not be left blank and no special character should be entered while typing the name
Description	Optionally describe the policy for other users to identify its purpose.
Owner	Displays the admin domain to which the policy belongs
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are **Owner and child domains** and **Owner domain only**.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
DoS Response Sensitivity	Defines the level of sensitivity to potential Denial-of-Service attacks. The available options are **Low**, **Medium** and **High**.
Policy Direction	Select the option to specify the direction to which the policy should be applied. The available options are **Consider Direction** and **Ignore Direction**.
Attack Set Profile	Select the attack set profile for inbound and outbound traffic. **NOTE** This field is displayed only when you select the **Policy Direction** option as **Ignore Direction**.
Inbound Attack Set Profile	Select the inbound attack set profile from the drop-down list. Click + to add a new attack set profile. Click ✎ to edit or view the selected attack set profile. **NOTE** This field is displayed only when you select the **Policy Direction** option as **Consider Direction**.

Option	Definition
Outbound Attack Set Profile	Select the outbound attack set profile from the drop-down list. Click + to add a new attack set profile. Click ✎ to edit or view the selected attack set profile. **NOTE** This field is displayed only when you select the **Policy Direction** option as **Consider Direction**.
Statistics	
Lasted Updated	Displays the time stamp when the policy was last modified
Last Updated By	Displays the user who last modified the policy
Assignments	Indicates the number of inline ports to which the policy is assigned
Revisions	
Prompt for assignment after save	If you clear this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the **Assignments** window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Cancel	Reverts to the last saved configuration

5. Click **Evaluate Attack Set Profiles**.

   The **Attack Definitions** tab is displayed.

Figure 329. Attack Definitions tab



6. The following fields are displayed:

Option	Definition
State	Displays the state as **Enabled** or **Disabled**
Name	Specifies the name of the attack
Direction	Displays the direction of attack as **Inbound**, **Outbound** or **Any**
Severity	Displays the severity level as **High**, **Medium**, **Low**, or **Informational** • For **High** severity, the score ranges between 7 and 9. • For **Medium** severity, the score ranges between 4 and 6. • For **Low** severity, the score ranges between 1 and 3. • For **Informational** severity, the score is 0.
Prority	Specifies the attack priority as **High**, **Medium**, or **Low**. By default, the **Priority** column is hidden. **NOTE** The **Prority** attribute for any attack definition is pre-defined by Trellix Researchers to categorize the attack definitions available for different Sensor models and is not applicable for custom attacks.

Option	Definition
BTP	Displays the BTP level as **High**, **Medium** or **Low** • For **High** BTP, the score ranges between 7 and 9. • For **Medium** BTP, the score ranges between 4 and 6. • For **Low** BTP, the score ranges between 0 and 3.
RfSB	Displays whether the attack is enabled for Smart blocking. The display is **Yes** for attacks with Smart blocking and **No** for attack without Smart blocking.
Protection category	Displays the protection category as **Client Protection**, **Server Protection**, **Malware**, **Advanced Protection Options**, or **Network Protection**
Target	Displays the target as **Server**, **Client** or **Server or Client**
HTTP Response Attack	Specifies the HTTP response as **No**, **Yes** or **Auto**
Industry IDs	**Trellix IPS** — Displays the unique identifier link for Trellix IPS. **CVE** — Displays the unique identifier link for the Common Vulnerability and Exposure standard. By clicking on the link you can view more details about the vulnerability. **Microsoft** — Displays the ID of attack as listed in the Microsoft Security Bulletin **Bugtraq** **CERT** **ArachNIDS**
Protocols	Displays the type of protocol
Attack Category	Displays the attack category. The attack categories are: • **Exploit** • **DoS Learning Attack** • **DoS Threshold Attack** • **Reconnaissance Attack** • **Policy Violation** • **Malware**
Attack SubCategory	Displays the sub-category of the attack
Customization	Specifies whether the attack is customized or not (**Yes** or **No**)
Manager Actions	Specifies the Manager's action for the attack

Option	Definition
Sensor Actions	**Response**: Displays the Sensor's response actions **Capture Packets**: Displays whether the captured packets are pre-attack packets or post attack packets
Last Updated	The most recent version of the signature set in which the attack definition was updated
Prompt for assignment after save	If you clear this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the **Assignments** window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Save	Saves the attack definition configuration
Cancel	Reverts to the last saved configuration

To enable an attack, select the row of an attack and click on the **Enable** button. For enabling multiple attacks simultaneously, select the rows by holding the **Shift** or **Ctrl** key and click on the **Enable** button.

To disable an attack, select the row of an attack and click on the **Disable** button. For disabling multiple attacks simultaneously, select the rows by holding the **Shift** or **Ctrl** key and click on the **Disable** button.

To export the attacks, click the **Save as CSV** button. The attack list is exported as an excel file.

7. Click **Save** to save the IPS policy.

How to add Audit Log comments

You can add comments on the IPS policy that you create.

The **Save Confirmation** window is displayed after you click **Save** when you create an IPS Policy. This window allows you to enter a comment after you have made changes to the existing action. You can type the comments in the **Revision Comment** text field and click **Confirm**. The comments can be viewed by clicking the description hyperlink in the **User Activity Log** table.

User Activities

The User Activities tab enables the admin to view all user actions in the management system. An audit can help to determine what a user has done in order to determine mistakes, overwriting, or other issues about user activity.

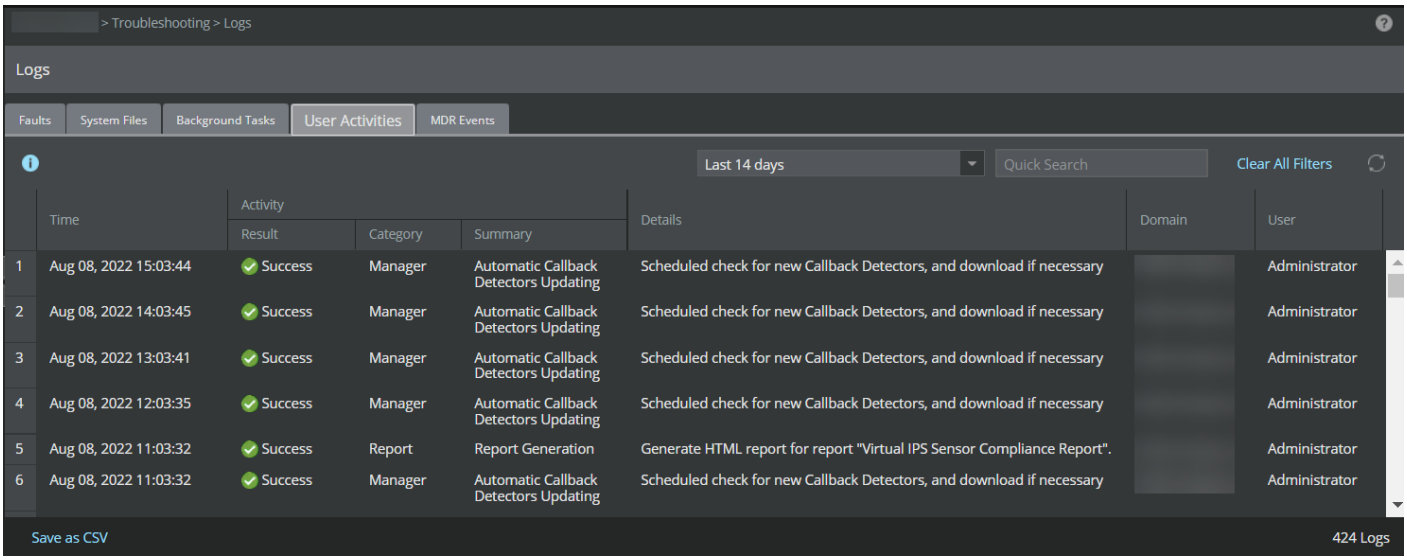
The various categories of user activities include:

- Admin Domain
- User
- Manager
- Sensor
- IPS Policy
- Report

- Update Server
- Operational Status
- Threat Analyzer
- NTBA
- FIPS Self Test
- ePolicy Orchestrator
- Controller
- Unspecified

To view the user activities, follow the steps below.

1. Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** and select **User Activities** tab to view the user activities table.



The data displayed in the table is based on the time frame of the core attribute in the user activities table. The data can be filtered for the time period of your preference using the **Custom Time Period** option. The default value is [last 7 days].

The following is table lists fields in the **User Activities** tab:

Options	Definition
Time	Displays date and time of activity occurrence.
Activity	Displays the following information for a user activity: • **Result**: Displays result of the activity. The result of the activity will either be **Successful** or **Failed**. • **Category**: Displays category of the activity. • **Summary**: Displays brief summary of the activity.
Details	Displays brief report of the activity.
Domain	Displays name of the admin domain where the activity is performed.

Options	Definition
User	Displays name of the user initiating the activity.

2. You can save a copy of user activities by clicking **Save as CSV**.

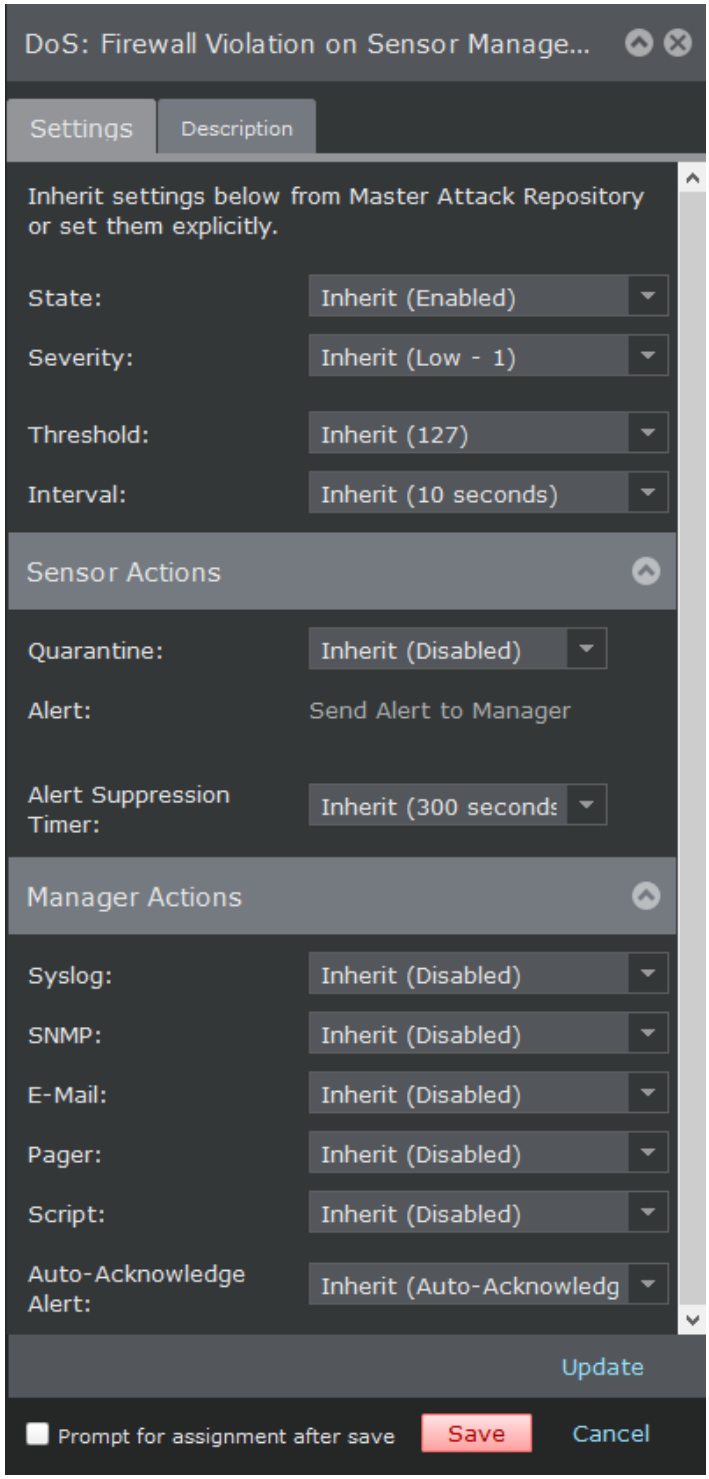
> **NOTE**
>
> The **Save as CSV** option saves only the copy of user activities based on the filters applied. To save a copy of all user activities, clear all filters before using saving it as CSV.

Configure attack details

You can configure and update the attack settings either by inheriting the settings from the master IPS policy or set them explicitly in the attack details panel. The attack details panel has two tabs: **Settings** and **Description**. On the **Settings** tab, you can set the configurable fields for Sensor and Manager actions. The **Description** tab is a read-only tab where you can view the attack and signature details.

1. On the **Attack Definitions** tab, double-click on the row of the attack that you want to configure and update the settings. The attack details are displayed on the right panel displaying the settings under the **Settings** tab.

Figure 330. Settings tab



2. Configure the settings for the attack definitions

   The following fields are displayed for attacks of categories such as exploit, policy violation, malware, and reconnaissance:

Option	Definition
State	Select any following options: • **Inherit (Enabled)** • **Enabled** • **Disabled**
Severity	Select the severity level of the attack: • **Inherit (Medium - 5)** • **Info - 0** • **Low - 1** • **Low - 2** • **Low - 3** • **Medium - 4** • **Medium - 5** • **Medium - 6** • **High - 7** • **High - 8** • **High - 9**
Threshold	This field is displayed only configuring attacks of type DoS Threshold and Reconnaissance Correlation attacks. Select the severity level of the attack: • **Inherit** • **Set explicitly** **NOTE** If you select the option **Set explicitly**, specify the threshold value in the number field.
Interval	This field is displayed only configuring attacks of type DoS Threshold and Reconnaissance Correlation attacks. Select the interval duration: • **Inherit** • **Set explicitly** **NOTE** If you select the option **Set explicitly**, specify the interval duration seconds in the number field.
Sensor Actions	
Response	

Option	Definition
Block	Select any of the following blocking options: • **Inherit (Disabled)** • **Enable Blocking** • **Enable SmartBlocking** • **Disabled**
Quarantine	Select any of the following quarantine options: • **Inherit (Disabled)** • **Quarantine Attacker** • **Quarantine and Remediate** • **Attacker** • **Disabled**
TCP Reset	Select any of the following TCP reset options: • **Inherit (Disbaled)** • **Reset Src** - resets to the source. • **Reset Dest** - resets to the destination. • **Reset Src and Dest** - resets to the source and destination. • **Disabled**
ICMP Message	Select any of the following ICMP message options: • **Inherit (Disabled)** • **Send ICMP Host Unreachable to Src** • **Disabled**
Alert	Select any of the following alert options: • **Inherit (Send Alert to Manager)** • **Send Alert to Manager** • **Disabled**
Alert Suppression Timer	This field is displayed only configuring Sensor response for attacks of type Reconnaissance Correlation attacks. Select the severity level of the attack: • **Inherit** • **Set explicitly** **NOTE** If you select the option **Set explicitly**, specify the seconds in the number field.

Option	Definition
Capture Packets	
Attack and Pre-Attack	Select any of the following pre-attack packet capture options: • **Inherit (Attack and Prior 128 Bytes)** • **Attack and Prior 128 Bytes** • **Disabled** **NOTE** If you include both HTTP and HTTP2 packets, it will be 256 bytes.
Post-Attack	Select any of the following post-attack packet capture options: • **Inherit (Disabled)** • **Enabled** • **Disabled**

Option	Definition
Flows to Capture	This field is displayed only when you select **Post-Attack** as **Enabled**. The following are the options available in this field: • **Inherit (Attack Flow Only)** • **Attack flow only** By selecting the option Attack flow only, a new drop-down list is displayed. Select any of the following options: • **Attack Packets only** • **Next N packets** - type the number of packets in the blank **packets** field. • **Next N time** - select the time options from the given drop-down list. The options are: • **Seconds** • **Minutes** • **Hours** • **Days** • **Rest of flow** • **Flows from Src and Flows to Src and Dest** By selecting the option **Flows from Src and Flows to Src and Dest**, a new drop-down list is displayed. Select any of the following options: • **Next N packets** - type the number of packets in the blank **packets** field. • **Next N time** - select the time options from the given drop-down list. The options are: • **Seconds** • **Minutes** • **Hours** • **Days**
Bytes to Capture	This field is displayed only when you select **Post-Attack** as **Enabled**. The following are the options available in this field: • **Inherit (All Bytes in Each Packet)** • **All Bytes in Each Packet** • **First N Bytes in Each Packet** By selecting the option **First N Bytes in Each Packet** , a new field to enter the number of bytes to capture is displayed. Type the number in the blank field.
Manager actions	

Option	Definition
Syslog	Select any of the following syslog options: • **Inherit (Disabled)** • **Send Syslog Message** • **Disabled**
SNMP	Select any of the following SNMP options: • **Inherit (Disabled)** • **Send SNMP Trap** • **Disabled**
E-Mail	Select any of the following email options: • **Inherit (Disabled)** • **Send E-Mail Message** • **Disabled**
Pager	Select any of the following pager options: • **Inherit (Disabled)** • **Send Page** • **Disabled**
Script	Select any of the following script options: • **Inherit (Disabled)** • **Run Script** • **Disabled**
Auto-Acknowledge Alert	Select any of the following auto-acknowledgment options: • **Inherit (Disabled)** • **Auto-Acknowledge Alert** • **Disabled**
Update	Click here to update the settings.

Fields in the **Capture Packets** and **Manager actions** sections are displayed only when alerting (**Alert** field option) is enabled or inherited.

The fields in the **Sensor actions** section is not displayed for malware attack definitions that support advanced malware policies as these settings are configured in the malware policy. However, the Manager actions are configurable for such malware attacks.

The following table explains the various Sensor responses that can be performed for different type of attacks. **Yes** signifies that the Sensor response can be performed for the attack type. **No** signifies that the Sensor response cannot be performed for the attack type.

Table 41. Sensor responses for attack types

Sensor response	Exploit	DoS Learning	DoS Threshold	Reconnaissance Signature	Policy Violation	Malware	Reconnaissance Correlation
Block	Yes	Yes	No	Yes	Yes	Yes	No
Quarantine	Yes	No	No	Yes	Yes	Yes	Yes
TCP Reset	Yes	No	No	Yes	Yes	Yes	No
ICMP Message	Yes	No	No	Yes	Yes	Yes	No
Alert	Yes	Yes	Yes	Yes	Yes	Yes	No
Capture packets	Yes	No	No	Yes	Yes	Yes	No
Alert Suppression Timer	No	No	No	No	No	No	Yes

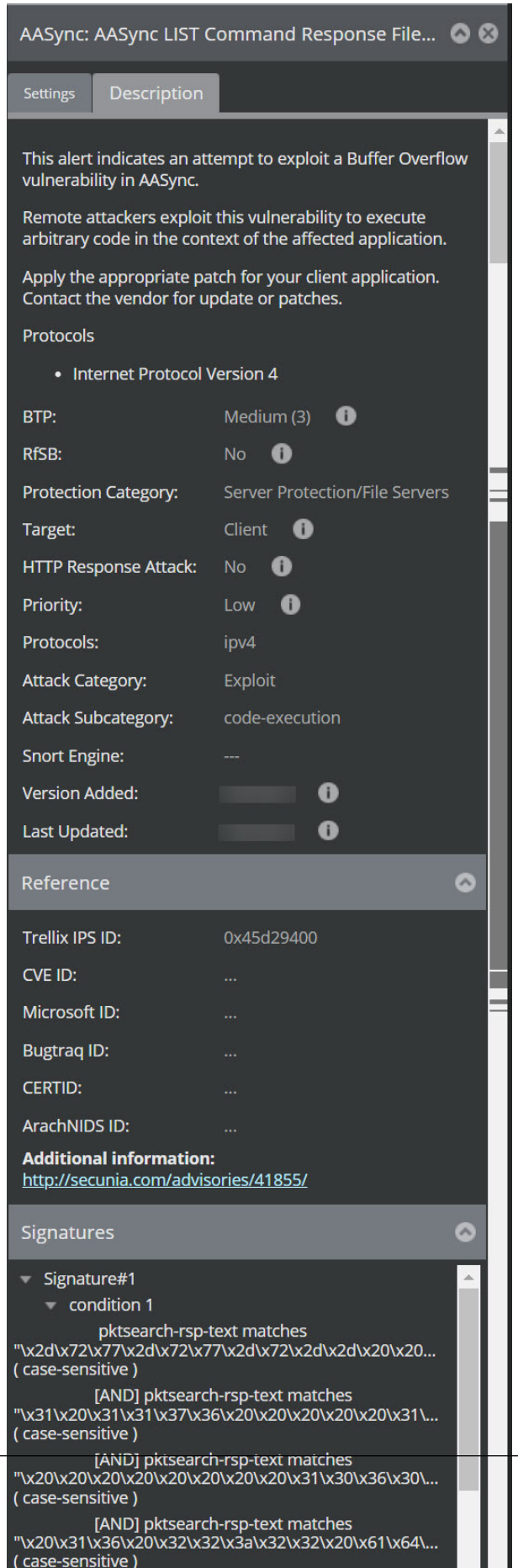
View attack description

The **Description** tab provides additional information about an attack. It also displays the signature descriptions, reference information.

Do the following steps to view the description of an attack.

1. On the **Attack Definitions** tab, double-click on the row of the attack that you want to view the attack description.
2. Click the **Description** tab in the right panel.

Figure 331. Description tab



The tab displays the description of the attack. The following details are also displayed:

- **BTP**
- **RfSB**
- **Protection Category**
- **Target**
- **HTTP Response Attack**
- **Protocols**
- **Attack Category**
- **Attack Subcategory**
- **Snort Engine**
- **Version Updated**
- **Last Updated**

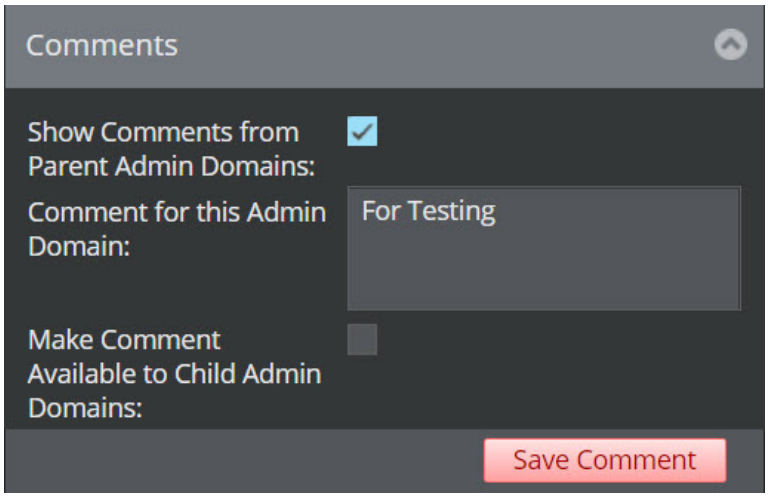
The **Reference** section displays the following details:

- **Trellix IPS ID**
- **CVE ID** - click the hyper-link to view details
- **Microsoft ID**
- **Bugtraq ID**
- **CERT ID**
- **ArachNIDS ID**
- Link for **Additional Information**, if any.

The **Signatures** section displays the list of attack signatures.

In the **Comments** section, you have an option to add comments in the text field **Comment for this Admin Domain** and click **Save Comment** to save the comment.

Figure 332. Comments section



To display the comments from the parent admin domain, select the checkbox **Show Comments from Parent Admin Domains**.

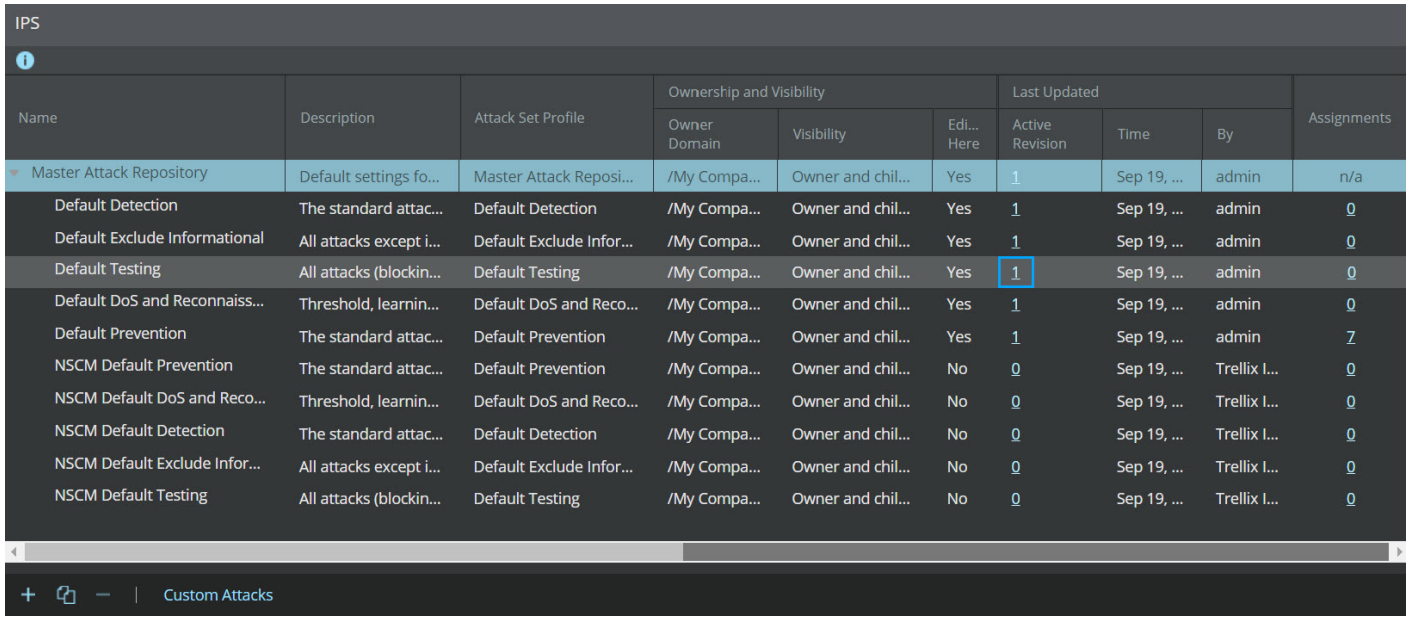
To make the comments to be displayed in the child admin domain, select the check-box **Make Comment Available to Child Admin Domains**.

Compare versions of IPS Policy

When you modify an IPS Policy, a new version is created that has the changes. To view or compare the version changes perform the following steps:

1. In the **IPS** page, click on the number link in the **Active Revision** column for the IPS policy for which you wish to see the version details. The **Version Control** page is displayed.

Figure 333. Active Revision number link



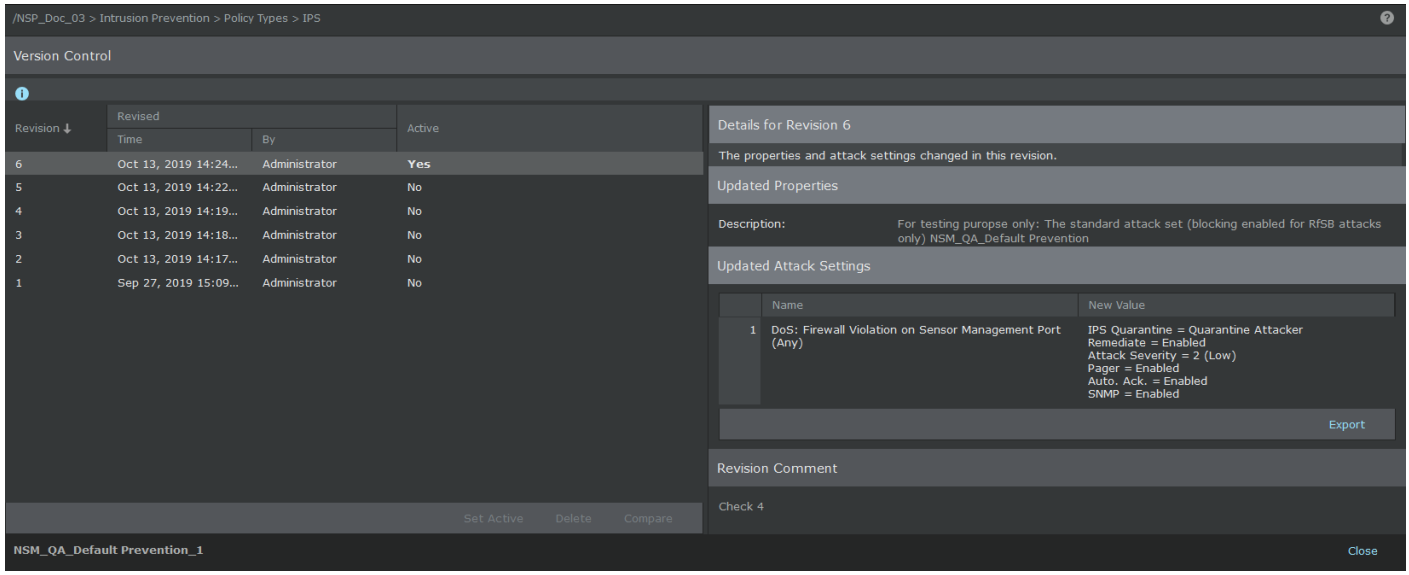
> **NOTE**
>
> The number in the link indicates the number of revisions made for the IPS Policy.

2. The left panel of the **Version Control** page displays the following details.

Option	Definition
Revision	Displays the revision number for the IPS policy
Revised	**Time**: Displays the date and time when the revision was made **By**: Displays the name of the user who made the revision
Active	Specifies whether the revision is the current revision. Displays **Yes** if it is the current revision. Displays **No** if it is not the current revision.

The right panel of the **Version Control** page displays the following revision details of the selected revision.

Figure 334. Version Control



Option	Definition
Details for Revision	Displays the changes made in the revision
Updated Properties	Lists the properties that are updated in the revision
Updated Attack Settings	Displays the name of the updated attack settings in the **Name** column and displays the new value of the updated attack settings in the **New Value** column
Revision Comment	Displays the revision comment, if provided

3. Press **Shift** and select the two versions to be compared.
4. Click **Compare** button. The **Comparison between Revision** window is displayed with the details of revision changes.

> **NOTE**
>
> The **Compare** button is disabled by default. The **Compare** button is enabled only when two versions are selected.
>
> - To set the selected version as active, click **Set Active**.
> - To delete the selected version, click **Delete**.

5. Click **Export** to export the list of revision changes in CSV format.

> **NOTE**
>
> If you attempt exporting policies using Internet Explorer 10 in combination with Windows Server 2008/2012, the Manager will generate the “Export of custom policy error”. To avoid this, go to Control Panel → Add or Remove Programs → **Add/ Remove Windows Components**; the **Windows Components Wizard** window opens. Select the **Internet Explorer Enhanced Security Configuration** and disable it. For more information on the fault, refer to [Trellix Intrusion Prevention System Product Guide].

6. Click **Close** to go back to the **IPS** page.

Use Bulk Edit for IPS policy

On the **Policy** tab, select the **Domain**. Then go to Intrusion Prevention → Policy Types → **IPS.**

The bulk edit feature enables you to select and edit multiple attack definitions at once. This operation is useful for configuring the same responses for multiple attacks at once, thus reducing overall configuration time.

1. In the **IPS** page, select the required policies from the list.

   NOTE

   You cannot bulk edit attack definitions with different attributes. For example, **Exploit** and **Policy Violation** attack categories can be edited at the same time, but the **DoS Learning Attack** can be edited only with other DoS Learning Attacks.

   The following attack categories combination can be edited at the same time:

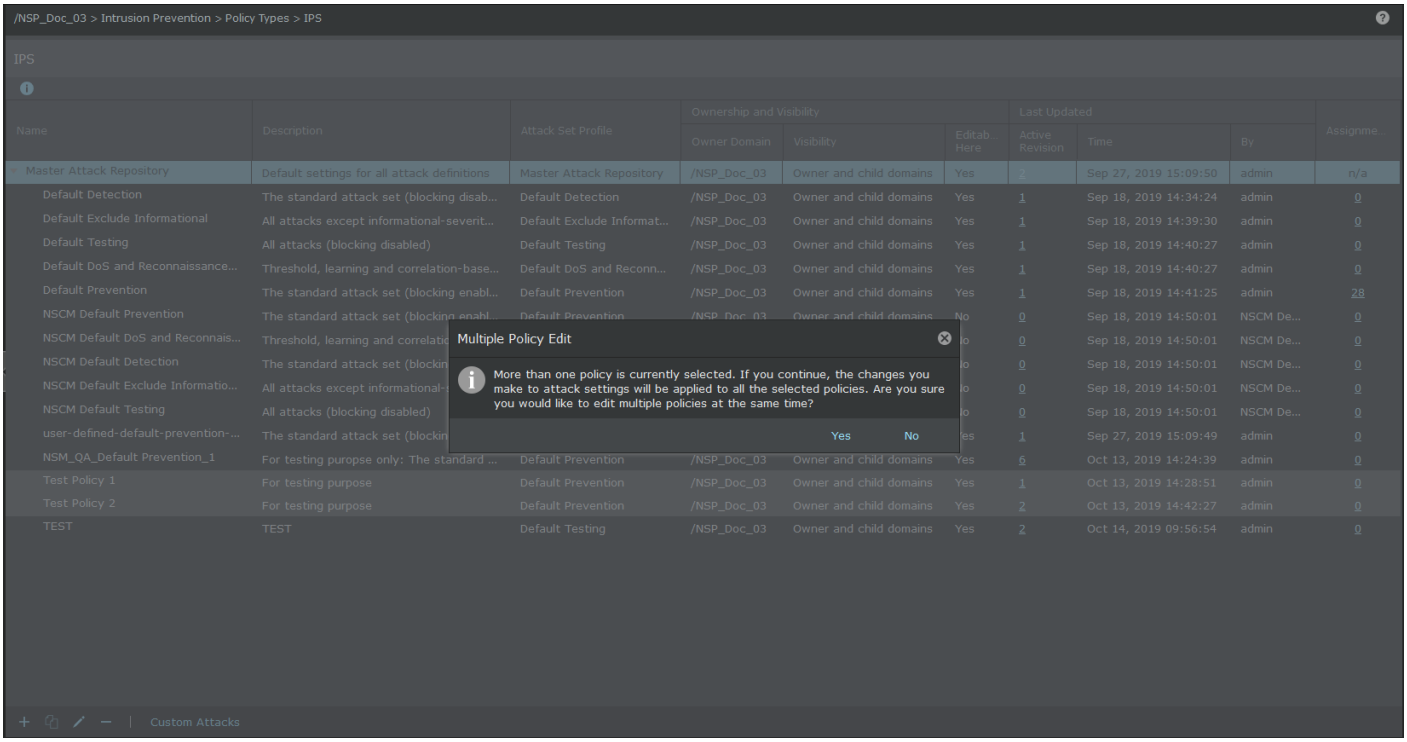
   - **Exploit**, **Policy Violation**, **Malware**, and **Reconnaissance Signature Attack**
   - **DoS Learning Attack**
   - **DoS Threshold Attack**
   - **Reconnaissance Correlation Attack**

   Press the **Shift** key (for continuous selection) or press the **Ctrl** key (for discontinuous selection), then select the policies.

2. Click  .

   The **Bulk Policies Edit** confirmation window appears, prompting to confirm whether you wish to edit multiple policies at the same time.

Figure 335. Bulk Policies Edit

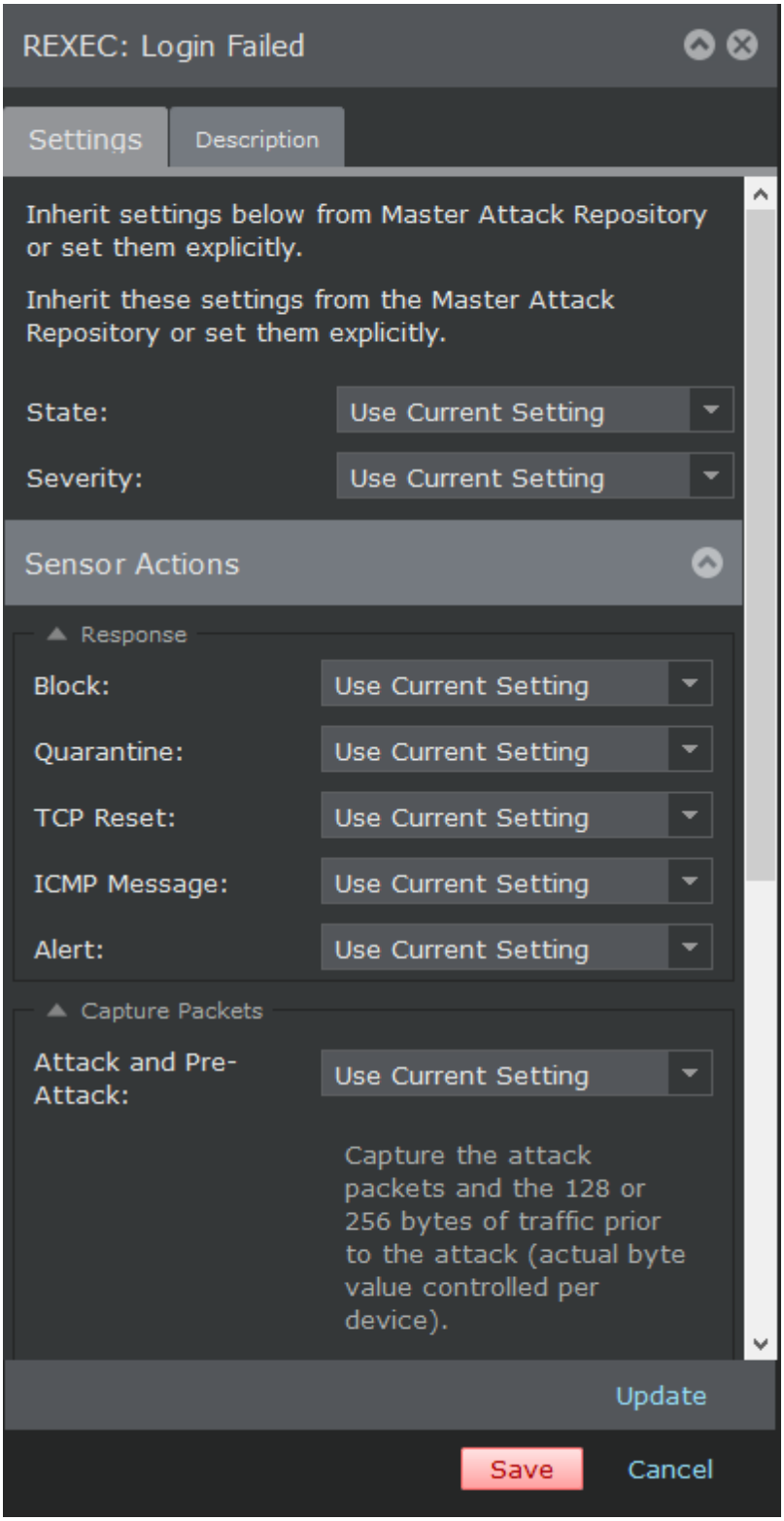


3. Click **Yes** to confirm.

   The **Attack Definitions** tab is displayed with the list of attacks.

4. On the **Attack Definitions** tab, double-click on the row of the attack that you want to configure and update the settings. The attack details are displayed on the right panel displaying the settings under the **Settings** tab.

Figure 336. Settings tab



5. Configure the settings for the attack definitions.
6. Click **Save** to save changes.

NOTE

The **Settings** tab in the bulk edit has the same configuration fields as displayed for the policy which is selected individually. But when you save the settings, the changes to the attack definitions are applied to all policies that are selected in bulk.

Customize IPS Policy

You can customize this IPS policy only for this interface. Such a customized IPS policy is referred to as the **Interface-Specific Customization**. The initial attack settings are inherited from the assigned policy, yet customization to the policy affect this interface only.

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Navigate to Intrusion Prevention → Policy Manager → **Interfaces**.
4. Double-click on the interface for which you want to customize the policy.

   The **<Device Name/Interface>** panel opens on the right side.
5. Under the **IPS** section, select the policy from the **Policy** drop-down list that you want to assign to the interface.
6. Click on **0** next to the **Customized Attacks** field under **Interface-Specific Customization**.

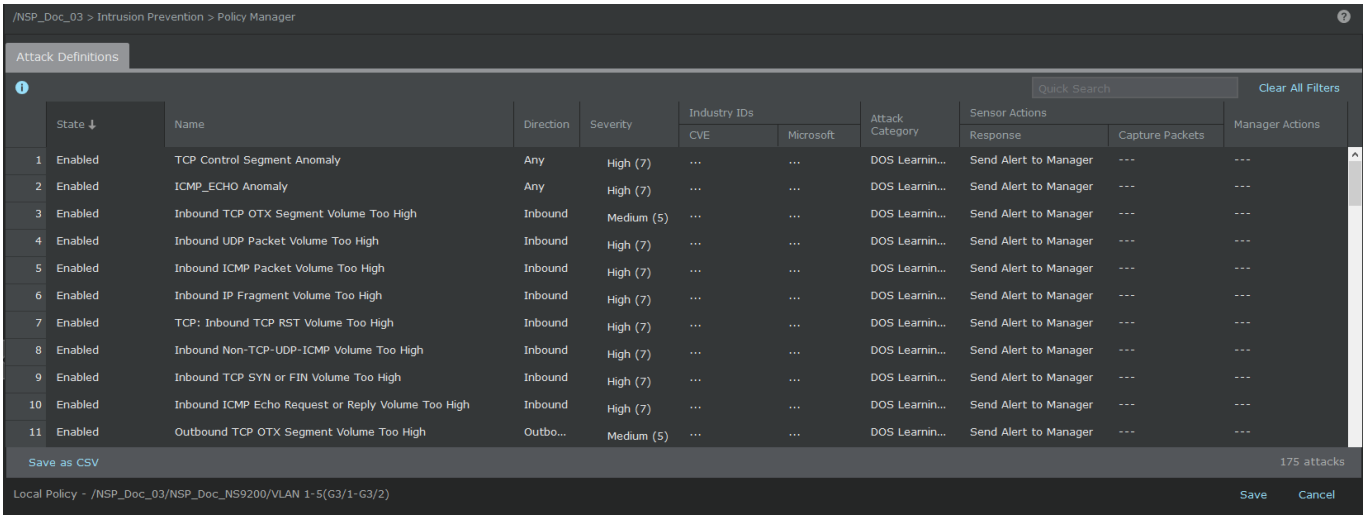
   The **Attack Definitions** window opens.
7. Select the policy you want to disable for the interface and click **Disable** one by one.

   To disable multiple policies at once, use the *Ctrl* key to select the policies and then click **Disable**.

NOTE

All the attacks are enabled by default.

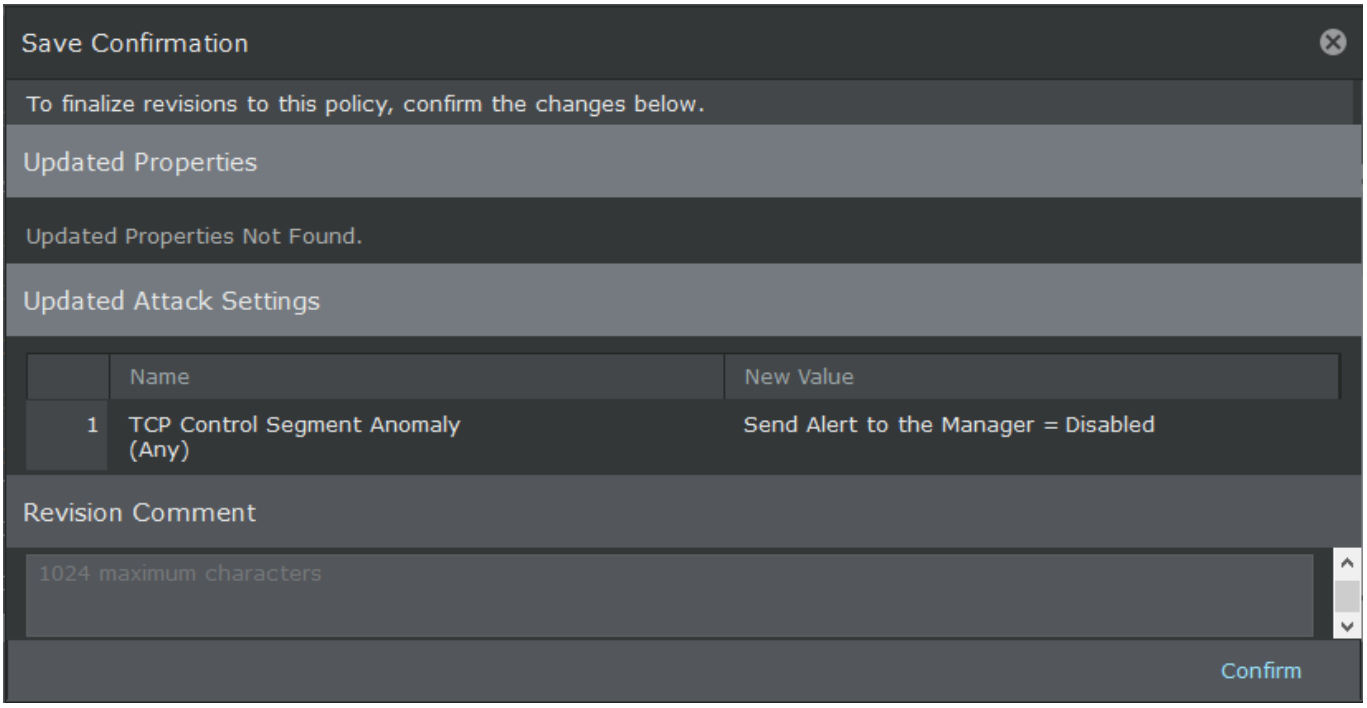
Figure 337. Attack Definitions page



8. Click **Save** to save the changes.

   A **Save Confirmation** window opens. Click **Confirm** to save the changes.

Figure 338. Confirmation message



   Click the **X** icon to exit the window without saving the changes.

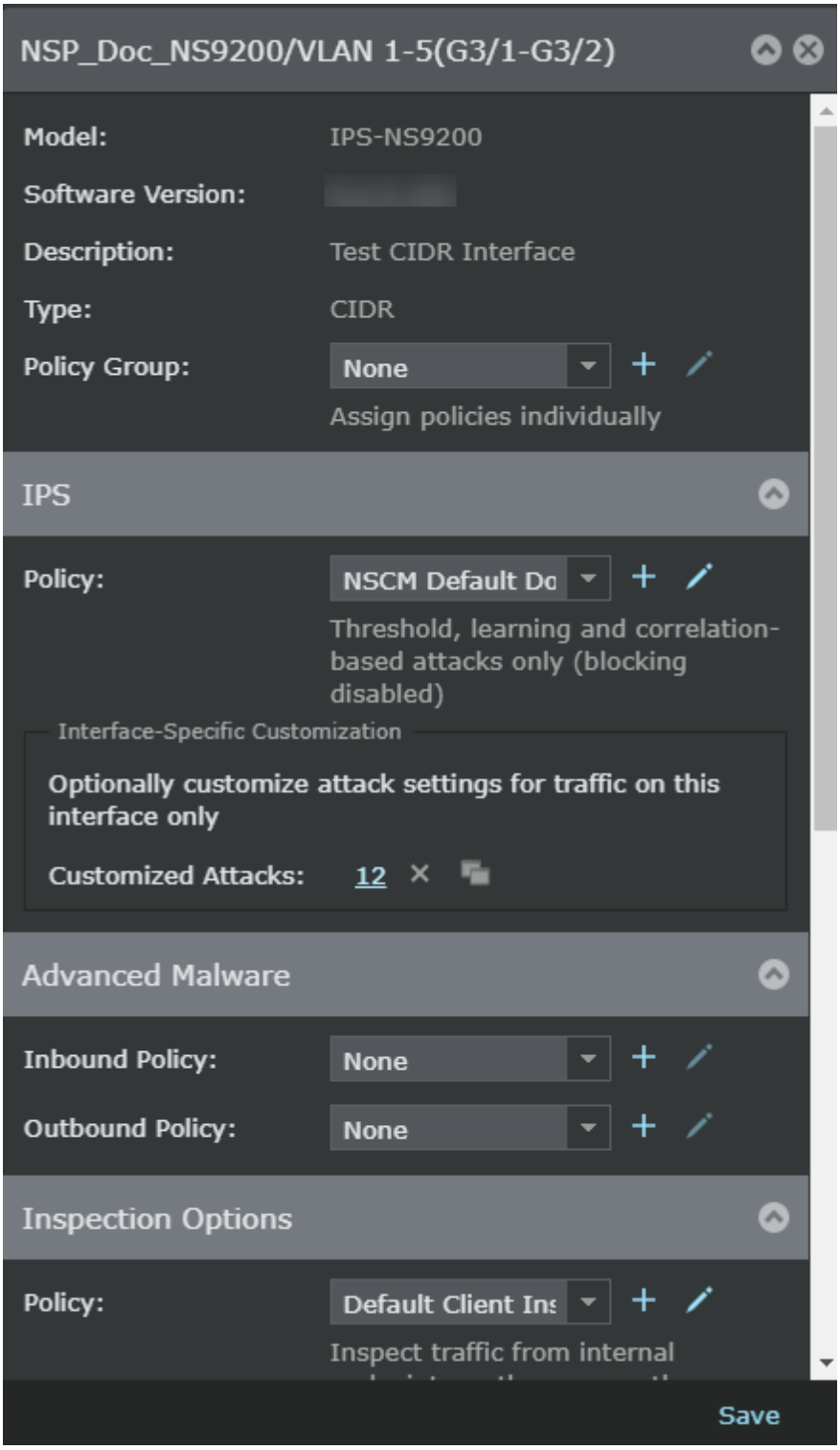
9. Click the **Save** button in the **<Device Name/Interface>** panel to save all the changes.

   The **Customized Attacks** field shows the integer value of the number of attacks customized for that policy.

10. Click the icon to merge the customized policy with the assigned policy.

    A confirmation message is displayed. Click **Yes** to confirm.

Figure 339. Customized attacks merge



11. After a successful merge, the **Customized Attacks** field shows the value as "0".

NOTE

You can customize the IPS policy in both the interface and subinterface levels.

12. Click the ✕ to delete any customization made to the policy, before merging it with the assigned policy.

    A confirmation message is displayed. Click **Yes** to confirm. The **Customized Attacks** field displays "0" as the integer value.

13. Do a configuration update for the corresponding Sensor for the changes to take effect.

Customize attacks across policies

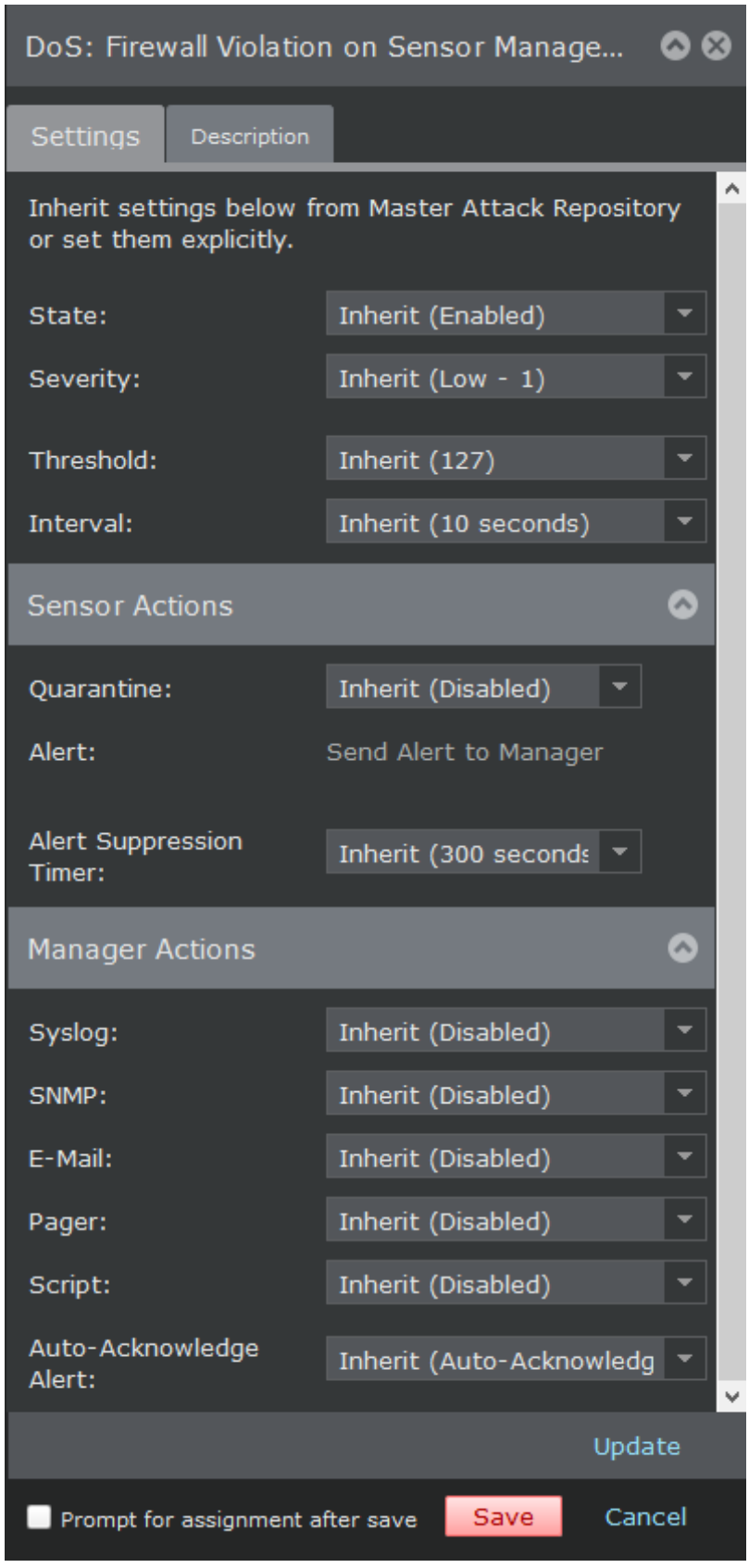
The **Master Attack Repository** (formerly Global Attack Response Editor or GARE) is an attack editor that works in concert with the policy and bulk editors. This editor, available only in the root admin domain, enables you to edit an attack definition's response once and have that modification applied across all policies that contain that attack definition, rather than having to find all policies that use a particular attack, and then modify the response on each of those policies one at a time. This includes the attack instances in the policies of a child domain. All attack response attributes can be customized (for example, Sensor response actions, logging, ignore rules, notifications).

Master Attack Repository displays the attacks that match the parameters in your selected attack set profile — all exploit attacks are categorized by protocol (that is, the application protocol they affect). From here, you can drill down to customize individual attack settings, such as ignore rules, Sensor responses, and notifications to be sent. This customization is optional, but Trellix recommends that you become familiar with them.

Using **Master Attack Repository**, you can modify exploit, DoS, and reconnaissance attack definitions. Do the following steps to view and configure the attack settings.

1. On the **Attack Definitions** tab, double-click on the row of the attack that you want to configure and update the settings. The attack details are displayed on the right panel displaying the settings under the **Settings** tab.

Figure 340. Settings tab



2. Configure the settings for the attack definitions

   The following fields are displayed for attacks of categories such as exploit, policy violation, malware, and reconnaissance:

Option	Definition
State	Select any following options: • **Inherit** • **Enabled** • **Disabled**
Severity	Select the severity level of the attack: • **Inherit** • **Info - 0** • **Low - 1** • **Low - 2** • **Low - 3** • **Medium - 4** • **Medium - 5** • **Medium - 6** • **High - 7** • **High - 8** • **High - 9**
Threshold	This field is displayed only configuring attacks of type DoS Threshold and Reconnaissance Correlation attacks. Select the severity level of the attack: • **Inherit** • **Set explicitly** **NOTE** If you select the option **Set explicitly**, specify the threshold value in the number field.
Interval	This field is displayed only configuring attacks of type DoS Threshold and Reconnaissance Correlation attacks. Select the interval duration: • **Inherit** • **Set explicitly** **NOTE** If you select the option **Set explicitly**, specify the interval duration seconds in the number field.

Option	Definition
Sensor actions	
Block	Select any of the following blocking options: • **Inherit** • **Disabled** • **Enable Blocking** • **Enable Smart Blocking**
Quarantine	Select any of the following quarantine options: • **Inherit** • **Quarantine attacker** • **Disabled**
TCP Reset	Select any of the following TCP reset options: • **Inherit** • **Reset src** - resets to the source • **Reset dest** - resets to the destination • **Reset src and dest** - resets to the source and destination
ICMP Message	Select any of the following ICMP message options: • **Inherit** • **Send host unreachable to source** • **Disabled**
Alert	Select any of the following alert options: • **Inherit** • **Send alert to Manager** • **Disabled**
Alert Suppression Timer	This field is displayed only configuring Sensor response for attacks of type Reconnaissance Correlation attacks. Select the severity level of the attack: • **Inherit** • **Set explicitly** **NOTE** If you select the option **Set explicitly**, specify the seconds in the number field.
Capture Packets	

Option	Definition
Pre-Attack Packets	Select any of the following pre-attack packet capture options: • **Inherit** • **Capture prior 128 bytes** • **Disabled**
Post-Attack Packets	Select any of the following post-attack packet capture options: • **Inherit** • **Capture subsequent bytes** • **Disabled**
Flows to Capture	This field is displayed only when you select **Post-Attack Packets** as **Capture subsequent bytes**. The following are the options available in this field: • **Inherit** • **Attack flow only** By selecting the option Attack flow only, a new drop-down list is displayed. Select any of the following options: • **Attack Packets only** • **Next N packets** - type the number of packets in the blank **packets** field. • **Next N time** - select the time options from the given drop-down list. The options are: • **Seconds** • **Minutes** • **Hours** • **Days** • **Rest of flow** • **Flows from src and flows to src and dest** By selecting the option **Flows from src and flows to src and dest**, a new drop-down list is displayed. Select any of the following options: • **Next N packets** - type the number of packets in the blank **packets** field. • **Next N time** - select the time options from the given drop-down list. The options are: • **Seconds** • **Minutes** • **Hours** • **Days**

Option	Definition
Bytes to Capture	This field is displayed only when you select **Post-Attack Packets** as **Capture subsequent bytes**. The following are the options available in this field: • **Inherit** • **All bytes in each packet** • **First N bytes in each packet** By selecting the option **First N bytes in each packet** , a new field to enter the number of bytes to capture is displayed. Type the number in the blank field.
Manager actions	
Syslog	Select any of the following syslog options: • **Inherit** • **Send syslog message** • **Disabled**
SNMP	Select any of the following SNMP options: • **Inherit** • **Send SNMP trap** • **Disabled**
Email	Select any of the following email options: • **Inherit** • **Send e-mail message** • **Disabled**
Pager	Select any of the following pager options: • **Inherit** • **Send page** • **Disabled**
Script	Select any of the following script options: • **Inherit** • **Run script** • **Disabled**
Auto-acknowledge	Select any of the following auto-acknowledgment options: • **Inherit** • **Auto-acknowledge alert** • **Disabled**
Update	Click here to update the settings.

Fields in the **Capture Packets** and **Manager actions** sections are displayed only when alerting (**Alert** field option) is enabled or inherited.

The fields in the **Sensor actions** section are not displayed for malware attack definitions that support advanced malware policies as these settings are configured in the malware policy. However, the Manager actions are configurable for such malware attacks.

Delete an IPS Policy

The following procedure explains the essential elements of a complete policy deletion.

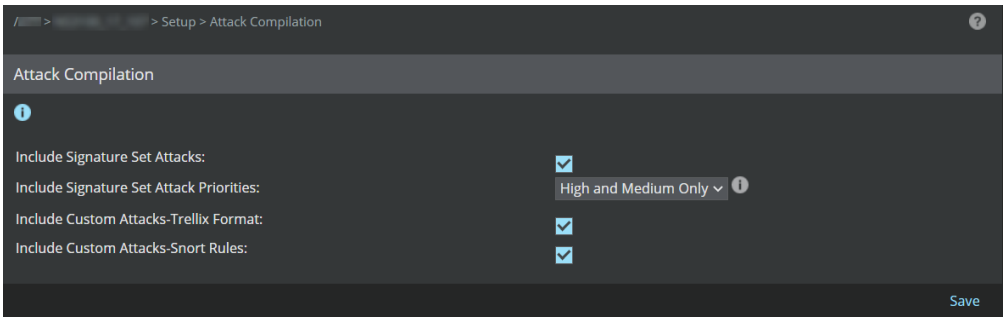
1. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Admin Domains**.
2. Select the admin domain and click .
3. Assign a default IPS policy to the admin domain which replaces the policy to be deleted and click **Save**.
4. Go to Policy → <Admin Domain Name> → Intrusion Prevention → **Policy Manager**.
5. Click Save.
6. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.
7. Select the IPS Policy, and click .

Configuration of attack compilation

The **Attack Compilation** page enables you to specify the type of attack definitions to be included in the IPS Policies for a specific Sensor.

To access the **Attack Compilation** page, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Attack Compilation**.

The **Attack Compilation** page opens.



You can select the following types of attack definitions for the Sensor:

- **Signature Set Attacks** - These are the attacks from Trellixsignature set.

  When the **Signature Set Attacks** option is selected, the Manager allows you to choose **Signature Set Attack Priorities** for the Sensor. This allows the Manager to dynamically compile only critical attacks from the standard signature set for Sensors that do not have enough resources to support all attacks.

  The signature set attack priorities available are as follows:

- **All**: Includes all attack definitions in the signature set. This is the default signature set attack priority selected for NS-series and Virtual IPS Sensors and provides complete attack coverage.
- **High and Medium only**: It comprises of high and medium priority attacks in the signature set.
- **High only**: It comprises of high priority signature set attacks. You can use this option to optimize Sensor resources on Sensor models running older Sensor software versions to support the latest signatures against most critical attacks.

> **WARNING**
>
> The **High Only** signature set attack priority provides an attack coverage only against the most critical attacks.

- **Custom Attacks – Trellix Format** — These are the Trellix Custom Attacks that are defined or received from Trellix.
- **Custom Attacks–Imported Snort Rules** — These are the Snort Custom Attacks that are imported or created in the Manager.

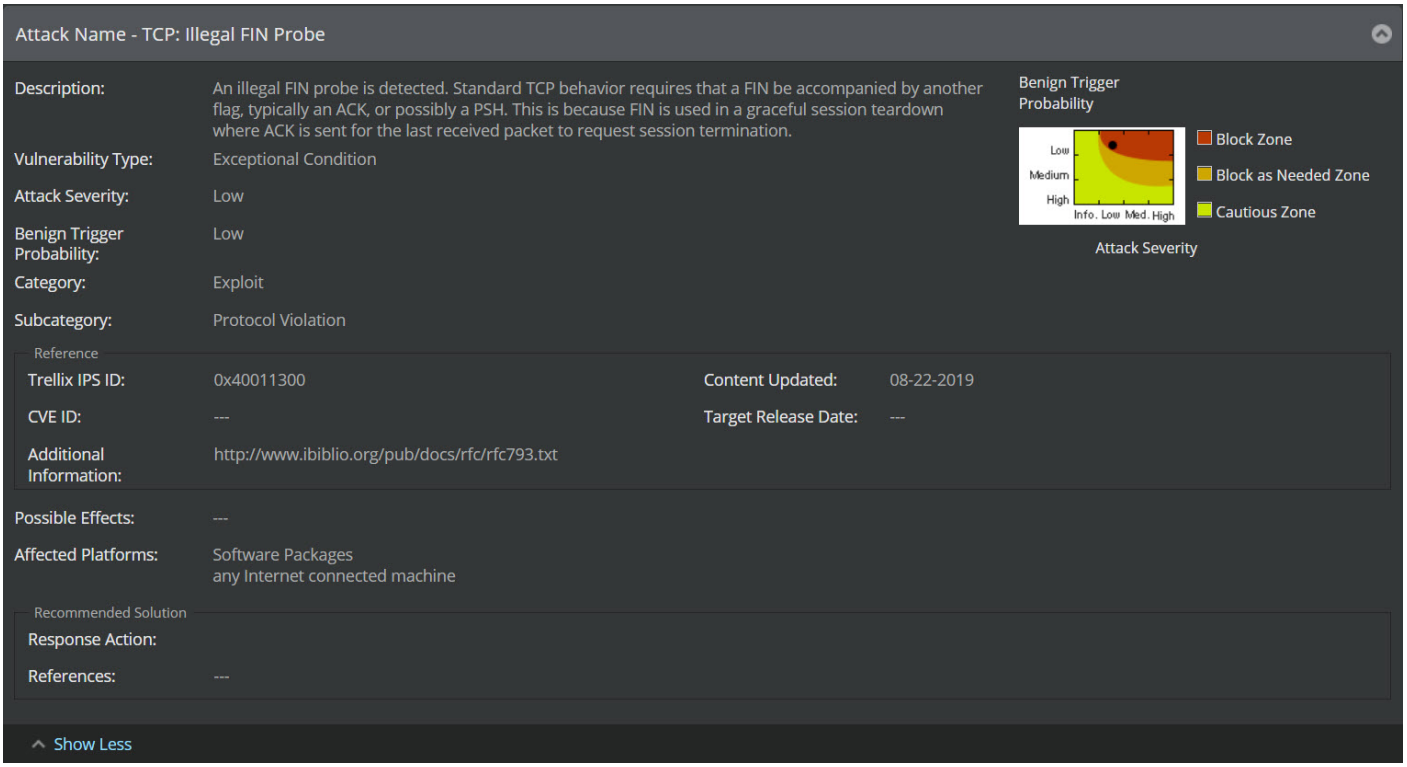
Attack descriptions

Every attack definition provided by Trellix includes an attack description. The information in this description is designed to give reference to what the attack does and how to defend against the attack in the future.

Attack descriptions can be accessed from a number of areas:

- **Policy** — during policy viewing/creation. Includes all Exploit, DoS, and Reconnaissance attacks.
- **Attack Log** — within the details of a detected attack.
- **Threat Explorer** — within the **Top Attacks** section by accessing any attack's hyperlink.
- Trellix IPS **KnowledgeBase** — all entries within the Attack Encyclopedia.

Figure 341. Attack description example



The **Attack Information & Description** fields are as follows:

Fields	Description
Name	Trellix IPS-designated name for an attack.
Vulnerability Type	Type of inherent system flaw that can be exploited by attackers.
Impact Category	Type of impact that it can have on a system.
Impact Subcategory	Type of inherent system flaw that can be exploited by attackers.
Severity	Malicious impact potential of the attack. The values are high, medium, and low.
Benign Trigger Probability	The benign trigger probability is the chance that the signatures for an attack may trigger a false positive.
Description	Attack definition and conditions
Possible Effects	The impact if the attack is successful.
Recommended Solution	Available workarounds and patches
Platforms Affected	Systems and/or software directly affected by the attack.

Fields	Description
Reference	Trellix IPS supports multiple standards and sources for finding information on known attacks. Cross-referencing a Trellix IPS attack name with a CVE name, BugTraq ID, or other link can assist your analysis of known attacks and vulnerabilities. Trellix IPS **ID** — globally unique attack ID within the Trellix IPS. **Last Rev Date** — last date attack information was updated. **CVE** — The Common Vulnerabilities and Exposures (CVE) name related to an attack. CVE maintains a list of standardized names related to publicly known vulnerabilities and security exposures. Refer to www.cve.mitre.org. A CVE name such as "CVE-1999-0001" is called an entry, denoted by "CVE" at the beginning of the name. An entry is a vulnerability or exposure that has been accepted by the CVE Editorial Board. A CVE name such as "CAN-2001-0002" is called a candidate, denoted by "CAN" at the beginning of the name. A candidate is a vulnerability or exposure that is "under consideration for acceptance into CVE." A CVE name has three fields — entry status, year of entry, and entry number during the year. Thus, if a CVE name reads "CVE-2000-0005," the vulnerability/exposure was the fifth accepted entry in the year 2000. Between candidacy and entry, a CVE entry will most likely change numeric ID along with the change from CAN to CVE-. Thus, CAN-2001-0023 may be accepted in the year 2002 and thus read — "CVE-2002-0002.". BugTraq: ID of attack as listed in the BugTraq database. Refer to http://online.securityfocus.com/. **Microsoft** — ID of attack as listed in the Microsoft Security Bulletin. **Links** — additional information sources.
User Comments	Any comments that you have entered for the attack description.

Creating Custom Attacks

Custom Attacks or Custom Attack Definitions are user-defined attack definitions. You create such definitions to supplement the attack definitions (Signature Set) that Trellix provides.

Custom Attack Editor enables you to create Trellix Custom Attacks as well as Snort Custom Attacks. Using this tool, you can also import custom attacks in bulk against defining them individually. You use the Custom Attack Editor to manage custom attacks. You can launch it from the Custom Attacks page of the Manager. From the Manager, select Policy → <Root Admin Domain> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

For more information, see Create custom attacks (page 1726).

Assign IPS policies at the admin-domain level

Sensor allows very granular policy application and enforcement; multiple IPS and DoS policies can be enforced on a single port or port pair. For example, suppose you are a super user at the root admin domain level, and you deploy a single Sensor. You edit the details of your root domain and decide to keep the **Default Prevention** policy that is applied by default upon Manager installation. When you add the Sensor, the **Default Prevention** policy is inherited from the root domain and applies to the Sensor and all of the Sensor's interfaces by default. If you want to apply a different IPS policy, you can easily re-assign policies applied to the Sensors and their interfaces/subinterfaces within the current admin domain or child admin domains.

You can quickly find and reassign policies applied to multiple Sensors and their resources (interfaces/ subinterfaces) without having to search extensively in Trellix IPS. You can filter your search results by *policies* (for example, IPS policy), or *Sensors*. From the search results, you can select the resources and re-assign policies, as required.

Assign IPS policy to interfaces and subinterfaces

Make sure the IPS policies that you want to assign to Sensor resources are available.

In Trellix IPS, IPS policies are enforced at the interfaces and subinterfaces, not at the Sensor level. Since the Sensors are multi-port devices with multiple interfaces and subinterfaces, this allows multiple policies to be enforced within a single Sensor rather than a single catch-all policy. Compared to some other IPS products, this is like having several Sensors in one box.

When you create an admin domain, you can select the **Default Prevention** and **Default Reconnaissance Policy** for that admin domain. When you add a Sensor to that domain or allocate interfaces and subinterfaces, these policies are applied to those Sensor resources by default. You can assign different policies to those Sensor interfaces and subinterfaces through the corresponding **Policy Manager** page. An alternative method is to assign an IPS policy from the **IPS** page itself. This is especially useful when you want to define an IPS policy and also quickly assign it to Sensor interfaces and subinterfaces.

NOTE

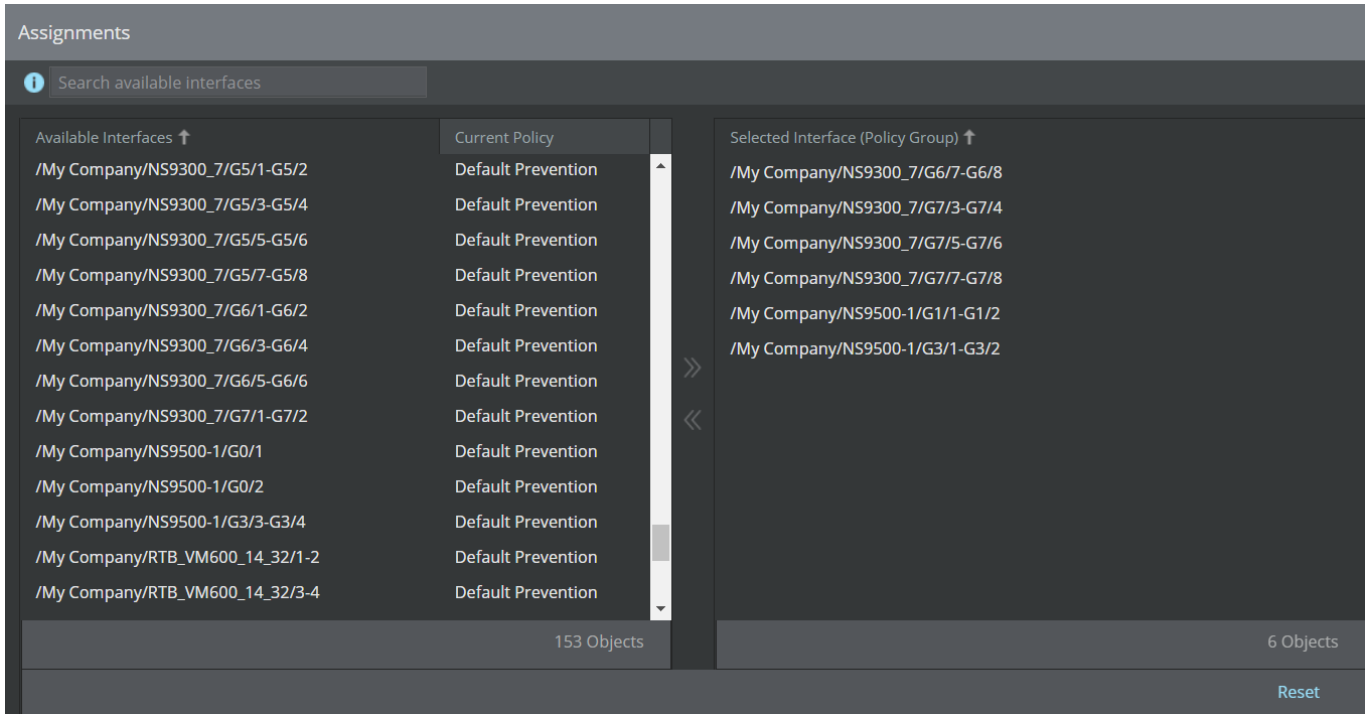
Interfaces assigned to a policy group can only be managed from the **Policy Manager** page and not from the **IPS** page.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Policy Types → **IPS**.
4. Click the **Assignments** value of the policy that you want to assign.

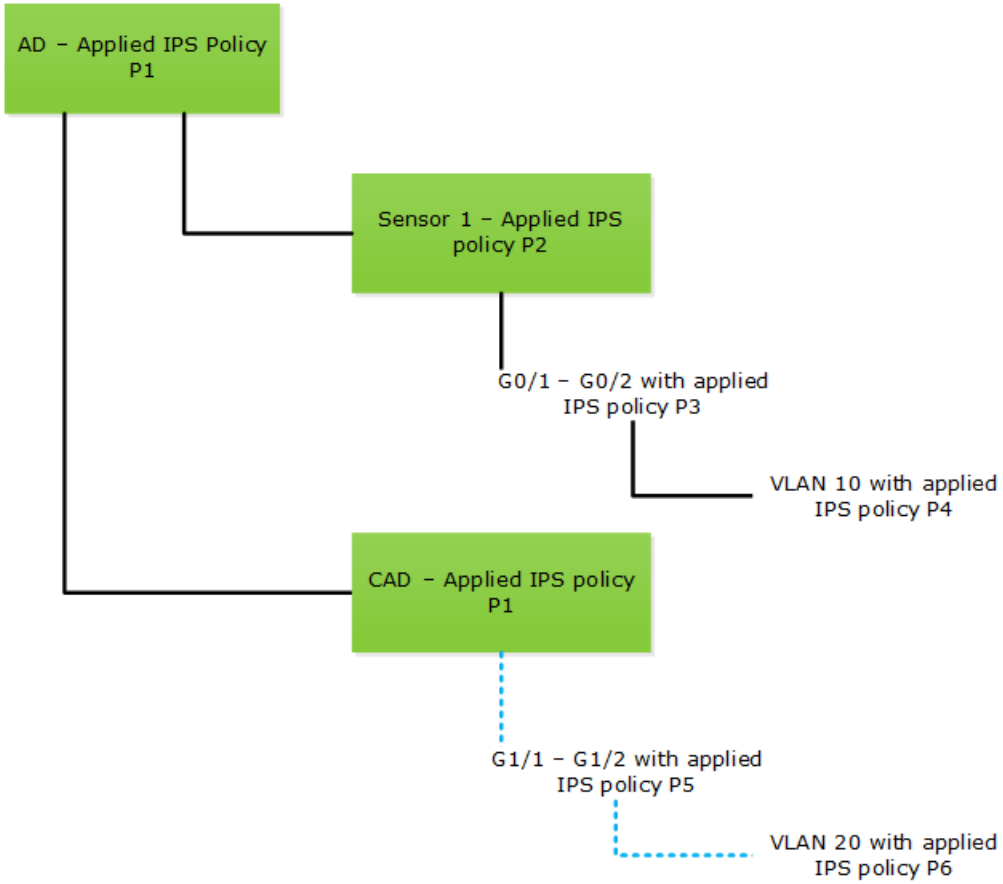
   The **Assignments** window is displayed.
5. Assign the IPS policy to the required interfaces and subinterfaces.

Figure 342. Assignments window



Option	Definition
Search Interfaces	To filter the list of available interfaces, enter a string that is part of the **Available Interfaces**.
Available Interfaces	Lists the interfaces and subinterfaces of the Sensors in the admin domain. The Sensor interfaces to which you have already assigned this IPS policy are displayed under **Selected interfaces.** **NOTE** In case of Sensors in failover, the ports used for interconnection of the Sensors are not displayed. If you assign an IPS policy to an interconnect port, the assignment is automatically removed when you create the HA pair. Select a resource and click » to move it to **Selected Interface**.
Current Policy	The IPS policy that is currently assigned to an interface. To replace that policy with the policy that you are currently assigning, move the interface to **Selected Interface**.
Selected Interface (Policy Group)	Lists the Sensor interfaces to which you have assigned the selected IPS policy
Reset	Reverts to last saved configuration
Save	Saves the changes to the Manager database
Cancel	Closes the **Assignments** window without saving the changes

6. If you move a Sensor resource from **Selected Interface** to **Available Interfaces**, the Sensor's IPS policy is automatically applied to those Sensor resources.



- Consider a scenario illustrated by the diagram. The admin domain AD is assigned the IPS policy - P1. It has Sensor 1 under it and a child admin domain named CAD.
- CAD is assigned the IPS policy P1. Sensor 1 is assigned the IPS policy P2. The interface G0/1-G0/2 is assigned the IPS policy P3.
- The subinterfaces VLAN10 is assigned the IPS policy P4.
- The interface G1/1-G1/2 of Sensor 1 is allocated to CAD. This is assigned IPS policy, P5.
- VLAN20 is a subinterfaces of G1/1-G1/2 and is assigned a policy P6.
- In the **Assignments** window of P3, if you move G0/1-G0/2 from **Selected Interface** to **Available Interfaces**, P2 is applied to this interface. Similarly, if you move VLAN10 for P4, then P2 is applied to this subinterfaces, which means these resources fall back to the Sensor's policy.
- Similarly, if you move G1/1-G1/2 and VLAN20 from **Selected Interface** to **Available Interfaces** in the corresponding policies, the IPS policy P1 is applied. That is, these interfaces fall back to the IPS policy of the domain to which they are allocated.
- If any resource has a local IPS policy customization and you remove this interface from **Selected Interface** to **Available Interfaces** in the corresponding policy, the same local policy customization is made to the policy to which it falls back. However, for this, the same attacks must be present in this fallback IPS policy as well.

7. Do a configuration update for the corresponding Sensors to enforce the policy.

Scenario: Apply different policies to multiple subinterfaces

Multi-port Sensors support multiple applied IPS policies for interfaces and subinterfaces. This is particularly useful if you have segmented your network traffic by VLAN tags or CIDR addressing. For this scenario, the sample network has been segmented by CIDR addressing. Your Sensor monitors traffic to three networks from an aggregation point. By using Trellix IPS's multiple policy functionality, you can apply appropriate policies to individual networks, thus tuning out alerts for traffic rarely seen in those network segments. This "tuning out" dramatically reduces the number of alerts you see, thus positively affecting your total cost of ownership of a Trellix IPS solution.

1. You designate port pair G0/1-G0/2 to be a CIDR interface.

   The **Default Prevention** policy is inherited from the admin domain and enforced across the entire interface.

2. You add three CIDR network addresses to your interface:
   - 192.168.0.0/24: multiple file servers
   - 192.168.1.0/24: multiple file servers
   - 192.168.2.0/24: multiple Windows servers
3. You create a subinterface, *File_Servers,* to protect networks 192.168.0.0/24 and 192.168.1.0/24 with a more appropriate policy. You create a File Server policy to protect *File_Servers.*

   TIP

   The name *File_Servers* is used instead of a generic name, such as *Sub-interface1*, because a unique name describing the subinterface environment is more effective for later identification.

4. You create another subinterface, *Windows_Servers* to protect 192.168.2.0/24 with a more appropriate policy. You create a Windows Server policy to protect *Windows_Servers*.

   All interface traffic through port pair G0/1-G0/2 that is not a part of the two subinterfaces mentioned is protected by the Default Prevention policy. The File Server policy is most effective for *File_Servers* because both networks consist of multiple file servers, and it is specifically tuned to known file server traffic elements. In the same way, the Windows Server policy is most effective for *Windows_Servers* because this policy is specifically tuned for Windows server traffic. Either of these policies can be cloned and customized, for example, to remove attacks that may be generating false positives and/or to set an automatic response upon detection of specific attacks.

Manage assigned policies

After a new Sensor is installed, a policy is inherited from the admin domain and enforced on all Sensor interfaces. In large deployments or ones that have a significant number of policies configured in the Manager, it can take a long time to download the signature sets and apply the policy changes to the Sensors. You define policies at the admin domain level. This becomes your Baseline Policy. When two or more Sensor interfaces protect similar types of traffic, you can assign the same baseline policy to each of these interfaces, and optionally customize specific attack settings per interface, as required. This helps in minimizing scalability issues, and enhances the overall policy management process in the Manager. The baseline policy is assigned to the interface and now functions as a starting point for the local attack settings.

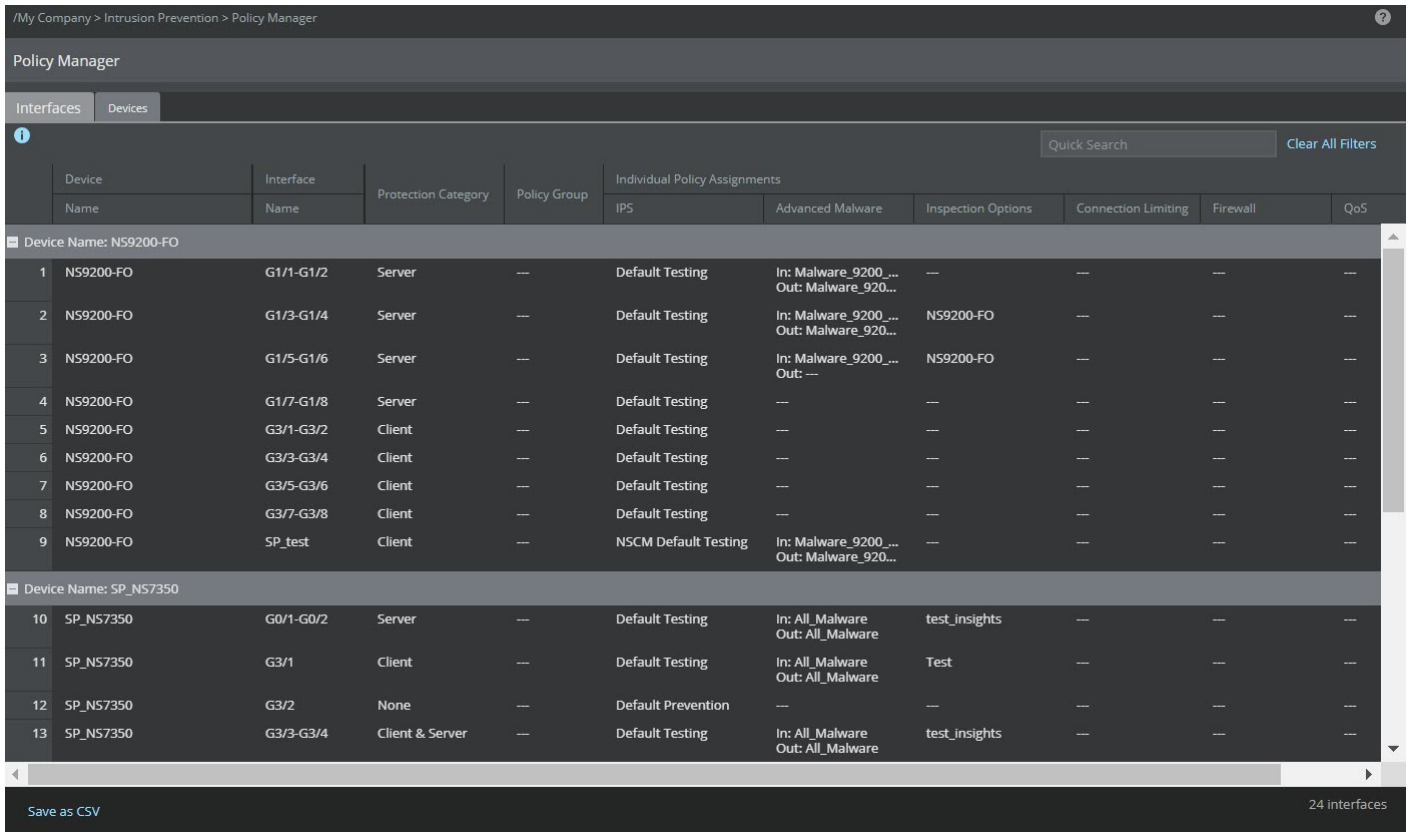
Each subinterface created within an interface can have a specific IPS policy applied. For example, if you have created three subinterfaces using VLAN tags, you can apply individual policies different from that of the parent interface to each of the three subinterfaces, respectively. When you create a subinterface, you can specify an IPS policy or simply inherit the IPS policy of the

parent interface. This policy can be changed at any time per subinterface. The procedure to apply IPS policies to subinterfaces is similar to that of interface. However, note this important point regarding how the policies are enforced. If you apply a policy to a subinterface that is different than the inherited policy, the policy enforced at the interface level protects all traffic not specific to the subinterface. That is, the IPS policy of the subinterface exclusively protects all of the traffic that meets the criteria of the subinterface, which is typically any specified CIDR-based network or VLAN-tagged traffic flowing through the parent interface. All other traffic monitored by the interface is thus subject to the applied policy of the interface.

1. In the Manager, click **Policy** and then select the required **Domain**.
2. Go to Intrusion Prevention → **Policy Manager**.

   The **Policy Manager** page is displayed.

Figure 343. Policy Manager page



The **Policy Manager** page has the following tabs:

- **Interfaces** tab
- **Devices** tab

Interfaces tab

In the **Interfaces** tab, you can view and edit the policy assignments at the interface level.

The **Interfaces** tab is displayed by default. This tab displays the summary of the interface-level assignments. The following details are displayed.

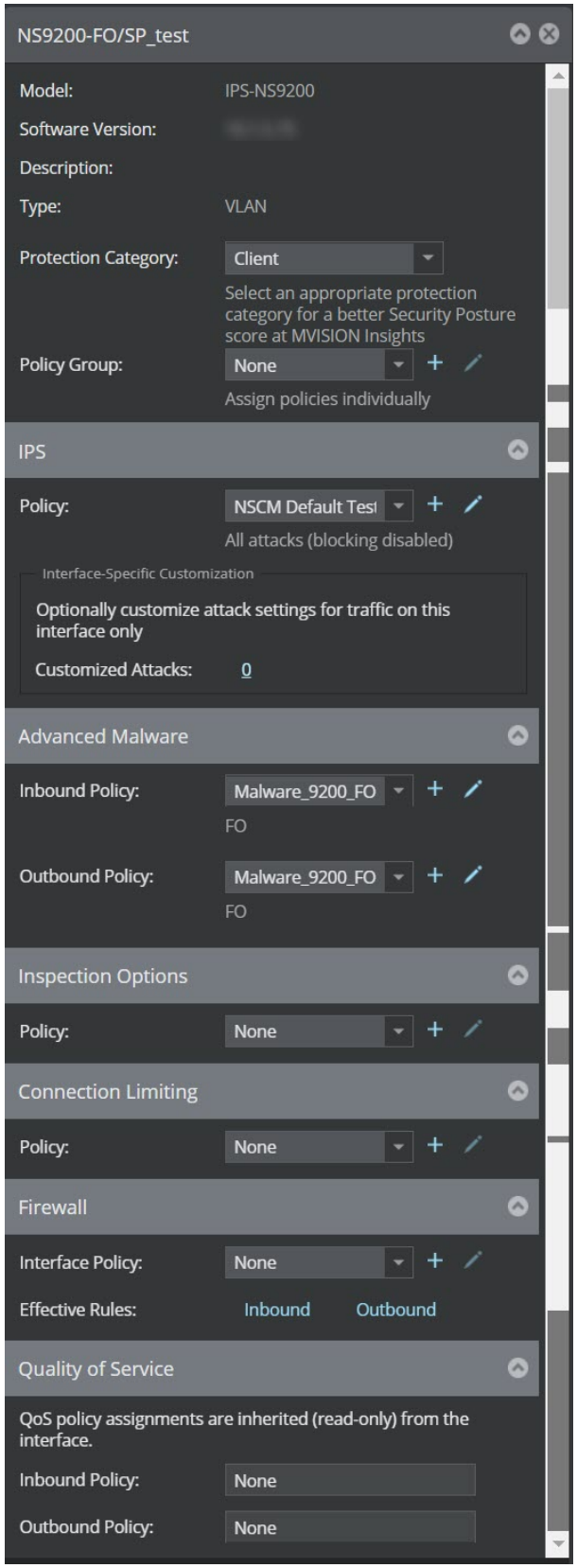
Option	Definition
Device	**Name** — Displays the name of the device to which the policy is assigned. **Model** — Displays the Sensor model. **Software Version** — Displays the software version running on the Sensor.
Interface	**Name** — Displays the name of the interface to which th policy is assigned. **Description** — Displays the description for the interface. **Type** — Displays the type of interface. It can be dedicated, VLAN, bridge VLAN or CIDR.
Protection Category	Displays the protection category for the interfaces and sub-interfaces. **NOTE** The selection of a protection category gives a more precise security posture score at Trellix Insights.
Policy Group	Specifies the name of the policy group that is assigned.
Individual Policy Assignments	Displays the policy type details in various columns. The policy types are **Advanced Malware**, **Firewall** , **QoS** , **IPS**, **Inspection Options** and **Connection Limiting**.
Save as CSV	Exports information about all interfaces in a .csv format.

Edit interface-level assignments

You can view and edit the interface-level assignments. To edit an assignment:

1. In the Manager, navigate to Policy → <Admin Domain Name> → Intrusion Prevention → **Policy Manager**.
2. Double-click on the row of a policy assignment. The interfaces details panel is displayed on the right side of the page.

Figure 344. Interfaces tab



The following fields are displayed.

Option	Definition
Model	Specifies the model of the device
Software Version	Specifies the software version running on the device
Description	Displays the description of the interface assignments
Type	Specifies the type of interface
Protection Category	Select a protection category from the drop-down list for a better security posture score at the Trellix Insights. The protection category options available are: • **None** • **Server** • **Client** • **Client & Server** • **Exclude** By default, the protection category is **None** . When the option **None** is selected, the telemetry data sent to Trellix Insights flags the interface for incomplete configuration. The protection category **Exclude** can be selected in case you want to exclude the interface configuration from security posture scoring on Trellix Insights.
Policy Group	Select the type of policy group from the drop-down list. Click + to add a new policy group. Click ✎ to edit or view the existing policy group details.

Option	Definition
IPS	Select the type of IPS policy from the drop-down list. Click + to add a new IPS policy. Click ✎ to edit or view IPS policy details. **NOTE** If the **Policy Group** option selected as **None**, you can manually assign the IPS policy. If the **Policy Group** option is already selected, you will not have the option to edit the IPS policy because these details are defined in the selected policy group. In the **Customized Attacks** field, click on the hyperlink to customize the attacks. By default value is 0. The hyperlink is displayed only if the number of customized attack is more than 0. Click − to reset the customization to the local attack definitions. This option is not displayed if the number of customized attacks is 0. Click ⧉ to merge the local policy with the baseline policy. This option is not displayed if the number of customized attacks is 0.
Advanced Malware	Select the type of advanced malware policy from the drop-down list. In the **Inbound Policy** field, select the inbound policy from the drop-down list. Click + to add a new advanced malware policy. Click ✎ to edit or view the advanced malware policy. In the **Outbound Policy** field, select the outbound policy from the drop-down list. Click + to add a new advanced malware policy. Click ✎ to edit or view the advanced malware policy. **NOTE** If the **Policy Group** option selected as **None**, you can manually assign the advanced malware policy. If the **Policy Group** option is already selected, you will not have the option to edit the policy because these details are defined in the selected policy group.
Inspection Options	Select the type of Inspection Options policy from the drop-down list. Click + to add a new Inspection Options policy. Click ✎ to edit or view Inspection Options policy details. **NOTE** If the **Policy Group** option selected as **None**, you can manually assign the Inspection Options policy. If the **Policy Group** option is already selected, you will not have the option to edit the Inspection Options policy because these details are defined in the selected policy group.

Option	Definition
Connection Limiting	Select the type of Connection Limiting policy from the drop-down list. Click + to add a new Connection Limiting policy. Click ✎ to edit or view Connection Limiting policy details. **NOTE** If the **Policy Group** option selected as **None**, you can manually assign the Connection Limiting policy. If the **Policy Group** option is already selected, you will not have the option to edit the Connection Limiting policy because these details are defined in the selected policy group.
Firewall	In the **Interface Policy** field, select the interface policy from the drop-down list. Click + to add a new interface policy. Click ✎ to edit or view the interface policy. **NOTE** If the **Policy Group** option selected as **None**, you can manually assign the firewall policy. If the **Policy Group** option is already selected, you will not have the option to edit the policy because these details are defined in the selected policy group. In the **Port Policy** field, select the port policy from the drop-down list. Click + to add a new port policy. Click ✎ to edit or view the port policy. **NOTE** The **Port Policy** field is displayed only for interfaces and is not displayed for sub-interfaces. To view the effective rules, in the **Effective Rules** field click **Inbound** button to view the inbound rules, or click **Outbound** button to view the outbound rules.
Quality of Service	In the **Inbound Policy** field, select the inbound policy from the drop-down list. Click + to add a new QoS policy. Click ✎ to edit or view the inbound policy. In the **Outbound Policy** field, select the outbound policy from the drop-down list. Click + to add a new QoS policy. Click ✎ to edit or view the outbound policy. **NOTE** If the **Policy Group** option selected as **None**, you can manually assign the QoS policy. If the **Policy Group** option is already selected, you will not have the option to edit the QoS policy because these details are defined in the selected policy group.

The **Interfaces** tab has some useful filtering options to locate and view the policy assignments. String based filter is available for those columns where policy assignments are displayed based on the text typed in the text field of the **Filters** option. By typing the first few characters in the text field, the policies matching the typed characters are displayed on the page.

> **NOTE**
>
> When the policy assignments are displayed by using the **Filters** option, the header of column by which the policy assignments are filtered is highlighted in orange color. By clicking the **Clear All Filters** button, the filter is removed and all the policy assignments are displayed on the page.

Click a column header and select the option to sort based on ascending or descending order. The options are **Sort Ascending** and **Sort Descending**.The column based on which the list is sorted is indicated in the column header by an up arrow icon for ascending order and down arrow icon for descending order.

For a consolidated view of a group of policy assignments, click on the column header of the field (Example : **Direction**) by which it should be grouped and click **Group by this field**.

> **NOTE**
>
> To remove the display of policy assignments by groups, unselect the **Show in groups** check-box option from the column header. The **Show in Groups** option is enabled only if the **Groups by this field** option is selected.

3. Click **Save** to save the changes.

> **NOTE**
>
> You must assign an alternate policy for a Sensor's interfaces/subinterfaces in cases where the original policy needs to be deleted. For example, you have created an IPS policy called **Custom1**. You apply it to interfaces G1/2, G1/3, and G1/4 on a Sensor. After some time, you determine **Custom1** does not work effectively, and you want to delete it. The Manager will not allow you to delete a policy that is currently enforced. You have to change the policy of each Sensor resource where the custom policy is applied before deleting the custom policy itself.

Devices

On the **Devices** tab, you can view and edit the policy assignments at the device level.

The **Devices** tab displays the summary of the device-level assignments.

The following details are displayed:

Option	Definition
Device	**Name** — Displays the name of the Sensor. **Model** — Displays the Sensor model. **Software Version** — Displays the software version running on the Sensor.

Option	Definition
Policy Assignments	Displays the details of policy assignments for the device. **Reconnaissance** — Displays the reconnaissance policy assigned for the device. **Firewall-Device First** — Displays the pre-device level policy. **Firewall- Device Last** — Displays the post device level policy.
Save as CSV	Exports information about all the devices in a .csv format.

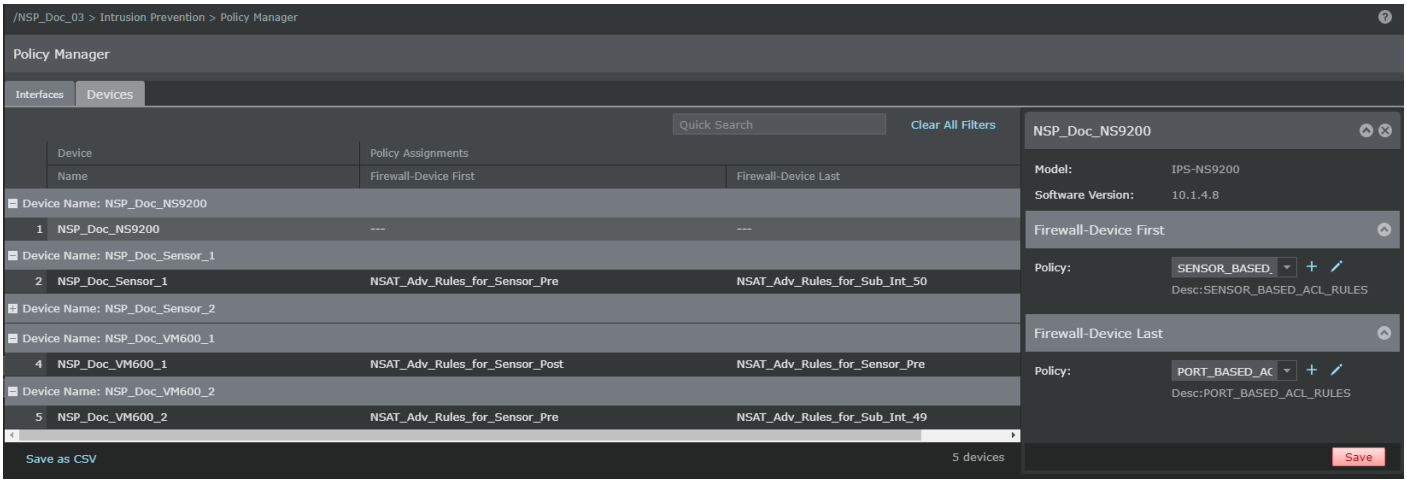
Edit Device-level assignments

You can assign the policies such as the Reconnaissance and Firewall policies at the Sensor level. These policies are applied to all the resources of that Sensor.

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Intrusion Prevention** tab.
4. Click Policy Manager. Select the **Devices** tab.

   List of Sensors configured are displayed.

Figure 345. Devices tab



5. Double-click on the Sensor for which the policy has to be applied. The **<Device Name>** window opens in the right panel.

   For example if the device name is "Trellix —2050", the window name is displayed as 'Trellix —2050'.
6. Select the firewall policy in the **<Device Name>** window from the **Policy** drop-down list.

   Click the + to add a new policy. Click the ✎ icon to edit the selected policy.

   For information on these policies, see the corresponding sections.
7. Click **Save**.
8. Click **OK**, and then update the configuration change to the Sensor.

Manage policy groups

For managing the assignment of policies, a new page is created under Policy → Intrusion Prevention → Objects → **Policy Groups**.

In the **Policy Groups** page, you can create and manage a group of policies. After creating a policy group, it is assigned to the corresponding Sensor interfaces and sub-interfaces to manage the inbound and outbound traffic. The following columns are displayed in the **Policy Groups** page:

- **Name**
- **Description**
- **Individual Policy Assignments**
- **Search**

In the column header an option can be selected to sort based on ascending or descending order. The options are **Sort Ascending** and **Sort Descending**. The column based on which the list is sorted is indicated in the column header by an up arrow icon for ascending order and down arrow icon for descending order.

In the **Policy Group** page, a new policy group can be created by clicking on the Add button. It displays the **Policy Group Details** panel. The **Policy Group Details** panel has the following fields:

- **Name**
- **Description**
- **Owner Domain**
- **Visibility**
- **Editable here**
- **IPS: Policy**
- **Advanced Malware: Inbound Policy and Outbound Policy**
- **Inspection Options: Policy**
- **Connection Limiting: Policy**
- **Firewall: Interface Policy**
- **Quality of service: Inbound Policy and Outbound Policy**

In the **Assignments** page, the assignments of policy groups are displayed:

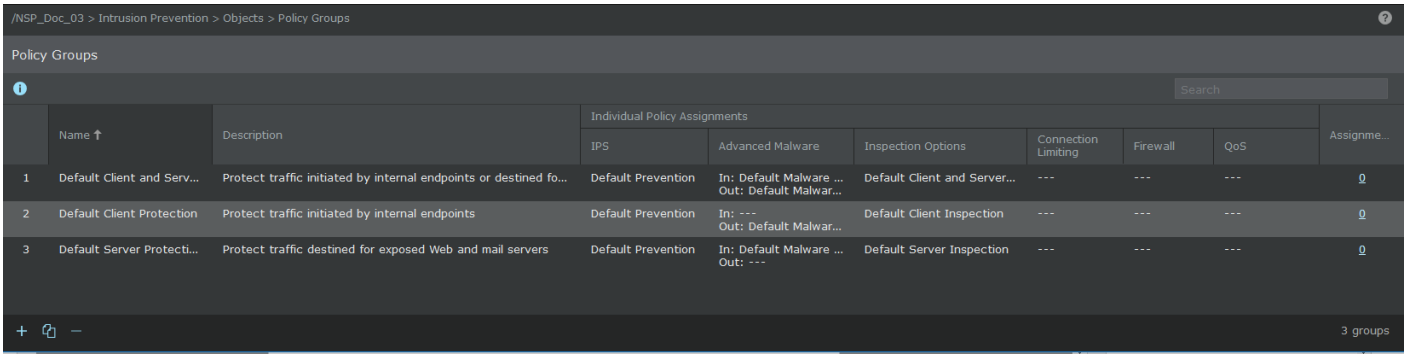
- **Available Interfaces** — Lists the interfaces and sub interfaces of the Sensors in the admin domain
- **Selected Interfaces** — The policy group that is currently assigned to an interface
- **Search Interfaces** — To filter the list of available interfaces, enter a string that is part of the Available Interfaces

You can create and manage policy groups and assign them to the corresponding Sensor interfaces and sub-interfaces to manage the inbound and outbound traffic.

To access and manage policy groups:

1. Click the **Policy** tab, and select the admin domain from the **Domain** drop-down list.
2. Select Intrusion Prevention → Objects → **Policy Groups**. The **Policy Groups** page is displayed.

Figure 346. Policy Groups page

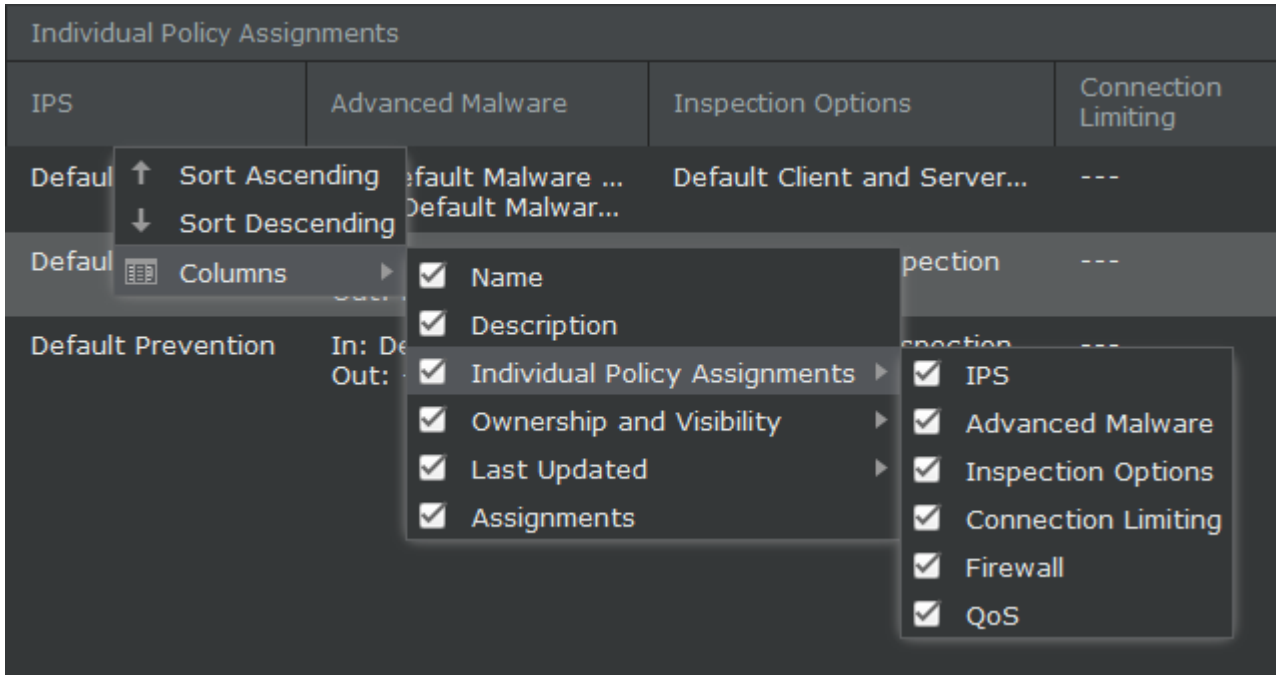


The **Policy Groups** page displays the following details :

Option	Definition
Name	Displays the name of the policy group
Description	Displays the description of the policy group
Individual Policy Assignments	**IPS** — Specifies the type of IPS policy. Example: Default Prevention. **Advanced Malware** — Specifies the inbound and outbound type of advanced malware policy **Inspection Options** — Specifies the type of Inspection Options policy **Connection Limiting** — Specifies the type of connection limiting policy **Firewall** — Specifies the type of Firewall policy **QoS** — Specifies the type of inbound and outbound QoS policy
Ownership and Visibility	**Owner Domain** — Specifies the ownership of the domain **Visibility** — Specifies the visibility level of the domain **Editable Here** — The status **Yes** indicates that the policy is owned by the current admin domain.
Last Updated	**Time** — Displays the time when the firewall policy was last updated **By** — Displays the user who modified the policy
Assignments	Indicates the number of Sensor resources to which the policy is assigned
Search	Type your search criteria in the field to find policy groups with matching elements.
+ icon	Click here to create a policy group.
icon	Clones a policy group
− icon	Deletes the selected policy group
To view or edit a policy group	Double-click the row of the specific policy group.

You can filter the display of columns by clicking a column header and selecting or unselecting the check-box for the list of columns you wish to view in the **Policy Groups** page.

Figure 347. Column filter



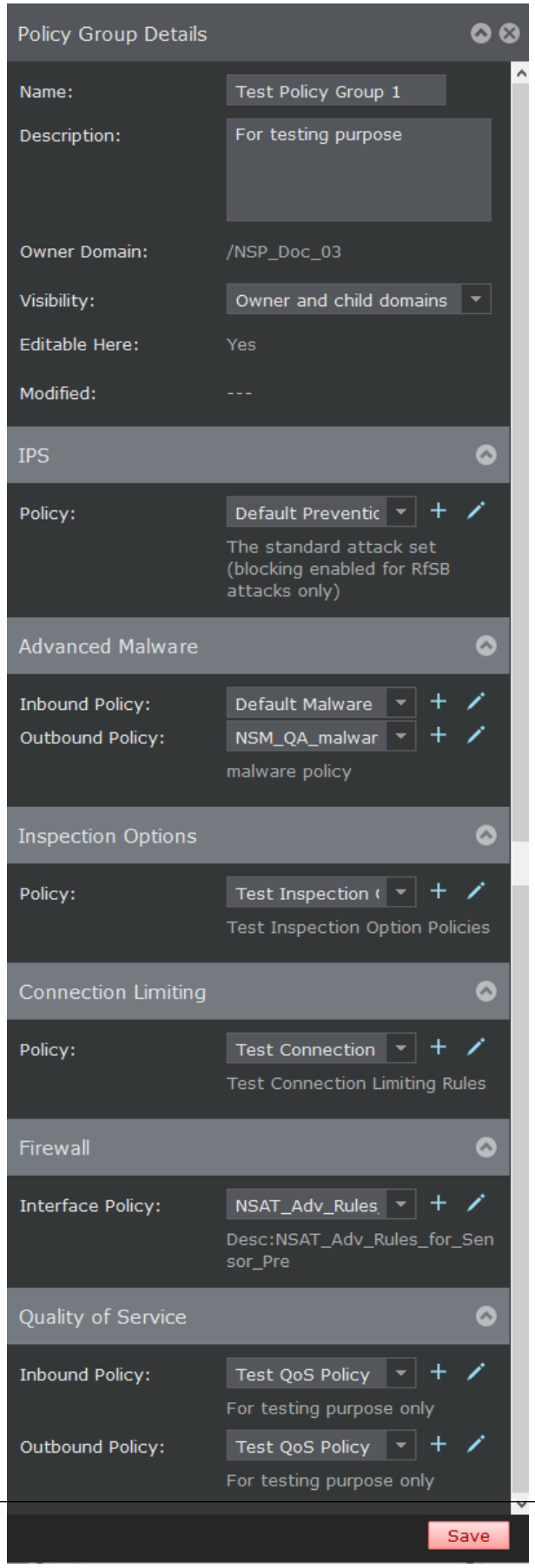
Click a column header and select the option to sort based on ascending or descending order. The options are **Sort Ascending** and **Sort Descending**.The column based on which the list is sorted is indicated in the column header by an up arrow icon for ascending order and down arrow icon for descending order.

Add a policy group

You can add a new policy group from the **Policy Group Details** panel.

1. In the **Policy** tab, select <Admin Domain Name> → Intrusion Prevention → Objects → **Policy Groups**. The **Policy Groups** page is displayed.
2. Click + in the **Policy Group** page. The **Policy Group Details** panel is displayed.

Figure 348. Policy Group Details



3. Update the following fields:

Option	Definition
Name	Type the name of the policy group.
Description	Type the description of the policy group.
Owner Domain	Displays the admin domain to which the policy belongs.
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are **Owner and child domains** and **Owner domain only**.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Modified	Displays the user who last modified the policy along with the date and time.
IPS:	
Policy	Select the IPS policy from the drop-down list. The following are the available default IPS policies: • **Default Exclude Informational** • **Default DoS and Reconnaissance Only** • **Default Prevention** • **Default Testing** • **Default Detection** Click + to add a new IPS policy. Click ✎ to edit or view the selected IPS policy.
Advanced Malware:	
Inbound Policy	Select the inbound policy from the drop-down list. Click + to add a advanced malware policy. Click ✎ to edit or view the selected advanced malware policy.
Outbound Policy	Select the outbound policy from the drop-down list. Click + to add a new advanced malware policy. Click ✎ to edit or view the selected advanced malware policy.
Inspection Options :	

Option	Definition
Policy	Select the Inspection Options policy from the drop-down list. The following are the available default inspection options policies: • **Default Client Inspection** — To inspect traffic from internal endpoints as they access the Internet. • **Default Server Inspection** — To inspect traffic to exposed Web and mail servers. • **Default Client and Server Inspection** — To inspect traffic both from internal endpoints and to exposed Web and mail servers. Click  to add a new Inspection Options policy. Click  to edit or view the selected Inspection Options policy.
Connection Limiting:	
Policy	Select the Connection Limiting policy from the drop-down list. Click  to add a new Connection Limiting policy. Click  to edit or view the selected Connection Limiting policy.
Firewall:	
Interface Policy	Select the Firewall interface policy from the drop-down list. Click  to add a new Firewall policy. Click  to edit or view the selected Firewall policy.
Quality of Service:	
Inbound Policy	Select the QoS inbound policy from the drop-down list. Click  to add a new QoS inbound policy. Click  to edit or view the selected QoS inbound policy.
Outbound Policy	Select the QoS outbound policy from the drop-down list. Click  to add a new QoS outbound policy. Click  to edit or view the selected QoS outbound policy.

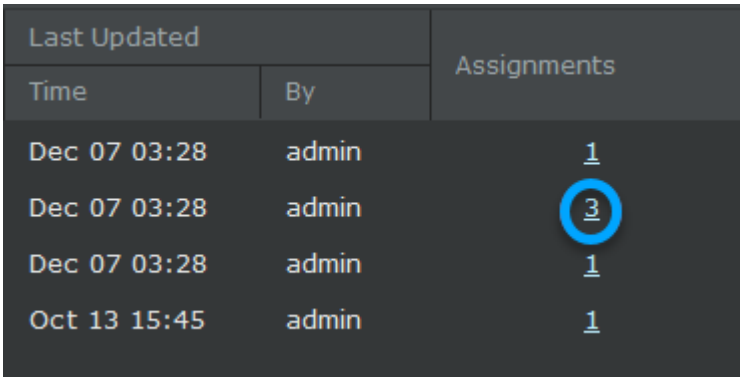
4. Click **Save** to save the policy group.

Assign policy groups

You can assign policy groups to interfaces and subinterfaces. This is especially useful when you want to define policy groups and also quickly assign it to Sensor interfaces.

1. In the **Policy** tab, select <Admin Domain Name> → Intrusion Prevention → Objects → **Policy Groups**.
2. Click the **Assignments** value of the policy group that you want to assign.

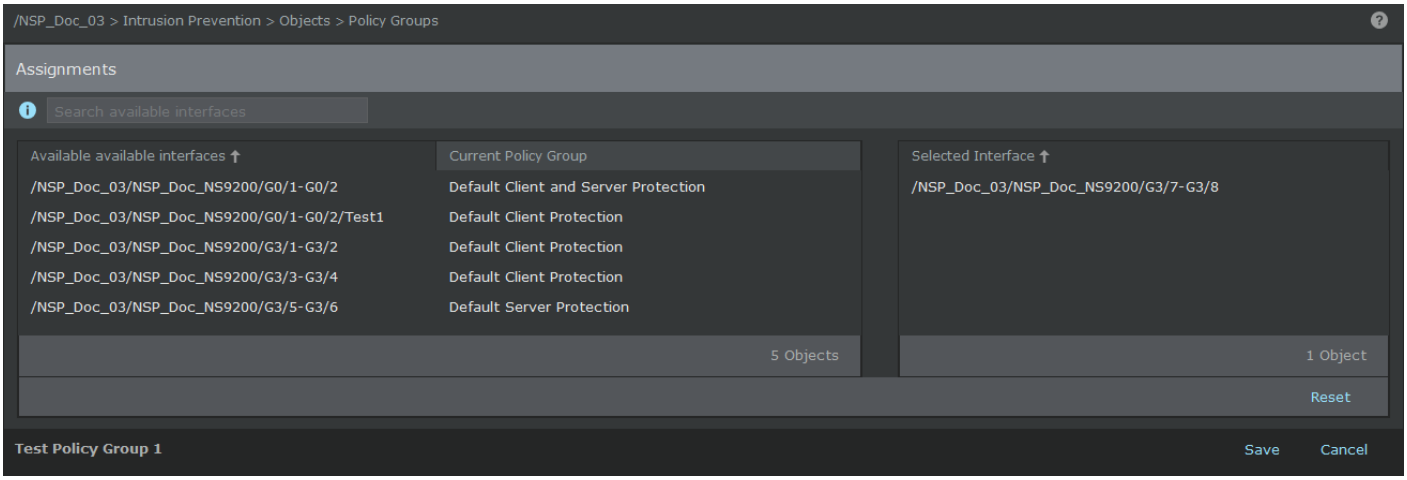
Figure 349. Assignments



The **Assignments** window for the policy group is displayed.

3. Assign the policy group to the required interfaces and subinterfaces.

Figure 350. Assignments for Policy Group



Option	Definition
Search Interfaces	To filter the list of available interfaces, enter a string that is part of the **Available Interfaces**.
Available Interfaces	Lists the interfaces and subinterfaces of the Sensors in the admin domain. The Sensor interfaces to which you have already assigned policy group are displayed under **Selected Interfaces.** Select a interface and click » to move it to **Selected Interface**.
Current Policy Group	The policy group that is currently assigned to an interface. To replace that policy with the policy that you are currently assigning, move the resource to **Selected Interface**.

Option	Definition
Selected Interface	Lists the Sensor interfaces to which you have assigned the selected policy group.
Reset	Reverts to last saved configuration.
Save	Saves the changes to the Manager database.
Cancel	Closes the **Assignments** window without saving the changes.

How to export and import policies

Trellix IPS gives you the ability to create/clone a policy on a non-production Manager server, then import the new policy/ignore rule to your production Manager. Also, you can export custom policies/filters from your Manager to a non-production machine for editing or other purposes.

- Exporting policies — Export policies from your Manager to your client.
- Importing and comparing policies — Import policies to your Manager.

Export policies

Policy export enables you to save one or more custom (created/cloned) IPS policies and reconnaissance policies from your Manager server to your client. This is effective for archiving as well as transferring a policy from a test Manager environment to your live environment. For example, you log in to your test Manager from a client and create a policy. After creation, you export the policy to your client. You then log into your live Manager from the client and import the policy for active use.

NOTE

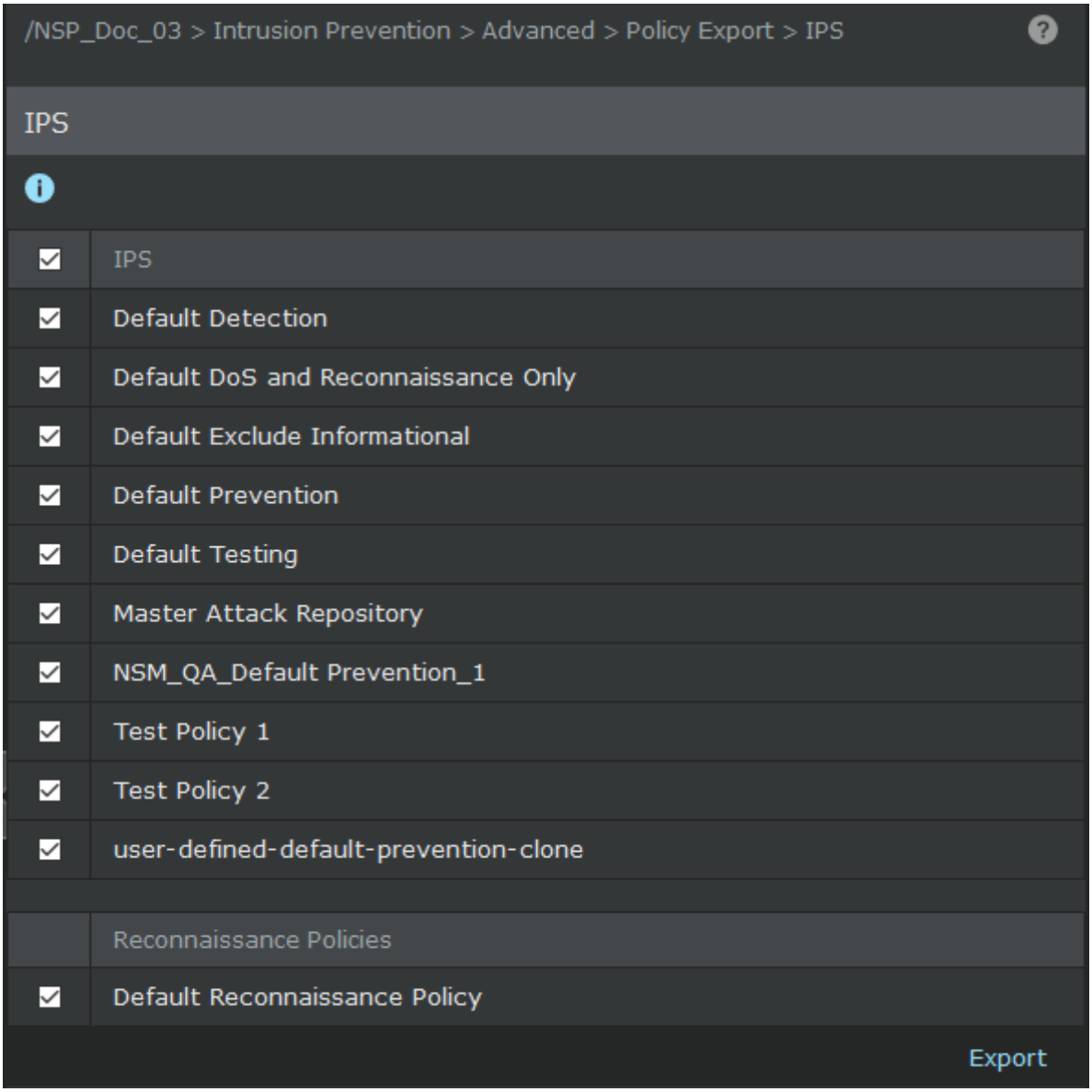
Policies of the Central Manager are not available for export.

You can export policies as an excel file using the **Save as CSV** option. This option is available only for few policies. You can also export policies from an NTBA device. For more information, see the [McAfee Network Threat Behavior Analysis Product Guide].

1. In the Manager, click **Policy** and select the required **Domain**.
2. Select Intrusion Prevention → Advanced → Policy Export → **IPS**.
3. Select the policies you want to export from the **IPS** and **Reconnaissance Policies** tables.

   Master Attack Repository corresponds to the Master Attack Repository from the root admin domain.

Figure 351. Export IPS and Reconnaissance policies



4. Click **Export** when you have selected the wanted policies.
5. Browse to the location on your client where you want to save the exported file.
6. Verify successful export by checking the destination for the exported file. The policy file is saved as an XML file, and it contains all of the policies you selected for export. Thus, if you selected two policies for export, both policies are saved in the same file.

IMPORTANT

Although this feature outputs an XML file, this file is NOT intended for reading or editing. Any manipulation of this file besides regular copying from/to different media will result in possible import failure.

How to import and compare policies?

You can compare and add a policy to the Manager from a different location on your network or from a storage device.

NOTE

Visibility rules, as they pertain to a policy being available to a child domain, apply to imported policies. Thus, for any custom (created or cloned) policy you import, if you unchecked the **Visible to Child Admin Domains** checkbox during creation, the imported policy will only be visible in the Admin Domain.

Importing and comparing policies involves the following:

- Selecting a policy to import
- Comparing policies before importing
- Completing the policy import

Import IPS policies into the Manager

Make sure the XML file containing the exported policies is not open or is being imported by some other user.

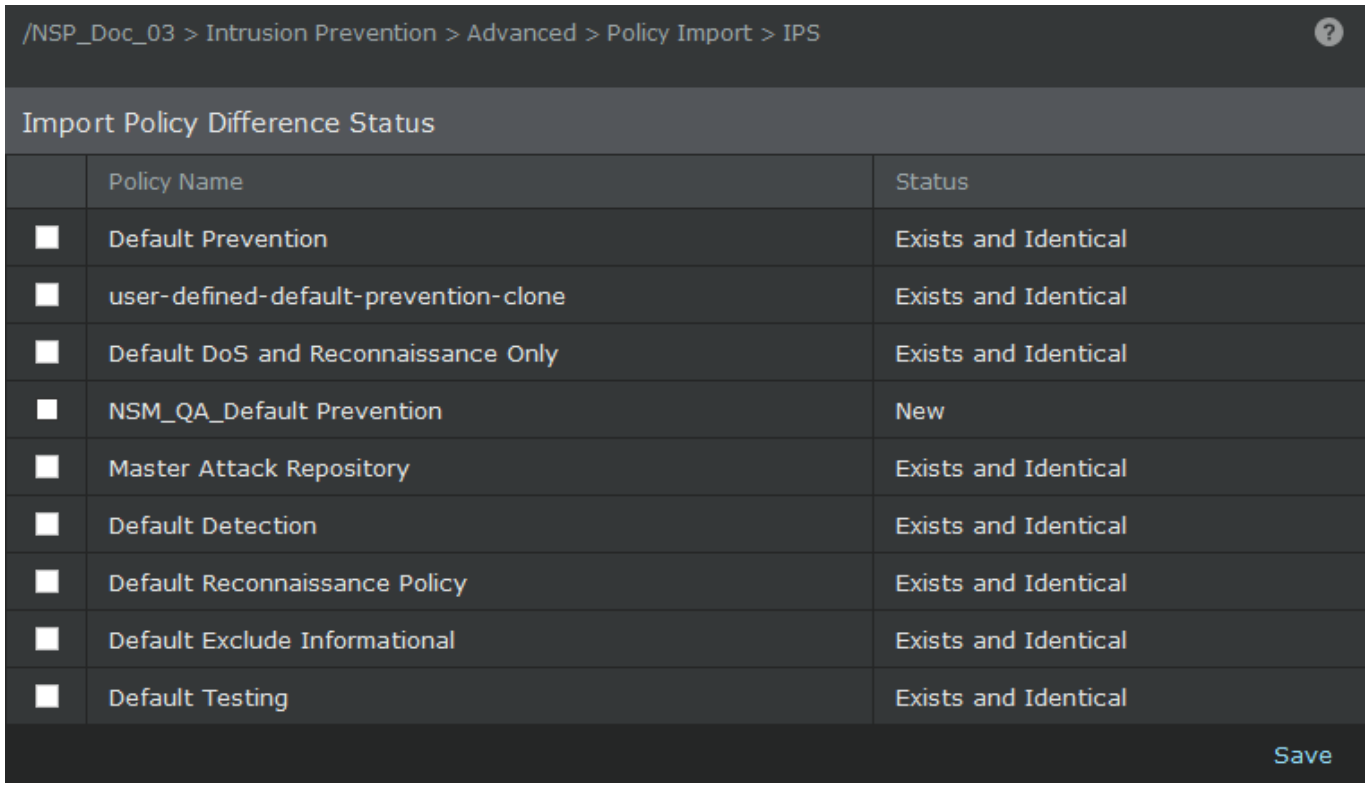
You can import the XML file containing the exported IPS and reconnaissance policies into a Manager.

Notes:

- The version of the Manager from which you exported the policies and the current version of the Manager must be an exact match.
- You should not have modified contents or the properties of the XML file.
- If the same policy exists in the Manager, you can import only if there is a difference and only at the admin domain of the existing policy. The Manager checks if the same policy exists based on the policy name mentioned inside the XML file and not based on the name of the XML file.

1. In the Manager, click **Policy** and select the required **Domain.**
2. Select Intrusion Prevention → Advanced → Policy Import → **IPS.**
3. Click **Choose File** to locate the XML file you want to import.
4. Click **Next** to download the file to the Manager.

Figure 352. View the differences and import the policy



5. Select the policies that you want to import and click **Save**.

   The imported policies are listed in the **IPS** page.

6. Click **Manager** and select the required **Domain**.
7. Navigate to Troubleshooting → **Manager Policy Cache**.
8. Click **Clear Caches**.

   You will get a confirmation massage stating **Note: Cleared policy caches from Web tier successfully.** This action reloads the policy cache and brings the imported IPS policies into effect.

> **NOTE**
>
> Alternatively, you can schedule a signature set update which will reload the cache automatically.

Deploy pending changes to a device

When you make any configuration changes or policy changes on the Manager, or a new/updated signature set is available from Trellix, you must apply these updates to the devices (such as Sensors and NTBA Appliances) in your deployment for the changes to take effect.

Note the following:

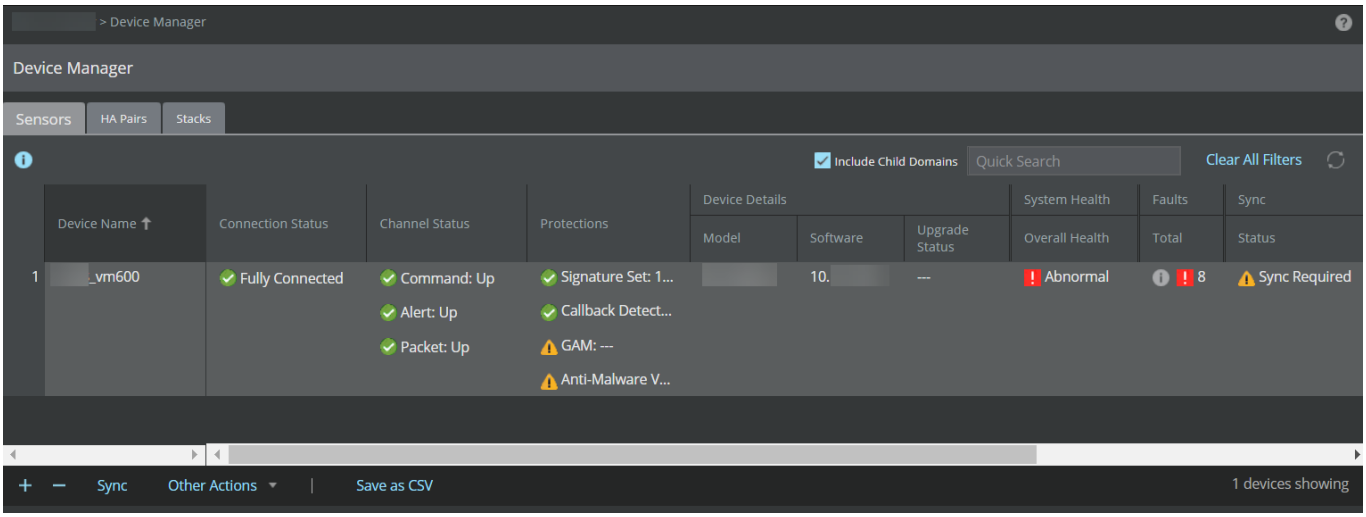
- Configuration changes such as port configuration, non-standard ports, and interface traffic types are updated regardless of the changes made to the Sensor, interface/ subinterface.
- NTBA configuration updates refer to the changes done in the several tabs of the **Devices** node.
- Policy changes are updated on the Sensor or NTBA Appliance in case of a newly applied policy, or change made to the current enforced policy.
- Signature updates contain new and/or modified signatures that can be applied to the latest attacks.
- When policy and rule updates are applied to the devices, the current traffic analysis is not impacted until the last phase of configuration updates (i.e the Manager status update is at 95%).

Refer the following steps to deploy the configuration changes to all devices in the admin domain or at a device level.

1. Go to Devices → <Admin Domain Name> → Global → **Device Manager**.

   The **Device Manager** page is displayed.

Figure 353. Device Manager

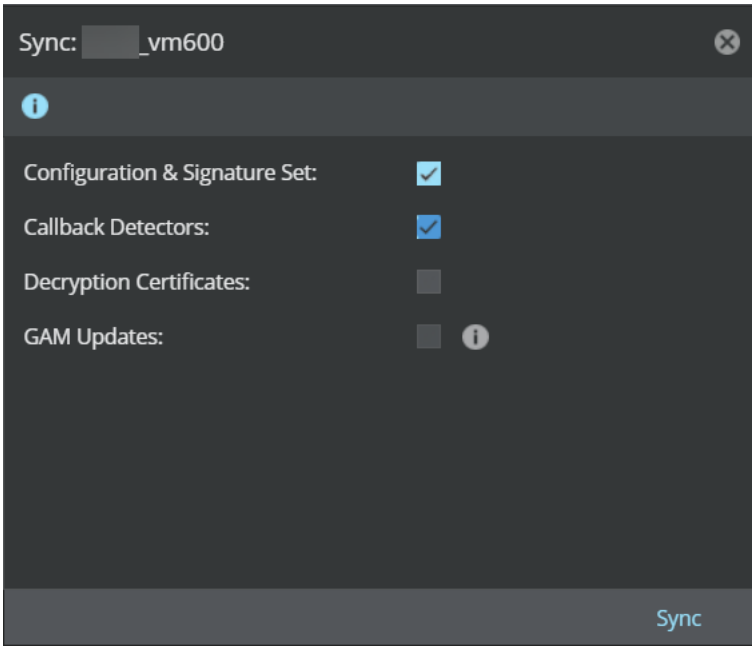


2. Click **Sensors** tab. Select the required Sensor from the list.
3. Select **Sync**.

   The **Sync: <Device Name>** window is displayed.
4. Select the required configurations and click **Sync**.

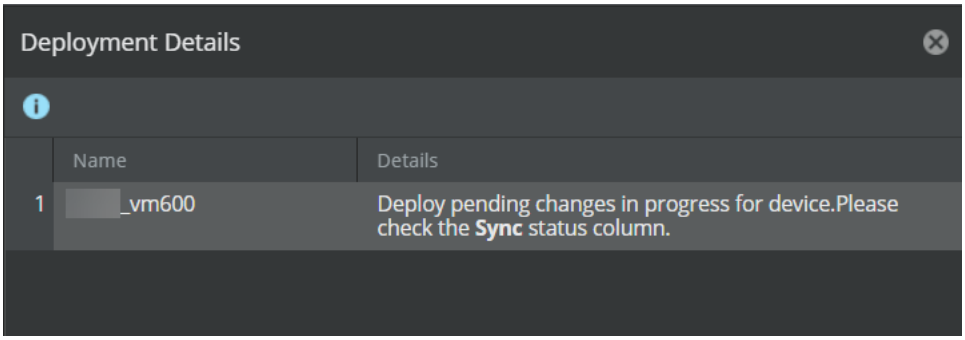
> **NOTE**
>
> The Manager provides an option to concurrently deploy pending changes for multiple Sensors. When you select multiple Sensors for deployment, the **Bulk Sync** window is displayed and enables all check-boxes by default. Select the options you wish to deploy and click **Sync**.

Figure 354. Sync: <Device Name> window



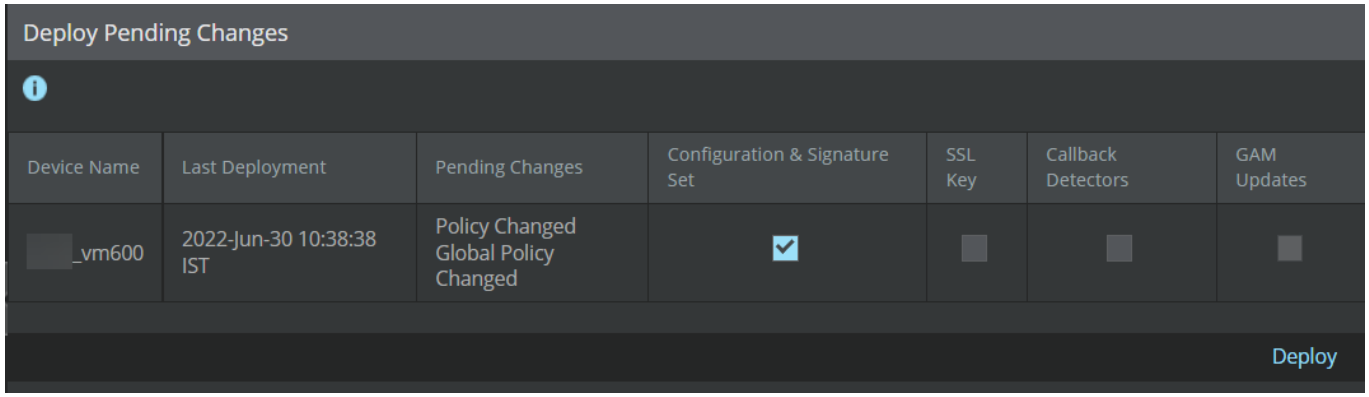
A **Deployment Details** dialog box is displayed. Click .

Figure 355. Deployment Details



You can also deploy the changes to a specific device from **Devices <Admin Domain Name> Devices <Device Name> Deploy Pending Changes**. Select the required configurations and click **Deploy**.

Figure 356. Device-level deploy pending changes



The following status can be viewed from **Sync** section of **Status** column:

Status	Description
Synchronized	Indicates that no pending changes are required.
Sync in progress	Indicates when the deployment is in progress.
Sync required	Indicates if any pending changes are required.
---	Indicates that there is no trust established between the Sensor and the Manager.

5. Click **Export Sync File** under **Other Actions** to view and export the deployment changes file to indirect mode Sensors. The changes can then be deployed to the Sensors manually using the CLI command window.
6. Click to refresh the page and the status of the deployment.

Defining and using user-customizable blocking strategy to make self-adaptable IPS policies

Trellix IPS Manager offers a simplified and automated IPS policy management mechanism for blocking attacks. It enables the users to define and store one or more customizable rules for blocking attacks as per their network requirements during attack set profile configuration. When the same attack set profile is used in the IPS policy, the Manager automatically correlates the blocking criteria set by the user with the new and existing attack signatures. This enables IPS policies to automatically block attacks that match the user's blocking strategy and makes them self-adaptable to any new signature set release.

The automated blocking mechanism by IPS policies as per user-defined blocking strategy helps in the following ways:

- It minimizes the need to manually edit the IPS policies for the blocking of attacks in which one had to manually look for attack definitions that match their blocking criteria, bulk edit them, and set the **Block** field under **Sensor Actions** to **Enable Blocking**.
- As the attack set profile mapped to the IPS policy stores the user-defined blocking criteria for attacks, it is automatically applied to any new/modified attack definitions included in any signature set update that match the set criteria. This eliminates the requirement of repeated manual intervention and provides user-customizable and automated attack blocking mechanism that helps users maintain their network security posture.

IMPORTANT

Automating the blocking of attacks as per user-defined blocking strategy is available in Manager and Central Manager version **11.1 Update 3** and above.

How to automate blocking of attacks based on user-defined blocking strategy

While creating or editing an attack set profile, you can create one or more rules with the categories, subcategories and minimum severity level of attacks that you want to be blocked by the Sensor as per the blocking strategy that suits your network environment and use the same profile during any IPS policy configuration. You can then enforce the IPS policy at the interface and sub-interface level for the required Sensor(s) and deploy these configuration changes to the required devices in the admin domain level or at a device level. When the policy and rule updates are applied to the required Sensor(s), those automatically block all attacks that match your blocking criteria as set in the attack set profile and send an alert to the Manager.

Automating the process of blocking attacks in the Manager and Sensor involves the following steps:

- Creating or editing an attack set profile that includes rules for blocking attacks specific to any network environment
- Creating or editing an IPS Policy that uses the attack set profile created for blocking specific attacks.
- Assigning the IPS policy to specific interfaces and sub-interfaces of the required Sensor(s)
- Deploying the configuration changes to the required Sensors

Configuring attack set profile that include user-defined rules for blocking attacks

Perform the following steps to include the rules for blocking specific attacks as per your network requirements while creating or editing an attack set profile.

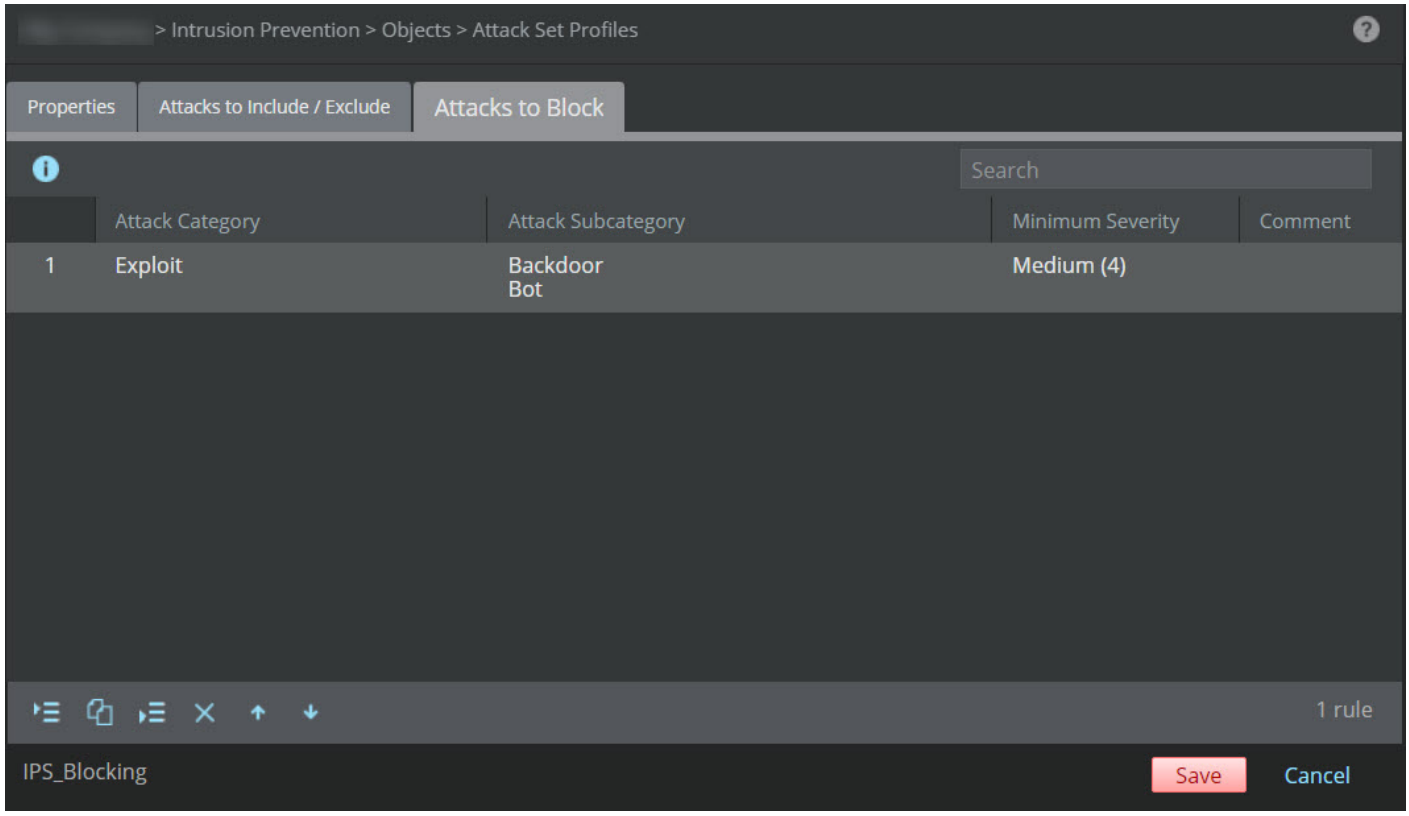
1. In the Manager, click **Policy** and select the required **Domain**.
2. Navigate to Intrusion Prevention → Objects → **Attack Set Profiles** page.

   The **Attack Set Profiles** page is displayed that includes all pre-configured and user-configured attack set profiles.
3. Click + icon if you want to create a new attack set profile with your specific blocking strategy. If you want to add your blocking criteria to an existing attack set profile, you may do so by double-clicking that specific profile.

   NOTE

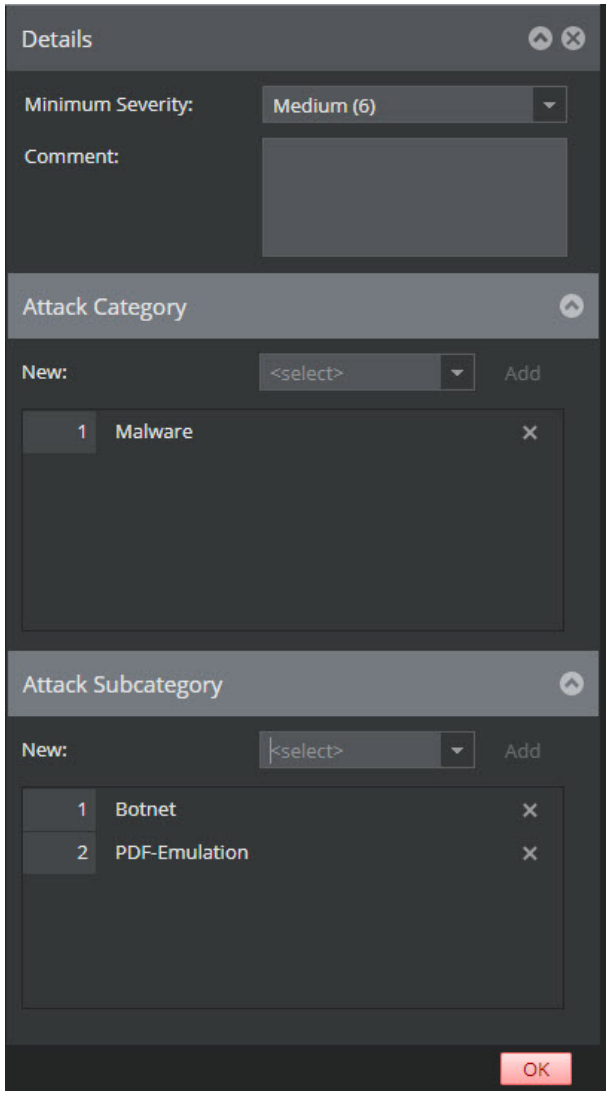
   You can create rule for blocking in custom attack set profiles only, as the default or preconfigured attack set profiles are read-only.
4. Enter appropriate details on the **Properties** tab and configure **Include** and **Exclude** rules on the **Attacks to Include/Exclude** tab as per your network requirement.
5. Once the rules to include and exclude attacks have been added, click **Next** to save the changes made on the **Attacks to Include/Exclude** tab and go to the **Attacks to Block** tab. This tab helps you define rules that determine whether the attack definitions, that are to be included in the IPS policy as per the configured **Include** rules on the **Attacks to Include/Exclude** tab, are automatically set to be blocked in the corresponding IPS policy.

Figure 357. Attacks to Block tab as displayed during attack set profile configuration



6. On the **Attacks to Block** tab, click the appropriate button to insert a new rule. You can insert a new rule by clicking either or icon. The **Details** panel is displayed.

Figure 358. Details panel on Attacks to Block tab



7. Select the appropriate options in the **Details** panel:

Option	Definition
Minimum Severity	Select the minimum severity level from the drop-down list. The default value selected while creating a rule is set to **High (9)**. **IMPORTANT** Rules created for automatic blocking of attacks are not applicable to **Informational** and **Low** severity attacks.
Comment	Enter additional comments, if any.

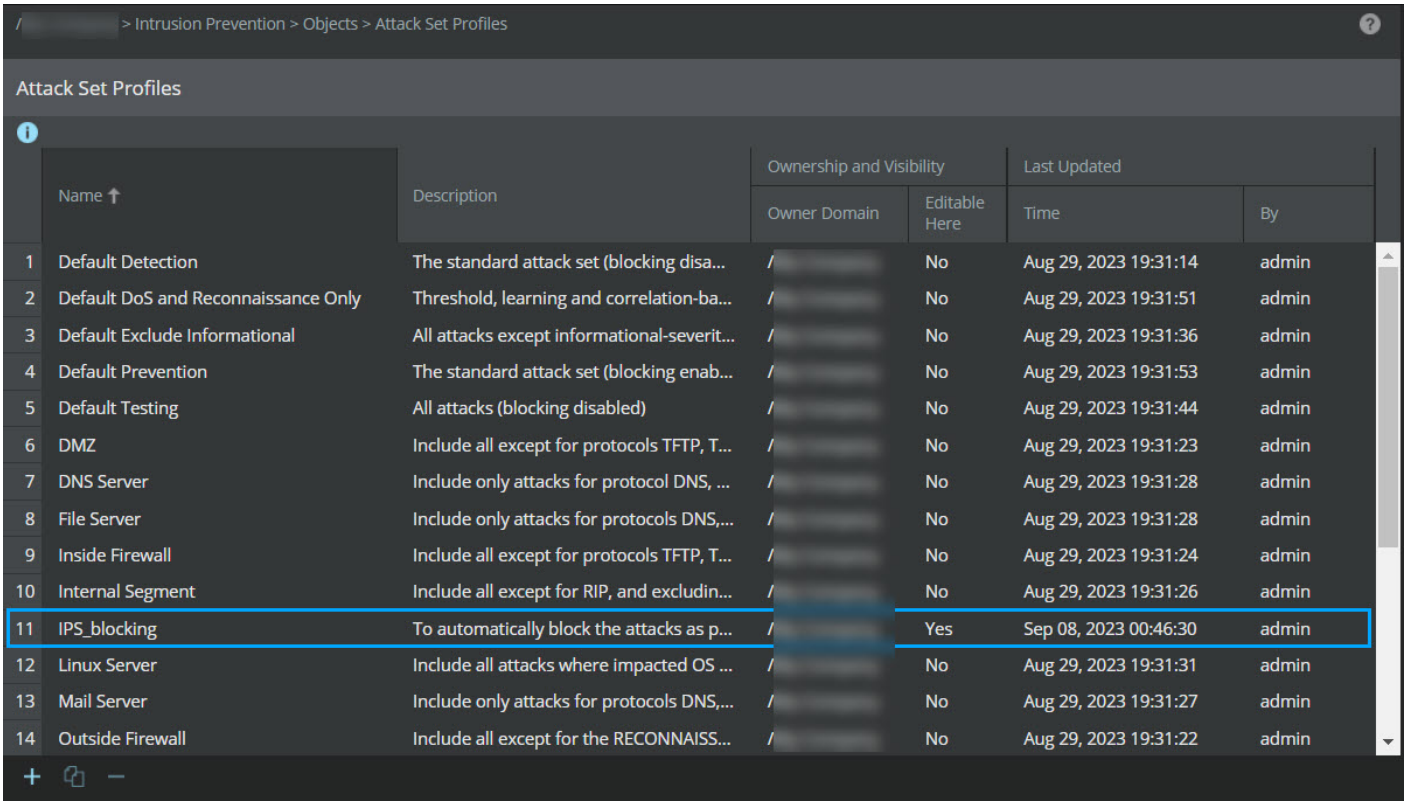
Option	Definition
Attack Category	Select one or more attack categories as per your requirement from the drop-down-list. Click the **Add** button to add the attack category to the list. Click ✕ to remove the item from the list.
Attack Subcategory	Select one or more attack subcategories for the attack category selected. Click the **Add** button to add any subcategory to the list. Click ✕ to remove the item from the list.

NOTE

For more information on the configuration options available on the above-mentioned tabs during attack set profile creation, refer to the section Create an attack set profile (page 798).

8. Click **OK** to confirm the configuration changes and **Save** to save the attack set profile configuration. Your new attack set profile is listed in the **Attack Set Profiles** page.

Figure 359. Attack set profile configured with the user-defined blocking criteria



	Name	Description	Ownership and Visibility		Last Updated	
			Owner Domain	Editable Here	Time	By
1	Default Detection	The standard attack set (blocking disa...	/	No	Aug 29, 2023 19:31:14	admin
2	Default DoS and Reconnaissance Only	Threshold, learning and correlation-ba...	/	No	Aug 29, 2023 19:31:51	admin
3	Default Exclude Informational	All attacks except informational-severit...	/	No	Aug 29, 2023 19:31:36	admin
4	Default Prevention	The standard attack set (blocking enab...	/	No	Aug 29, 2023 19:31:53	admin
5	Default Testing	All attacks (blocking disabled)	/	No	Aug 29, 2023 19:31:44	admin
6	DMZ	Include all except for protocols TFTP, T...	/	No	Aug 29, 2023 19:31:23	admin
7	DNS Server	Include only attacks for protocol DNS, ...	/	No	Aug 29, 2023 19:31:28	admin
8	File Server	Include only attacks for protocols DNS,...	/	No	Aug 29, 2023 19:31:28	admin
9	Inside Firewall	Include all except for protocols TFTP, T...	/	No	Aug 29, 2023 19:31:24	admin
10	Internal Segment	Include all except for RIP, and excludin...	/	No	Aug 29, 2023 19:31:26	admin
11	IPS_blocking	To automatically block the attacks as p...	/	Yes	Sep 08, 2023 00:46:30	admin
12	Linux Server	Include all attacks where impacted OS ...	/	No	Aug 29, 2023 19:31:31	admin
13	Mail Server	Include only attacks for protocols DNS,...	/	No	Aug 29, 2023 19:31:27	admin
14	Outside Firewall	Include all except for the RECONNAISS...	/	No	Aug 29, 2023 19:31:22	admin

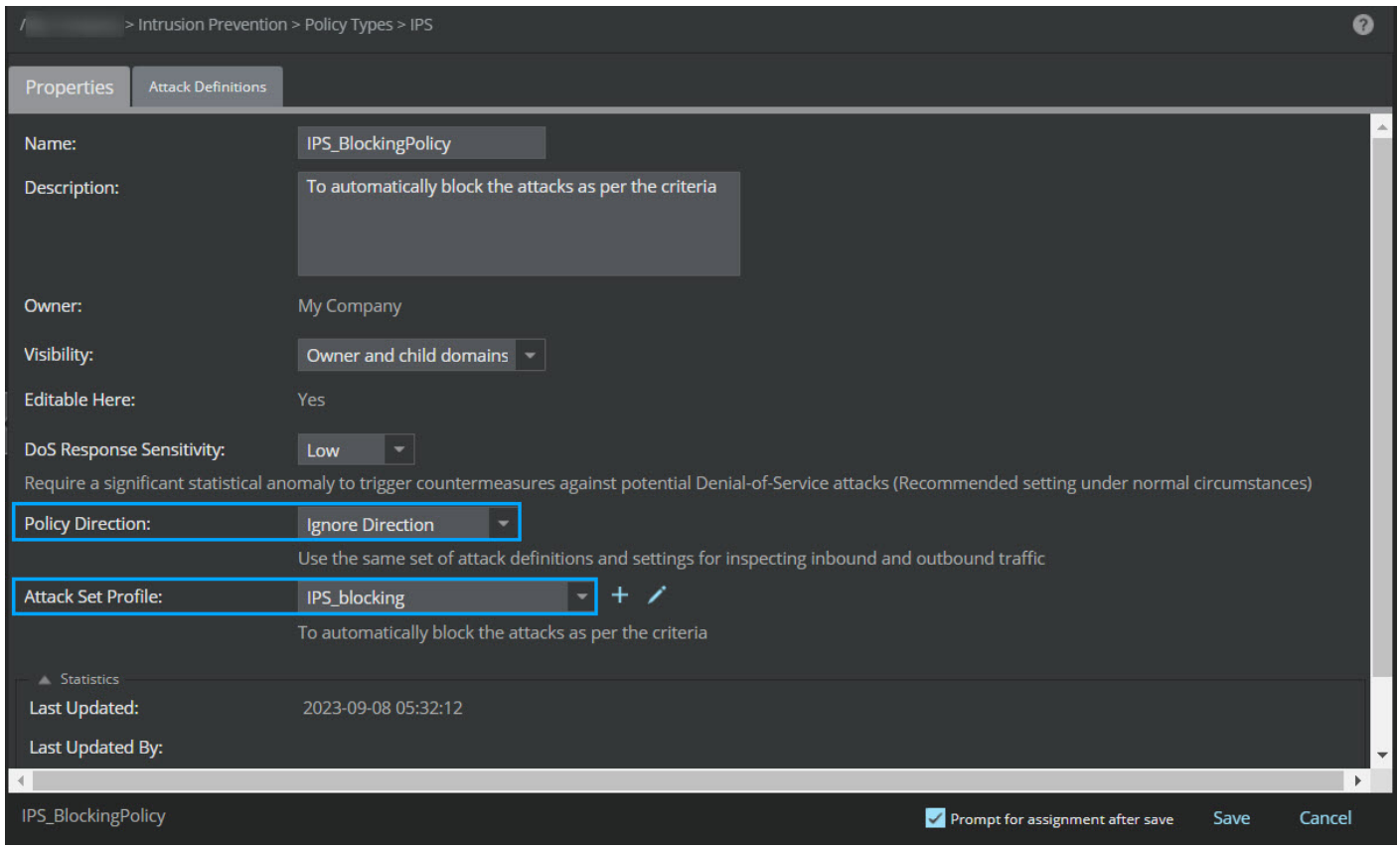
Configuring an IPS Policy that uses the attack set profile created for automatic blocking of specific attacks

Once the attack set profile, which includes rules for automatic blocking of specific attacks, is configured, you can use that profile during the IPS policy configuration. To do so, perform the following steps.

1. In the Manager, click **Policy** and select the required **Domain.**

2. Navigate to the Intrusion Prevention → Policy Types → **IPS** page.
3. Click + icon, if you want to add a new IPS policy. If you want to edit an existing IPS policy, you may do so by double-clicking it.
4. On the **Properties** tab that opens, choose the **Policy Direction** as per your requirements and map the attack set profile that contains the rules defining your blocking criteria in the **Attack Set Profile** field.

Figure 360. Using the selected attack set profile in the IPS policy

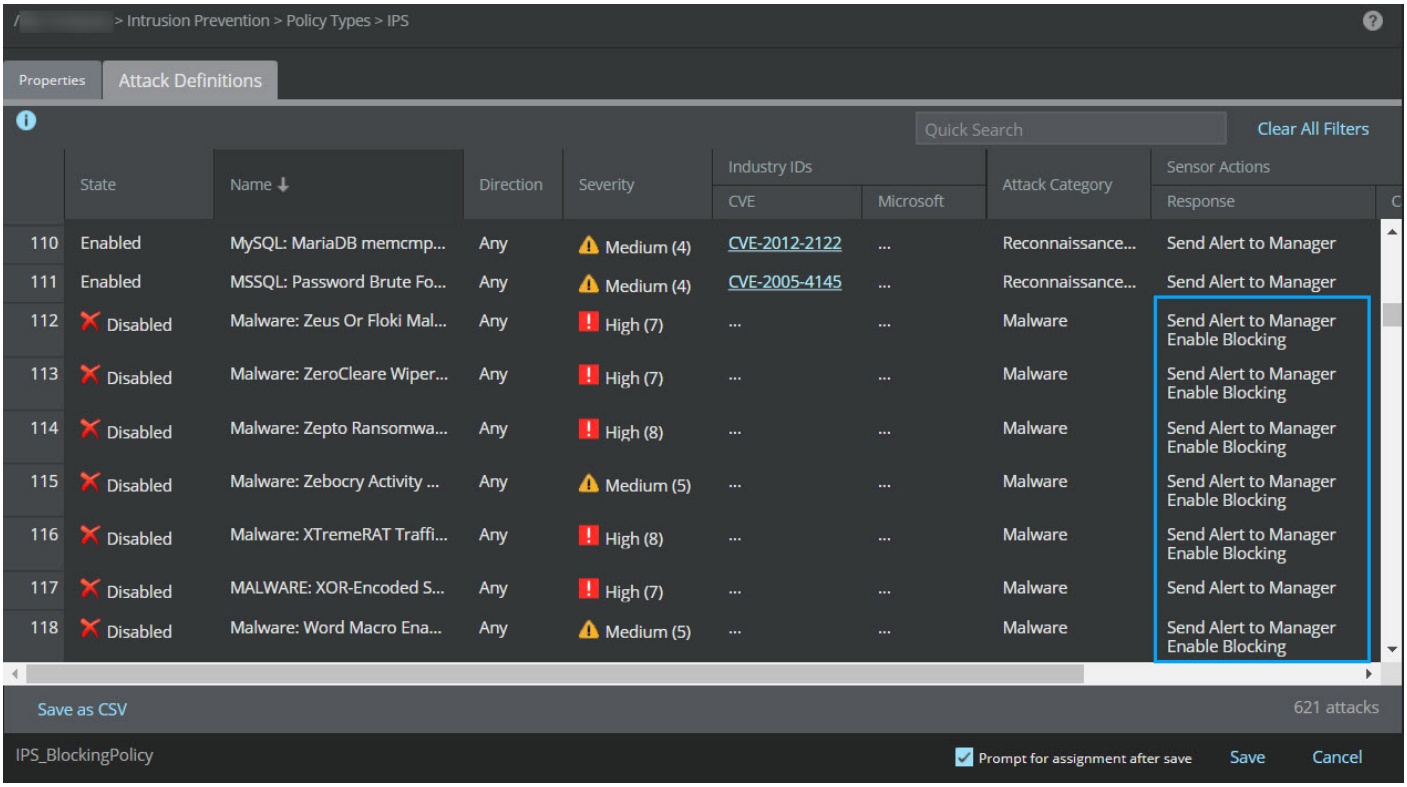


NOTE

When you select the **Policy Direction** option as **Consider Direction**, you can select one attack set profile for inbound traffic and another for outbound traffic. Separate attack set profiles for inbound and outbound can be applied to Sensors in SPAN or tap mode. If the Sensor is unable to determine the direction of the traffic, it enforces the rules and configuration updates of the inbound attack set profile.

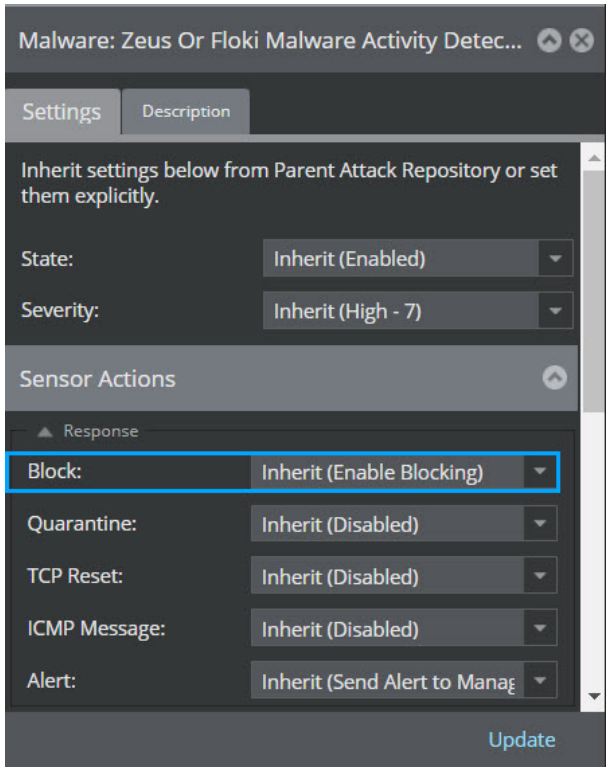
5. Click **Evaluate Attack Set Profiles**. This redirects you to the **Attack Definitions** tab which displays all attack definitions that match the Include rule criteria in the attack set profile. For attacks that fall under the blocking criteria in the attack set profile and are set to be automatically blocked, you would notice the **Response** column under **Sensor Actions** showing the alert messages **Send Alert to Manager Enable Blocking**.

Figure 361. Attack Definitions tab showing the attacks automatically set to blocking



6. Double-clicking any attack definition marked to be automatically blocked as per the attack set profile configuration shows the Block field under **Sensor Actions - Response** to be **Inherit (Enable Blocking)**. This Sensor response action is only visible for attacks that are set to be automatically blocked in the selected attack set profile.

Figure 362. Sensor response action for block is shown as Inherit (Enable Blocking)



IMPORTANT

If you wish, you can override the automatic blocking behavior of any attack by manually setting the Sensor blocking action during IPS policy configuration. Sensor response actions customized in the IPS policy always takes precedence over automatic blocking of attacks criteria set in the **Attack Set Profiles** page.

7. Review the attack details as shown on the **Attack Definitions** tab and click **Save** to save the IPS policy.

   For more information on how to add/edit an IPS policy or customize it, refer to the section Manage IPS policies (page 808).

Assigning the IPS policy to interfaces and subinterfaces

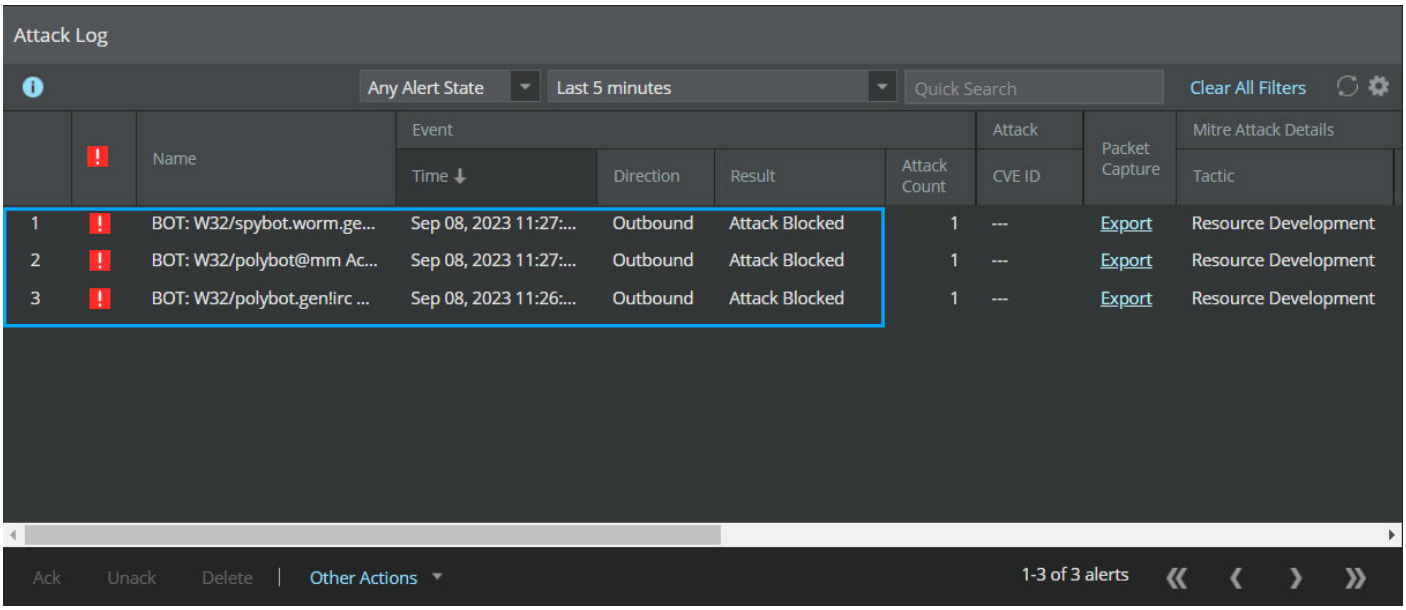
Once the desired IPS policy is mapped to the attack set profile that includes the rules for attack blocking, you can assign that policy to the specific interfaces and subinterfaces of the required Sensors. For more information, refer to the section Assign IPS policy to interfaces and subinterfaces (page 851).

Deploying configuration changes to the required Sensors

Post the assignment of the policy to the required interfaces and subinterfaces, perform a configuration update for the corresponding Sensors to enforce the policy. For more information, refer to the section Deploy pending changes to a device (page 873).

Post the successful assignment of the IPS policy, the concerned Sensor detects attacks and blocks them if it matches the blocking criteria of the attack set profile. Along with the blocking action, it also generates an alert which is sent to the Manager and can be viewed using the Analysis → <Admin Domain Name> → **Attack Log** page.

Figure 363. Attack Log showing attacks that have been blocked as per the user-defined blocking criteria



Automated blocking of attacks and Master Attack Repository

While setting up blocking criteria in attack set profile for the attacks to be automatically blocked, remember the following:

If an attack is set to be automatically blocked as per the blocking criteria set in attack set profile and the blocking action for that attack is disabled manually in **Master Attack Repository**, the configuration set for blocking the attack would take precedence over the **Master Attack Repository**. This means that the blocking action for that attack would be set to **Inherit (Enable Blocking)** in **Sensor Actions - Response** segment in IPS policy.

IMPORTANT

If you wish, you can override the automatic blocking behavior of any attack by manually setting the Sensor blocking action during IPS policy configuration. Sensor response actions customized in the IPS policy always takes precedence over automatic blocking of attacks criteria set in the **Attack Set Profiles** page.

Automated blocking of attacks: Exceptions

While this feature helps automating the process of blocking of specific attacks in your network environment, the underlying mechanism has been carefully designed to avoid blocking of false-positives which may result in network disruptions. Some of the exceptions to these rules for blocking include the following:

- There are certain attacks which should never be blocked the user, irrespective of their network infrastructure and requirements. Blocking these attacks can cause anomaly and unexpected network outages. Trellix Advanced Research Center provides guidelines on the attack IDs and criteria defining the attacks which should not be blocked. The blocking mechanisms in the **Attack Set Profiles** page as well as **IPS** page of the Manager are built following these guidelines so as to prevent the accidental blocking of such attacks.
- Rules created for automatic blocking of attacks are not applicable to **Informational** and **Low** severity attacks.

- Rules created on the **Attacks to Block** tab during attack set profile configuration do not control the automatic blocking of DoS threshold, DoS learning and Correlation-based Reconnaissance attacks.
- The default or preconfigured attack set profiles are read-only. So, these rules for blocking can be created for custom attack set profiles only.

Response management

When a Sensor detects activity to be in violation of a configured policy, a preset response from the Sensor is integral to the protection or prevention process. Proper configuration of responses is crucial to maintaining effective protection. Critical attacks like buffer overflows and DoS attacks require responses in real time, while scans and probes can be logged and researched to determine compromise potential and the source of the attack. Developing a system of actions, alerts, and logs based on specific attacks or attack parameters (such as severity) is recommended for effective network security.

For example, since Trellix IPS can be customized to protect any zone in a network, knowing what needs to be protected can help to determine the response type. If monitoring outside of the firewall in Inline Mode, preventing DoS attacks and attacks against the firewall is crucial. Most other suspicious traffic intended for the internal network, including scans and low-impact well-known exploits, are best logged and analyzed as the impact is not immediate and a better understanding of the potential attack purpose can be determined. Thus, if you are monitoring outside of a firewall in Inline Mode, it is important to not set the policies and responses so fine that they disrupt the flow of traffic and slow down the system; rather, prevent the crippling traffic from disrupting your network.

NOTE

Setting a response type during policy configuration is critical for an effective intrusion management system.

Response types

The response types offered by Sensors and Manager are as follows:

Sensor response actions

Sensor actions are responses your Sensor enacts or sends through the network to prevent or deter further attacks.

- **Drop further packets** (Inline mode only) — Dropping the specific attack packets is a key advantage of inline mode. When detecting inline (real time), the packets that trigger signatures and (optionally) all subsequent packets related to that connection can be dropped before they reach the intended target system. This capability provides true "intrusion prevention." This action is also known as "blocking."
- **Send an alert** (default) — When traffic violates a Sensor policy, an alert is generated and sent to the Manager to be viewed using the Attack Log. Alerts can be examined for content and sorted by key fields, such as severity level, attack category, and so on. For more information on the Attack Log, see the [Trellix Intrusion Prevention System Product Guide].
- **Quarantine**— Sensor performs the quarantine of infected host, by isolating the host for a specified period.
- **Packet log** — Sends a log or copy of the packet information to the Manager database; this information acts as a record of the actual flow of traffic that triggered the attack and can be used for detailed packet analysis. When the data is viewed in the **Attack Log**, the data is converted to libpcap format for presentation. Tools like Wireshark can be used to examine

the packet log data for more detailed analysis of attack packet data. In the IPS Policy Editor/ Master Attack Repository, the user can specify how many packets should be logged or for what duration. You can also choose to encrypt the packet log channel via SSL to protect the packet log data.

- **TCP reset** — For TCP connections only. TCP uses the RST (Reset) bit in the TCP header to reset a TCP connection. Resets are sent in response to a connection carrying traffic which violates the security policy of the domain. The user can configure reset packets to be sent to the source and/or destination IP address.
- **Ignore Rules** — Creating ignore rule enables you to filter out alerts based on the source or the destination of the security event. For example, if you know that your IT department executes vulnerability scans from a particular IP address, you can filter events originating from that address. The ignore rule editor provides a convenient interface for creating ignore rules.
- **ICMP host unreachable** — ICMP Host Unreachable packets can be sent in response to the source of UDP or ICMP attacks.

Recommended for SmartBlocking (RfSB)

Trellix IPS attack definitions contain an attribute that indicates whether an attack is considered *Recommended for Blocking (RFB)* by Trellix. A flag may be set in any cloned policy to block on the RfSB attacks within the policy.

The attack signatures within a single attack definition can be composed of several different attacks. Each attack has a different Benign Trigger Probability (BTP) value (ranging from 0 to 7). The attack definition can contain a very specific signature (lower BTP) and a more generic signature (higher BTP). The attack confidence values are inversely related to the Benign Trigger Probability (BTP) values of attack signatures. For example, a BTP value of 2 indicates that there is low possibility of the attack being a false-positive.

If you manually select **Enable Blocking** or **Inherit (Enable Blocking)** is selected by default, the Sensor blocks traffic that matches any signature in the attack, regardless of the BTP value of the signature.

If you select **Enable SmartBlocking**, the Sensor blocks traffic only when the traffic has at least one signature, with BTP value equal to or lower than 2.

You can additionally enable **GTI IP Reputation** (evaluates the risk of the IP address and port combined) to be used as a factor while Smart Blocking. When this option is enabled, the Sensor considers the GTI reputation of the source while making its blocking decision. If the GTI reputation of the source IP or port is **High Risk**, the Sensor effectively treats the matched signature as if its BTP was one level lower than it actually is. In such a case, the Sensor treats a matched signature that has a BTP value of 3 as if it had a BTP value of 2, and then evaluate blocking against the threshold. A source with a Minimal Risk IP or port will have no effect on the evaluation.

Manager response actions

There are three notification responses that can be configured to alert users of malicious activity: email, pager, or script notification. These responses are sent directly to admins based on either a configured severity level—represented as Low, Medium, or High severity—or based on the occurrence of a particular attack, regardless of the severity level.

Simulated Blocking

Simulated Blocking enables you to put the Sensor in a non-blocking mode whereby exploit attacks are not blocked even if the applied IPS policy is configured to do so. Alerts are still raised based on the configured policy. When Simulated Blocking

is enabled, response actions that affect the flow of traffic, such as blocking, sending a TCP reset, and sending an ICMP host unreachable message, are not applied. This feature does not affect the Quarantine actions.

This feature allows an IPS *sanity check* where you get to know the specific attacks that would have hit a blocking rule, that is, which attacks would be blocked during normal operation without actually blocking them (the alerts explicitly mention that blocking has been simulated). You can also use this feature to temporarily disable blocking for troubleshooting.

NOTE

Simulated blocking applies to signature-based attack definitions only. Denial-of-Service and reconnaissance attacks will continue to activate response actions if configured to do so.

Simulated Blocking does not change the behavior of certain features of the Sensor. Further, these features will need to be disabled individually if required. The following list includes all such features:

- DoS blocking
- IP Reputation (formerly TrustedSource)
- Firewall drop action
- Host quarantine
- IP sanity errors checks

You may choose to enable Simulated Blocking and configure the response action in your policy as a TCP Reset or ICMP Unreachable. In such instances, the Sensor does not carry out a designated response action; the **Result** column in the Attack Log displays one of the standard attack results, such as **Attack Failed**, **Attack Successful**, **Attack Blocked**, **Inconclusive**, or **n/a**. These attack result statuses are identical to those that are displayed when Simulated Blocking is disabled.

NOTE

Disable Simulated Blocking before performing an upgrade using the CLI. This allows data in the Manager to synchronize with the Sensor immediately after the upgrade. If not disabled, the first sigfile push will disable this option (by default it is disabled at device level).

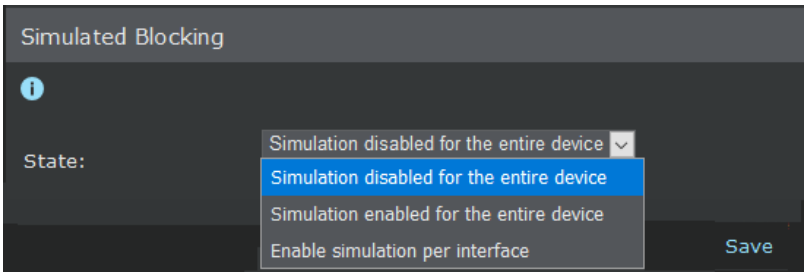
Configure Simulated Blocking at the interface level

You can configure Simulated Blocking at the interface level.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Simulated Blocking**.

   By default, **Simulated Blocking** is disabled for the entire device.

Figure 364. Simulated Blocking dialog



6. Select **Simulated Blocking** for inbound/outbound traffic.

> **NOTE**
>
> Simulated Blocking is not supported separately for the traffic directions. If one is configured (enabled/disabled), the other is also configured similarly.

7. From the **State** drop-down list, make a selection.
   - To enable Simulated Blocking device wide, select **Simulation enabled for the entire device**.
   - To disable Simulated Blocking device wide, select **Simulation disabled for the entire device**.
   - To control Simulated Blocking per VIDS, select **Enable simulation per interface**.
8. Click **Save**.

   The device level settings override the interface level settings, that is, you cannot configure Simulated Blocking at the interface level if it is configured at the device level.

Packet logging

Logging attack packets for analysis is an effective means of preparing for future attacks. A packet log is created by a Sensor capturing the network traffic around an offending transmission. An expert in protocol analysis can use the log information to determine what caused the alert and what can be done to prevent future alerts of the same nature. Packet logs are retrieved from the database via the Attack Log and can be opened and examined using a program called Wireshark. By default, UDP and TCP protocol attacks generate a packet log for the attack plus the previous 128 bytes in the flow. You can configure to enable previous 256 bytes logging using the Sensor CLI. For more information, see the [CLI commands] section.

> **TIP**
>
> Trellix recommends using Wireshark (formerly known as Ethereal) for packet log viewing. Wireshark is a network protocol analyzer for Unix and Windows servers that enables you to examine the data captured by your Sensor. For information on downloading and use of Wireshark, go to www.wireshark.org.

Alert notification options

The Manager can send alert information to third-party repositories, such as SNMP servers and syslog servers. Further, you can configure your Sensor to forward syslog notifications directly to a syslog server, thereby ensuring that the Sensor forwards alerts to a server other than that assigned to the Manager.

In addition to SNMP and syslog notifications, the Manager can also be configured to notify you through email, pager, or script of detected attacks.

For the alert notifications for the Sensor and the NTBA Appliance, select Manager → <Admin Domain Name> → Setup → Notification → **(IPS/NTBA) Events**.

Alert notifications are forwarded to syslog servers based on the configuration. Within the configuration, settings notification destination form only one aspect. The Manager and Sensor send notifications depending on the attack, the attack severity, or both.

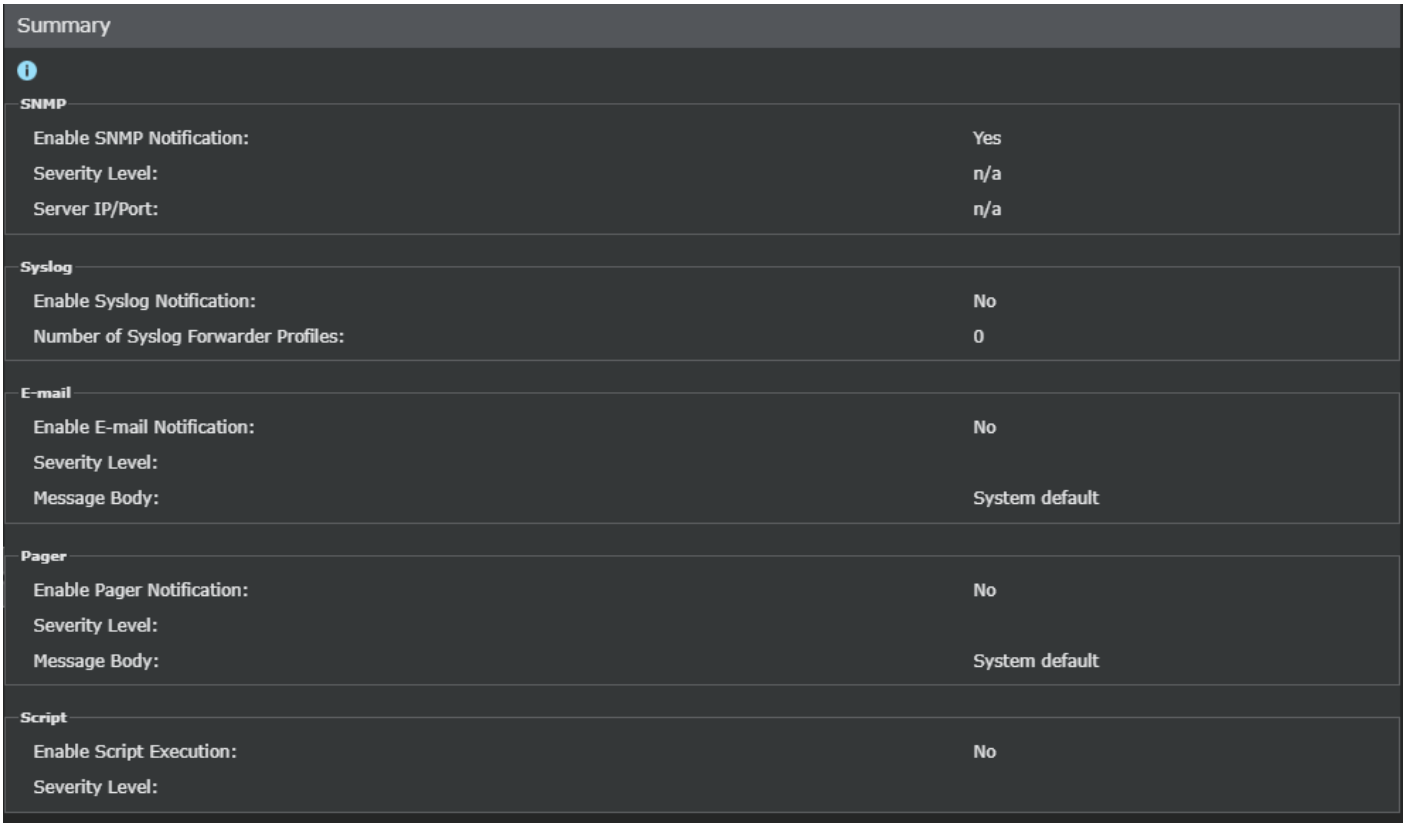
TIP

The Manager forwards all the audit records to a syslog server over a TLS secured connection in real-time.

How to view alert notification details

The **Summary** page for alert notification (Manager → <Admin Domain Name> → Setup → Notification → (IPS/NTBA) Events → **Summary**) displays a summary of configured alert notification settings. The summary displays your configuration settings made for each individual notification option.

Figure 365. Summary page



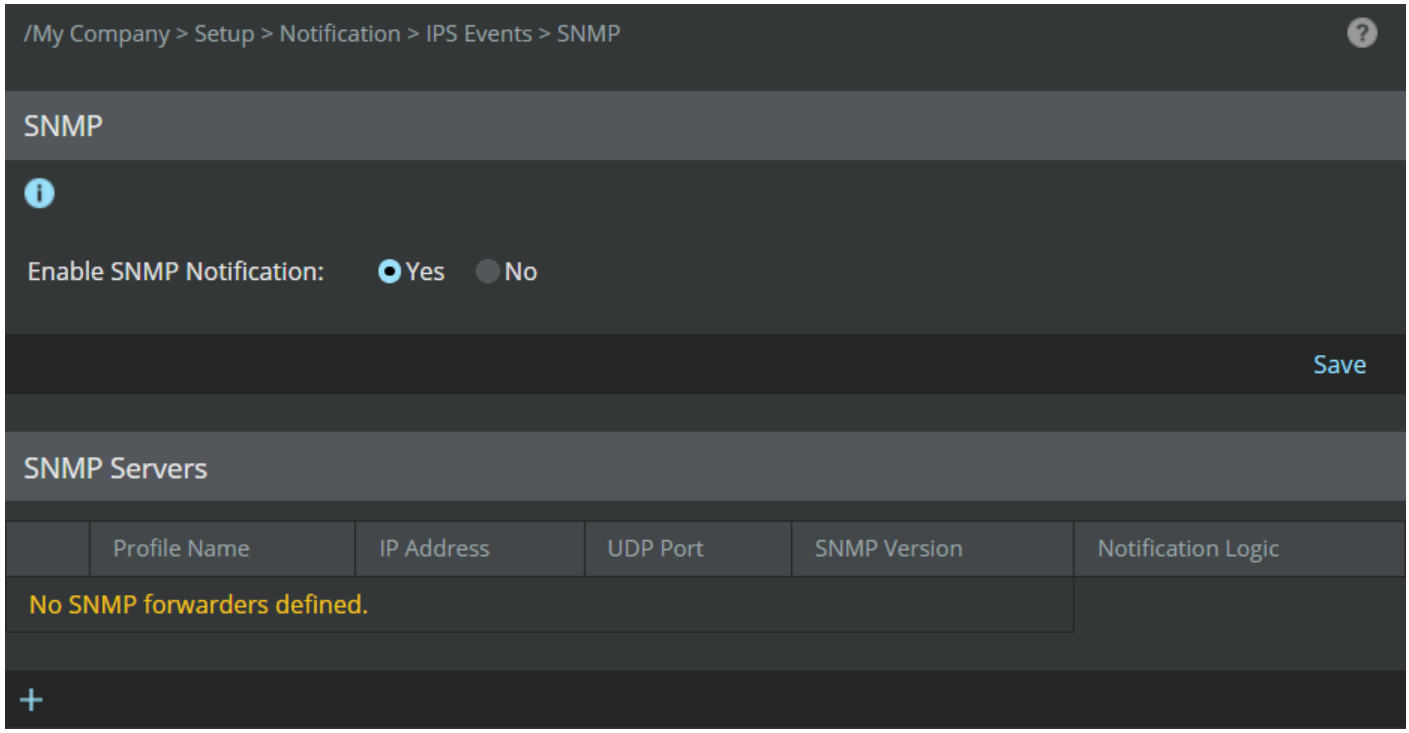
Forward alerts to an SNMP server

You can configure the SNMP server to which alert information for Sensor or NTBA Appliance is to be sent.

You can configure more than one SNMP server. You can configure the SNMP servers for each admin domain separately. The SNMP server configured for a root admin domain can be different from the SNMP server configured for its child domains. When the **Children** and the **Current** checkboxes are selected while configuring an SNMP server for the root admin domain, the SNMP server configured for the child domain will forward notifications to both the parent and child domain SNMP servers. When the **Children** checkbox is not selected in the root admin domain, then the child domain will use only the SNMP server configured for that domain to forward notifications. The **SNMP Servers** list on the **SNMP** tab displays the SNMP servers you have configured.

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS Events/NTBA Events → **SNMP**.

   The **SNMP** tab is displayed where **Enable SNMP Notification** option and the configured **SNMP Servers** list is displayed.



2. Select **Yes** against **Enable SNMP Notification** and click **Save**.
3. The columns displayed under the **SNMP Servers** section are as follows:

Field	Description
Profile Name	The profile name from where notifications are sent
IP Address	IP address of the target server
UDP Port	SNMP listening port of the target server
SNMP Version	The version of SNMP server
Notification Logic	The logic by which the notifications are sent to the target server

Modify or delete SNMP server settings

You can modify or delete the SNMP server settings at the **Manager** node.

Steps:

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **SNMP.**

   The **SNMP** tab with the **Enable SNMP Notification** option and the **SNMP Servers** list is displayed.
2. Select the configured SNMP server instance from the **SNMP Servers** list.
3. Configure the following:
   a. To edit the settings, click , modify the fields as required, and click **Save**.
   b. To delete the settings, click and click **OK** to confirm deletion.

Syslog notifications

The Sensor and Manager can independently be configured to forward alert information to a syslog server. By default, the Sensor forwards alert information to the Manager, and if configured, the Manager forwards this information to the syslog server.

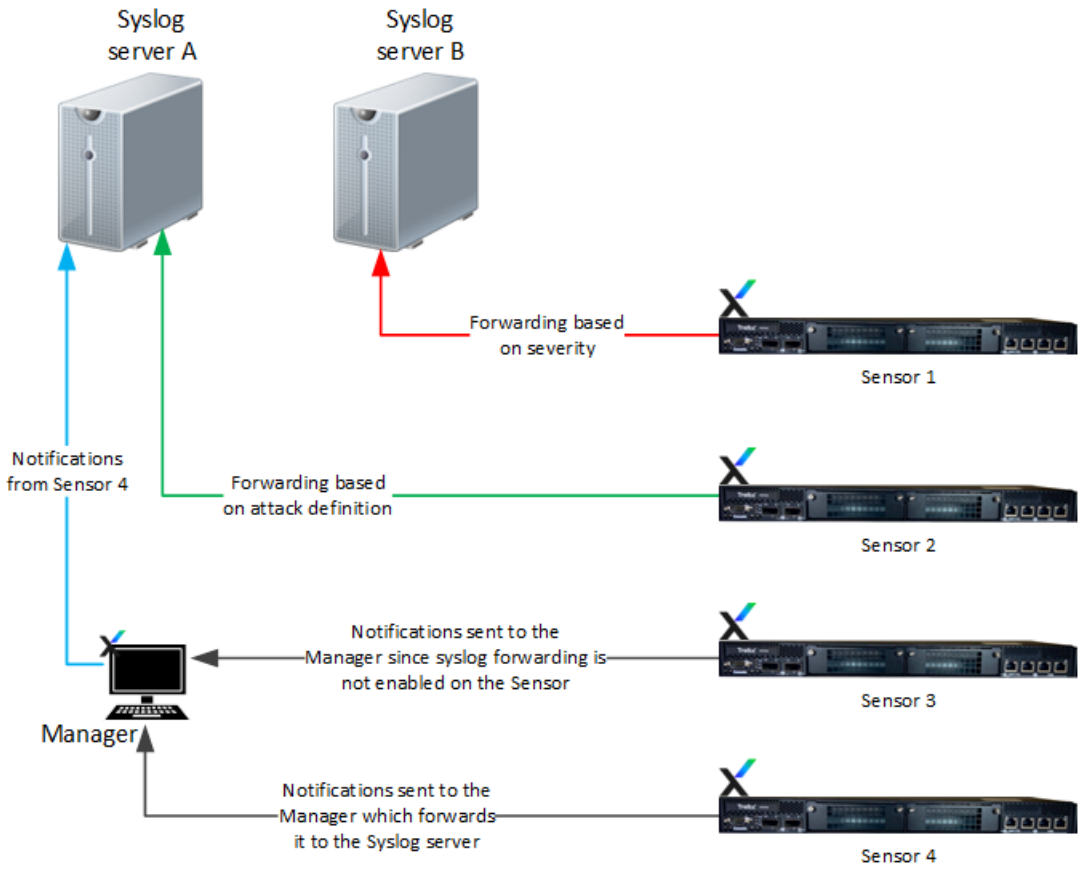
However, consider an organization that has more than one Sensor associated with a single Manager. Let's assume that each Sensor represents a business unit. Security analysts for each business unit might ask to receive alert information associated only with their business unit. To accommodate such environments, provision is made to configure those Sensors to forward notifications to a specific syslog server.

Summarizing the steps that needs to be followed to forward alert notifications to a syslog server:

- Configure a syslog server to make sure it is accessible to the Sensor or the Manager.
- Either configure the Sensor to directly send notifications to the syslog server or configure the Manager to send such notifications after consolidating alert information from all devices where syslog notification is enabled.
- Enable syslog fowarding in the Manager – at the Manager level, global level, or device level.
- Determine whether you want to receive all alert notifications or only some depending on the attacks or the attack severity.
- If you have chosen to receive syslog notifications based on the attack definition, configure those attacks.
- If you have chosen to receive alert notification based on both attack severity and definition, the Sensor will give preference to the severity of the attack when deciding whether to forward the notification or not.

This illustration represents a sample syslog forwarding scenario.

Figure 366. Sample syslog forwarding scenario



Alert notifications from the Sensor

You can configure the Sensor to forward alert notifications either at the domain level or the Sensor level. The next two sections tell you how you can configure the Sensor at different levels.

Enable syslog forwarding for alert notifications at the domain level

Make sure you have configured a syslog server with an IP address that will be reachable to the respective Sensors.

By configuring settings in the page, you can enable syslog forwarding for all devices in the domain.

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **IPS Event Logging**.
2. Configure the following fields.

Field	Description
Enable Logging	Select the checkbox to configure the settings.
Syslog Server IP Address	The IP address of the syslog server which becomes the destination of the alert notifications sent by all devices.

Field	Description
Syslog Server Port (UDP)	Port on the target syslog server that is authorized to receive syslog messages. The default protocol for syslog forwarding from Sensors is UDP. Therefore, this port must not be altered.
Syslog Facility	Standard syslog prioritization value. The choices are as follows: • **Security/authorization (code 4)** • **Security/authorization (code 10)** • **Log audit (note 1)** • **Log alert (note 1)** • **Clock daemon (note 2)** • **Local user 0 (local0)** • **Local user 1 (local1)** • **Local user 2 (local2)** • **Local user 3 (local3)** • **Local user 4 (local4)** • **Local user 5 (local5)** • **Local user 6 (local6)** • **Local user 7 (local7)**
Attack Severity to Syslog Priority Mapping	You can map each severity (Informational, Low, Medium, or High) to one of these standard syslog severities: • **Emergency** – System is unusable • **Alert** – Action must be taken immediately • **Critical** – Critical conditions • **Error** – Error conditions • **Warning** – Warning conditions • **Notice** – Normal but significant condition • **Informational** – Informational messages • **Debug** – Debug-level messages
Send Test Message	Clicking this option sends a test message from the Manager to the syslog server. It is used to check whether the syslog server is reachable.

3. Provide any filtering parameters that you want to provide.

Field	Description
Attack Logging	**Log All Attacks** sends notifications about every attack that passes through the Sensor. **Log Some Attacks** sends notifications about specific attacks based either on the severity or the settings in the attack definition. • Selecting **The attack definition has syslog notification explicitly enabled** instructs the Sensor to check the attack definition before sending out syslog notifications. **NOTE** If you only select this checkbox and do not configure any of the attack definitions for syslog notification, no notifications will be forwarded to the server. • Selecting **Minimum Severity of** instructs the Sensor to check the severity of the attack before forwarding the notification. Only attacks of a specific severity and higher will be forwarded; therefore, you must specify the lowest severity attacks. For example, if you only select this checkbox and specify **Low**, all attacks that have a severity of low or higher will be notified to the server.

4. Select the message you want displayed in the notification.

Field	Description
Message	The default message is a quick summary of an alert with two fields for easy recognition: **Attack Name** and **Attack Severity**. A default message reads: **`Attack $IV_ATTACK_NAME$ ($IV_ATTACK_SEVERITY$)`**.

The variables listed in the table are supported by the Sensor.

NOTE

Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

Syslog variable name	Description	Attack Log column
IV_ADMIN_DOMAIN	The domain to which the Sensor that detected the attack belongs.	Domain
IV_ALERT_ID	The globally unique ID that the Manager assigns to an alert.	Alert ID
IV_ALERT_TYPE	The Sensor decides the type of alert. This is mainly used by the Manager for its internal processing. This is not related to the Attack Category or Attack Sub-category. Some example alert types are signature, statistical anomaly, threshold anomaly, port scan, and host sweep.	Not available

Syslog variable name	Description	Attack Log column
$IV_APPLICATION_PROTOCOL$	The application-layer protocol associated with the attack traffic. This is not related to the Application Identification feature, and this information is displayed even if you have not enabled Application Identification. There could be instances when a Sensor might not be able to detect the protocol.	Not available
$IV_ATTACK_CONFIDENCE$	This is a value between 1 and 7. For example, a confidence level of 7 indicates that there is low possibility of the attack being a false-positive. The attack confidence values are inversely related to the Benign Trigger Probability (BTP) values of attack signatures. • Confidence 1 = BTP 7 (high) • Confidence 2 = BTP 6 (high) • Confidence 3 = BTP 5 (medium) • Confidence 4 = BTP 4 (medium) • Confidence 5 = BTP 3 (medium) • Confidence 6 = BTP 2 (low) • Confidence 7 = BTP 1 (low) **NOTE** When the BTP value is 0, there is no corresponding confidence value for the attack.	Not available
IV_ATTACK_COUNT	The number of times the attack occurred. This information is more relevant for suppressed alerts. Consider you have enabled alert suppression such that the alert is raised only when the attack is seen 5 times within 30 seconds. Subsequently, the Sensor detected this attack 10 times within 30 seconds. Then the attack count for this alert is 10.	Attack Count
IV_ATTACK_ID	Trellix Advanced Research Center assigns a universally unique hexadecimal value to each attack. This field displays the integer value of the hexadecimal ID assigned by Trellix ARC.	The equivalent hexadecimal value is displayed in the **Attack Information & Description** page as **Intruvert ID**.

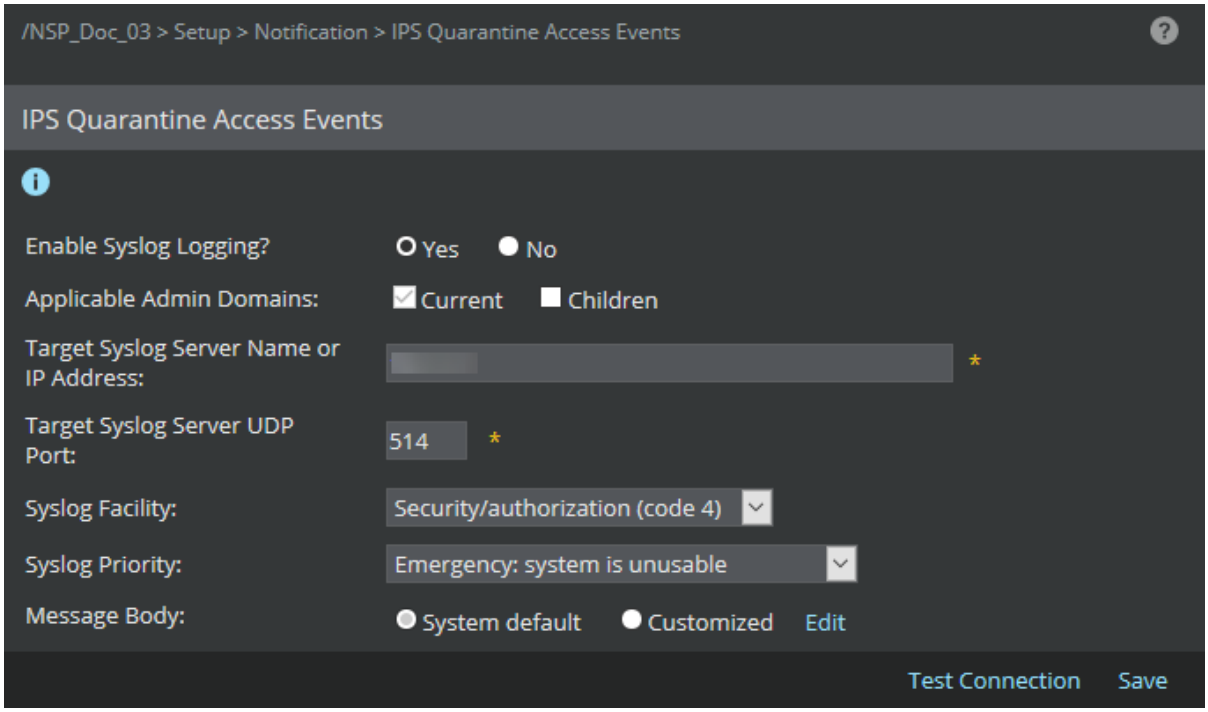
Syslog variable name	Description	Attack Log column
IV_ATTACK_NAME	The name assigned by Trellix ARC to an attack.	Name
$IV_ATTACK_SEVERITY$	Indicates the severity value of an attack specified in the corresponding attack definition. • 0 - Informational • 1 to 3 - low • 4 to 6 - medium • 7 to 9 - high	Attack Severity (high, medium, low, or informational)
$IV_ATTACK_SIGNATURE$	The ID of the signature that matched the attack traffic.	Not available
IV_ATTACK_TIME	The time when the Sensor created the alert.	Time
$IV_CALLBACK_ACTIVITY	The name of the Callback Activity family.	Callback Activity
$IV_CATEGORY$	The category to which the attack belongs. This is decided by Trellix ARC. Some examples are exploit, policy violation, and reconnaissance. You can view the attack categories in the IPS Policy Editor when you group by Attack Category.	Attack Category
$IV_CC_DOMAIN	The name of the Callback Activity domain.	C&C Domain
$IV_DESTINATION_IP$	The destination IP address to which the attack is destined.	Target IP Address
$IV_DESTINATION_PORT$	The port number on the destination host to which the attack traffic is sent.	Target Port
IV_DEST_APN	This is the destination Access Point Name (APN). This information is part of a mobile subscriber's identity data and is relevant only if you have deployed Sensors to monitor mobile networks. To see this data, you must enable capturing and tagging of mobile subscriber data in the alerts by using the **`set mnsconfig`** Sensor CLI command.	Not available
IV_DEST_IMSI	This is the destination International Mobile Subscriber Identity (IMSI). The details provided for APN apply to this as well.	Not available
IV_DEST_OS	The operating system installed on the destination host.	Target OS (in Alert Details panel)
$IV_DEST_PHONE_NUMBER$	This is the destination mobile phone number. The details provided for APN above apply to this as well.	Not available
$IV_DETECTION_MECHANISM$	The method the Sensor used to detect the attack. For example, signature, multi-flow-correlation, threshold, and so on. Each method relates to a specific attack category.	Detection (in Alert Details panel)

Syslog variable name	Description	Attack Log column
$IV_DIRECTION$	Indicates whether the attack traffic originated from your network or the outside network. For example, inbound direction means that the attack traffic originated from the outside network, targeting the hosts on your network.	Direction
$IV_INTERFACE$	The interface or sub-interface on which the Sensor detected the attack traffic.	Interface
$IV_LAYER_7_DATA	Provides the Layer 7 data.	Layer 7 Data
$IV_MALWARE_CONFIDENCE$	Confidence level of the malware as detected by the engine	Malware Confidence
$IV_MALWARE_DETECTION_ENGINE$	Engine which detected the malware(GAM,GTI,PDF-JS,etc).	Engine
$IV_MALWARE_FILE_LENGTH$	The length of the malware file.	Not available
$IV_MALWARE_FILE_MD5_HASH$	The MD5 hash of the malware file(fingerprint).	File Hash
$IV_MALWARE_FILE_NAME$	The name of the malware file. For SMTP traffic, it displays the file name of the attachment and for HTTP traffic, it displays the URL of the file.	File Name
$IV_MALWARE_FILE_SHA1_HASH$	The SHA1 hash of the malware file (fingerprint).	File Hash
$IV_MALWARE_FILE_SHA256_HASH$	The SHA256 hash of the malware file (fingerprint).	File Hash
$IV_MALWARE_FILE_TYPE$	The file type of the malware file	Not available
$IV_MALWARE_VIRUS_NAME$	The virus name as detected by GAM.	Not available
$IV_NETWORK_PROTOCOL$	The network protocol, such as TCP, of the attack traffic.	Protocol (in the Alert Details panel)
$IV_QUARANTINE_END_TIME$	The time when the attacking host will be out of quarantine. This is relevant only if you had enabled **Quarantine** feature.	Not available
IV_RESULT_STATUS	Indicates whether the attack traffic reached the victim host.	Result
$IV_SENSOR_ALERT_UUID$	The universally unique ID assigned by the Sensor for the alert. For a specific alert raised by a specific Sensor, the Central Manager also displays the same ID.	Alert ID
$IV_SENSOR_CLUSTER_MEMBER$	The member Sensor of a HA pair that generated the alert.	Not available

Syslog variable name	Description	Attack Log column
IV_SENSOR_NAME	The Sensor that generated the alert.	Device
IV_SOURCE_IP	The IP address of the attacking host.	Attacker IP Address
IV_SOURCE_OS	OS of the attacking host.	Attacker OS (in Alert Details panel)
IV_SOURCE_PORT	The port number on the attacking host from which the attack traffic is sent.	Attacker Port
IV_SRC_APN	This is the source Access Point Name (APN). This information is part of a mobile subscriber's identity data and is relevant only if you have deployed Sensors to monitor mobile networks. To see this data, you must enable capturing and tagging of mobile subscriber data in the alerts by using the **`set mnsconfig`** Sensor CLI command.	Not available
IV_SRC_IMSI	This is the source International Mobile Subscriber Identity (IMSI). The details provided for APN apply to this as well.	Not available
$IV_SRC_PHONE_NUMBER$	This is the source mobile phone number. The details provided for APN apply to this as well.	Not available
$IV_SUB_CATEGORY$	The subcategory to which the attack belongs. This is decided by Trellix ARC, and is a classification within Attack Category. Some examples are brute-force, buffer-overflow, host-sweep, and restricted-application. You can view the attack subcategories in the IPS policy editor when you group by Attack Subcategory.	Attack Subcategory (in Alert Details panel)
IV_VLAN_ID	The VLAN ID seen on the attack traffic.	VLAN

5. Click **Save**.

You have now enabled syslog forwarding for all Sensors belonging to a domain. You will notice in the **IPS Event Logging** page of a Sensor that all settings you have just configured are automatically inherited by each Sensor. The only remaining step to begin sending notifications will be to perform a configuration update in each Sensor.



However, if you want to modify settings for any of the Sensors, you will need to configure these settings individually for each Sensor. To configure a Sensor for syslog forwarding, go to Enable syslog forwarding for alert notifications at the Sensor level (page 899).

Enable syslog forwarding for alert notifications at the Sensor level

Make sure you have configured a syslog server with an IP address that will be reachable to the respective Sensors.

By configuring settings in this page, you will be able to enable syslog forwarding for the Sensor. Unless you inherit settings from the domain, any configuration in this page will override settings defined at the domain level.

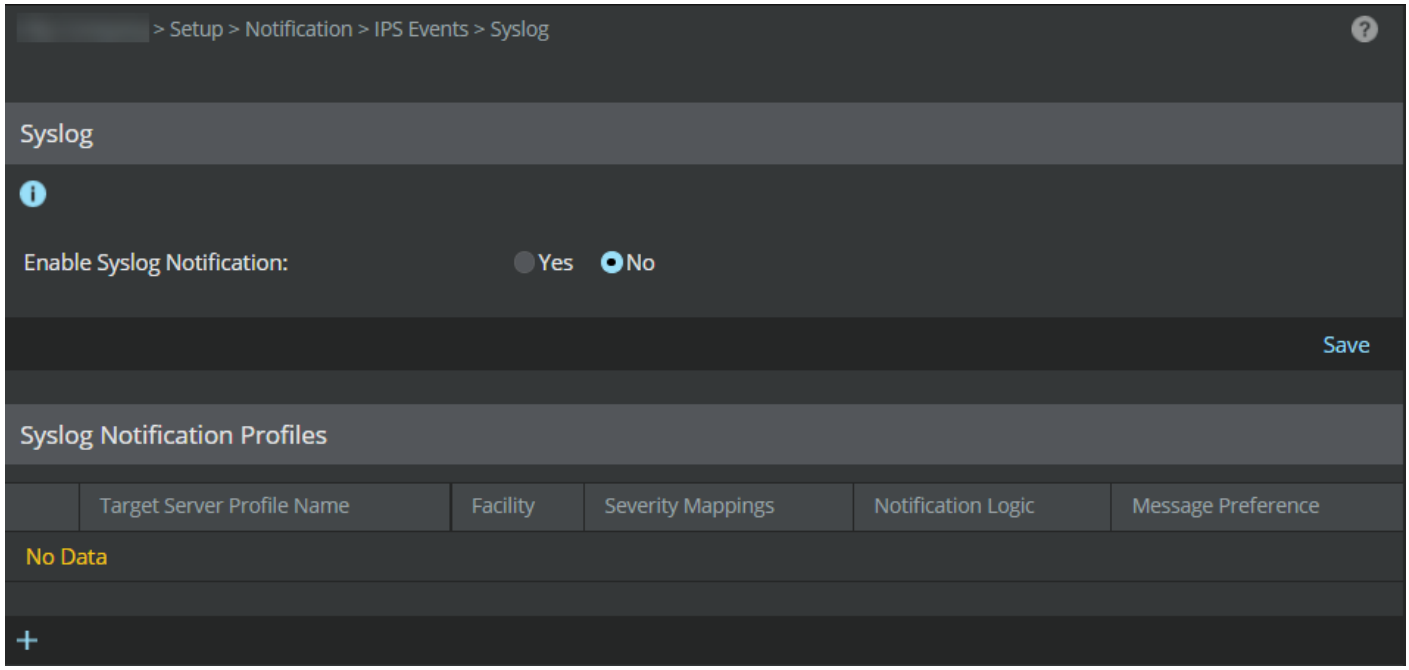
1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Logging → **IPS Event Logging**.
2. If you want to use settings configured for the domain, select the **Inherit Settings** checkbox.
3. Click **Save** to complete the configuration. However, if you want to configure settings at the domain level, see Enable syslog forwarding for alert notifications at the domain level (page 892).

After you complete configuring these settings, syslog forwarding for the Sensor is enabled.

Forward alert notifications from the Manager to a syslog server

Alerts forwarded from the Manager to a syslog server enable you to view the alerts on the third-party applications that support UDP and TCP over SSL, for example, Syslog NG.

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS Events → **Syslog**.



2. Click **Yes** in **Enable Syslog Notification** to enable syslog forwarding of alerts.
3. Click **Save.**

> **NOTE**
>
> You can forward Sensor alerts to multiple syslog servers by creating new syslog notification profiles. You can forward IPS alerts to syslog servers using UDP or TCP (with or without SSL).

4. The columns displayed under the **Syslog Notification Profiles** section are as follows:

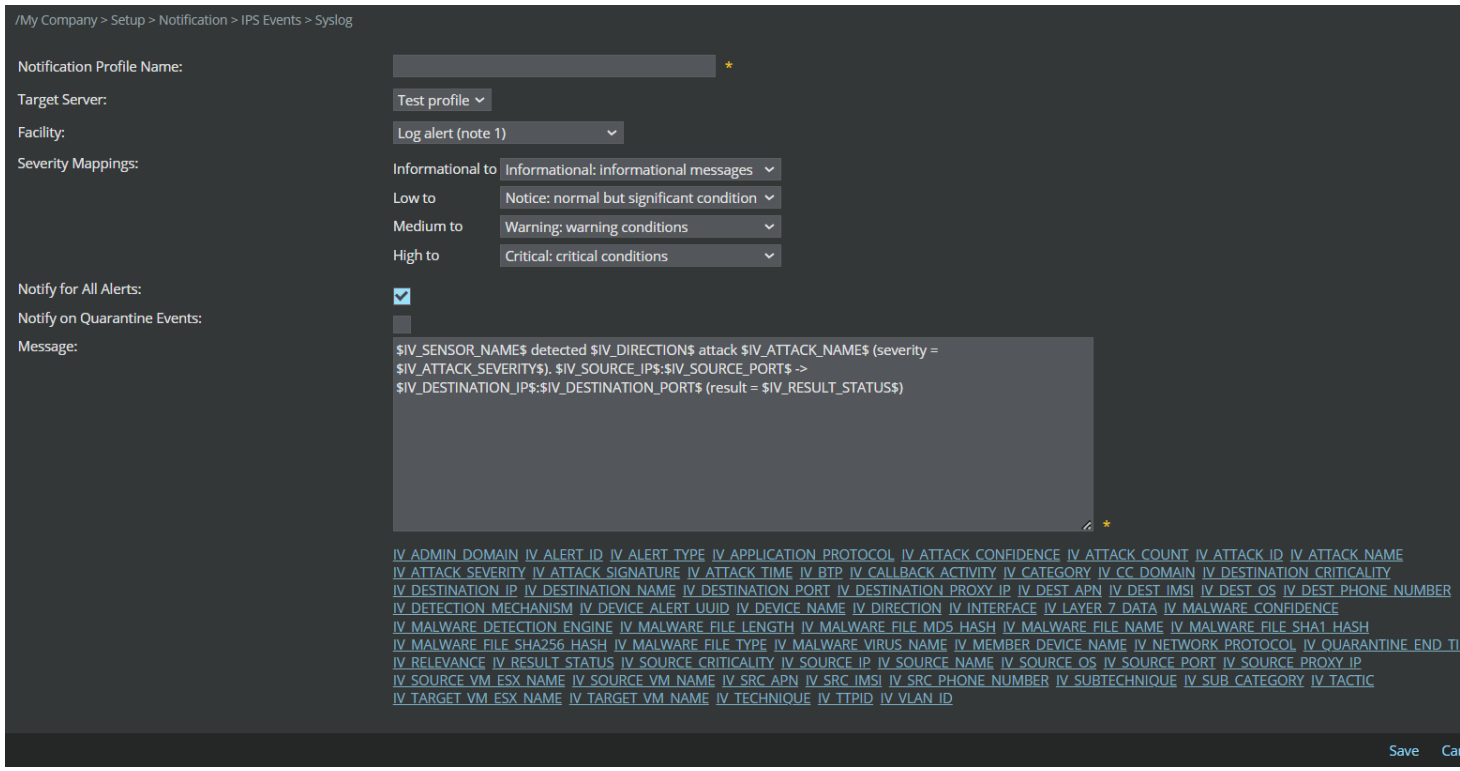
Field	Description
Target Server Profile Name	The profile name of the target server from where notifications are sent
Facility	The facility defined in the **Edit a Syslog Notification Profile** page
Serverity Mappings	The severity mappings defined in the **Edit a Syslog Notification Profile** page
Notification Logic	The logic by which the notifications are sent to the target server
Message Preference	The message preference you defined - **Default** or **Custom**

Add a Syslog notification profile to forward alerts

You can add notification profiles that will be displayed in the **Syslog** page.

1. Click + in the **Syslog** page.

   The **Add a Syslog Notification Profile** page is displayed.
2. Specify your options in the corresponding fields.



Field	Description
Admin Domain	• **Current** — Send notifications for alerts in the current domain. Always enabled for current domain by default. • **Children** — Include alerts for all child domains of the current domain (Not applicable to NTBA)
Notification Profile Name	Profile name from where notifications are sent
Target Server	Choose the target server from the drop-down to which notifications are forwarded.

Field	Description
Facility	Standard syslog prioritization value. The choices are as follows: • **Security/authorization (code 4)** • **Security /authorization (code 10)** • **Log audit (note 1)** • **Log alert (note 1)** • **Clock daemon (note 2)** • **Local user 0 (local0)** • **Local user 1 (local1)** • **Local user 2 (local2)** • **Local user 3 (local3)** • **Local user 4 (local4)** • **Local user 5 (local5)** • **Local user 6 (local6)** • **Local user 7 (local7)**
Severity Mappings	You can map each severity (Informational, Low, Medium, or High) to one of the standard syslog severities listed below: • **Emergency** — System is unusable • **Alert** — Action must be taken immediately • **Critical** — Critical conditions • **Error** — Error conditions • **Warning** — Warning conditions • **Notice** — Normal but significant condition • **Informational** — Informational messages • **Debug** — Debug-level messages
Notify for All Alerts	By default, this checkbox will be selected. Notifies for *all* discovered attacks.
The following field is enabled only on deselecting the **Notify for All Alerts** checkbox.	

Field	Description
Only Notify When	**The attack definition has this notification option explicitly enabled** Send notification for attacks that match customized policy notification settings, which you must set when editing attack responses within the policy editor (Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types) → **IPS** based on the following filters: • **Severity High** — Includes only high severity alerts • **Severity Informational and above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium and high severity alerts
Notify on Quarantine Events (not applicable to NTBA Appliance)	Select this checkbox to see quarantine events.
Message	The default message is a quick summary of an alert with the following fields for easy recognition: **Device Name**, **Direction**, **Attack Name**, **Attack Severity**, **Attacker IP: Attacker Port**, **Target IP: Target Port**, and **Result**. A default message reads: IV_SENSOR_NAME detected $IV_DIRECTION$ attack IV_ATTACK_NAME (severity = $IV_ATTACK_SEVERITY$). IV_SOURCE_IP:IV_SOURCE_PORT -> $IV_DESTINATION_IP$:$IV_DESTINATION_PORT$ (result = IV_RESULT_STATUS) **NOTE** For syslog message to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each parameter. Example: $ATTACK_TIME$ Type a message and select (click) the parameters for the wanted alert identification format. You can type custom text in the **Message** field. IV_ADMIN_DOMAIN IV_ALERT_ID IV_ALERT_TYPE IV_APPLICATION_PROTOCOL IV_ATTACK_CONFIDENCE IV_ATTACK_COUNT IV_ATTACK_ID IV_ATTACK_NAME IV_ATTACK_SEVERITY IV_ATTACK_SIGNATURE IV_ATTACK_TIME IV_BTP IV_CALLBACK_ACTIVITY IV_CATEGORY IV_CC_DOMAIN IV_DESTINATION_CRITICALITY IV_DESTINATION_IP IV_DESTINATION_NAME IV_DESTINATION_PORT IV_DESTINATION_PROXY_IP IV_DEST_APN IV_DEST_IMSI IV_DEST_OS IV_DEST_PHONE_NUMBER IV_DETECTION_MECHANISM IV_DEVICE_ALERT_UUID IV_DEVICE_NAME IV_DIRECTION IV_INTERFACE IV_LAYER_7_DATA IV_MALWARE_CONFIDENCE IV_MALWARE_DETECTION_ENGINE IV_MALWARE_FILE_LENGTH IV_MALWARE_FILE_MD5_HASH IV_MALWARE_FILE_NAME IV_MALWARE_FILE_SHA1_HASH IV_MALWARE_FILE_SHA256_HASH IV_MALWARE_FILE_TYPE IV_MALWARE_VIRUS_NAME IV_MEMBER_DEVICE_NAME IV_NETWORK_PROTOCOL IV_QUARANTINE_END_TIME IV_RELEVANCE IV_RESULT_STATUS IV_SOURCE_CRITICALITY IV_SOURCE_IP IV_SOURCE_NAME IV_SOURCE_OS IV_SOURCE_PORT IV_SOURCE_PROXY_IP IV_SOURCE_VM_ESX_NAME IV_SOURCE_VM_NAME IV_SRC_APN IV_SRC_IMSI IV_SRC_PHONE_NUMBER IV_SUBTECHNIQUE IV_SUB_CATEGORY IV_TACTIC IV_TARGET_VM_ESX_NAME IV_TARGET_VM_NAME IV_TECHNIQUE IV_TTPID IV_VLAN_ID **NOTE** Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

3. Click **Save.**

The newly added notification profile will be displayed in the **Syslog** page.

Table 42. Syslog variables for alert notification and the equivalent Attack Log columns

Syslog variable name	Description	Attack Log column
IV_ADMIN_DOMAIN	The domain to which the Sensor that detected the attack belongs	Domain
IV_ALERT_ID	The globally unique ID that the Manager assigns to an alert	Alert ID
IV_ALERT_TYPE	The Sensor decides the type of alert. This is mainly used by the Manager for its internal processing. This is not related to the Attack Category or Attack Sub-category. Some example alert types are signature, statistical anomaly, threshold anomaly, port scan, and host sweep.	Not available
$IV_APPLICATION_PROTOCOL$	The application-layer protocol associated with the attack traffic. This is not related to the Application Identification feature, and this information is displayed even if you have not enabled Application Identification. There could be instances when a Sensor might not be able to detect the protocol.	Not available
$IV_ATTACK_CONFIDENCE$	This is a value between 1 and 7. For example, a confidence level of 7 indicates that there is low possibility of the attack being a false-positive. The attack confidence values are inversely related to the Benign Trigger Probability (BTP) values of attack signatures. • Confidence 1 = BTP 7 (high) • Confidence 2 = BTP 6 (high) • Confidence 3 = BTP 5 (medium) • Confidence 4 = BTP 4 (medium) • Confidence 5 = BTP 3 (medium) • Confidence 6 = BTP 2 (low) • Confidence 7 = BTP 1 (low) **NOTE** When the BTP value is 0, there is no corresponding confidence value for the attack.	Not available
IV_ATTACK_COUNT	The number of types the attack occurred. This information is more relevant for suppressed alerts. Consider you have enabled alert suppression such that the alert is raised only when the attack is seen 5 times within 30 seconds. Subsequently, the Sensor detected this attack 10 times within 30 seconds. Then the attack count for this alert is 10.	Attack Count

Syslog variable name	Description	Attack Log column
IV_ATTACK_ID	Trellix Advanced Research Center assigns a universally unique hexadecimal value to each attack. This field displays the integer value of the hexadecimal ID assigned by Trellix ARC.	The equivalent hexadecimal value is displayed in the **Attack Information & Description** page as **Intrusvert ID**.
IV_ATTACK_NAME	The name assigned by Trellix ARC to an attack	Name
$IV_ATTACK_SEVERITY$	Indicates the severity value of an attack specified in the corresponding attack definition. • 0 - Informational • 1 to 3 - low • 4 to 6 - medium • 7 to 9 - high	Attack Severity (high, medium, low, or informational)
$IV_ATTACK_SIGNATURE$	The ID of the signature that matched the attack traffic	Not available
IV_ATTACK_TIME	The time when the Sensor created the alert	Time
$IV_CALLBACK_ACTIVITY$	The name of the Callback Activity family	Callback Activity
$IV_CATEGORY$	The category to which the attack belongs. This is decided by Trellix ARC. Some examples are exploit, policy violation, and reconnaissance. You can view the attack categories in the IPS Policy Editor when you group by Attack Category.	Attack Category
IV_CC_DOMAIN	The name of the Callback Activity domain	C&C Domain
$IV_DESTINATION_CRITICALITY$	Displays the risk level as High Risk, Medium Risk or Low Risk	Target Risk
$IV_DESTINATION_IP$	The destination IP address to which the attack is destined	Target IP address
$IV_DESTINATION_NAME $	The name of the host to which the attack is destined	Target Hostname
IV_DESTINATION_PORT$	The port number on the destination host to which the attack traffic is sent	Target Port
$IV_DESTINATION_PROXY_IP	The IP address of the proxy server	Target Proxy IP

Syslog variable name	Description	Attack Log column
IV_DEST_APN	This is the destination Access Point Name (APN). This information is part of a mobile subscriber's identity data and is relevant only if you have deployed Sensors to monitor mobile networks. To see this data, you must enable capturing and tagging of mobile subscriber data in the alerts by using the **`set mnsconfig`** Sensor CLI command.	Not available
IV_DEST_IMSI	This is the destination International Mobile Subscriber Identity (IMSI). The details provided for APN apply to this as well.	Not available
IV_DEST_OS	The operating system installed on the destination host	Target OS
$IV_DEST_PHONE_NUMBER$	This is the destination mobile phone number. The details provided for APN above apply to this as well.	Not available
$IV_DETECTION_MECHANISM$	The method the Sensor used to detect the attack. For example, signature, multi-flow-correlation, threshold, and so on. Each method relates to a specific attack category.	Detection (in Alert Details panel)
$IV_DEVICE_ALERT_UUID$	ID assigned to the alert	Alert ID
IV_DEVICE_NAME	Name of the device that detected the attack	Device
$IV_DIRECTION$	Indicates whether the attack traffic originated from your network or the outside network. For example, inbound direction means that the attack traffic originated from the outside network, targeting the hosts on your network.	Direction
$IV_INTERFACE$	The interface or sub-interface on which the Sensor detected the attack traffic	Interface
$IV_LAYER_7_DATA$	Provides the Layer 7 data	Layer 7 Data
$IV_MALWARE_CONFIDENCE$	Confidence level of the malware as detected by the engine	Malware Confidence
$IV_MALWARE_DETECTION_ENGINE$	Engine which detected the malware (Gateway Anti-Malware, Global Threat Intelligence, PDF-JS, etc)	Engine
$IV_MALWARE_FILE_LENGTH$	The length of the malware file	Not available
$IV_MALWARE_FILE_MD5_HASH$	The MD5 hash of the malware file (fingerprint)	File Hash
$IV_MALWARE_FILE_NAME$	The name of the malware file. For SMTP traffic, it displays the file name of the attachment and for HTTP traffic, it displays the URL of the file.	File Name
$IV_MALWARE_FILE_SHA1_HASH$	The SHA1 hash of the malware file (fingerprint)	File Hash
$IV_MALWARE_FILE_SHA256_HASH$	The SHA256 hash of the malware file (fingerprint)	File Hash
$IV_MALWARE_FILE_TYPE$	The file type of the malware file	Not available
$IV_MALWARE_VIRUS_NAME$	The virus name as detected by Gateway Anti-Malware	Not available

Syslog variable name	Description	Attack Log column
$IV_MEMBER_DEVICE_NAME$	Name of the device that detected the attack	Device
$IV_NETWORK_PROTOCOL$	The network protocol, such as TCP, of the attack traffic	Protocol (in Alert Details panel)
$IV_QUARANTINE_END_TIME$	The time when the attacking host will be out of quarantine. This is relevant only if you had enabled **Quarantine** feature.	Not available
$IV_RELEVANCE$	Indicates if the endpoint is vulnerable to this particular attack	Relevance
IV_RESULT_STATUS	Indicates whether the attack traffic reached the victim host	Result
$IV_SOURCE_CRITICALITY$	Displays the risk level as High Risk, Medium Risk or Low Risk	Attacker Risk
$IV_SENSOR_ALERT_UUID$	The universally unique ID assigned by the Sensor for the alert. For a specific alert raised by a specific Sensor, the Central Manager also displays the same ID.	Alert ID
$IV_SENSOR_CLUSTER_MEMBER$	The member Sensor of a HA pair that generated the alert	Not available
IV_SENSOR_NAME	The Sensor that generated the alert	Device
IV_SOURCE_IP	The IP address of the attacking host	Attacker IP address
IV_SOURCE_NAME	Name of the host from where the attack was generated	Attacker Hostname
IV_SOURCE_OS	OS of the attacking host	Attacker OS (in Alert Details panel)
IV_SOURCE_PORT	The port number on the attacking host from which the attack traffic is sent	Attacker Port
$IV_SOURCE_PROXY_IP$	The IP address of the proxy server	Attacker Proxy IP
$IV_SOURCE_VM_NAME$	Name of the virtual machine from where the attack was generated	Attacker VM Name
IV_SRC_APN	This is the source Access Point Name (APN). This information is part of a mobile subscriber's identity data and is relevant only if you have deployed Sensors to monitor mobile networks. To see this data, you must enable capturing and tagging of mobile subscriber data in the alerts by using the **`set mnsconfig`** Sensor CLI command.	Not available
IV_SRC_IMSI	This is the source International Mobile Subscriber Identity (IMSI). The details provided for APN apply to this as well.	Not available
$IV_SRC_PHONE_NUMBER$	This is the source mobile phone number. The details provided for APN apply to this as well.	Not available

Syslog variable name	Description	Attack Log column
$IV_SUBTECHNIQUE$	Name of the corresponding adversarial sub-technique matching with the attack or alert	Sub-Technique
$IV_SUB_CATEGORY$	The subcategory to which the attack belongs. This is decided by Trellix ARC, and is a classification within Attack Category. Some examples are brute-force, buffer-overflow, host-sweep, and restricted-application. You can view the attack subcategories in the IPS policy editor when you group by Attack Subcategory.	Attack Subcategory (in Alert Details panel)
IV_TACTIC	Name of the adversarial tactic matching with the attack or alert	Tactic
$IV_TARGET_VM_NAME$	Name of the virtual machine to which the attack is directed	Target VM Name
$IV_TECHNIQUE$	Name of the corresponding adversarial technique matching with the attack or alert	Technique
IV_TTPID	ID of the specific technique/sub-technique in the<techniqueID.sub-techniqueID> format	Technique/Sub-Technique ID
IV_VLAN_ID	The VLAN ID seen on the attack traffic	VLAN

NOTE

Mitre Attack Details can be currently forwarded through the Manager alone. So, if you plan to forward details such as the **Tactic**, **Technique**, **Sub-Technique**, or **Technique/Sub-Technique ID**, you need to assign the relevant variables only through this page.

Edit or delete a syslog notification profile

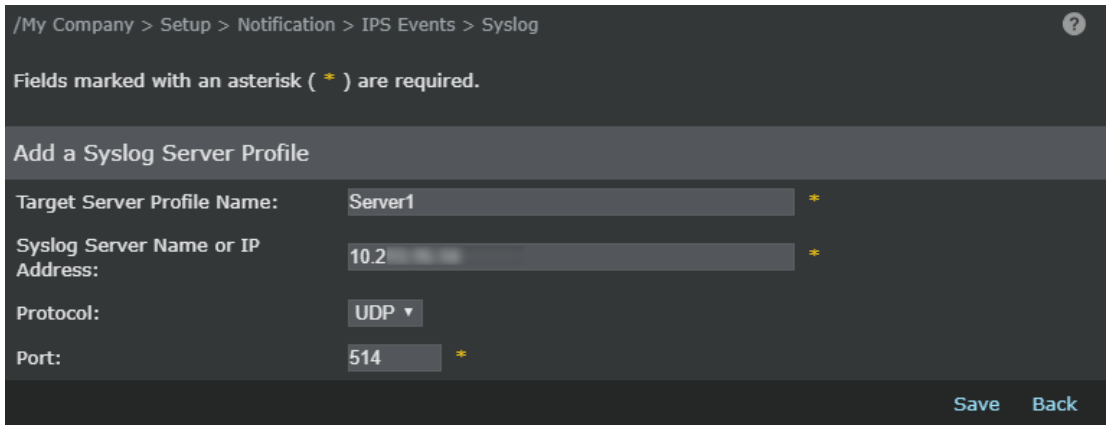
You can edit or delete a syslog notification profile by clicking the or in the **Syslog Notification Profiles** section.

Add a syslog server profile

You can add server profiles that will be populated in the **Target Server** drop-down list on the **Add a Syslog Notification Profile** page.

1. Click **Add** beside the **Target Server** drop-down list.

   The **Add a Syslog Server Profile** page is displayed.



2. Enter the **Target Server Profile Name**.
3. Enter the syslog server name or IP address.

> **NOTE**
>
> The length of server name has been increased to support up to 255 characters from 40 characters.

4. Select *TCP* or *UDP* from the **Protocol** drop-down list.

> **NOTE**
>
> If you select the TCP protocol:
>
> - You will have to provide a certificate when you select the **Use SSL** checkbox.
> - Click **Test Connection** to check if the connection is successful. If a TCP server is down, at least five attempts will be made to ping the server before a fault is raised.

5. Specify the port. By default, the port is set to 514.
6. Click **Save**.

   Now you can select the server where you want to forward the alert.

Edit or delete a syslog server profile

You can edit or delete a syslog server profile by clicking the **Edit** or **Delete** in the **Edit a Syslog Notification Profile** section.

> **NOTE**
>
> You can delete a syslog server only when it is not in use, else you will see an error message.

Configure email or pager alert notifications

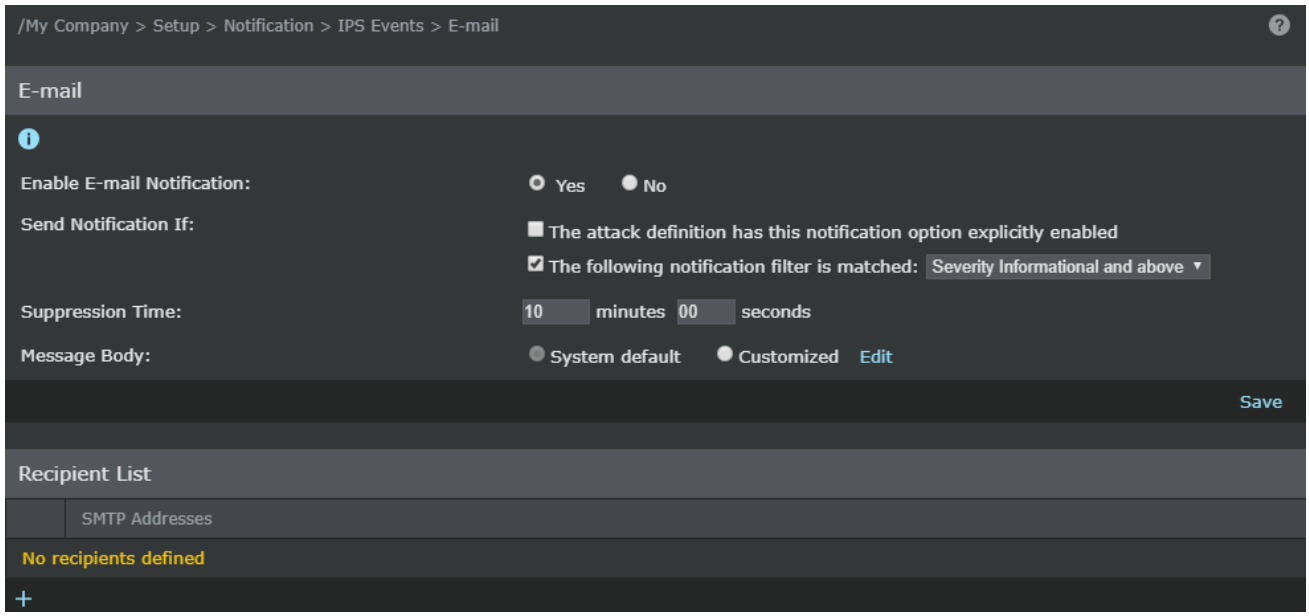
You must identify a mail server for email notifications in the **E-mail** page (Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **E-mail**).

Users can be alerted by email or pager when an alert is generated that matches a chosen severity or customized attack setting.

The procedure for configuring email alerts is described here. The procedure for configuring pager is similar.

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **E-mail**.

   The **E-Mail** and **Recipient List** information is displayed under the **E-mail** tab.



2. Specify your options in the corresponding fields.

Field	Description
Enable E-mail Notification	Select **Yes** to enable alert notification through email.
Send Notification If	**The attack definition has this notification option explicitly enabled** — Send notification for attacks that match customized policy notification settings, which you must set when editing attack responses within the policy editor. **The following notification filter is matched** — Send notification based on the following filters: • **Severity Informational and above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium and high severity alerts • **Severity High** — Includes only high severity alerts The table below explains the functional interdependency of the two options.
Suppression Time	Type a **Suppression Time** for the notification. The suppression time is the duration (minutes and seconds) to wait after an alert notification has been sent before sending another alert notification. The default and minimum value is 10 minutes and 0 seconds. Suppression time is useful to avoid sending excessive notifications when there is heavy attack traffic.

Field	Description
Message Body	The *message body* is a preset response sent with the notification with information pertaining to the alert. **System Default** — The system default message provides the notified admin with the most basic attack details so that an immediate response can be made. Details include the attack name, time detected, attack type, severity, the Sensor interface where detected, and the source and/or destination IP addresses. **NOTE** You cannot edit the **System Default** message. **Customized** — Select **Customized** against **Message Body** and click **Edit** to view the **Custom Message** page. You can type custom text in the **Subject** field or **Body** section, as well as click one or more of the provided variable links at **Subject Line Variables** or **Content-Specific Variables**. **NOTE** Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

Notification option explicitly enabled	Notification filter is matched	Functionality
✔		Emails are sent only for the attacks where the notification option is enabled.
	✔	Emails are sent only when the defined severity level is matched and the notification option is disabled.
✔	✔	If the attack matches at least one of the criteria, an email is sent.

3. Click **Save** to return to the email or pager notification settings page.
4. Click + in the **Recipient List** section of the **E-mail** page.

   The **Add a Recipient** page is displayed.
5. Enter the Recipient email address in the **SMTP Address** field and click **Save**.

   The email address is listed under the **Recipient List** on the **E-mail** tab.

   - You can configure pager settings using a similar procedure in the **Pager** page. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **Pager** to view the **Pager** page.
   - Email and pager notifications are configured per admin domain.

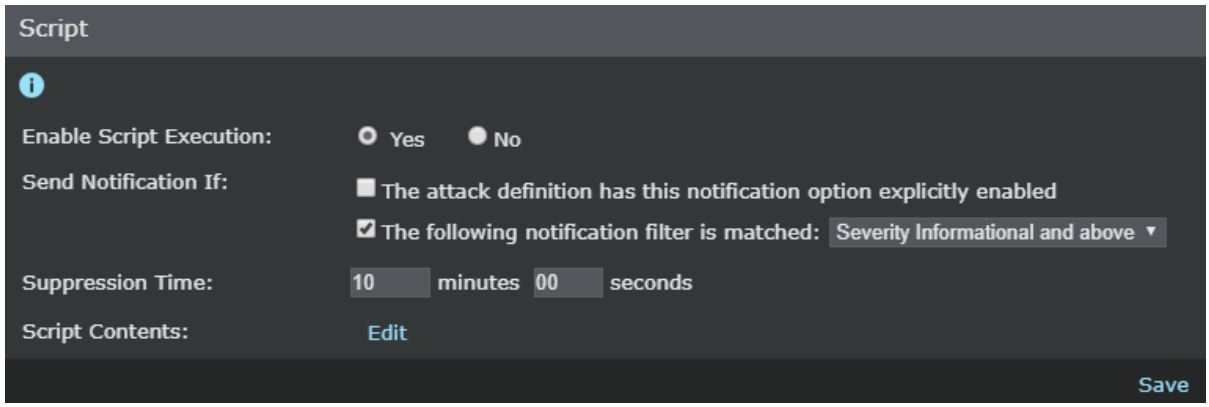
Enable alert notification by script

Users can be alerted through an executed script when an alert is generated that matches a chosen severity or customized attack setting.

1. Select Manager → <Admin Domain Name> → Setup → Notification → IPS/NTBA Events → **Script**.

   The **Script** page is displayed.

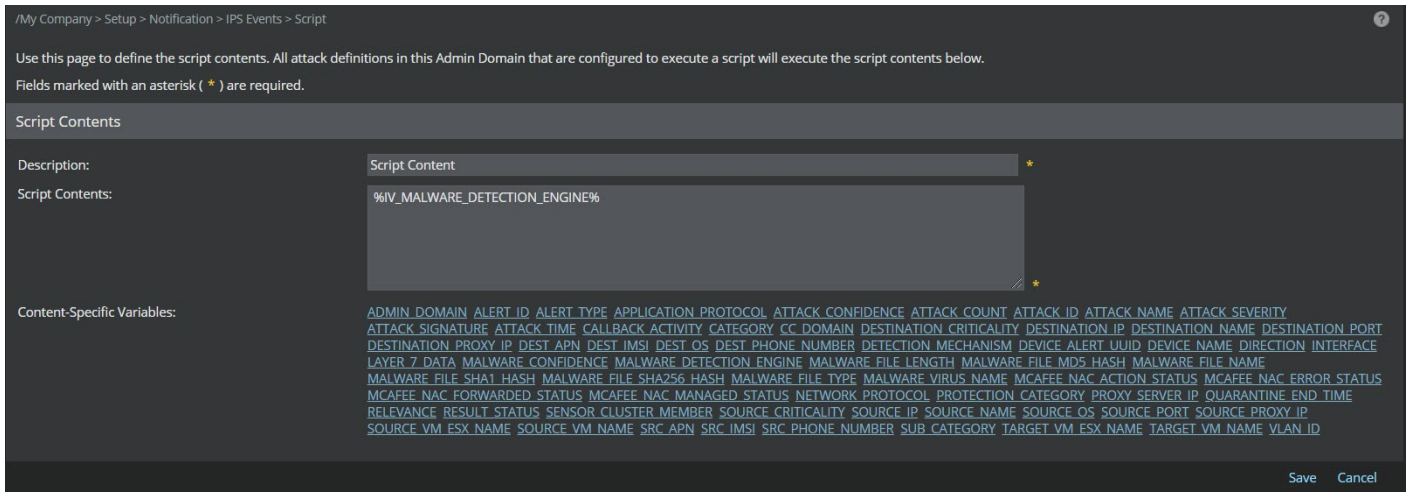
2. Specify the options in the corresponding fields.



Field	Description
Enable Script Execution	Select **Yes** to enable alert notification through an executed script.
Send Notification If	**The attack definition has this notification option explicitly enabled** — send notification for attacks that match customized policy notification settings, which you must set when editing attack responses within the policy editor. **The following notification filter is matched**: • **Severity Informational and above** — Includes all alerts • **Severity Low and above** — Includes low, medium, and high severity alerts • **Severity Medium and above** — Includes both medium and high severity alerts • **Severity High** — Includes only high severity alerts
Suppression Time	Enter a **Suppression Time** for the notification. The suppression time is the amount of time (minutes and seconds) to wait after an alert has been generated before sending the notification. This will prevent alerts being sent through notification in the event an alert has been acknowledged or deleted through the **Attack Log** page within the suppression time. The default and minimum value is 10 minutes and 0 seconds.

3. Click **Edit**.

   The **Script Contents** page is displayed.



- Enter a description in the **Description** field.
- Enter the required text in the **Script Contents** field. Click the links provided against **Content-Specific Variables** to add variables in the **Script Contents** field.

> **NOTE**
>
> Prior to Sensor software version 10.1.5.116, the variables $IV_MALWARE_FILE_SHA1_HASH$ and $IV_MALWARE_FILE_SHA256_HASH$ do not display the file hashes.

4. Click **Save** to return to the **Script** page.
5. Click **Save** to save your settings.
   - The local system user needs to have permission to create the script output file on the Manager installation directory.
   - Notifications are configured per admin domain.

Device Profiling and Alert Relevance

Device Profiling

Device profiling (also referred to as OS fingerprinting) is a method by which Trellix IPS collects information about a remote computing device to decipher its operating system and device type. Trellix IPS carries out device profiling by using DHCP DISCOVER and REQUESTS, HTTP User Agent field, and TCP SYN and SYN + ACK packets.

If device profiling is enabled, the following Trellix products, when integrated, participate in device profiling:

- IPS
- NTBA
- Trellix ePO - On-prem

Device profiling can be carried out in three ways:

- Active device profiling

- Passive device profiling
- Device profiling using Trellix ePO - On-prem

Active device profiling involves querying a device and observing its responses. Active device profiling systems gain access to information, such as MAC addresses, operating system, and device type. In Trellix IPS, this method of profiling is used by NTBA. For information about device profiling using NTBA, refer to the [Trellix Intrusion Prevention System Product Guide].

Passive device profiling involves collecting information without invasive device querying. Information is collected from one or more Sensors. It uses DHCP DISCOVER and REQUESTS, HTTP User Agent field, and TCP SYN and SYN + ACK to gather operating system information about a device. The operating system information about a specific device is displayed in the Attack Log. In Trellix IPS, this method of profiling is used by IPS Sensors.

Device profiling using Trellix ePO - On-prem functions by making use of communication established Trellix Agent and Trellix ePO - On-prem. When Trellix Agent is installed on any system, that system comes to be known as a managed host and passes device, operating system and other event details at regular intervals to Trellix ePO - On-prem. When Trellix ePO - On-prem is integrated with the Manager, it passes on information necessary for device profiling.

Passive Device Profiling

Passive device profiling is a method used specifically by IPS Sensors which are one of the primary sources of device profile information. Device profiling through IPS is passive. When traffic passes through a Sensor, its packets are examined and device information extracted by the Sensor, which then forwards the information to the Manager.

Setting device profiling parameters for all Sensors belonging to a domain

1. Go to Devices → <Admin Domain Name> → Global → IPS Devices Settings → **Passive Device Profiling**.

   The **Passive Device Profiling** page appears.

2. Select the technique that you would like the Manager to use for device profiling.

   You will notice three checkboxes:

   - **DHCP** indicates the use of DHCP DISCOVER and REQUESTS packets for device profiling.
   - **TCP** indicates the use of TCP SYN and SYN + ACK packets for device profiling.
   - **HTTP** indicates the use of HTTP User Agent field for device profiling.

   > **IMPORTANT**
   >
   > The above mentioned techniques are enabled by default at the global level. However, to ensure that device profiling is enabled, you must configure the settings per device or per interface using the **Policy Manager** page.

3. Specify the **Profile Expiration** duration.

   This timer ensures that the periodic re-profiling of a device happens only once within that interval. Trellix recommends this duration be set at 5 minutes. However, you can alter this and increase it up to 12 hours.

4. Specify the **Endpoint Inactivity Timer** duration.

   This value specifies the duration after which information for a device is considered invalid. It occurs when the host has remained idle for the said duration. This timer ensures that the Sensor will renew its detection of the IP if it is noticed again. Trellix recommends this duration be set at 1 hour. However, you can alter this and increase it up to 24 hours.

NOTE

The parameters set in steps 2, 3, and 4 can be overridden or inherited at the device or interface level using the **Policy Manager** page.

5. Click **Save**.

Configure device profiling per device

To access device profiling settings in the Manager, perform the following steps:

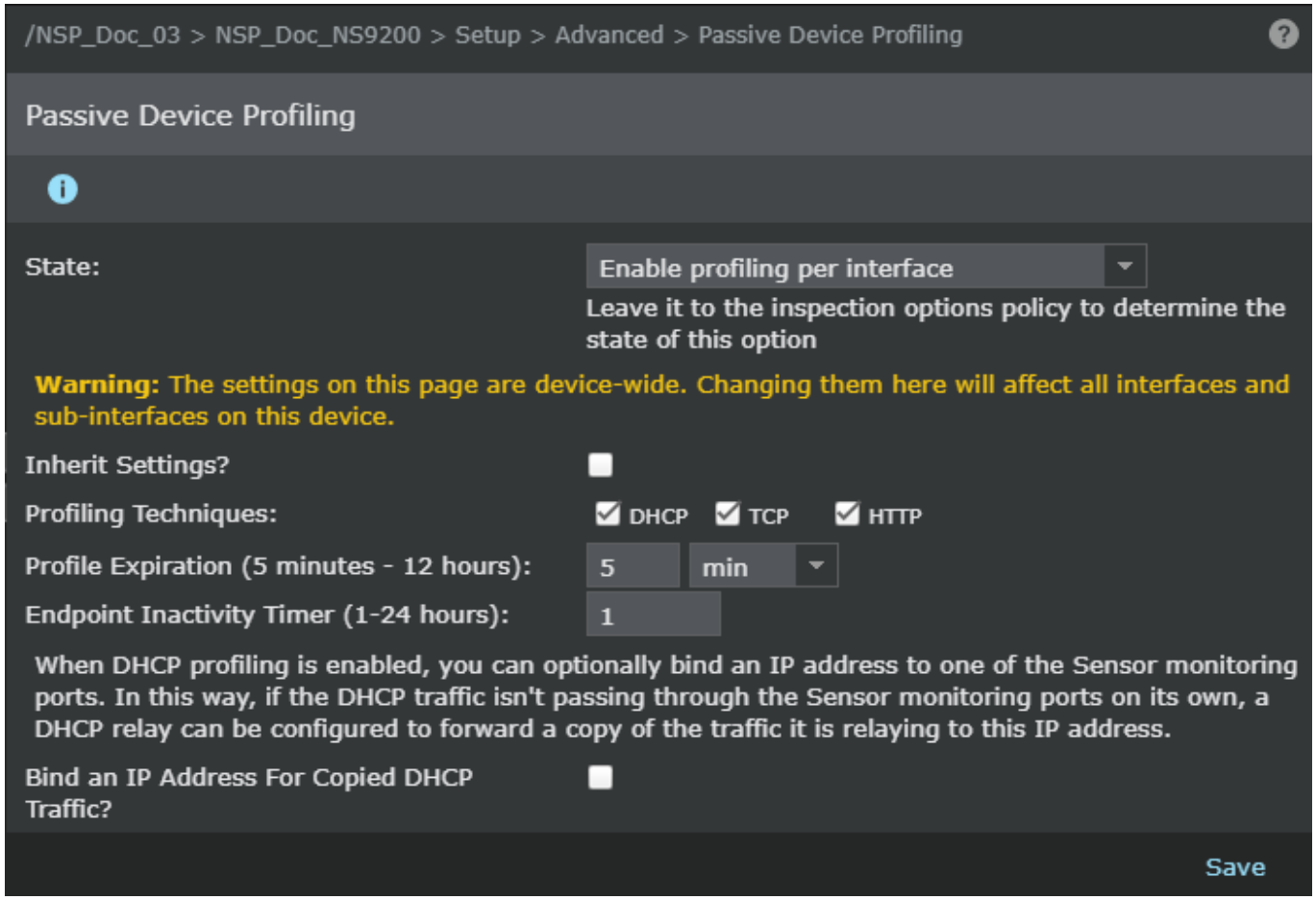
1. The Manager allows you to define settings for the device as follows:

   To modify device profile settings at the device level, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Advanced**.

2. Click **Passive Device Profiling**.

   The **Passive Device Profiling** page appears.

Figure 367. Passive Device Profiling Page



3. Select the **State**.

If you select **Profiling enabled for the entire device** or **Enable profiling per interface**, proceed with the configuration. If you select **Profiling disabled for the entire device**, click **Save** to complete the configuration.

4. You must now decide whether you want to inherit settings from the IPS admin domain by selecting the **Inherit Settings** checkbox.

   NOTE

   Selecting this checkbox means either the entire device or the interfaces will inherit global settings and no further options will appear in this page. If you have not chosen to inherit settings from the admin domain, proceed to Step 5.

5. Select the techniques that you want to use for device profiling.

   You will find three checkboxes:

   - **DHCP** indicates the use of DHCP DISCOVER and REQUESTS packets for device profiling.
   - **TCP** indicates the use of TCP SYN and SYN + ACK packets for device profiling.
   - **HTTP** indicates the use of HTTP User Agent field for device profiling.

6. Specify the **Profile Expiration** duration.

   This timer ensures periodic re-profiling of a device to detect any changes in that period. Trellix recommends this duration be set at 5 minutes. However, you can increase it up to 12 hours.

7. Specify the **Endpoint Inactivity Timer** duration.

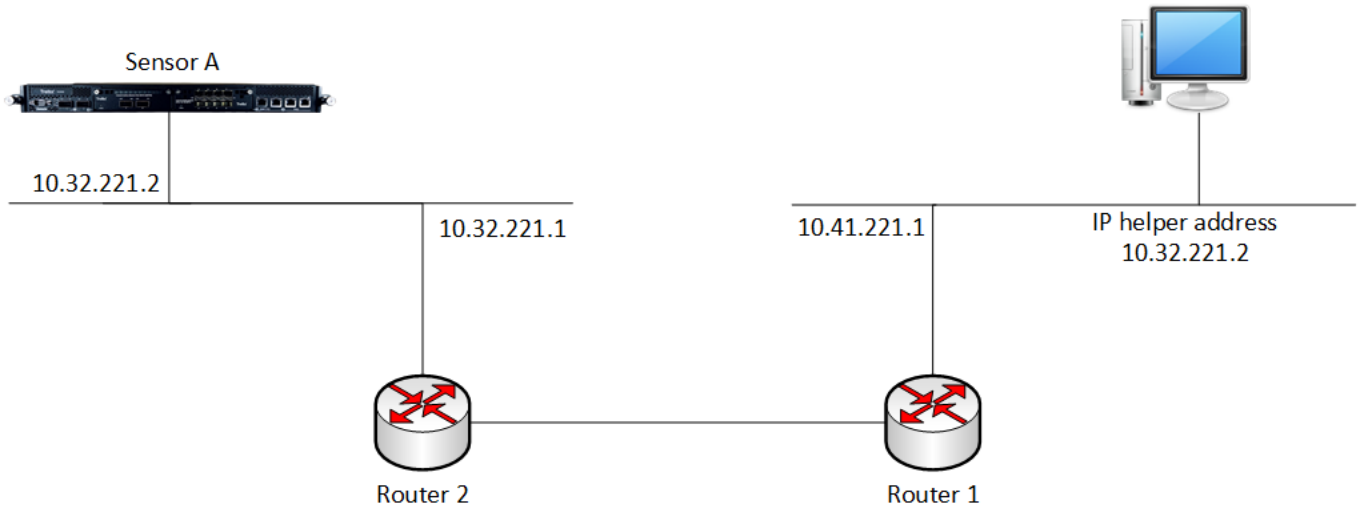
   This value specifies the duration after which information for a device is considered invalid. It occurs when the host has remained idle for the said duration. This timer ensures that the Sensor will renew its detection of the IP address if it is noticed again. Trellix recommends this duration be set at 1 hour. However, you can increase it up to 24 hours.

8. If you selected DHCP as your preference, you will need make sure that DHCP traffic actually passes through the Sensor monitoring port. If not, you have the provision to configure the monitoring port of a Sensor with an IP address to receive DHCP traffic through a relay agent. Provide these settings by selecting **Bind an IP Address For Copied DHCP Traffic?**.

   Using the DHCP Relay Agent

   A DHCP relay agent is any host that facilitates transfer of DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. In the illustration provided below, Sensor A exists in a specific physical subnet and the clients for which the Sensor needs to monitor DHCP traffic exist in another physical subnet. In such a network, you can use a DHCP Relay Agent to make sure that DHCP traffic from the clients in the other subnet reaches Sensor A. To accomplish this, you will need use a device, such as a router (we will consider a CISCO router that runs CISCO IOS software). The DHCP client broadcasts a request for an IP address and additional configuration parameters on its local LAN. Router 1, which plays the role of a DHCP relay agent, picks up the broadcast and generates a new DHCP message to send out on another interface. As part of this DHCP message, the relay agent inserts the IP address of the interface containing the **ip helper-address** command into the gateway IP address (giaddr) field of the DHCP packet, which will be the Sensor monitoring port IP address, 10.32.221.2. The DHCP relay agent sends the local broadcast, via IP unicast, to the Sensor monitoring port address, 10.32.221.2, specified by the ip helper-address interface configuration command. This enables Sensor A to monitor DHCP traffic in another physical subnet.

Figure 368. DHCP Relay Agent



a. Select the **Designated Port** which will function as the monitoring port.

b. Enter the **Port IP Address**, **Network Mask**, **Default Gateway**, and **VLAN ID** of the Sensor monitoring port.

This is the same IP address that you will provide in the relay agent configuration settings.

9. Click **Save**.

Configure device profiling at interface level

You can configure device profiling at the interface level as follows:

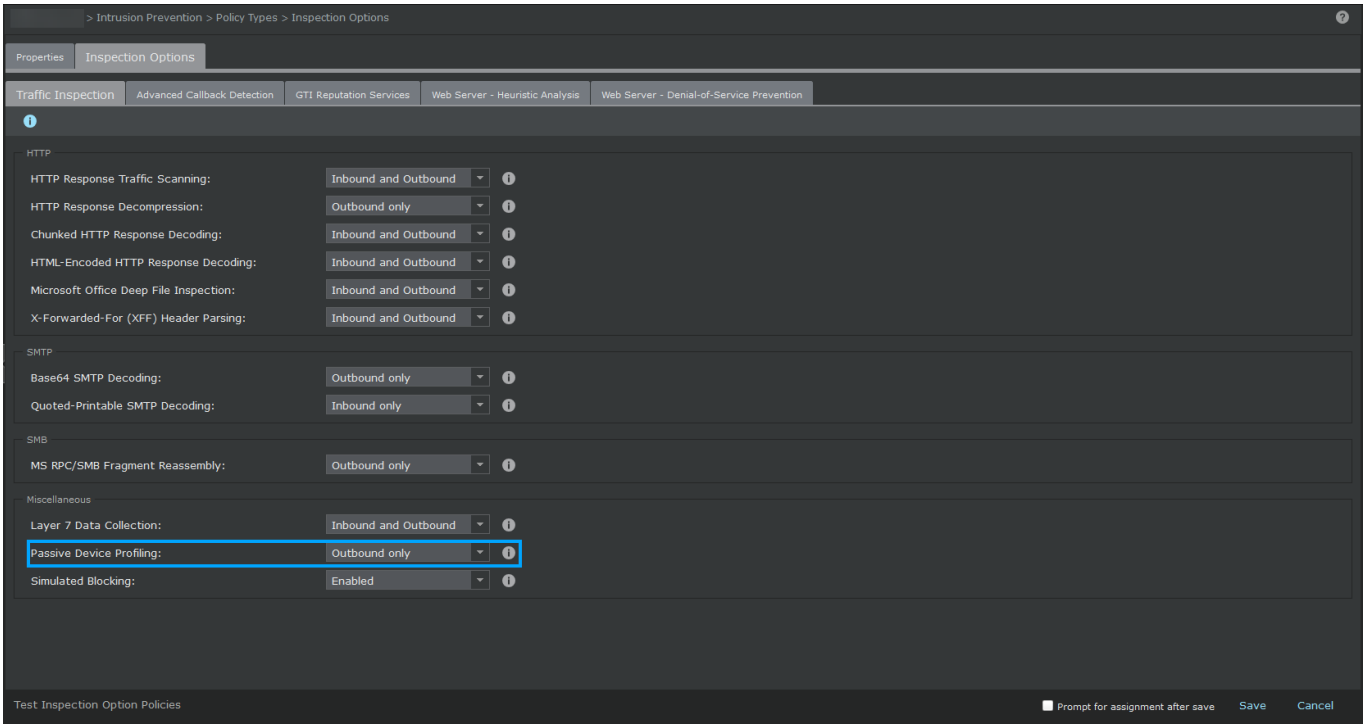
1. Navigate to Policy → <Admin Domain Name> → Intrusion Prevention → **Policy Manager**.
2. On the **Interfaces** tab, double-click on the interface to which you would like to enable device profiling.

   The **<Device Name/Interface>** panel opens.
3. In the **Inspection Options** section, select the policy from the **Policy** drop-down list.

   To create a new policy, click the + icon or click the ✎ icon to edit an already assigned policy.

   If you are creating a new policy proceed to step 4. If you are editing an existing policy proceed to step 5.
4. The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and click **Next**.

   The **Inspection Options** page opens.



5. On the **Traffic Inspection** tab, under **Miscellaneous**, enable **Passive Device Profiling** in the required direction.
6. Click **Save** in the **Inspection Options** page.
7. To save the configuration changes, click **Save** in the **<Device Name/Interface>** panel.

Limitations of passive device profiling

Passive device profiling in IPS consists of certain limitations that are enforced by other settings or hardware. These limitations are as follows:

- Profiling for devices with IPv6 addresses is currently supported only for HTTP device profiling.
- Device profiling will not happen for a host which:
  - Has the SYN cookie feature activated.
  - Has encountered an IGNORE firewall rule.
- Sensors have a limit on the number of profiles that they can process. This limit depends on the Sensor model. The Sensor models along with their specific limits are listed in the table below.

Table 43. Profile Limits

Sensor	Profile Limits (No. of profiles)
NS9500 stack - 100 Gbps throughput	100,000
NS9500 stack - 60 Gbps throughput	100,000
NS9500 stack - 40 Gbps throughput	100,000
NS9500 standalone - 30 Gbps throughput	100,000
NS9500 standalone - 20 Gbps throughput	100,000

Sensor	Profile Limits (No. of profiles)
NS9500 standalone - 10 Gbps throughput	100,000
NS9300, NS9200, NS9100	100,000
NS7600 - 15 Gbps	100,000
NS7600 - 10 Gbps	100,000
NS7600 - 5 Gbps	100,000
NS7500 - 7.5 Gbps	100,000
NS7500 - 5 Gbps	100,000
NS7500 - 3 Gbps	100,000
NS7350	100,000
NS7250	50,000
NS7150	25,000
NS7300	100,000
NS7200	50,000
NS7100	25,000
NS5200	15,000
NS5100	15,000
NS3600 - 5 Gbps	100,000
NS3600 - 3 Gbps	100,000
NS3600 - 1 Gbps	100,000
NS3500	10,000
NS3200/NS3100	10,000
IPS-VM600	15,000
IPS-VM5000	15,000

Device Profiling using Trellix ePolicy Orchestrator - On-prem

Trellix ePolicy Orchestrator - On-prem software is a management platform that enables centralized policy management and enforcement of your security products and the systems on which they reside. However, for ePolicy Orchestrator - On-prem to function, Trellix Agent needs to be installed on the client systems. The agent facilitates enforcement between the ePolicy Orchestrator - On-prem server and each managed client system. It retrieves updates, ensures task implementation, enforces policies, and forwards events for each managed system. As a ePolicy Orchestrator - On-prem becomes a repository of information and can be used in device profiling.

CAUTION

This information can also be viewed directly in ePolicy Orchestrator - On-prem, even if it does not participate in device profiling.

The Manager sends a query to ePolicy Orchestrator - On-prem when seeking information about a device profile. It accepts device information from ePolicy Orchestrator - On-prem and in case of Windows platforms, always trusts information received from ePolicy Orchestrator - On-prem over others.

Requirements for device profiling using ePolicy Orchestrator - On-prem

The list of requirements to consider before you begin using ePolicy Orchestrator for device profiling is as follows:

- Server that hosts ePolicy Orchestrator - On-prem 4.6 Patch 3 or above.
- Trellix Agent 4.6 Patch 2 or above installed on the clients, for which device profiling is necessary.
- Integration of ePolicy Orchestrator - On-prem with the Manager.

Set up the ePolicy Orchestrator - On-prem server

To find out how you can setup an ePolicy Orchestrator - On-prem server, please refer the [*Trellix ePolicy Orchestrator - On-prem* Installation Guide].

Set up Trellix Agent on managed clients

To find out how you can setup Trellix Agent on managed client systems, refer the [Trellix Agent Product Guide].

Integrate ePolicy Orchestrator - On-prem and the Manager

1. Go to Manager → <Admin Domain Name> → Integration → ePO → **ePO Integration**.

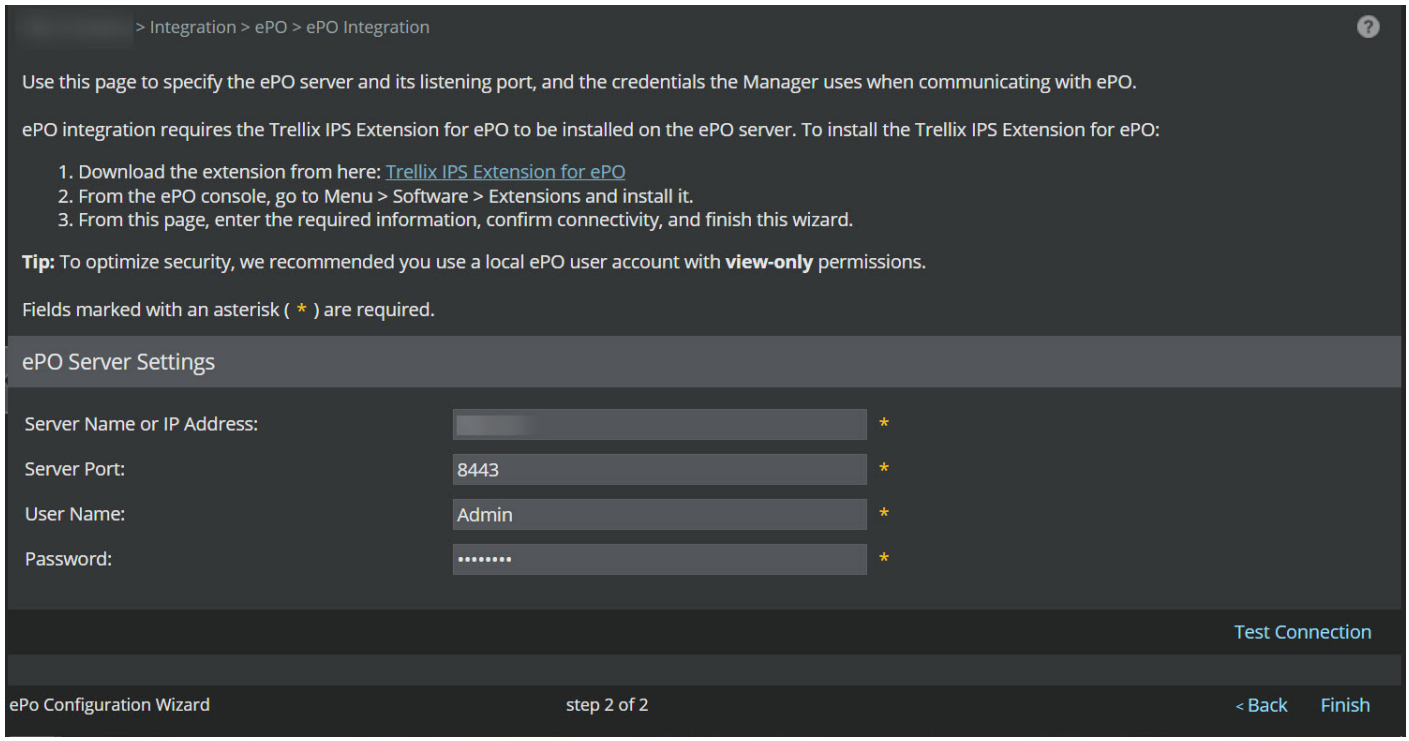
   The **Enable ePO Integration** page appears.
2. Select the checkbox for **Enable Endpoint Lookup?**.

   Enabling this option provides endpoint details like hostname, current user and OS version in the Attack Log.
3. Select the checkbox for **Enable Endpoint Tagging?**.

   Enabling this option allows you to tag endpoints in Attack Log.
4. Click **Next**.

   The **ePO Server Settings** page appears.

Figure 369. ePO Server Settings page



5. Click the **Trellix IPS Extension for ePO** hyperlink to download the **TrellixIPSExtension.zip** file.
6. Save the file in a convenient location in the local hard disk.
7. Log on to the ePolicy Orchestrator - On-prem console.

   The ePolicy Orchestrator - On-prem home page appears.
8. Go to Menu → Software → **Extensions**.

   The **Extension** page appears.
9. Click **Install Extension** at the bottom of the page.
10. Browse to the location that you have stored **TrellixIPSExtension.zip** file.

    Once installed, the Manager is listed under the Extensions list.
11. Close ePolicy Orchestrator - On-prem and return to the Manager.
12. Go to Manager → <Admin Domain Name> → Integration → ePO → **ePO Integration**.

Field	Description
Server Name or IP Address	Enter the name or the IP of the Trellix ePO - On-prem server running the extension file. Note that this Trellix ePO - On-prem server should have the details of the hosts covered by the admin domain. Contact your Trellix ePO - On-prem administrator for the server name and IP.
Server Port	Specify the HTTPS listening port on the Trellix ePO - On-prem server that will be used for the Manager -Trellix ePO - On-prem communication. Contact your Trellix ePO - On-prem administrator for the port number.

Field	Description
User Name	Enter the username to be used while connecting to the Trellix ePO - On-prem server. Trellix recommends you create an Trellix ePO - On-prem user account with **view-only** permissions required for integration.
Password	Enter the password for connecting to the Trellix ePO - On-prem server.

13. Click **Test Connection** to ensure that the extension file is installed and started on the Trellix ePO - On-prem server.
14. If the connection is up, then click **Finish**.

Display of device profiles in the Manager

After you have configured the various sources for device profiling, you will be able to view device profiles in the Manager. There are two methods to view device profiles:

- Using the Attack Log: In this method, the device profiles are visible in the form of source and destination operating systems. As stated earlier, the Manager receives device profile information from three sources: IPS Sensors, NTBA Appliances, and ePolicy Orchestrator - On-prem. Each of these inputs consists of a confidence level which is compared by the Manager, which then presents the device profile that has the highest confidence. Knowledge of the operating system allows the Manager to ascribe a relevance to each alert. Relevance helps prioritize an alert since certain alerts will only be relevant to certain operating systems; if not applicable to an operating system, such alerts are treated as not relevant. For more information on relevance, refer to the section [Alert Relevance].
- Using the device-profile script: In this method, you initiate the device-profile script that is bundled with the Manager installable. This script fetches the device profiles of all the hosts that the Manager currently has in its database. The script displays this data in a .csv file.

  In the Attack Log, you can only view the source and destination operating systems of the hosts associated with an alert. That is, if a host is not associated with an alert, you cannot view its operating system even if the Manager has this information. If you use the device-profile script, you can view the following details for all the hosts that are currently profiled:

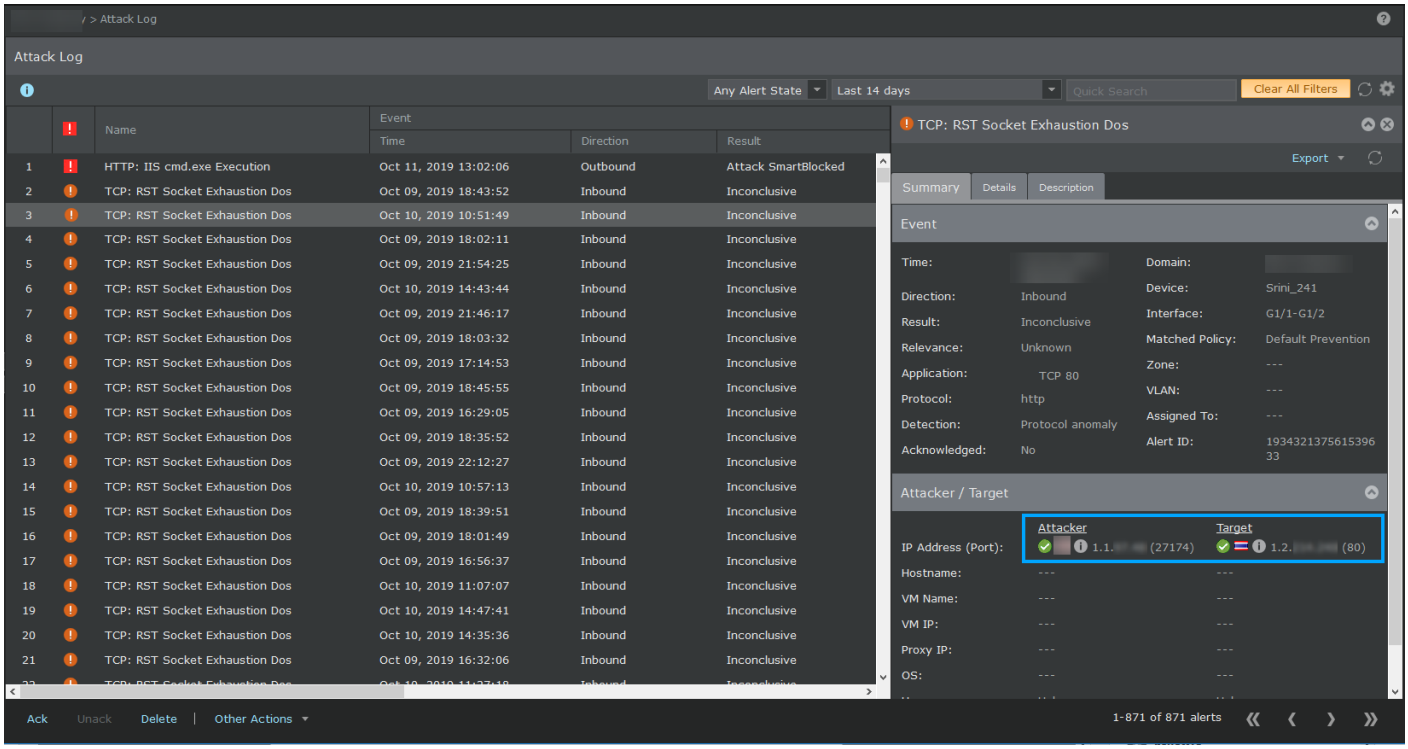
  - operating system
  - the device type
  - the source of the profile - IPS Sensor, NTBA Appliance, or ePolicy Orchestrator - On-prem

View device profiles in the Attack Log

You can view the device profiles in the Attack Log. To view device profiles in the Attack Log of the Manager:

1. Go to Analysis → <Admin Domain Name> → **Attack Log**.
2. Double-click on any alert for which you want to view the device profile.

   The alert details panel opens.
3. Under the **Attacker/Target** section, you can view the **Attacker** IP Address and the **Target** IP Address.



View device profiles using the device-profile script

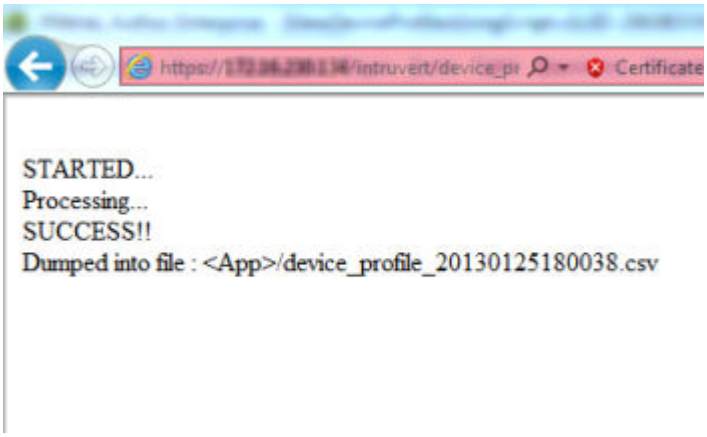
You need access to the Manager installation folder on the Manager server to view the generated .csv file.

1. Log on to the Manager using a supported browser.
2. After successful logon, duplicate the Manager session.

   For example, open the same browser that you used to log on in the previous step and enter the Manager URL.
3. In the duplicate Manager session, enter the following URL: `https://<Manager server IP or name>/intruvert/device_profile_csv.jsp`

   If the script runs successfully, a message is displayed in the browser.

Figure 370. Running the device-profile script



4. In the Manager server, go to `%programfiles%\Trellix\IPS Manager\App` and open the .csv file named device_profile_<time stamp>.csv.

Figure 371. Device profiles in a .csv file

	A	B	C	D	E	F
1	Host IP	Device	OS	Source	Creation Time	Last Modification Time
2	2001:0B00	General Purpose Computing Device	Microsoft Windows XP	1450-1 (IPS)	1/24/2013 12:43	1/24/2013 14:01
3	2001:0B00	General Purpose Computing Device	Microsoft Windows XP	1450-1 (IPS)	1/24/2013 12:45	1/24/2013 13:59
4	2001:0B00	General Purpose Computing Device	Microsoft Windows XP	1450-1 (IPS)	1/24/2013 12:43	1/24/2013 13:59
5	2001:0B00	General Purpose Computing Device	Microsoft Windows XP	1450-1 (IPS)	1/24/2013 12:45	1/24/2013 13:59
6	2001:0B00	General Purpose Computing Device	Microsoft Windows XP	1450-1 (IPS)	1/24/2013 13:01	1/24/2013 13:59
7	2001:0B00	General Purpose Computing Device	Microsoft Windows XP	1450-1 (IPS)	1/24/2013 13:07	1/24/2013 13:56

- Host IP: This is the IP address of the host. Only one row is maintained per IP address.
- Device: This is the type of the host. General Purpose Computing Device refers to desktops, laptops, and so on. Some other types are Android Device, Apple iOS Device, and HTC Device.
- OS: This is the operating system detected on the host.
- Source: This refers to the source of the profile - IPS Sensor, NTBA Appliance, or ePolicy Orchestrator - On-prem
- Creation Time: The time the host was profiled first.
- Last Modification Time: The time when the profile was last updated.

Troubleshooting for device profiling

This section includes troubleshooting that is specific to device profiling in IPS, ePolicy Orchestrator - On-prem, and NTBA.

Operating system or device does not match

When you are using ePolicy Orchestrator - On-prem for device profiling and encounter a situation in which the operating system or device type details do not match the actual system details, check the ePolicy Orchestrator - On-prem console to know whether the operating system and device type information is correct here.

- If the information displayed here is incorrect, refer to the [Trellix ePolicy Orchestrator - On-prem Product Guide].
- If the information displayed here is correct, to the <app folder> for the Manager and open `dpinfo.log` or `ePO.log`.

> **NOTE**
>
> The logging to `ePO.log` will not be enabled by default. To enable this, refer to the section [Enable ePO.log].

Alert relevance

When you see an alert in the Attack Log, you are being shown the details pertinent to an attack attempt. One of the factors that can help you make a decision on whether or not to act is the result of the attack. Ultimately, it is the relevance of the attack that can assist you with this decision.

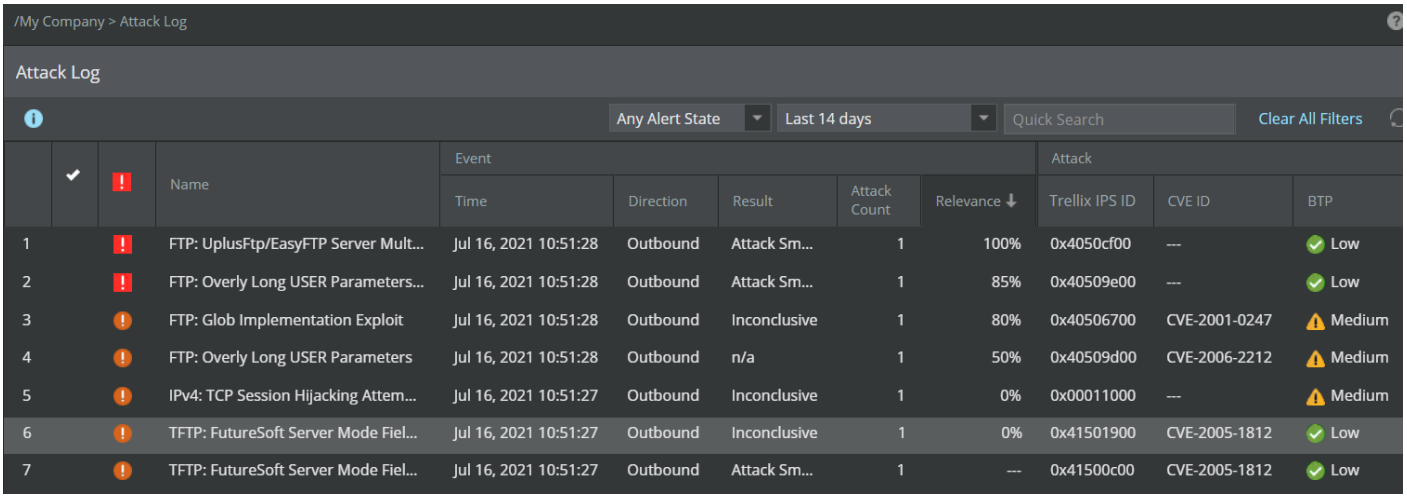
Alert relevance (also called relevance) is the extent to which the alert generated is relevant. It is defined numerically and calculated for signature based attacks.

Relevance is a score that is displayed in the Attack Log under a separate column labeled **Relevance**. Relevance is represented as a percentage of relevance of an alert to the target host and it ranges from 0% to 100%.

NOTE

The Relevance column is hidden by default and will need to be enabled manually.

Figure 372. Relevance column in Attack Log



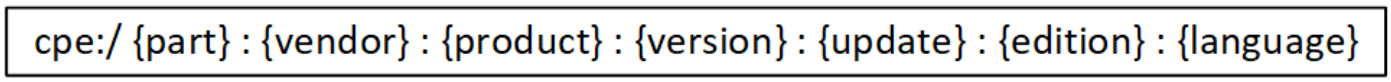
The relevance scoring algorithm

Common Platform Enumeration to identify vulnerable systems

If the operating system does not completely match, the result of the attack is inconclusive. In such circumstances, the Manager assigns a partial relevance score by way of a scoring algorithm. Scoring relies on the matching each component of the Common Platform Enumeration (CPE) name of attack signature with CPE name of the target system. CPE™ is a standardized method of describing and identifying classes of applications, operating systems, and hardware devices present among an enterprise's computing assets. CPE can be used as a source of information for enforcing and verifying IT management policies relating to these assets, such as the vulnerability of a target system to a malicious attack. Trellix IPS collects information about servers, workstations and other devices on the network, identifies these products using their CPE names, and uses this standardized information when matching the CPE of the attack signature to the CPE of each device. For more information on CPE, you can go to http://cpe.mitre.org.

CPEs are represented in a certain order and with a specific syntax. The universal CPE format is represented in the following figure.

Figure 373. CPE Format



How CPE influences the relevance score

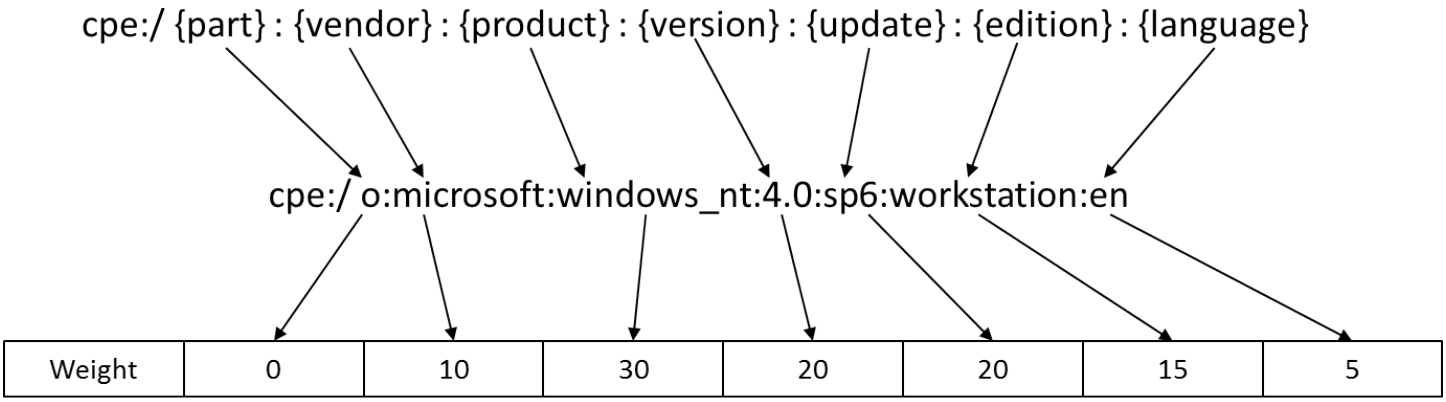
Each component in the CPE is given a specific weight depending on the potential of that component to contribute to the vulnerability of the system. The table below presents the various components in the CPE that are used to compute the relevance score:

Table 44. Components of a CPE and their weights

Component	What it signifies	Carries a weight of
Part	First component in the CPE, which is a single letter code that designates the particular platform part that is being identified. The following codes are defined for the part: • h – hardware part • o – operating system part • a – application part	0
Vendor	Second component in the CPE name, which refers supplier or vendor of the platform part. Example: Microsoft, Redhat, etc.	10
Product	Third component in the CPE name, which refers a specific product developed by the vendor. Example: Windows XP, Windows NT, Enterprise Linux, etc.	30
Version	Fourth component in the CPE name, which refers to a specific version of the product. Example: 4.0 for Window NT, 4 for Enterprise Linux, etc.	20
Update	Fifth component in the CPE name, which refers to a specific update of the version. Example: SP6 for Wndows NT, Update 4 for Enterprise Linux, etc.	20
Edition	Sixth component in the CPE name, which refers to the edition of the product. Example: Workstation, Server, etc.	15
Language	Seventh component of the CPE name, which refers to the language of the product. Example: English, Spanish, etc.	5

The illustrative diagram below shows the format and correlates it with real world products and in turn with weights as displayed in the table above.

Figure 374. CPE Illustration



Following are a few examples of CPEs:

- `cpe:/o:microsoft:windows_xp:::pro`
- `cpe:/a:adobe:reader:8.1`
- `cpe:/o:redhat:enterprise_linux:4:update4`

CPE name matching logic

To compute the relevance score, the CPE of the attack signature is matched with every component of the CPE of the target system. If any component is not mentioned in the attack signature CPE, it applies to all instances that can occupy that position. For example `cpe:/o:microsoft:windows_xp` applies to all versions, updates, editions, and languages of Microsoft Windows XP.

A CPE match is considered definitive.

A few more examples to illustrate the name matching logic are presented below:

- Case 1 – `cpe:/o:microsoft:windows:xp` will match all the operating system variants mentioned below:
  - `cpe:/o:microsoft:windows:xp::sp1`
  - `cpe:/o:microsoft:windows:xp::sp2`
  - `cpe:/o:microsoft:windows:xp`
  - `cpe:/o:microsoft:windows:xp::sp1:professional`
  - `cpe:/o:microsoft:windows:xp::sp1::en`
- Case 2 – `cpe:/o:microsoft:windows:xp::sp1` will not match `cpe:/o:microsoft:windows:xp::sp2` because not all parameters of the attack signature CPE match the target system CPE.

Scenarios to understand score computation

Refer to the table below to view some scenarios for alert relevance scoring.

Table 45. Illustrating relevance score calculation through examples

Attack signature CPE	Description of the attack signature CPE	Target system CPE	How the two CPEs match up	Relevance score
`cpe:/o:microsoft:windows_xp::sp2`	This attack is relevant to all Microsoft Windows XP SP2 systems, irrespective of which version, edition, and language they use.	`cpe:/o:microsoft:windows_xp::sp2:professional`	Since the CPE from the attack signature is considered definitive, and all components of the target system CPE match the components of the attack signature CPE, the alert generated is 100% relevant.	100%
		`cpe:/o:microsoft:windows_xp`	Since the CPE from the attack signature is considered definitive, and only the `{part}`, `{vendor}`, and `{product}` components of the attack signature CPE, and not the `{update}` component, matches the target system CPE, the alert generated has a relevance of 100 - 20 = 80%.	80%

Attack signature CPE	Description of the attack signature CPE	Target system CPE	How the two CPEs match up	Relevance score
		`cpe:/o:microsoft:windows_xp::sp3`	Since the CPE from the attack signature is considered definitive, and the `{part}`, `{vendor}`, and `{product}` components of the attack signature CPE match that of the target system CPE, the alert might initially appear relevant. However, notice that the `{update}` component of the target system CPE is present but different than that of the attack signature CPE. This means that the alert generated will not be relevant and the score will be 0%.	0%

Special scenarios in which the relevance score is computed

- In day-to-day operations, not every attack that is mounted and consequently every attack signature CPE that is extracted is as straightforward as those that are mentioned above. In some cases of device profiling, a thorough analysis might not be possible. As a result, device profiling does not isolate the operating system and presents a possibility of more than one operating system. The relevance score is calculated by as the average relevance score of all the matched CPEs.

  Presented in the table below are some such scenarios where the relevance score is computed for a group of CPEs.

Figure 375. Representation of a group CPE

cpe:/ o:microsoft:windows_2000_windows_xp_windows_2003

Table 46. Illustrating relevance score calculation for group CPEs through examples

Host group CPE	Maps to individual CPEs	CPE match scenarios	Relevance score logic	Relevance score

`cpe:/o:microsoft:windows_2000_windows_xp_windows_2003`	`cpe:/o:microsoft:windows_xp`
	`cpe:/o:microsoft:windows_2000`
	`cpe:/o:microsoft:windows_server_2003`
		Case 1: All CPEs match
		`cpe:/o:microsoft:windows_xp`
		`cpe:/o:microsoft:windows_2000`
		`cpe:/o:microsoft:windows_server_2003`
			Since all the CPEs match, the relevance score is computed as the maximum.	100%

Host group CPE	Maps to individual CPEs	CPE match scenarios	Relevance score logic	Relevance score

		Case 2: Two CPEs match
		`cpe:/o:microsoft:windows_xp`
		`cpe:/o:microsoft:windows_server_2000`
			Since only two of three CPEs match, the score will be computed as 200/3 = 66%.	66%

		Case 3: One CPE matches
		`cpe:/o:microsoft:windows_xp`
		`cpe:/o:microsoft:windows_server_2008`
			Since only one of three CPEs matches, the score will be computed as 100/3 = 33%.	33%

		Case 4: Two CPEs match
		`cpe:/o:microsoft:windows_xp`
		`cpe:/o:microsoft:windows_server_2000`
		`cpe:/o:microsoft:windows_server_2008`
			Since only two of three CPEs match, the score will be computed as 200/3 = 66%.	66%

- There are also cases when conventional methods of calculating a relevance score are not able to provide a score. This is especially noticed when the exact details of the operating system are not available. It can also be noticed when the attack is being launched through an application and details of the application are not available. In such instances, the Manager relies on the attack signature to be able to provide you more clarity.

  The Manager determines the vulnerable application and uses the signature to decipher the operating system it is compatible with. It then compares this operating system to the target operating system. If they match, a default score of 50% is displayed. If they do not match, a score of 0% is displayed. For example, if the application is one that runs only on a Linux-based operating system but the attack is directed at a system running Microsoft Windows, the attack will not be relevant. Or, assume that the attack is one that exploits a vulnerability in Microsoft Word (which is assumed to only be compatible with Microsoft Windows) and the target environment is running some Microsoft product, a default score of 50% will be displayed, prompting you to further investigate.

Special circumstances

Your network may have specific settings or deployments that affect the way alert relevance works. The following scenarios discuss this:

- **Management disaster recovery (MDR)** – If your network is configured for management disaster recovery, the relevance is calculated separately in each of the Managers.

- **Simulated blocking** – In case an attack is blocked, the alert relevance will be calculated using target host details. The same steps will be followed for Simulated Blocking.

Enable alert relevance

By default, you will find alert relevance enabled in the Manager. If you want to alter alert relevance settings in the Manager at any time, perform the following steps.

1. Select Manager → <Admin Domain Name> → Troubleshooting → **Alert Relevance**.

   The **Alert Relevance** page appears.
2. Select the **Alert Relevance Analysis?** checkbox.
3. Click **Save**.

Advanced Malware Policies

Modern advanced malware based attacks pose acute security threats to enterprises. Trellix IPS provides several features to detect and prevent the advanced threats prior to infection. You can also detect post infection by monitoring the bot command and control server activity. Trellix IPS provides visibility across multiple network vectors (host, IP, user, and so on) and the ability to correlate this information over a period of time. Once a threat is identified, understanding the root cause and exposure are critical to avoid similar threats in the future.

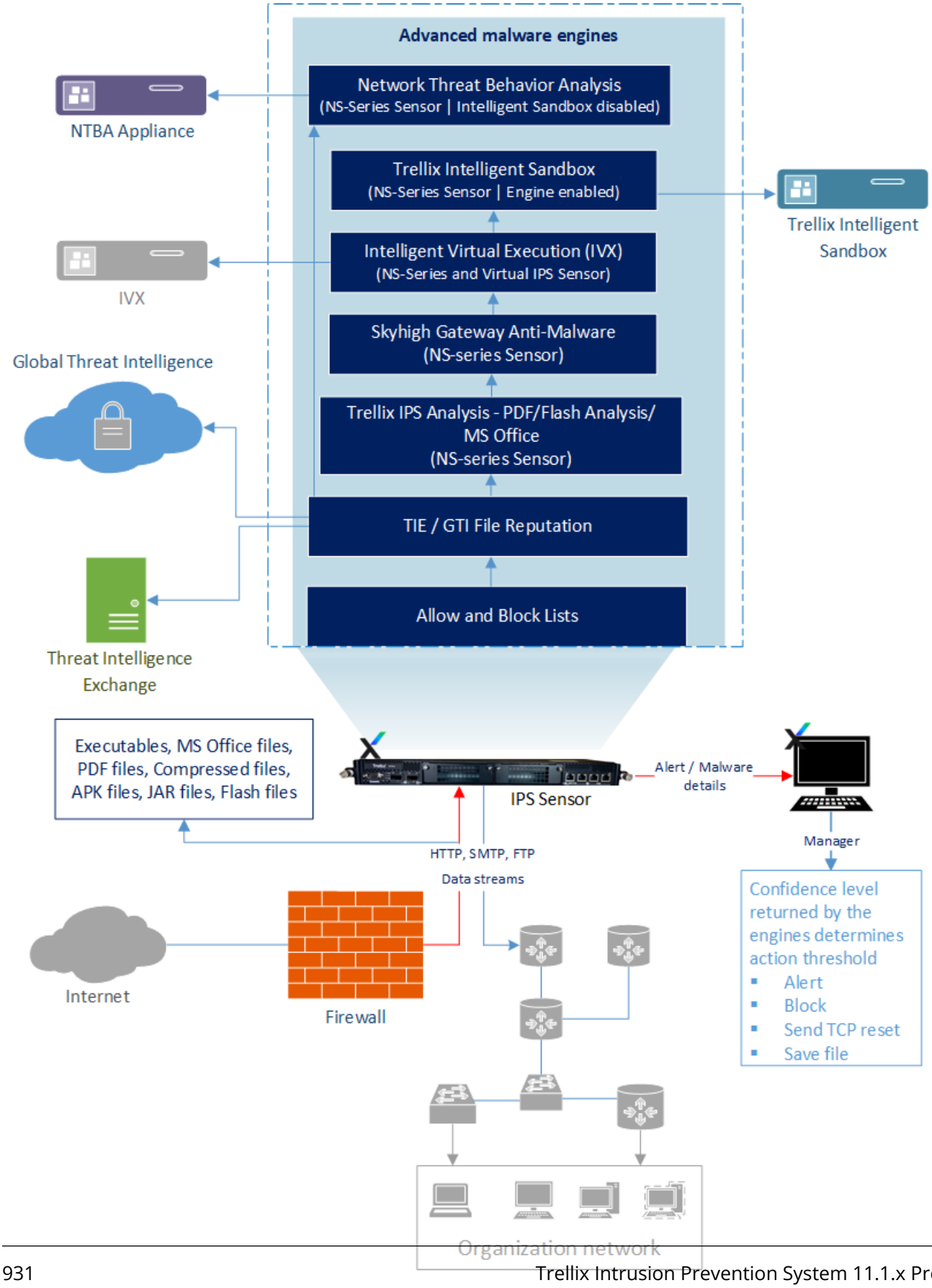
The primary functionality of the **Advanced Malware Protection** feature is to provide a prioritized list of hosts that need remediation based on a risk score determined on a set of threat vectors and events correlated over time.

How an Advanced Malware policy works

A malware policy is a set of rules that scans the traffic across your network, and determines how to respond to malware detected in the network. An effective policy is customized to the network environment being monitored.

A Trellix malware policy is a set of rules that define the traffic to be scanned for the detection of malware and how you want to respond if the malicious activity is detected. Creating a policy enables you to define an environment to protect by the different operating systems, applications, and protocols in your network. These parameters, or rules, relate to all of the attacks defended against by Trellix IPS.

Figure 376. Advanced malware detection



A malware policy has various components. The malware policy allows you to select the **Protocols to Scan**. You can select the protocol streams which are monitored by the Sensor according to the configured malware policy. The Sensor can extract files from the HTTP, FTP, and SMTP traffic for scanning.

In general, when a user downloads a file, it might either be a file that was downloaded as a complete file or one that was downloaded as many segments and then reassembled to form the original file. Files are, at times, split by browsers or download managers to speed up the download. The Sensor can scan and analyze files that are downloaded as a complete file or as many segments.

Specific **File Type** in the HTTP, FTP, and SMTP data streams can be scanned, selected based on the kind of traffic your network experiences. Various **Malware Engines** are supported to scan the selected file types in the network traffic. You can configure one or more supported engines for a specific file type.

NOTE

Blocking malware over FTP is not always possible. For blocking malware, the Sensor needs to know the file size or the end of the file. If file size is not known when using FTP utility, the Sensor raises an alert with **Inconclusive** results in the Manager when FTP file blocking/alert/tcp-reset option is enabled in the malware policy. If the file size is known, the file transfer is blocked and the Sensor raises an alert with the result as **Attack Blocked** in the Manager.

There is, however, an exception to this case. If the file size is not known but end of file is read by Trellix Advanced Research Center, the file transfer is blocked in that case, and **Attack Blocked** is displayed in the alert generated in the Manager.

Trellix IPS performs malware analysis on APK files in the following sequence:

- **NS-series**: Allow and Block Lists → TIE/GTI File Reputation → Trellix IPS Analysis → Gateway Anti-Malware → IVX → Trellix Intelligent Sandbox → **NTBA**
- **Virtual IPS**: Allow and Block Lists → TIE/GTI File Reputation → Trellix IPS Analysis (PDF/Flash files only) → IVX → Trellix Intelligent Sandbox → **NTBA**

Trellix IPS performs malware analysis on Executables and PDF files in the following sequence:

- **NS-series**: Allow and Block Lists → TIE/GTI File Reputation → Trellix IPS Analysis (PDF/Flash/Microsoft Office files) → Gateway Anti-Malware → IVX → Trellix Intelligent Sandbox → **NTBA**
- **Virtual IPS**: Allow and Block Lists → TIE/GTI File Reputation → Trellix IPS Analysis (PDF/Flash/Microsoft Office files) → IVX → Trellix Intelligent Sandbox → **NTBA**

After the scanning is complete, these engines report a certain confidence level for the scanned file. The confidence level is based on the specificity and severity of the malware and is indicative of the extent to which the file is infected, for example, a high confidence level indicates a high probability of the file being infected. The **Action Thresholds** are set to be triggered based on the confidence level returned. Since, dynamic analysis is a time taking process, there is a need to carefully employ this process for improved user experience. Trellix IPS submits files to Trellix Intelligent Sandbox for dynamic analysis only if other engines that are enabled report back a malware confidence lower than medium.

You can remediate the threat through configured response actions like blocking and quarantining infected hosts, stopping malicious file download and identifying hosts with a high threat score through the dashboard. You can prevent the malware from reaching the host by blocking it or sending TCP resets. You can analyze malware using the malware dashboards. The malware dashboards allow you to drill down into each piece of detected malware. The **Malware Files** page provides you with more details of the detected malware. You can also save the malicious file and submit it for analysis.

The supported parameters for a malware policy are:

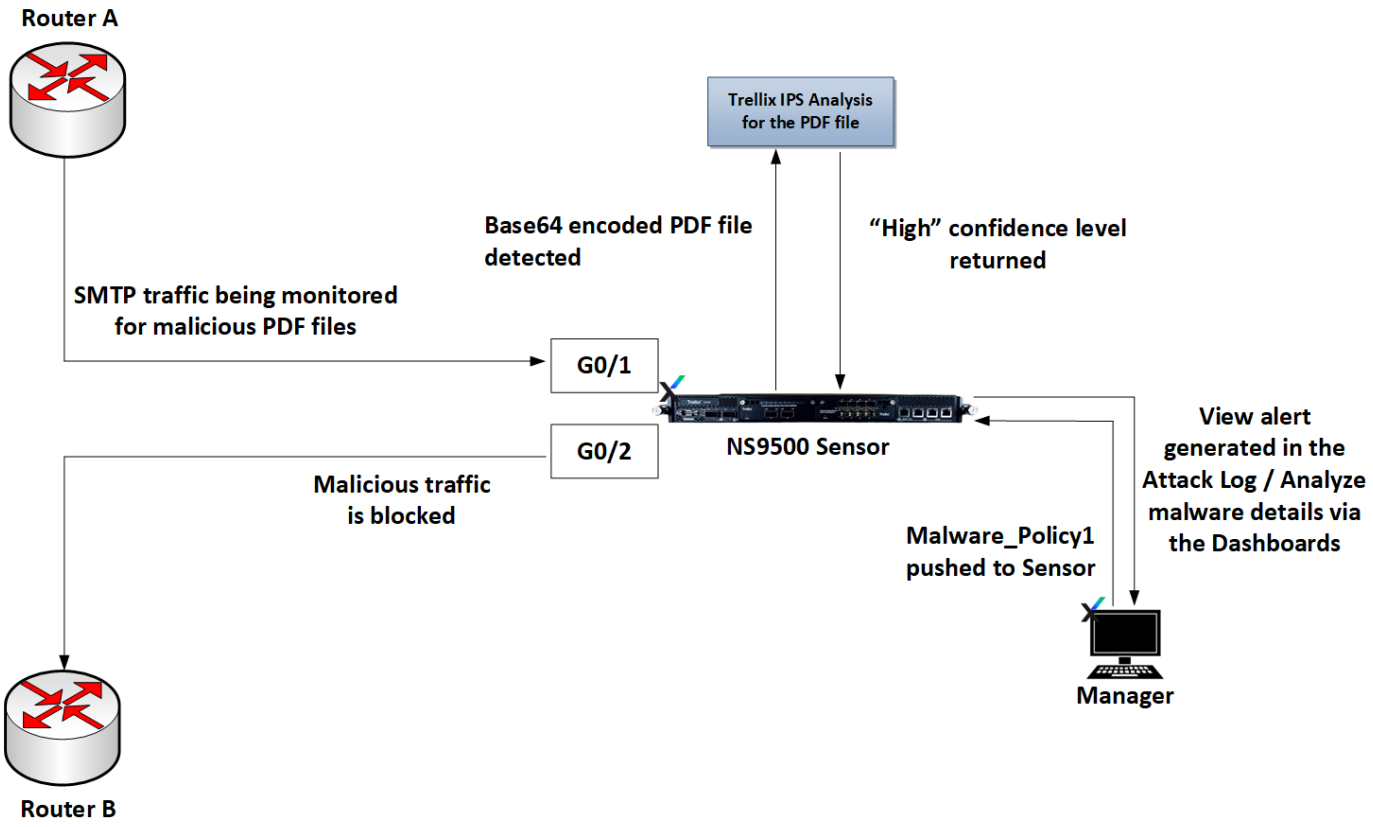
- **File Type**: Executables, Microsoft Office files, PDF files, compressed files, Android application package, Java archive, and flash files.
- **Malware Engines**: Allow and Block Lists, GTI File Reputation, Trellix IPS Analysis, Skyhigh Gateway Anti-Malware (GAM), Intelligent Virtual Execution (IVX), and Trellix Intelligent Sandbox.
- **Action Thresholds**: Alert, Block, Send TCP Reset, Add to Block list, and Save File.

Consider the following example.

- The Sensor is deployed in the inline mode. Monitoring ports G0/1 and G0/2 inspect traffic flowing between router A and router B.
- Create an Advanced Malware policy, *Malware Policy_1* with the following PDF malware rule enabled for SMTP traffic and push the policy to the Sensor.
    - **File Type**: PDF
    - **Malware Engine**: Trellix IPS Analysis
    - **Action Thresholds**: For *Very low*, *low* and *medium* confidence level returned, the configured action is to generate an *Alert*.

      For *High* and *Very high* confidence levels, the configured response action is to *Block* and *Send TCP Reset*.
    - Configure the malicious file to be saved for analysis.
- Assign the policy to both inbound and outbound traffic and to the available interfaces (in this case to ports G0/1 and G0/2), according to your requirement.

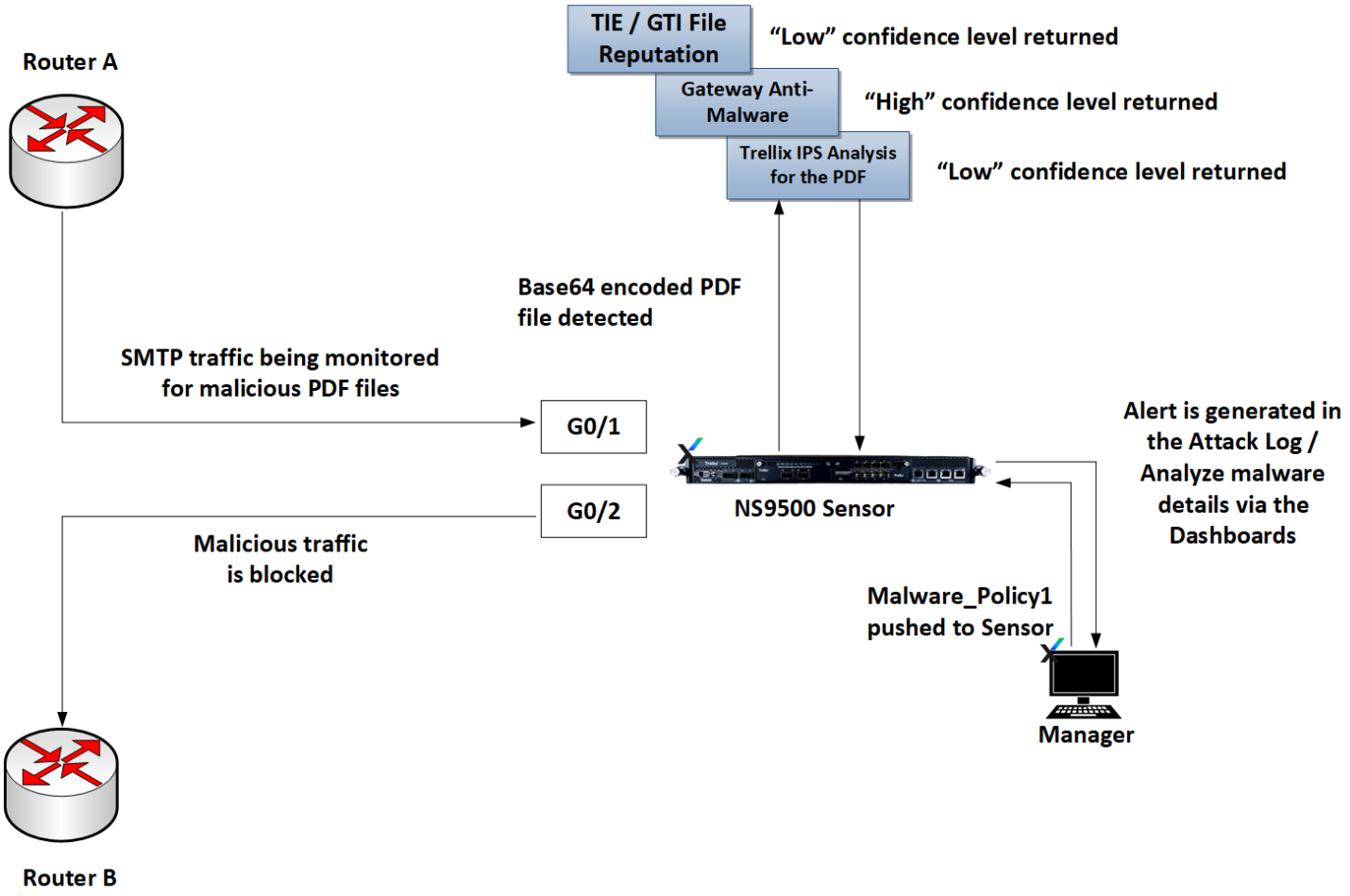
Figure 377. Advanced malware detection using Trellix IPS Analysis



- The PDF files are extracted from the SMTP data streams and scanned by the PDF-JavaScript component of the Trellix IPS Analysis engine. The engine detects a Base64 encoded PDF file.
- Based on the severity and the extent to which the file is infected the Trellix IPS Analysis engine returns a confidence level. In this case, the confidence level returned is *high*. An alert is raised in the Attack Log.
- As defined by the malware policy, the response action is triggered for a *high* confidence level. The detected malware infected data packets are dropped. Thus, malicious files are prevented from reaching the host.
- You can drill down and analyze the infected hosts and the malware details through the various dashboards.

Consider some variation to the above example and have multiple engines configured, namely, Skyhigh Gateway Anti-Malware, Trellix IPS Analysis, and TIE / GTI File Reputation. Multiple engines report varying confidence levels; Trellix IPS Analysis and TIE / GTI File Reputation report a low confidence level while Gateway Anti-Malware reports a high confidence level. In such a scenario, the highest confidence level returned is considered by the Sensor when evaluating its response action. In this case, based on the high confidence level returned by the NTBA engine, traffic is blocked.

Figure 378. Advanced malware detection using multiple engines



Trellix advises you to create multiple, specific policies that focus on the specific needs of unique zones in your network, rather than a one-size-fits-all policy for the entire network.

- **TIE / GTI File Reputation**

  Trellix IPS integrates with Threat Intelligence Exchange (TIE) and Trellix GTI File Reputation. While Trellix GTI is a cloud-based service that provides real-time protection from malicious file downloads, Threat Intelligence Exchange is an enterprise repository for file reputation which is provided by several individual security products.

  For more information on both these products, see [Trellix Intrusion Prevention System Integration Guide].

  Sources, such as Intelligent Sandbox and Trellix GTI, provide file reputation for several file hashes to Threat Intelligence Exchange. You, as a security administrator, have the discretion to override this file reputation with an enterprise specific reputation to suit your environment. This management is carried out through the ePO console. In future, when the same file hash is detected by the Sensor, it queries Threat Intelligence Exchange which responds with the customized file reputation. You then have the ability to make a decision based on that file reputation response.

  GTI File Reputation scans the selected file type for potential malware including encoded files. The Sensor creates a finger-print (MD5 hash value) of the file that is seen as potentially malicious, embeds the fingerprint in a standard HTTPS request, and sends it to a Trellix GTI cloud server. The cloud server compares the fingerprint against the threat database maintained by Trellix ARC. If the fingerprint is identified as a known malware, the cloud server notifies the Sensor and it enforces a response action for the malware.

- **Allow and Block Lists**

  Trellix IPS also provides users the option to upload custom fingerprints to the Manager, which can be used for file reputation instead of GTI lookups or to complement them. The Manager then sends these fingerprints to the Sensors.

  You can add the MD5 or SHA256 hash values of known malicious files to the block list and MD5 or SHA256 hash values of trusted files to the allow list. The Sensor scans the specified file types for potential malware, including encoded files, and compares it with custom fingerprints. This enables the Sensor to immediately identify known malware and also identify the trusted files, without having to analyze such files further. This saves both time and valuable Sensor resources.

  NOTE

  - The Manager running on **11.1 Update 1** or later releases supports addition of up to 400,000 hash entries (allowed and blocked combined) with a limit of 200,000 per each hash type. Manager prior to **11.1 Update 1 release** supports addition of only MD5 hashes up to 100,000 entries (allowed and blocked combined).
  - Sensors prior to **11.1 Update 1 release** do not support SHA256 hashes. The maximum number of hashes supported (cumulative of Blocked Hashes and Allowed hashes) by these Sensors is 100,000.
  - Sensors running on **11.1 Update 1** or later releases support both SHA256 and MD5 hashes. NS-series Sensors support a maximum of 200,000 hashes for each hash type while Virtual IPS Sensors support a maximum of 100,000 hashes for each hash type. If the Manager has both NS-series and virtual Sensors, entries over 100,000 in each hash type are pushed only to the NS-series Sensors. The push fails on virtual Sensors and a fault is raised which can be noticed in the **Faults** (Manager → Troubleshooting → Logs → **Faults**) tab.
  - In case of heterogeneous environments, if the total MD5 hash entries exceed 100,000:
    - A limit exceed error can be seen in **filetransfer.log** during a bulk (full) update
    - A fault will be raised in the **Faults** tab and error count will be incremented at the Sensor level during an incremental update. Refer to **`show ab stats`** command for more information.

      NOTE

      A Full update is triggered when the total entries are more than 4000; else, an incremental update is triggered to all the Sensors connected to the Manager.
  - In case MD5 and SHA256 hashes of the same file are added, the MD5 hash takes precedence over SHA256 hash of the file during analysis.

  NOTE

  The Sensor checks the allow list before the block list.

  If a match is found in the block list, it enforces a response action. It can also be configured per interface. Note the following when custom fingerprints is configured among multiple engines.

  - When multiple engines are selected, allow list and block list get the highest priority. It is the first engine to scan the file.
  - If the scanned file finds a match in the allow list, the file is considered to be clean.
  - If the scanned file finds a match in the block list, none of the other configured engines scans the file. A confidence level of **Very High** is returned and the configured response action is triggered.

- If the scanned file does not find a match in the allow or block list, other applicable engines scan the file. The highest confidence level returned is considered for the response action.

For more information on block and allow lists, see the [Trellix Intrusion Prevention System Integration Guide].

- **Trellix IPS Analysis**

  On board the Sensor are various individual engines that make it possible to scan for advanced malware threats emerging through several vectors. These engines, although individual, focus on a common objective and are called Trellix IPS Analysis. Trellix IPS Analysis is capable of analyzing the following files for threats:

  - JavaScript in PDF files
  - Shell code in Flash files and those that are embedded in PDF files
  - Shell code in Microsoft Office files

  Trellix IPS Analysis is enabled by default with scanning enabled for Microsoft Office files, PDF files, and Flash files.

  PDF-JavaScript: Trellix IPS Analysis extracts JavaScript in the PDF and executes the extracted JavaScript. It uses heuristics to detect attacks. If any malicious content is found, the Sensor sends an alert to the Manager. Based on the confidence level returned, the configured response action takes place.

  For encrypted PDF files, the engine locates the encryption dictionary and generates the master key.

  If the file is in XDP format, the Base64 stream is decoded and the JavaScript extraction process begins.

  The PDF engine searches for objects containing embedded files. If embedded files are found, those are extracted. If the extracted embedded file is a PDF file, flash file (.cws, .fws, or .zws), Portable Executable (PE) file, or Microsoft Office file, the JavaScript extraction process begins.

  Shell code in Flash files: The Sensor supports detection of malicious flash files using heuristic analysis rather than signatures. The Sensor detects various flash exploitation techniques, such as Vector spraying, presence of shell code, and similar exploitation techniques.

  The Sensor transfers files to the flash engine after the flash file is successfully extracted. The flash engine scans incoming flash files. If any malicious content is found, the Sensor sends an alert to the Manager. Based on the confidence level returned, the configured response action takes place.

  Shell code in Microsoft Office files: Microsoft Office files sent over HTTP, SMTP, and FTP are examined for shell code that might be embedded. Further, if the shell code is XOR encrypted, the Sensor decodes the file. If the file contains shell code it is considered suspicious, and sent to the next engine for further analysis.

- **Skyhigh Gateway Anti-Malware Engine**

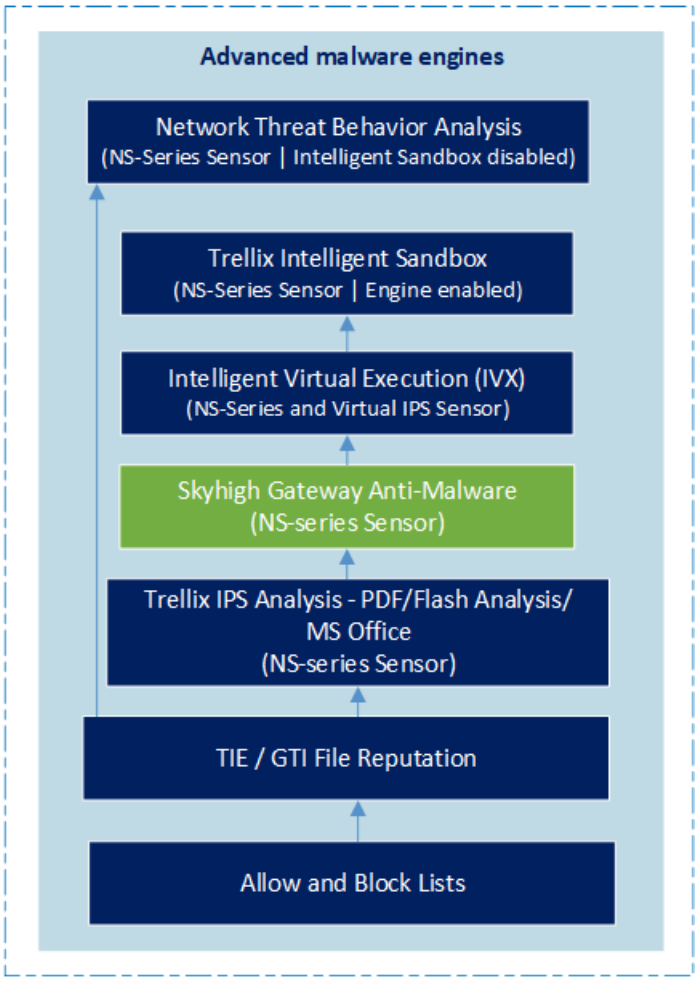
  The NS-series Sensors and NTBA appliances are equipped with the Skyhigh Gateway Anti-Malware Engine, which consists of the Gateway Anti-Malware DAT and engine, Anti-Virus DAT, and Anti-Malware Engine.

  Gateway Anti-Malware Engine operates on several platforms and detects and blocks malware threats — everything from viruses and worms to adware, spyware, and riskware. To further protect end users against emerging malware threats, zero-day threats, and targeted attacks, Gateway Anti-Malware Engine focuses on generic and heuristic detection of malware.

  If your deployment consists of an NS-series Sensor and an NTBA appliance, the files are scanned by Gateway Anti-Malware Engine present on the Sensor. The illustration shows you scenarios in which files are sent to Gateway Anti-Malware

  The illustration shows you scenarios in which files are sent to Gateway Anti-Malware.

Figure 379. Selection criteria to send files to Skyhigh Gateway Anti-Malware Engine



The file is scanned by Gateway Anti-Malware Engine which returns results (confidence level) to the Sensor. The Sensor sends the alert to the Manager and the response action configured in the Manager is acted upon.

The Sensor and NTBA appliances are configured to use a specific version of Gateway Anti-Malware Engine. This version depends on the Manager software version you are running to manage Sensors and NTBA Appliances. The table below illustrates different versions of Gateway Anti-Malware Engine that are compatible with different Sensor, Manager, and NTBA versions.

With support for Gateway Anti-Malware 2017 on NS-series Sensors, the engine supports proxy server for GTI integration with file reputation enabled. The Anti-Malware engine version available with Gateway Anti-Malware is 59xx.

Skyhigh Gateway Anti-Malware	Anti-Malware Engine Version	Manager	Sensor	NTBA
2014	5700	NA	NA	9.1.3.3 or later
2015		NA	NA	9.1.3.1 or later
2017	5900	10.1.7.4 or later	10.1.5.3 or later	NA

Skyhigh Gateway Anti-Malware	Anti-Malware Engine Version	Manager	Sensor	NTBA
2019	5900	10.1.7.29 or later	10.1.5.41 or later	NA
2021	5900	10.1.7.55 or later	10.1.5.153 or later	NA
2023	6600	11.1.7.81 or later	11.1.5.84 or later	NA

- **Intelligent Virtual Execution (IVX)**

  Intelligent Virtual Execution (IVX) Engine is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature-based and policy-based defenses. The IVX engine detects zero-day, multiflow, and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyberattack kill chain by identifying never-before-seen exploits and malware.

  Trellix IPS offers integration capability with Trellix Intelligent Virtual Execution - Server and Trellix Intelligent Virtual Execution - Cloud which utilize IVX engine's technology to perform malware analysis.

  When you integrate Trellix IPS with IVX, the Sensor initiates a communication channel with the Trellix VX or Trellix IVX Cloud. This channel is open unless the Sensor is down, the Trellix VX (IVX) or Trellix IVX Cloud (IVX Cloud) is down, or you disable the integration. By default, this communication channel is over HTTPS protocol and the IVX and IVX Cloud listen on port 443 which cannot be changed.

  The Manager accesses the RESTful APIs of IVX for its communication. When a connection is required, the Manager establishes an HTTPS connection. IVX and IVX Cloud listen on a fixed port number 443 for such connections.

  When you integrate Trellix IPS with IVX and the authentication is successful, IVX serves as an additional malware engine for all the supported file types in the Advanced Malware Policies. You can select this engine along with any of the other malware engines.

  For more information on IVX integration, see [Trellix Intrusion Prevention System Integration Guide].

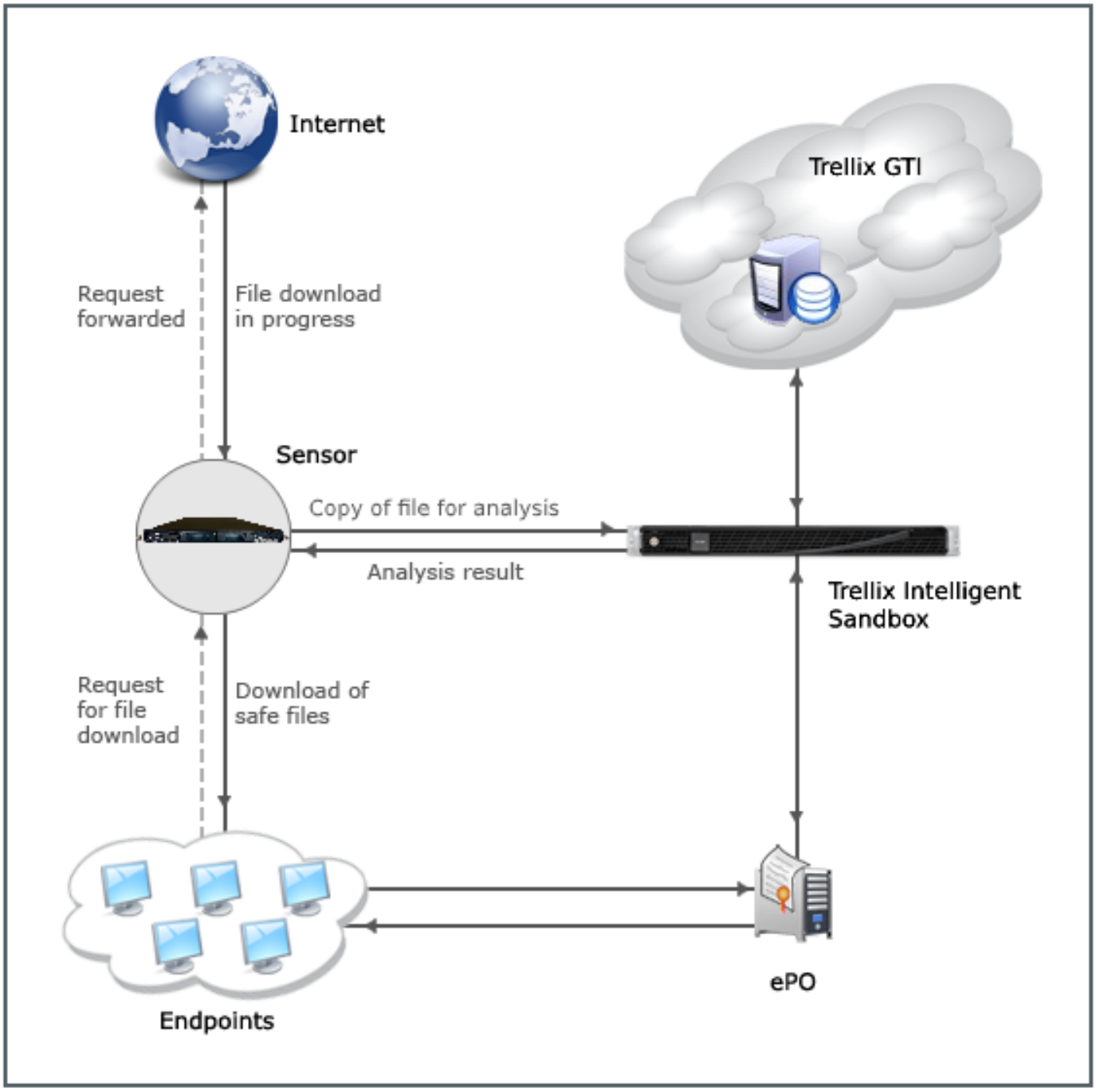
- **Trellix Intelligent Sandbox**

  Trellix Intelligent Sandbox is an on-premise appliance that facilitates detection and prevention of malware. Trellix Intelligent Sandbox provides protection from known, near-zero day, and zero-day malware without compromising on the quality of service to your network users.

  The Trellix Intelligent Sandbox solution primarily consists of the Trellix Intelligent Sandbox appliance and its pre-installed software. The Trellix Intelligent Sandbox appliance is available in two models. The low-end model is the ATD-3000. The high-end model is ATD-6000. For complete information on Trellix Intelligent Sandbox, see the [Trellix Intelligent Sandbox Product Guide].

  You can integrate Trellix Intelligent Sandbox with Trellix IPS. After you integrate, both the Sensor and the Manager communicate with Trellix Intelligent Sandbox separately to augment your defense against malware. This integration enables you to analyze files, for at least known malware, before they are downloaded into your network. For detailed information on how to configure this integration, see the [Trellix Intrusion Prevention System Integration Guide.]

Figure 380. Integration with Trellix Intelligent Sandbox



When you integrate with Trellix Intelligent Sandbox, Intelligent Sandbox is available as an additional malware engine for all the supported file types in the Advanced Malware Policies. You can select this engine along with any of the other malware engines except NTBA. Because Skyhigh Gateway Anti-Malware Engine is available in both Trellix Intelligent Sandbox and NTBA appliance, you can only select either of these engines for a file type.

Based on the configuration, an inline Sensor detects a file download. If the file is not listed in the block or allow list, it sends a copy of the file to the applicable malware engines, including Trellix Intelligent Sandbox. If Trellix Intelligent Sandbox is

able to detect a malware in real time, the Sensor blocks the download. If Trellix Intelligent Sandbox requires more time for analysis, the Sensor allows the file to be downloaded. If Trellix Intelligent Sandbox detects a malware after the file has been downloaded, it informs Trellix IPS, and you can use the Sensor to quarantine the host. Then, you can enforce remediation before allowing the host to come back online. If the same malicious file is downloaded again, the Sensor itself blocks it since it now has the information about that file. For detailed information on how this integration prevents known and unknown malware from entering you network, see the [Trellix Intrusion Prevention System Integration Guide.]

NOTE

GTI File Reputation is available both in the Advanced Malware policies in the Manager as well as in Trellix Intelligent Sandbox. However, Trellix recommends that you use the Advanced Malware policy for this feature. The Sensor can respond quicker if it is configured in the Advanced Malware policy because, in this case, it directly communicates with GTI.

Advanced malware scanning timeout options

All the advanced malware engines described above are designed to function based on certain parameters. These parameters are listed below:

- *Packet hold timeout* — This is the 6-second period per file for which the Sensor holds the last packet of the file before forwarding it through the egress port. The Sensor holds this packet until there is a report from all the configured malware engines. After this timeout, the Sensor takes the corresponding response action based on the results from those engines that responded within this timeout. If none of the engines responded within this timeout, the Sensor forwards the last packet without taking the response actions (block or TCP reset).
- *File session timeout* — This is the 5-minute period that the Sensor waits for a file to download. If the file download exceeds this time interval, the Sensor does not enforce the Advanced Malware policy for that file.
- *File scan timeout* — This is the time period for which the Sensor honors results from the configured malware engines. Any update from the engines after this time period are ignored. If **Trellix IPS Analysis** or **Save File** is configured, then the file scan timeout is 90 seconds from when the Sensor sent the file to the configured engines. If **Trellix IPS Analysis** or **Save File** is not configured, then it is 30 seconds.

NOTE

File extraction does not work when HTTP response is chunk encoded or Gzip compressed.

Malware engine CLI commands

You can view the malware engine and the malware file statistics using these commands.

- **`show malwareengine stats`**
- **`show malwarefile stats`**

You can view the malware server and the malware client statistics using these commands:

- **`show malwareserverstats`**
- **`show malwareclientstats`**

You can enable, disable, or view the status of the malware engines using these commands:

- `set malwareEngine <engine> <status>`
- `show malwareEngine status`

For more information, see the [CLI commands] section.

NOTE

Certain browsers or Smart downloaders continue to try to download file. Therefore, if you are not using the RFB policy, enable blocking of the **HTTP: Repeated Download Detected** attack.

Response actions

Trellix IPS allows you to detect malware in the monitored traffic by configuring a malware policy, suited for your enterprise/environment, in the Manager. The malware policy can be configured per interface. The policy can be configured for both inbound and outbound traffic. The same policy can be applied to both, or, separate policies can be applied to inbound and outbound traffic.

When a Sensor detects activity to be in violation of a configured policy, a preset response from the Sensor is integral to the protection or prevention process. Proper configuration of responses is crucial to maintaining effective protection.

NOTE

- Trellix recommends the following for optimum performance.
  - The Advanced Malware policies be configured only on the external (internet facing Sensors) and not on the internal ones.
    - Save malicious files, only if the number of files traversing the network is huge. Also, save files with a *high* or *very high* confidence level. Avoid using the *Always* save option.

      Trellix IPS Analysis on the Sensor is slower than on NTBA. For high volume deployments enable PDF detection only on NTBA using Gateway Anti-Malware Engine.
- When Advanced Malware policies are configured there is a performance impact of up to 6 seconds on both the Sensor and the Manager.

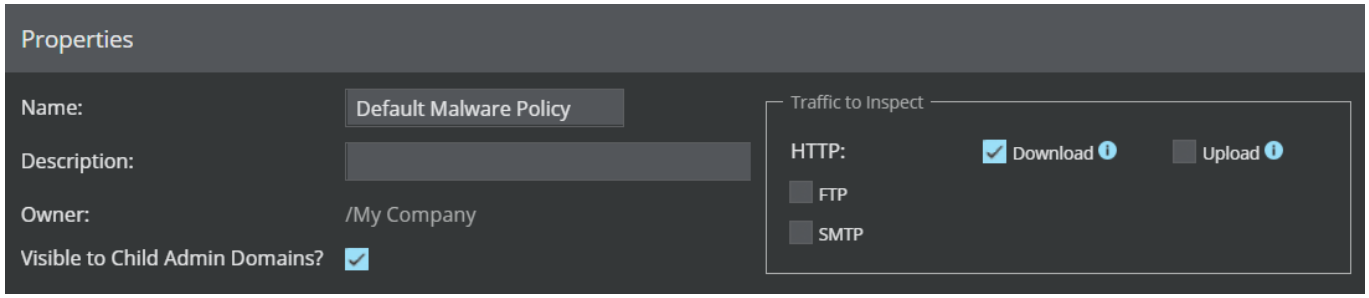
Add an Advanced Malware policy

You configure the anti-malware options in an Advanced Malware policy and then assign it to the required Sensor monitoring resources such as ports, interfaces, and subinterfaces. You must do a configuration and signature set update for any changes in the policy to take effect.

1. Select **Policy** and then select the required admin domain from the **Domain** drop-down list.
2. Select Intrusion Prevention → Policy Types → **Advanced Malware**.
3. Click  .

   The **Advanced Malware** page for a new policy opens.

Figure 381. Update the properties of the Advanced Malware policy

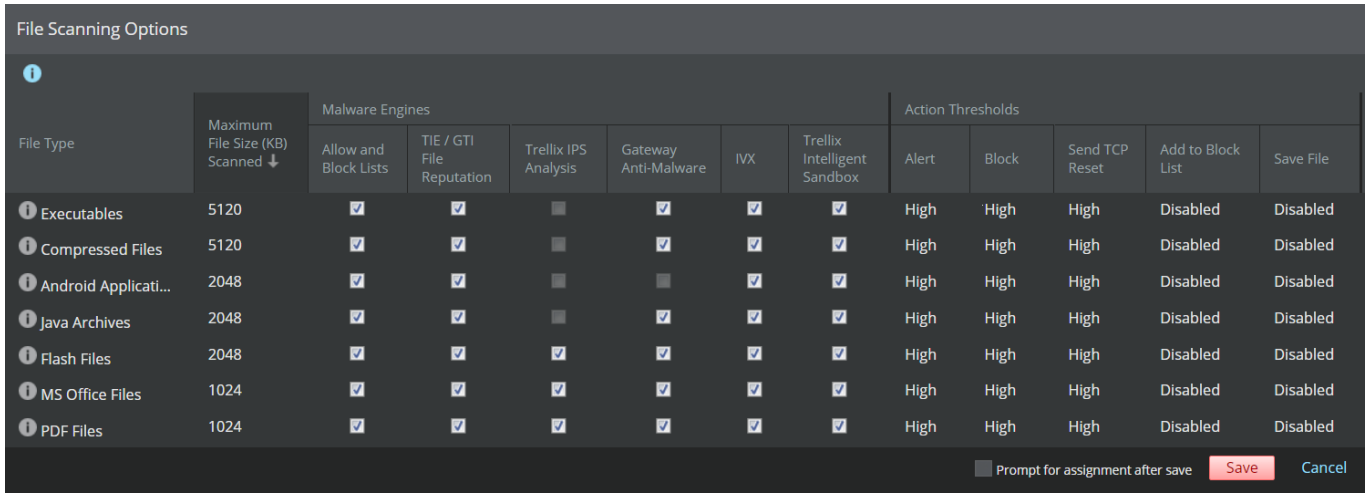


4. Update the following properties.

Field name	Description
Name	Name of the policy.
Description	Description of the policy.
Owner	Name of the admin domain to which the policy belongs.
Visible to Child Admin Domains?	Specifies whether the policy applies to all child admin domains.
Traffic to Inspect	Protocols over which advanced malware scanning is performed. The supported protocols are HTTP, FTP, and SMTP. **NOTE** • The HTTP **Download** option allows you to scan HTTP download/response traffic for the presence of malware. This option is enabled by default. • The HTTP **Upload** option allows you to scan HTTP upload (POST and PUT) requests for the presence of malware. This option is disabled by default. You need to select the **Upload** checkbox to enable it. For more information on scanning HTTP POST and PUT requests, see the section *Malware inspection on HTTP Upload requests* (page 948). **NOTE** FTP malware detection overrides the accelerate-ftp feature even if it is enabled. For more information on the **`accelerate-ftp`** CLI command, see the [CLI commands] section.

5. Update the **File Scanning Options**.

Figure 382. Update the scanning options of the Advanced Malware policy



NOTE

Name resolution must be enabled on devices that will be using the GTI File Reputation malware engine.

Table 47. File scanning options

Field name	Description
File Type	The file types to be scanned. For information about the supported file types, refer to the table [Advanced malware file extension support] below.
Maximum File Size (KB) Scanned	The maximum size currently supported for the corresponding file type. Files that exceed the specified size are not analyzed for malware by any of the engines, including the block and allow lists. The default values are displayed in the Default Malware Policy as well as when you create a policy. The default values are the optimum sizes recommended by Trellix Advanced Research Center based on their research on malware. You can set the maximum file size value up to (25*1024) KB/25 MB for all file types. However, the Trellix IPS Analysis engine has a file-size limit. The limits for each Sensor model are as follows: • NS-series Sensors - (50*1024) KB/50 MB • Virtual IPS Sensors- (5*1024) KB/5 MB **NOTE** Trellix recommends that for any file type, you do not set a value more than (5*1024) KB/5 MB as the maximum file size as this might affect the Sensor's performance.

Field name	Description
Malware Engines	The Malware engines to scan the selected file type. If you select **Gateway Anti-Malware** for a **File Type**, you must either use an NS-series Sensor or NTBA. For **IVX** to work, you must integrate the corresponding Sensors with the Trellix VX appliance or Trellix IVX Cloud. See the chapter [Integration with Sandbox Solutions] in the [Trellix Intrusion Prevention System Integration Guide] for more information. For **Trellix Intelligent Sandbox** to work, you must integrate the corresponding Sensors with Trellix Intelligent Sandbox. See the chapter, [Integration with Sandbox Solutions] in the [Trellix Intrusion Prevention System Integration Guide] for more information.

Field name	Description

Action Thresholds	Specifies the type of response to be made for the attack. The types of responses are:
	• **Alert**— Alerts are raised in the Attack Log.
	• **Block**— This action blocks packets for detected malware. Thus preventing the malicious file from reaching the host.
	The first step towards prevention is typically to block attacks that have a high severity level. When you know which attacks you want to block, you can configure your policy to perform the drop attack packets response for those attacks. If not configured in the policy, the Attack Log allows you to update the policy to block traffic.
	• **Send TCP Reset**— Disconnects a TCP connection at the source, destination, or both ends of the transmission. Thus preventing the malicious file from reaching the host.
	NOTE
	This response may not work effectively with SPAN and tap deployments.
	• **Add to Block List**— If any of the engines report the submitted file to be malicious, then the Manager adds the file's MD5 hash to the block list in its database. To be added to this list, the file's severity must be the same or more than what you specify in this field. For example, if you specify *high* as the criteria, then files of severity *high* and *very high* are added to the block list. Within the next 5 minutes, the Manager adds this file to the local block list of all the Sensors that it manages.
	NOTE
	The **TIE/GTI File Reputation** engine does not support **Add to Block List** response action. You can manually add the desired malware file's MD5 hash to the block list from the **Attack Log** page.
	NOTE
	In case the MD5 entries limit has been reached, the Manager adds SHA256 hash value(s) of the malware file(s) to its block list and sends the same hash value(s) to the Sensor through incremental or full update.
	• **Save File**— One of the response actions specified is the ability to archive the file in a file store based on the Advanced Malware policy. The files that are selected based on this configuration are forwarded to the Manager.
	  • For files greater than 5 MB, only the first 5 MB is available as the saved file.
	  • To prevent the Manager's disk from getting frequently filled up, use the **Save File** feature sparingly.
	  • The Sensor's simultaneous file scan capacity is reduced if the **Save File** option is enabled. See the table in this section for the details.

To know the list of advanced malware file extensions supported by signature sets, refer to KB96988.

Each file type is scanned by a Malware engine. Multiple malware engines can be selected to scan various file types. The Malware engines return a confidence level. Based on the confidence level, the following action thresholds can be set. The confidence levels supported are: Very low, low, medium, high, very high.

The Malware Engines supported per file type are:

File Type	TIE/GTI File Reputation	Allow and Block Lists	Trellix IPS Analysis	Gateway Anti-Malware	IVX	Trellix Intelligent Sandbox
Executables	✓	✓		✓	✓	✓
MS Office Files	✓	✓	✓	✓	✓	✓
PDF Files	✓	✓	✓	✓	✓	✓
Compressed Files	✓	✓		✓	✓	✓
Android Application Package	✓	✓			✓	✓
Java Archive	✓	✓		✓	✓	✓
Flash Files	✓	✓	✓	✓	✓	✓

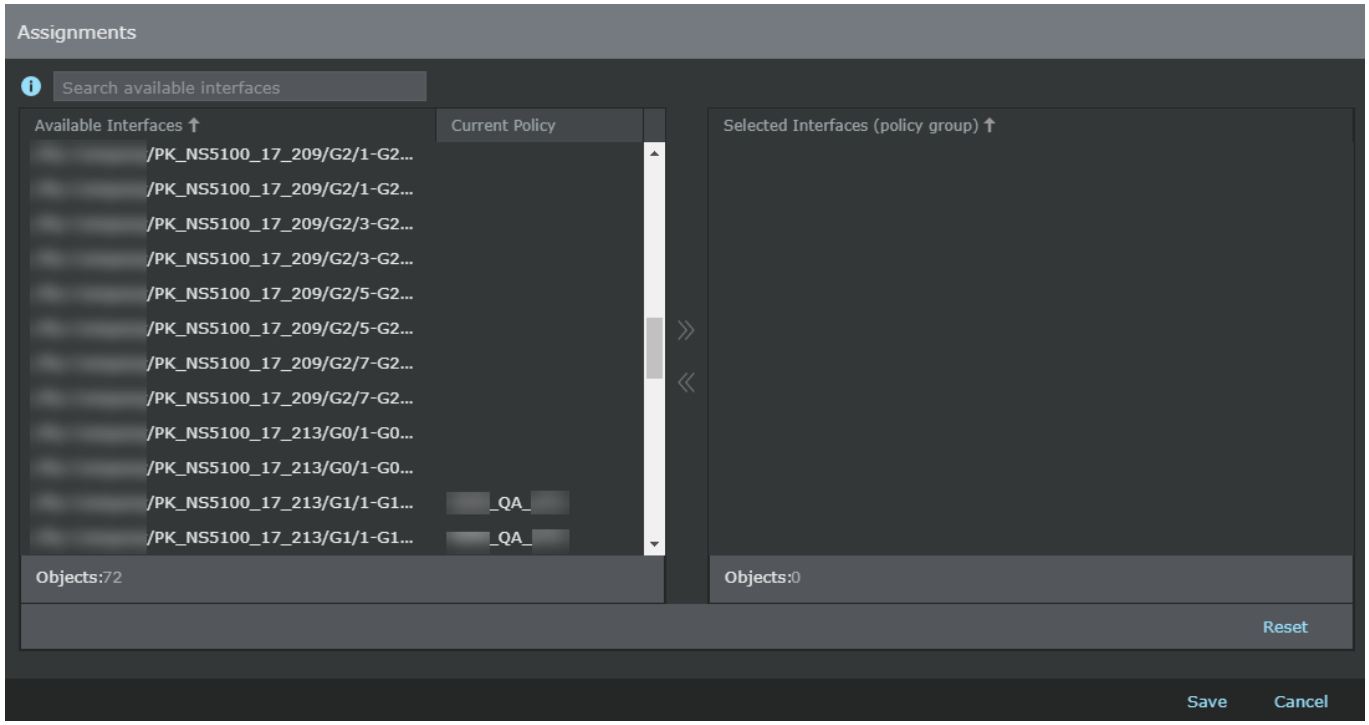
The maximum simultaneous file scan capacity per Sensor model is as follows.

Sensor	Maximum simultaneous file scan capacity with file save	Maximum simultaneous file scan capacity without file save
NS9500 stack - 100 Gbps throughput	1,000	4,096
NS9500 stack - 60 Gbps throughput	1,000	2,048
NS9500 stack - 40 Gbps throughput	1,000	2,048
NS9500 standalone - 30 Gbps throughput	1,000	1,024
NS9500 standalone - 20 Gbps throughput	1,000	1,024
NS9500 standalone - 10 Gbps throughput	1,000	1,024
NS9300, NS9200, NS9100	1,000	1,024
NS7600 - 15 Gbps throughput	1,000	4,094
NS7600 - 10 Gbps throughput	1,000	4,094
NS7600 - 5 Gbps throughput	1,000	4,094
NS7500 - 7.5 Gbps throughput	1,000	1,024
NS7500 - 5 Gbps throughput	1,000	1,024
NS7500 - 3 Gbps throughput	1,000	1,024
NS7350, NS7250, NS7150	1,000	1,024
NS7300, NS7200, NS7100	1,000	1,024
NS5200, NS5100	32	1,024
NS3600 - 5 Gbps throughput	1,000	4,094

Sensor	Maximum simultaneous file scan capacity with file save	Maximum simultaneous file scan capacity without file save
NS3600 - 3 Gbps throughput	1,000	4,094
NS3600 - 1 Gbps throughput	1,000	4,094
NS3500	16	255
NS3200, NS3100	16	255
IPS-VM600	32	1,024
IPS-VM5000	32	1,024

6. To assign the Advanced Malware Policy to the available interfaces and direction (Inbound, Outbound), select **Prompt for assignment after save**.

Figure 383. Assign Interfaces



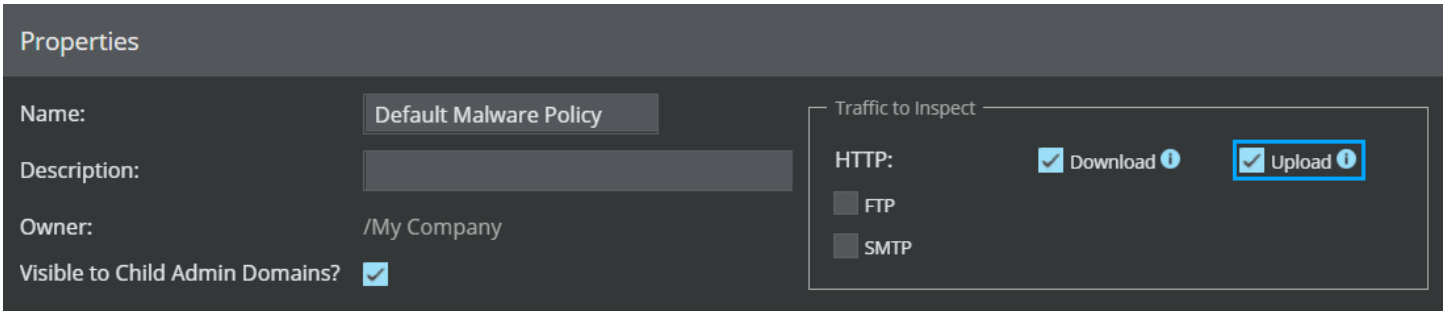
7. Select the required interface from the **Available Interfaces** column and add it to the **Selected Interfaces (Policy Group)** column.
8. Click **Save**.

   You are directed to the new policy window.

Malware inspection on HTTP Upload requests

Trellix Intrusion Prevention System offers malware inspection capabilities for HTTP upload requests generated in the network. The HTTP **Upload** option is useful in environments where files uploaded through the network need to be scanned.

Figure 384. Selecting HTTP Upload option



The Sensor has capabilities to scan both HTTP multipart and non-multipart requests for presence of malware.

In case of HTTP requests containing multiparts, malware inspection is supported only on the following multipart Content-Types:

- Multipart/alternative
- Multipart/digest
- Multipart/form-data
- Multipart/mixed
- Multipart/parallel
- Multipart/related
- Multipart/report

Multipart Content-Types that are currently not supported for inspection are:

- Multipart/signed
- Multipart/encrypted
- Multipart/byteranges
- Nested Multipart forms

NOTE

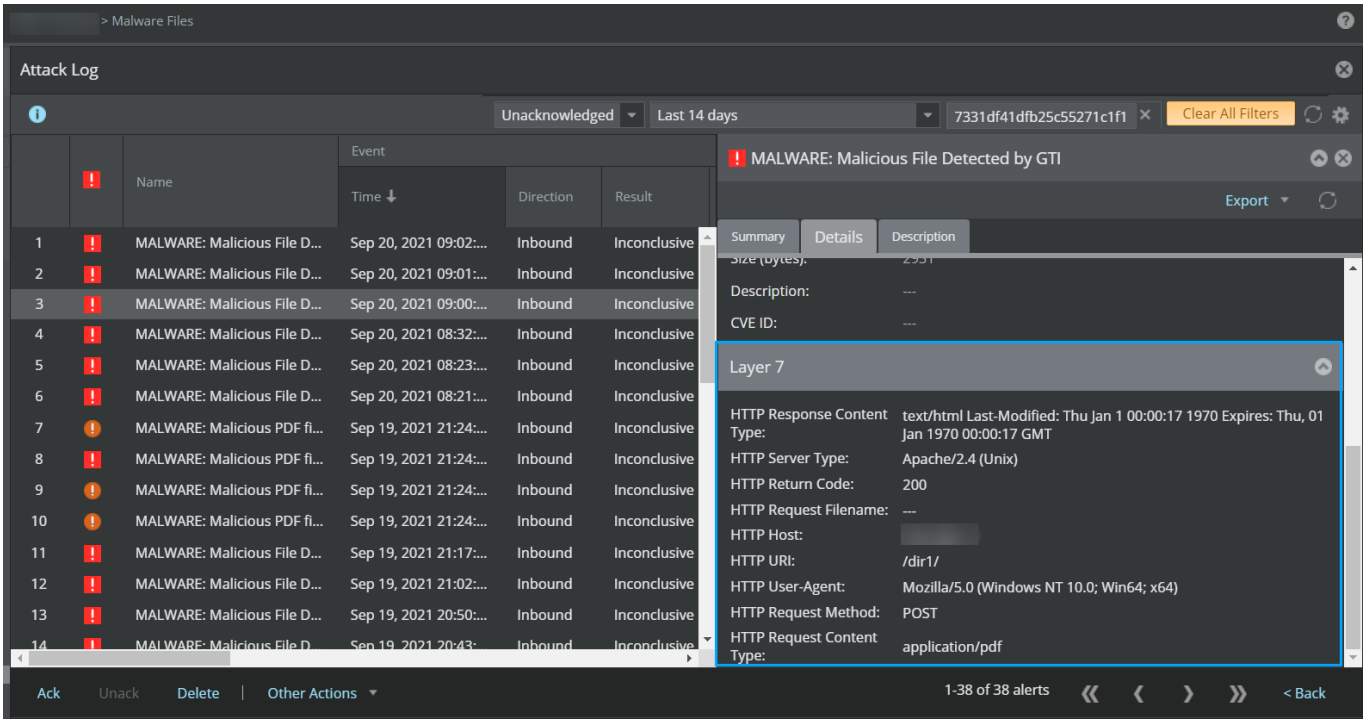
The Sensor does not support the inspection of malware files when files are transferred/uploaded using encoding mechanisms. These encodings are generally indicated by Content-Encoding/Content-Transfer-Encoding/Transfer-Encoding headers. To view the list of file types and their extensions supported for scanning, see the table [File scanning options] within the section *Add an Advanced Malware policy* (page 942).

NOTE

For information about the maximum file size that can be scanned, see the table [File scanning options] within the section *Add an Advanced Malware policy* (page 942).

You can view Layer 7 HTTP data for an alert from the **Attack Log** by following these tasks:

1. Navigate to Analysis → <Admin Domain Name> → **Malware Files**.
2. Double-click on the malware file hash that is associated with a malicious HTTP request. The **Attack Log** opens where you can view and analyze alerts related to the selected hash.
3. Double-click on an alert to view all information related to the attack.
4. The **<Attack Name>** panel opens on the right-hand side. Click the **Details** tab and scroll down to **Layer 7** section to view the HTTP fields associated with the alert.



The HTTP fields displayed under the Layer 7 section vary depending on the HTTP alert you select for examination.

NOTE

The limit for the number of files uploaded and scanned per single HTTP POST or PUT transaction is 10.

NOTE

Malware inspection on HTTP requests requires additional system resources and can therefore impact overall Sensor performance.

Malware engine updates

Among the malware scanning engines present on the Sensor, the Gateway Anti-Malware Engine and the Block list can be updated through the intervention of the security administrator. Updates for these engines can be carried out independently irrespective of the Sensor software version.

However, for Gateway Anti-Malware, you must be aware of the versions of the malware engines that are compatible with specific Sensor and Manager versions. Refer to Gateway Anti-Malware Engine in the section [How an Advanced Malware policy works] in [Trellix Intrusion Prevention System Product Guide].

Gateway Anti-Malware Engine for an airgap network

The Gateway Anti-Malware engine initialization in the Sensors requires an active connection to the GTI server. If your Sensors are in a network without an active GTI connection, the Gateway Anti-Malware engine initialization in the Sensor fails. In such a scenario, you must enable the airgap mode of Gateway Anti-Malware to initialize the Gateway Anti-Malware engine. You can achieve this by executing the **`set gam-airgap-network enable`** command in the Sensor CLI and reboot the Sensor for the changes to take effect.

For example, you can configure the Sensors to initialize the Gateway Anti-Malware engine in airgap mode when your network meets the following conditions:

1. The Sensors are in a private network.
2. You cannot use the Public GTI server.

You must enable the airgap mode of Gateway Anti-Malware before pushing the updates from the Manager to the Sensor. To view the status of the Gateway Anti-Malware updating for an airgap network, execute the **`show gam-airgap-network status`** command in the Sensor CLI.

NOTE

The Gateway Anti-Malware engine initialization for the Sensors in airgap network is supported on Gateway Anti-Malware 2019 version 0 and later.

Gateway Anti-Malware update

The Gateway Anti-Malware Engine, running either on an NS-series Sensor or on an NTBA appliance, can be updated from the Manager in the same way that you perform configuration and device software updates. You can set up automatic updates in the Manager for this engine using one of the methods mentioned in the subsequent sections.

NOTE

The deployment of Gateway Anti-Malware Engine is not supported on Virtual NTBA devices.

Set up automatic updates for Gateway Anti-Malware Engine for a domain

- Make sure that you have configured a DNS server for the domain to allow Sensors attached to this domain to download Gateway Anti-Malware Engine updates. If you have not done so, go to Devices → <Admin Domain Name> → Global → Common Device Settings → **Name Resolution** to configure a DNS server.
- You must be using either an NS-series Sensor or an NTBA Appliance to use this engine.

An update comprises the following components:

- Gateway Anti-Malware DAT and Gateway Anti-Malware Engine
- Anti-Virus DAT
- Anti-Malware Engine

The update can either be an incremental update or a full update. The full update is approximately 200 MB.

You can set up automatic updates for both these components using these steps. If you do not want to set up automatic updates, you can use the existing process for manual updates.

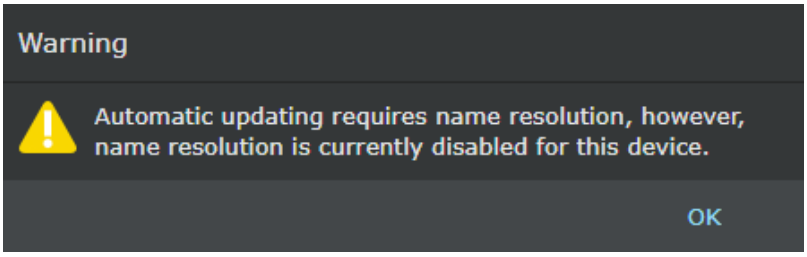
Steps:

1. Click Devices → <Admin Domain Name> → Global → Common Device Settings → **GAM Updating**.

   The **GAM Updating** page appears.

2. Select **Enable Automatic Updating?**.

   Figure 385. Notification to configure a DNS server

   If you have not configured a DNS server for this domain, you will receive a notification prompting you to do so.

3. Click the **Update Interval** drop-down.

   The range of the update interval is between 2 hours and 24 hours since Trellix provides updates several times in a day.

4. Click **Save** to complete the configuration.

You have now set up automatic updates for all devices that run Gateway Anti-Malware Engine in the domain.

Set up automatic updates for Gateway Anti-Malware Engine for a device

- Make sure that you have configured a DNS server for this device to allow the Sensor to download Gateway Anti-Malware Engine updates. If you have not done so, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Name Resolution** to configure a DNS server.
- You must be using either an NS-series Sensor an NTBA Appliance to use this engine.

An update comprises the following components:

- Gateway Anti-Malware DAT and Gateway Anti-Malware Engine
- Anti-Virus DAT
- Anti-Malware Engine

The update can either be an incremental update or a full update. The full update is approximately 200 MB.

You can use these steps to set up automatic updates for both these components. If you do not want to set up automatic updates, you can use the existing process for manual updates.

This page displays a grid that mentions the active version and latest available version of each component. If you are using the latest version the circle is green. If a newer version is available, the circle is colored red.

1. Click Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **GAM Updating**.

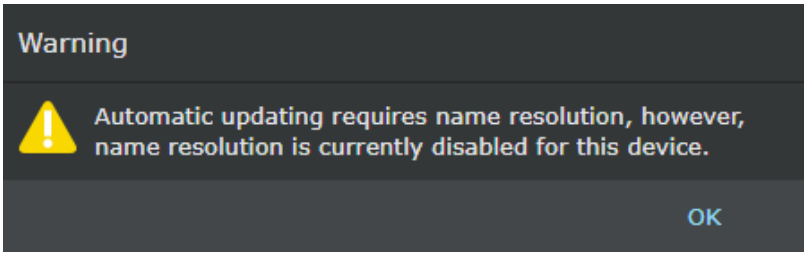
   The **GAM Updating** page appears.

2. You can choose to inherit settings of the domain by selecting the check-box.

   If you do not select this option, you can customize update settings for this device.

3. Select **Enable Automatic Updating?**.

Figure 386. Notification to configure a DNS server



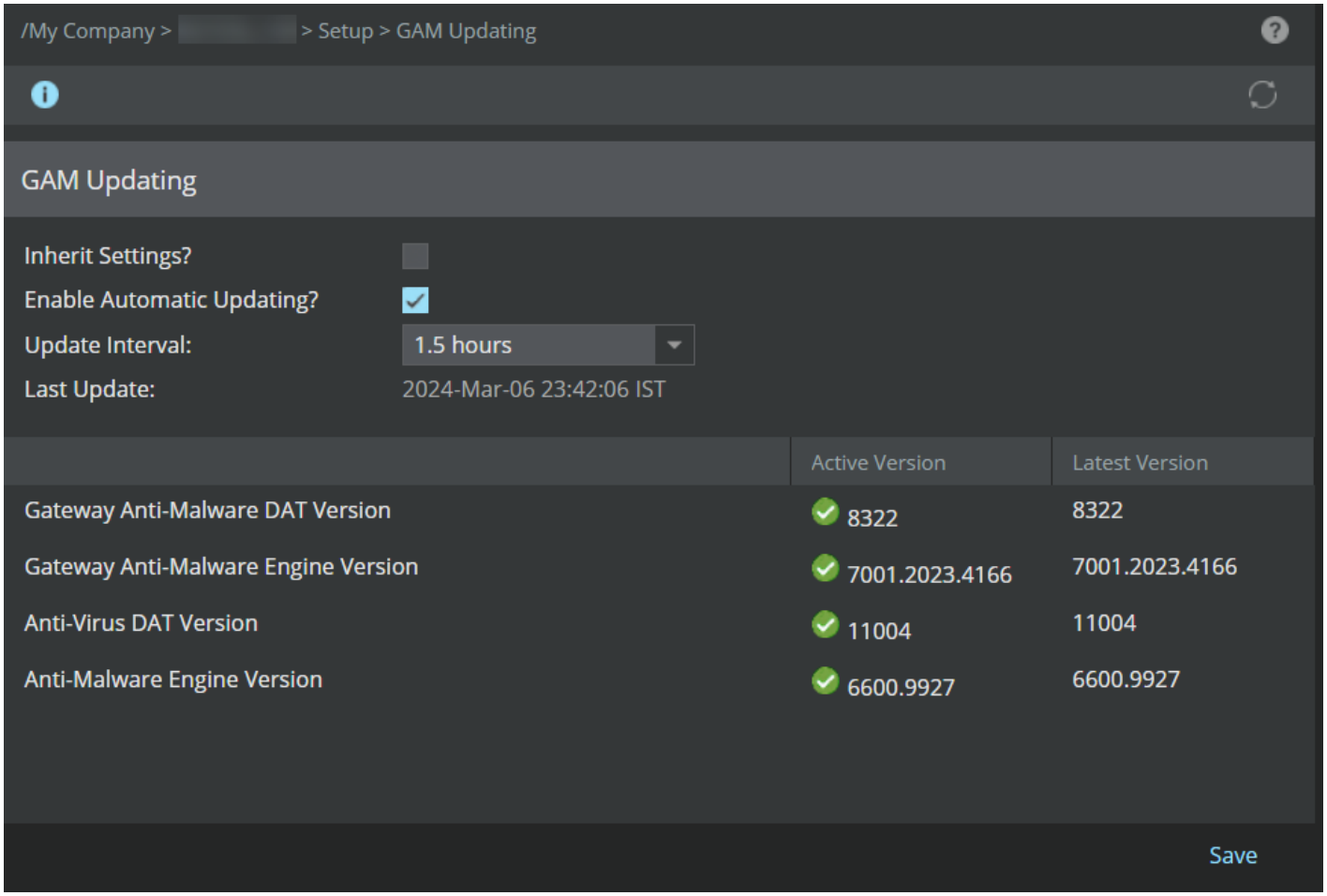
If you have not configured a DNS server for this device, you will receive a notification prompting you to do so.

4. Click the **Update Interval** drop-down.

   The range of the update interval is between 1.5 hours and 24 hours since Trellix provides updates several times in a day.

5. Click **Save** to complete the configuration.

Figure 387. GAM Updating page shows versions for individual items



You have now set up automatic Gateway Anti-Malware Engine updates for this Sensor.

Update Gateway Anti-Malware Engine manually

If you want to update the Gateway Anti-Malware Engine for an offline Sensor, you will need to manually download the appropriate software version and import it into the Manager.

When the Gateway Anti-Malware engine is enabled for the first time, the engine is in uninitialized state when integrated with a Private GTI cloud. To receive a manual update, the Gateway Anti-Malware engine has to be in initialized state. To initialize the engine, the Sensor has to be online and connected to the Private GTI server to receive the update for the first time. Once the Gateway Anti-Malware engine is initialized after receiving the update from Private GTI server, you can push the updates to the Sensor. For subsequent manual Gateway Anti-Malware engine update, you can download the update and import it to the Manager.

NOTE

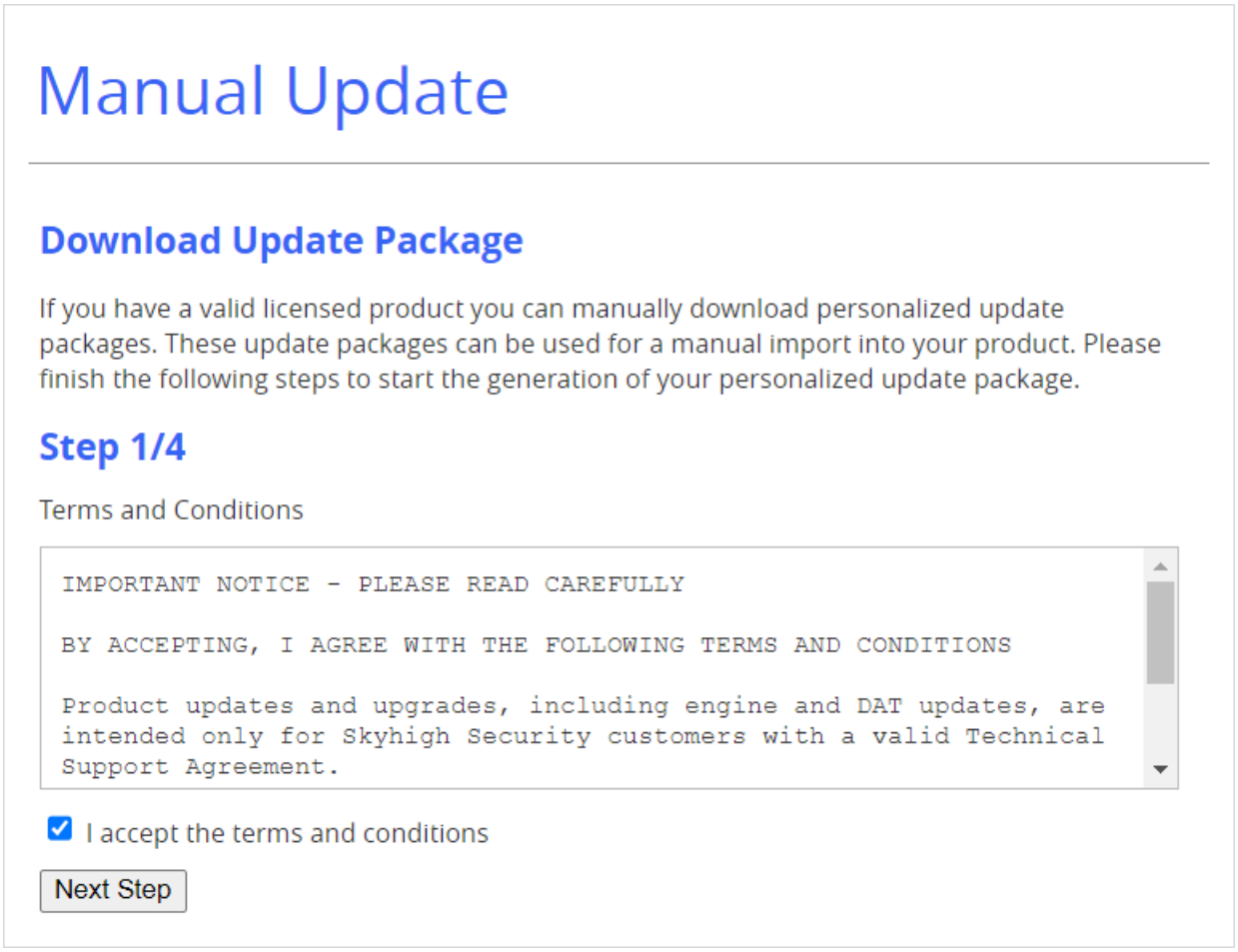
It is important that you download a compatible version of Gateway Anti-Malware Engine files to make sure the update is successful. To ascertain which software versions are compatible with which versions of the Sensor software, refer to Gateway Anti-Malware Engine in the section [How an Advanced Malware policy works] in [Trellix Intrusion Prevention System Product Guide].

Perform the steps listed below to manually download the Gateway Anti-Malware Engine update files and deploy them to your Sensor.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Name Resolution**.

   DNS server is configured for the Sensor to reach the GTI server.
2. Using a recent version of your browser, go to the Gateway Anti-Malware Update Server URL: https://contentsecurity.sky-high.cloud/UPDATE.
3. On the page that appears, review the terms and conditions and select the **I accept the terms and conditions** check-box, and click **Next Step**.

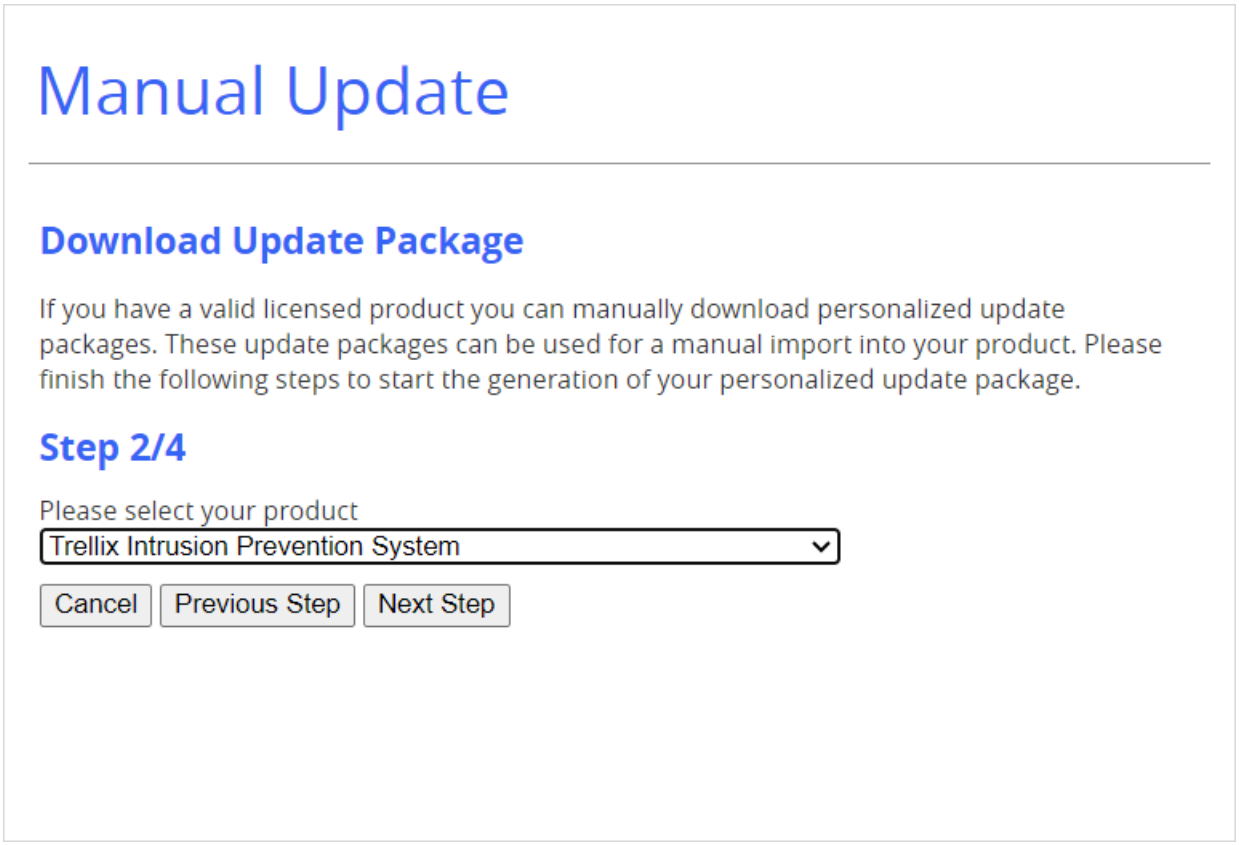
Figure 388. Accept License Agreement



You are routed to the next page where you will need to select the appropriate Trellix product.

4. On this page, click the drop-down to select **Trellix Intrusion Prevention System**, and click **Next Step**.

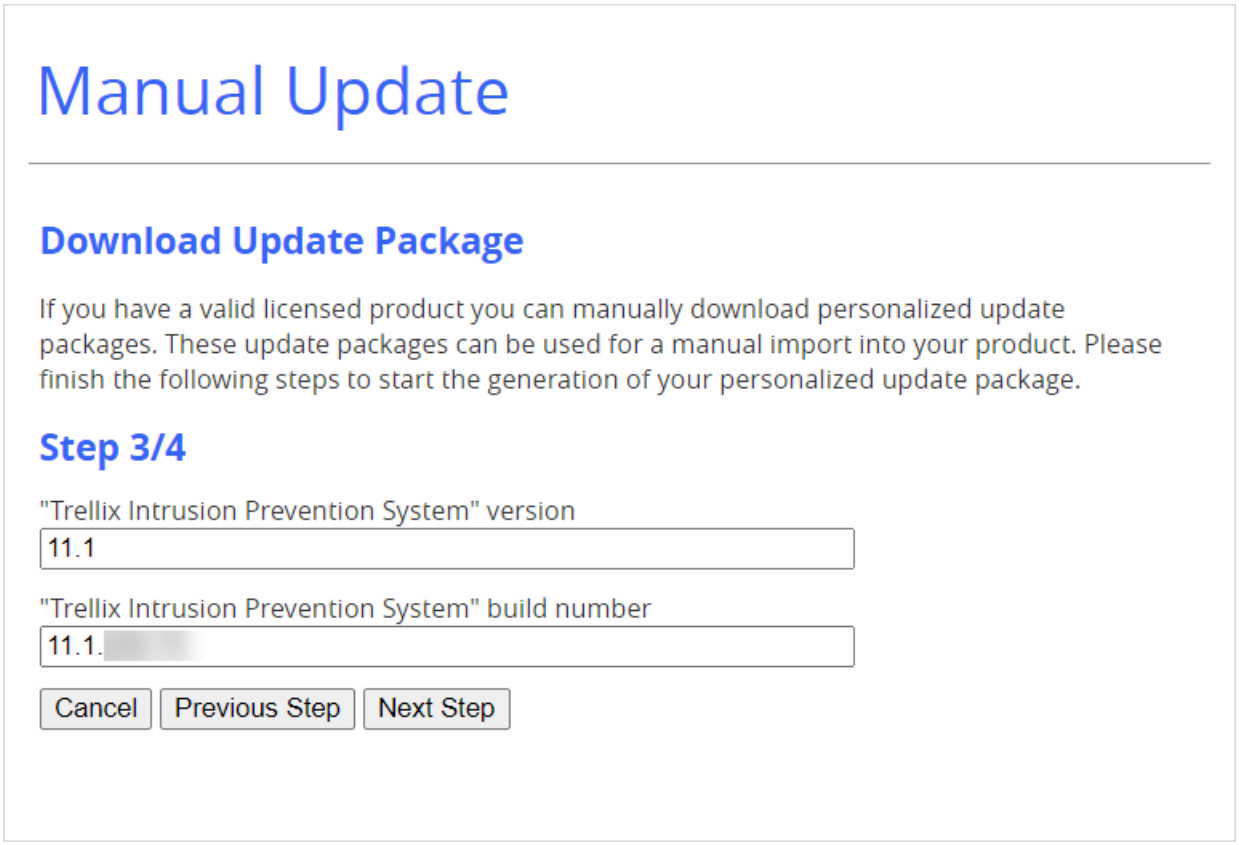
Figure 389. Select update package



You are routed to the next page where you must enter the appropriate version of Sensor software you are using.

5. Under step 3:
   a. For **"Trellix Intrusion Prevention System" version**, enter **`11.1`** if your Sensor runs on 11.1.5.x version, or enter **`10.1`** if your Sensor runs on 10.1.5.x version.
   b. For **"Trellix Intrusion Prevention System" build number**, enter **`11.1.5.x`** if your Sensor runs on 11.1.5.x version, or enter **`10.1.5.x`** if your Sensor runs on 10.1.5.x version.
   c. Click **Next Step**.

Figure 390. Specify version and build number



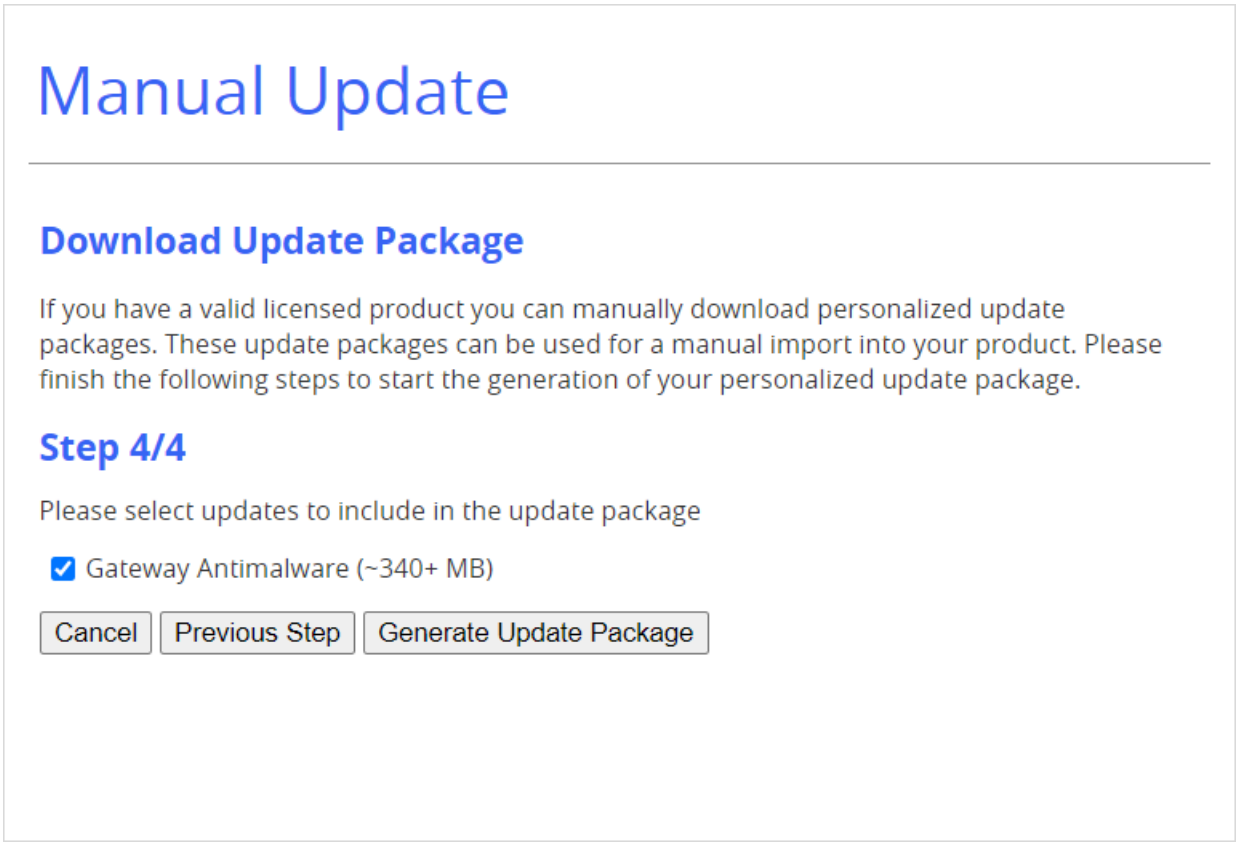
The success or failure of the update will vary depending on the Sensor and Manager software versions you are using. Review this table to know the various combinations and what version you must enter to make sure you download the appropriate Gateway Anti-Malware Engine version.

Table 48. Gateway Anti-Malware engine compatibility matrix

Manager	Sensor	Gateway Anti-Malware engine version downloaded	What you must enter...
10.1.7.55 or later	10.1.5.153 or later	2021	You must enter the Sensor software version as 10.1.5.x.
10.1.7.29 or later	10.1.5.41 or later	2019 version 0	You must enter the Sensor software version as 10.1.5.x.
10.1.7.4 or later	10.1.5.3 or later	2017 version 2	You must enter the Sensor software version as 10.1.5.x.
11.1.7.81 or later	11.1.5.84 or later	2023	You must enter the Sensor software version as 11.1.5.x.

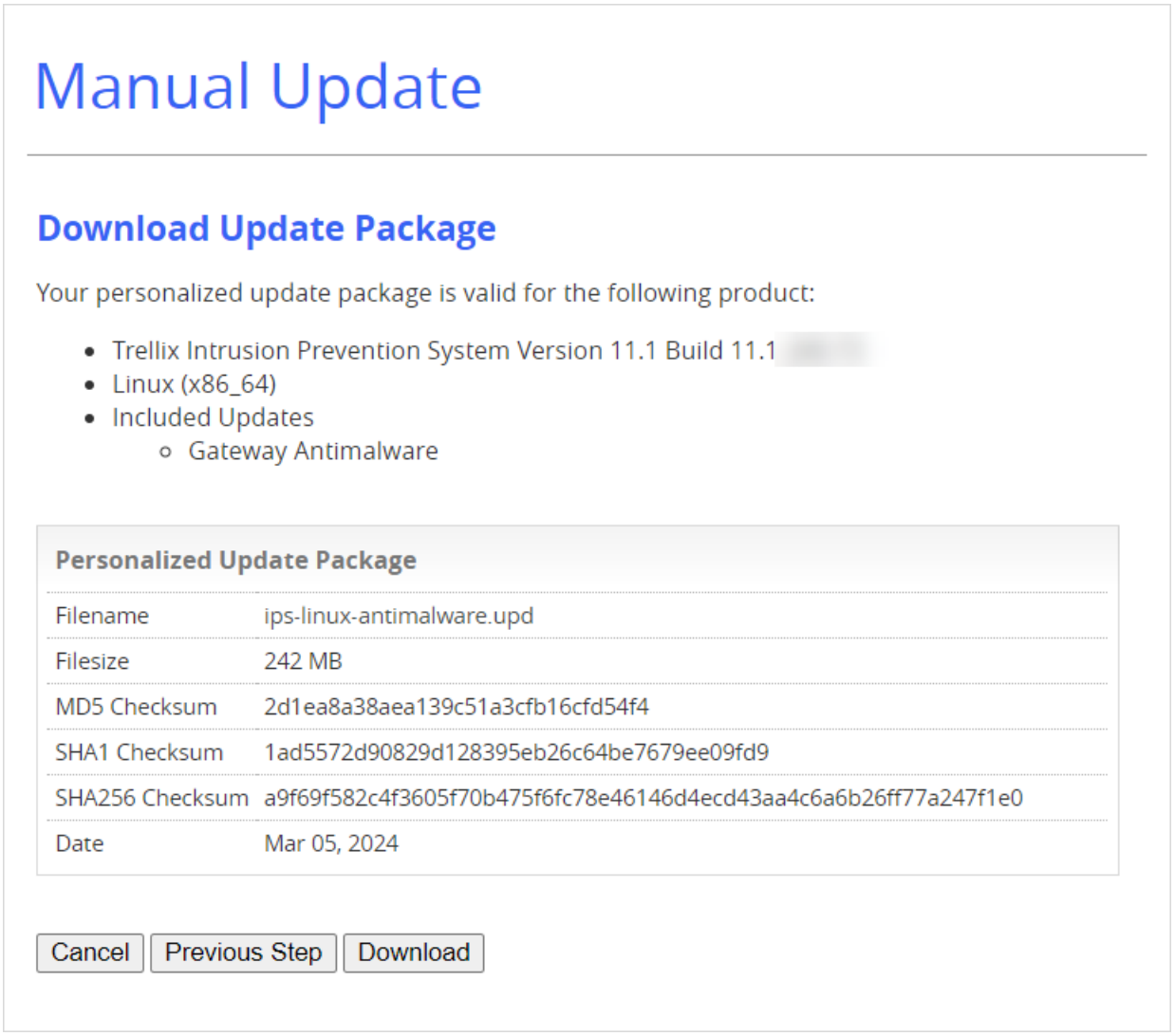
6. Click **Generate Update Package**.

Figure 391. Generate Update Package



7. Click **Download** and save the package to a convenient location.

Figure 392. Download Update Package



After the package is generated, you are shown details about the file such as filename, file size, MD5, SHA1, SHA256 checksums and date.

8. After the file is downloaded, log on to the Manager and go to Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Select **Manual Import** tab. The **Manual Import** tab is displayed.
9. In the **Manual Import** tab, click **Browse**, navigate to the file location, and select it.
10. Select the file and click **Import**.

    pop-up opens giving you the status of the upload.
11. If you have configured auto-deployment of new GAM updates on the **GAM Automatic Deployment** tab under Manager → <Admin Domain Name> → **Trellix IPS Protection Status**, the imported GAM file will be deployed automatically on all the attached Sensors at once at the scheduled time. You can check the deployment status on the **User Activities** tab under Manager → <Admin Domain Name> → Troubleshooting → **Logs**. For detailed information on how to configure and schedule auto-deployment of GAM updates, refer to the section [Automatic deployment of GAM updates] in [Trellix Intrusion Prevention System Product Guide].

NOTE

The automatic deployment of GAM updates is not applicable to NTBA or virtual NTBA devices.

Or,

12. After the file upload is complete, go to Devices → <Admin Domain Name> → Devices → <Device Name> → **Deploy Pending Changes**.

    the **Deploy Pending Changes** page, the **Pending Changes** column displays **New Gateway Anti-Malware Versions**.

13. Select the check-box for **GAM Updates** and click **Deploy**.

A pop-up window appears showing you the status of the update. Upon successful deployment, click **Close** in the pop-up window.

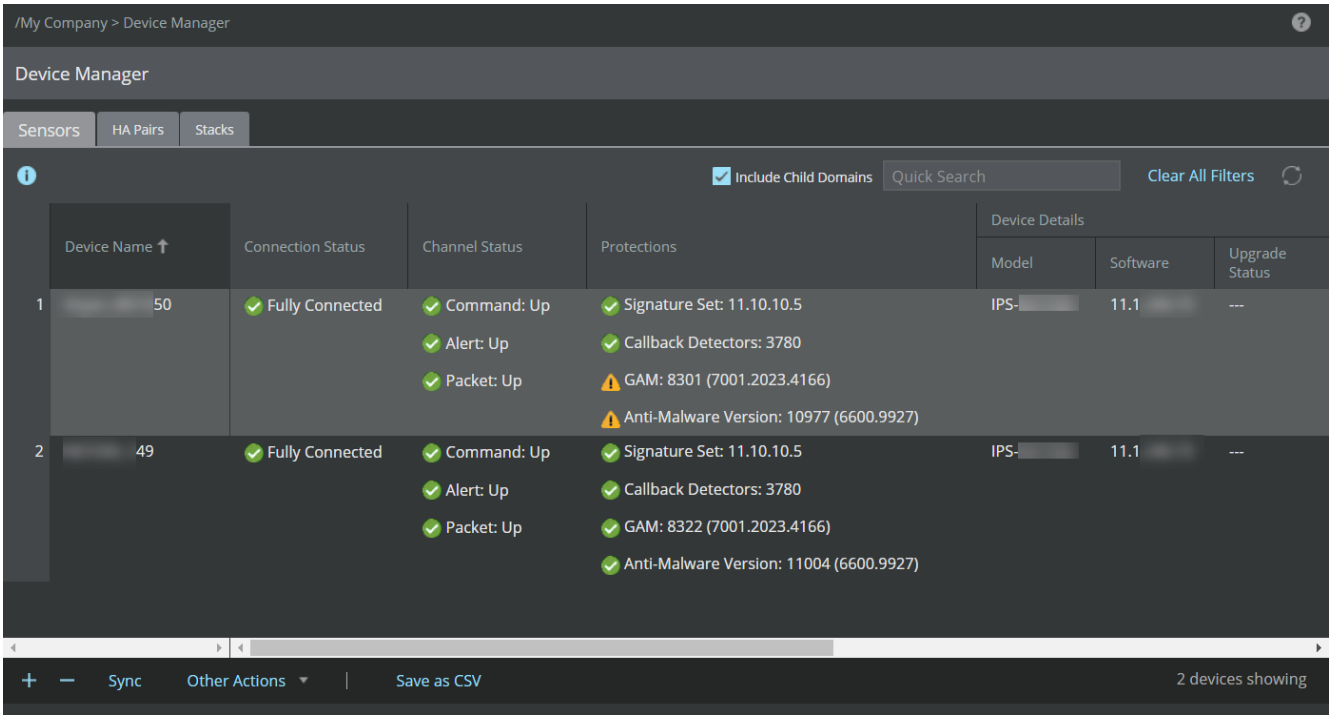
NOTE

If the update fails, it is likely that you have downloaded an incompatible version. Review the compatible versions and the combinations listed in the [Gateway Anti-Malware engine compatibility matrix] table to ascertain if you have downloaded the appropriate version.

There is an alternate way to deploy the GAM update file to your Sensor from the **Device Manager** page. To deploy:

1. Navigate to Devices → <Admin Domain Name> → Global → **Device Manager** and select **Sensors** tab. The **Sensors** tab is displayed listing all the attached Sensors.
2. Select the compatible Sensor on which you want to deploy the GAM update file, and click **Sync**.

Figure 393. Select Sensor to synchronize GAM Updates

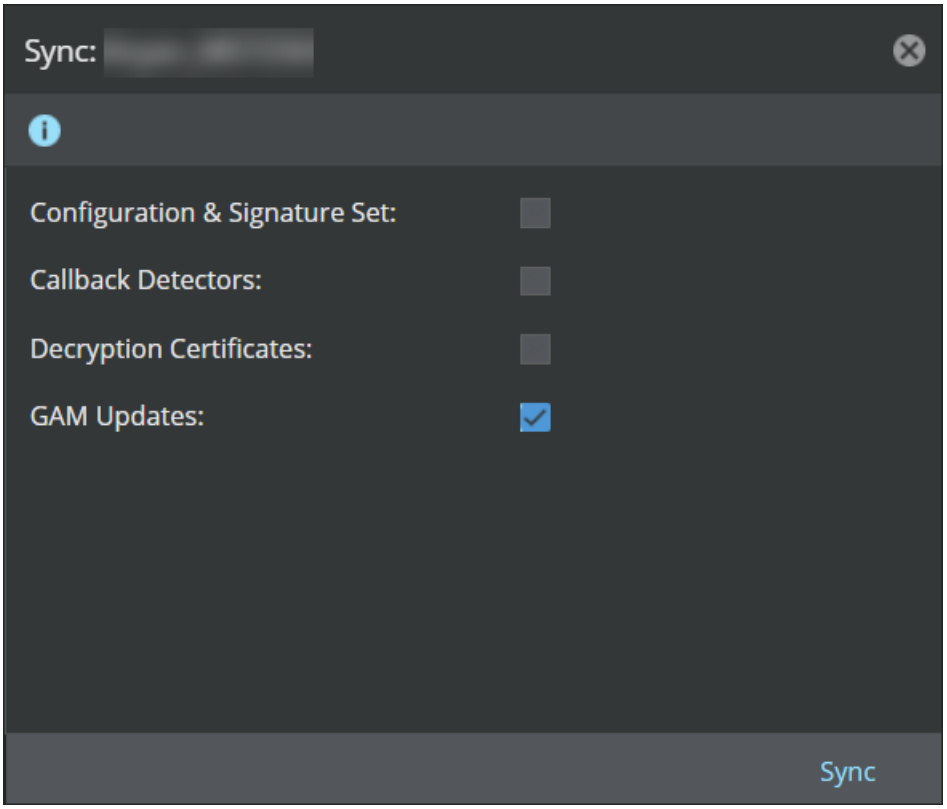


3. The **Sync: <Device Name>** window is displayed with **GAM Updates** check-box selected. If there are any other pending deployments, the respective check-boxes will also be selected by default. You may uncheck any of them if you want to skip their deployment.

> **NOTE**
>
> The Manager provides an option to concurrently deploy pending changes onto multiple Sensors. When you select multiple Sensors for deployment, a **Bulk Sync** window is displayed with all check-boxes selected by default. You may uncheck any of them if you want to skip their deployment.

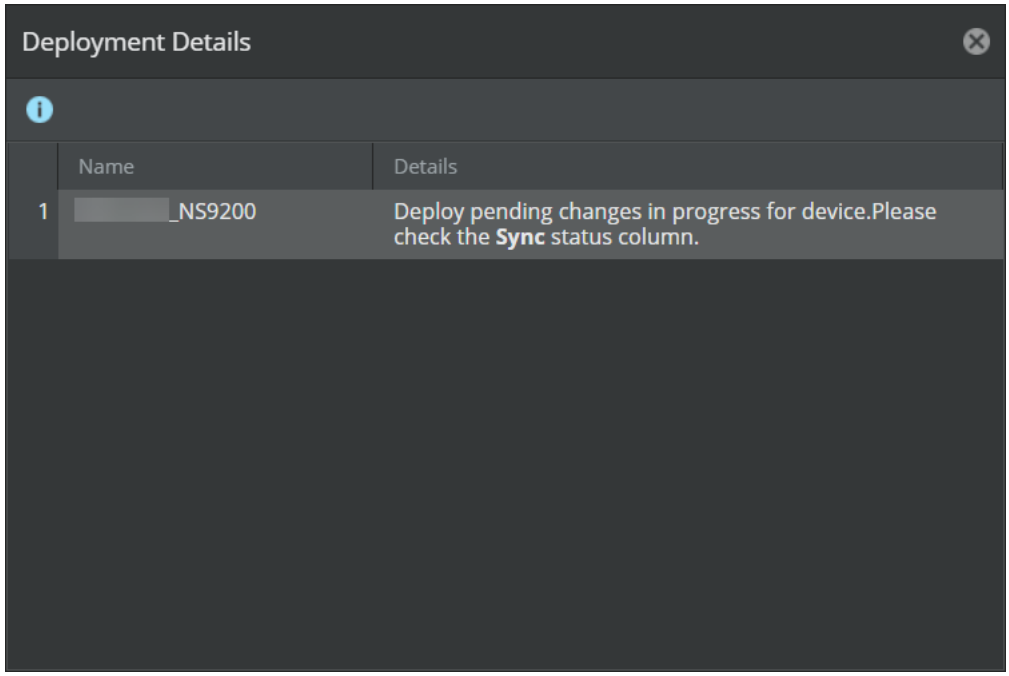
4. Click **Sync** to begin the deployment.

Figure 394. GAM Updates selected for synchronization



5. A **Deployment Details** dialog-box is displayed, click .

Figure 395. Deployment Details



6. You may click the icon to refresh the **Sensors** tab and view the latest Sync status.

   Upon successful deployment, the status is displayed as **Synchronized**, and the deployed version of GAM is displayed under the **Protections** column.

> **NOTE**
>
> You can also view the deployment status in Manager → <Admin Domain Name> → Troubleshooting → **Logs** under the **Background Tasks** tab. The status is displayed as **In Progress** during the deployment and **Complete** upon successful deployment. You need to refresh the tab to view the latest deployment status.

> **NOTE**
>
> If the Sync fails, it is likely that you have downloaded an incompatible GAM version. Review the compatible versions and the combinations listed in the [Gateway Anti-Malware engine compatibility matrix] table to ascertain if you have downloaded the appropriate version.

Manage Advanced Malware policies

You can perform the following operations on an existing Advanced Malware policy.

Operation	Description
View Advanced Malware policies	The **Advanced Malware** policies page allows you to view the Malware policies that have been assigned to the various resources of your Trellix IPS. Policies are listed per the Sensor, interface, and subinterface. From the root admin domain, you can see policies assigned to all child domains. For non-root parent domains, you only see the assigned policies in your parent and child domains. For child domains, you only see the policies assigned to the resources in your domain. Select Policy → <Admin Domain Name> → Policy Types → **Advanced Malware** to view the assigned Malware policies.
Edit an Advanced Malware policy	Editing an Advanced Malware policy allows you to make the changes necessary to match the policy with the traffic you are monitoring. Editing a policy permanently changes that policy. If you intend to make slight changes to a policy but want to save it under a different name, try cloning an Advanced Malware policy. To edit an Advanced Malware policy: 1. Select Policy → <Admin Domain Name> → Policy Types → **Advanced Malware**. The Advanced Malware policies are listed. 2. Double click the policy to edit. 3. Edit the policy parameters. 4. Click **Save**.
Clone an Advanced Malware policy	Cloning duplicates an existing policy, and is similar to a "save as" function. You can edit a Trellix IPS-provided policy. However, if you want to edit a copy of a policy, you can clone any existing policy to further refine the policy for application in a new environment. You can clone a provided policy, save it under a new name, and customize it for your unique environment. 1. Select Policy → <Admin Domain Name> → Policy Types → **Advanced Malware**. The policies are listed. 2. Select the policy you want to clone. 3. Click  . 4. Type a new name for the policy, if required and edit the policy parameters.
Delete an Advanced Malware policy	To delete an Advanced Malware policy you have created: 1. Select Policy → <Admin Domain Name> → Policy Types → **Advanced Malware**. The Advanced Malware policies are listed. 2. Select the policy to be deleted. 3. Click  . 4. Click **Yes** to confirm the deletion. You cannot delete a currently applied policy.

Operation	Description
Export an Advanced Malware policy	You can export and save one or more Advanced Malware policies into a file. 1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Advanced → Policy Export → **Advanced Malware**. The existing Advanced Malware policies are listed. 2. Select one or more policies to be exported. 3. Click **Export**. You are prompted to specify the location to save the file. The policy is saved in an XML format in the specified location.
Import an Advanced Malware policy	You can import an Advanced Malware policy from a saved file. 1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Advanced → Policy Import → **Advanced Malware**. To skip importing duplicate policy definition, select **Skip duplicate policy definitions**. 2. Browse to the file location. 3. Click **Import**. The import status is displayed.

Analyze Malware Files

You can leverage the analysis technique provided by Trellix IPS to perform an in-depth analysis of the malware detected in your network. The Manager provides you with a complete view of the malware and threats on your network for further analysis and actions, thus providing a comprehensive view of the threat landscape in your network. You can view the **Top Malware Files**. This dashboard is populated because a malicious file has been detected. In addition to viewing the threats to your network, the Manager also provides you the option to archive malware files.

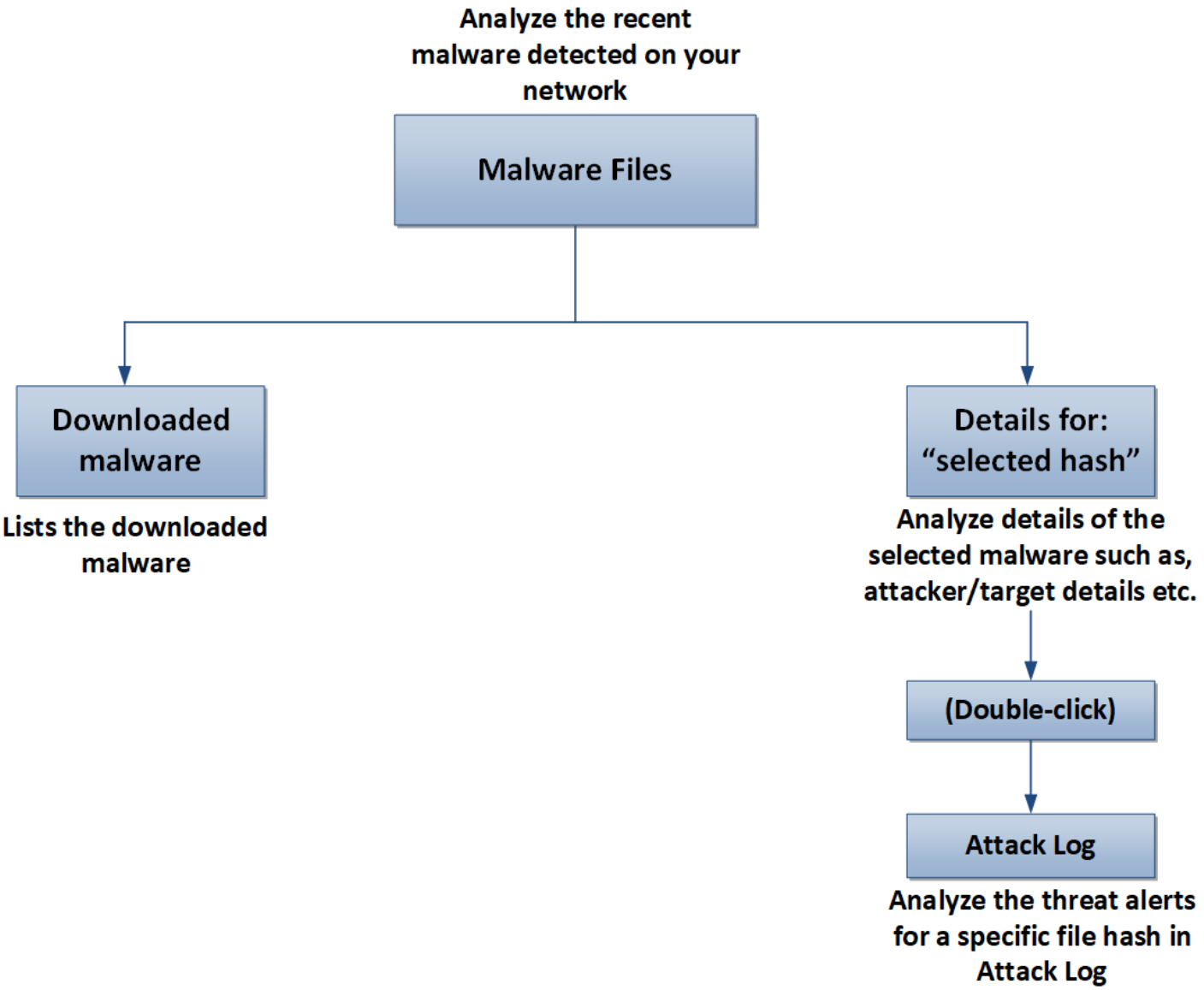
To view malware detected by Trellix IPS, use the **Top Malware Files** monitor. The dashboard displays the **Malware File Hash** and the **Attack Count** of the detected malware. Security monitors are displayed as bar charts in the **Dashboard** page.

Figure 396. Top Malware Files

If you want to drill down further on a specific malware, click on a bar, and you will be redirected to the Analysis → **Malware Files** page, which displays additional details on that malware. This page provides you with the flexibility of filtering and sorting the information displayed based on your choice. In addition to these filtering/sorting options, you can also view the alerts that match the filter criteria by opening the **Attack Log** page directly from the **Threat Explorer**. You can view the malware files specific to admin domains by selecting the required admin domain from the **Domain** drop-down list. Summarized data for malware files, which includes data from the child domains, also can be viewed. If you have integrated the Manager with ePolicy Orchestrator - On-prem or Logon Collector, you can view the host type, host name, user name, operating system details, top10 anti-virus events, and the details of system security products installed on the host.

The following chart gives you the comprehensive analysis options provided by the **Malware Files** page. These tabs are explained in the subsequent sections.

Figure 397. Malware analysis



The following filter options are provided.

Figure 398. View data specific to admin domain

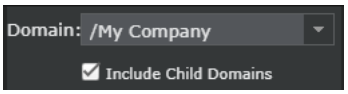


Figure 399. Analyze detected malware within a specific time

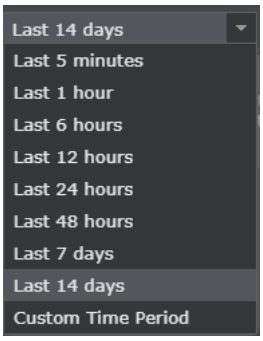


Figure 400. Analyze the type of malware, whether blocked, unblocked, or all

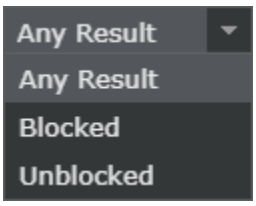


Figure 401. Analyze the malware based on malware confidence returned by engines

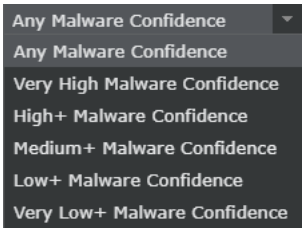
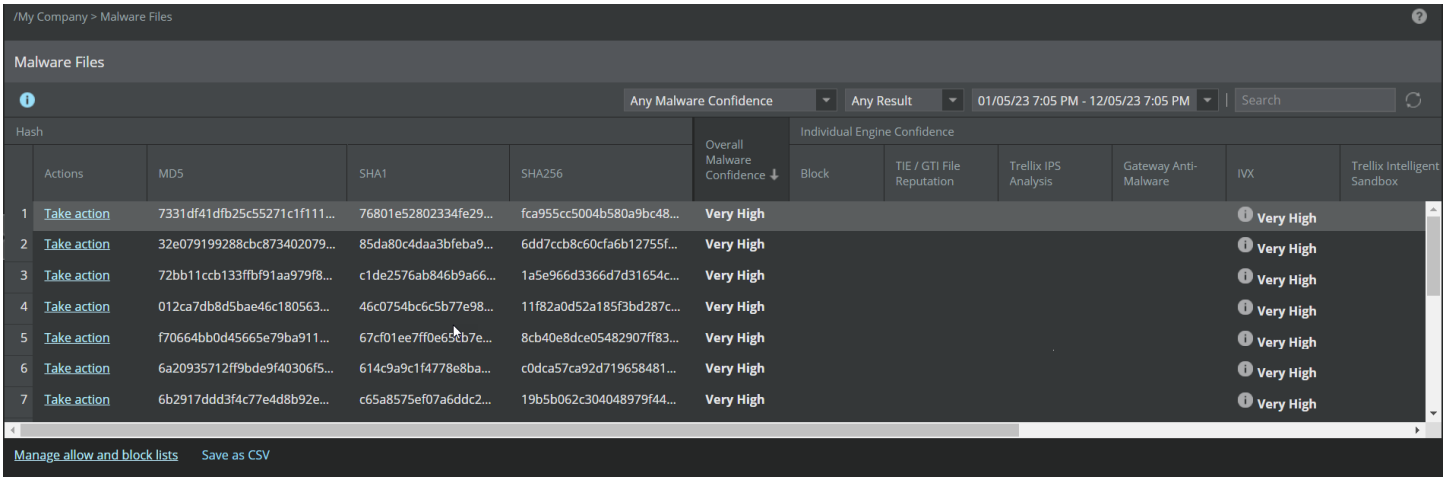


Figure 402. Details of the detected malware



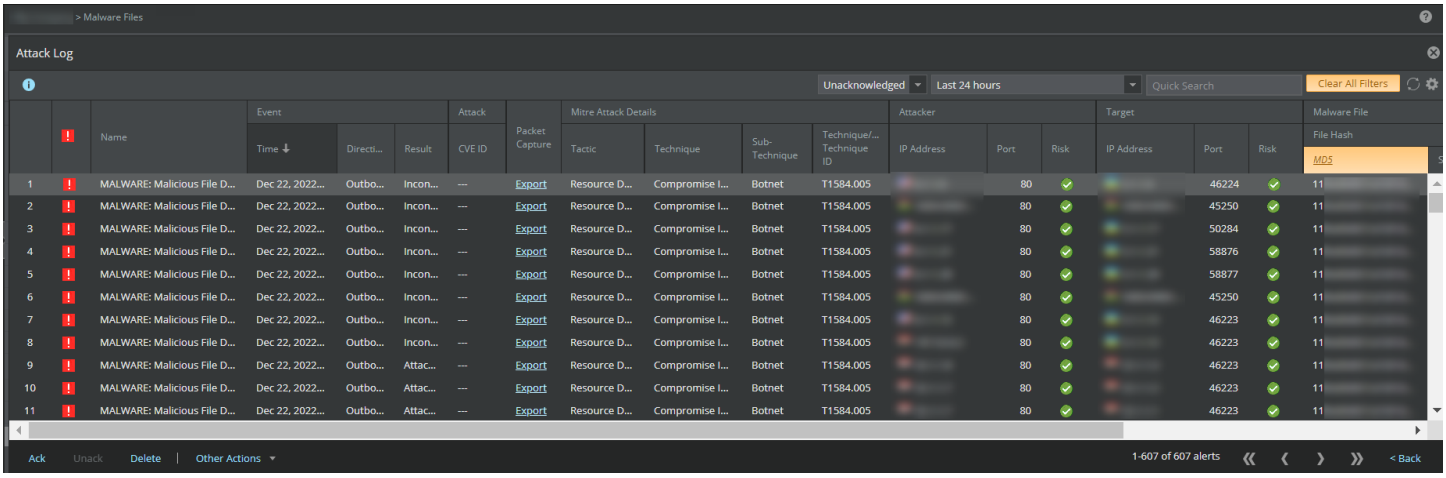
Option	Definitions
Hash	Displays the hash value of the file and the actions that you can take. • **Actions**— Click **Take action** to take the following actions: • **Export**— Click to download the malware file from the Manager server to a network location. The file is saved with an extension .trellix. This prevents you from even accidentally opening the malicious file. The file is available for download only if you enable the **Save File** option for the corresponding file type in the Advanced Malware policy that detected this malware. **NOTE** The antivirus program on your computer might prevent you from downloading the file. • **Allow**— Click to automatically add the file to the Manager's allow list. In the next 5 minutes, the Manager sends the MD5 hash value to the allow list of all the Sensors. **NOTE** In case MD5 entries limit has reached, the Manager adds SHA256 hash value(s) of the malware file(s) to its allow list and sends the same hash value(s) to the Sensor through incremental or full update. • **Block**— Click to automatically add the file to the Manager's block list. In the next 5 minutes, the Manager sends the MD5 hash value to the block list of all the Sensors. **NOTE** In case MD5 entries limit has reached, the Manager adds SHA256 hash value(s) of the malware file(s) to its block list and sends the same hash value(s) to the Sensor through incremental or full update. • **MD5** — Displays the MD5 hash of the file • **SHA1** — Displays the SHA1 hash of the file • **SHA256** — Displays the SHA256 hash of the file
Overall Malware Confidence	The overall malware confidence level returned by the configured malware scanning engines
Individual Engine Confidence	The confidence level returned by each configured malware scanning engine, individually. Click  to view the engine-specific details.
Last Attack	The date and time the last malware was detected.
Total Attacks	The number of times the malware was detected.

Option	Definitions
Last File Name	The name of the last saved malware file. In case of HTTP downloads it will be the URL.
File Size (bytes)	The size of the malware file saved
Comment	Additional comments on the detected malware

Attack Log

Upon double-clicking on the malware file hash, the **Attack Log** opens where you can view and analyze alerts related to the selected hash.

Figure 403. Attack log alerts for the hash selected



To close the attack log, click **Back** or icon.

Manage allow and block lists

The **Manage allow and block lists** is a link to the **File Hashes** page. For more information, see the [Trellix Intrusion Prevention System Product Guide].

View IVX Analysis Result for a detected malware

Similar to viewing the specific analysis results for other malware engines, you can also view the summary of the IVX analysis performed. In the **Malware Files** page, click next to the confidence level for **IVX**.

Figure 404. Details returned upon IVX Analysis

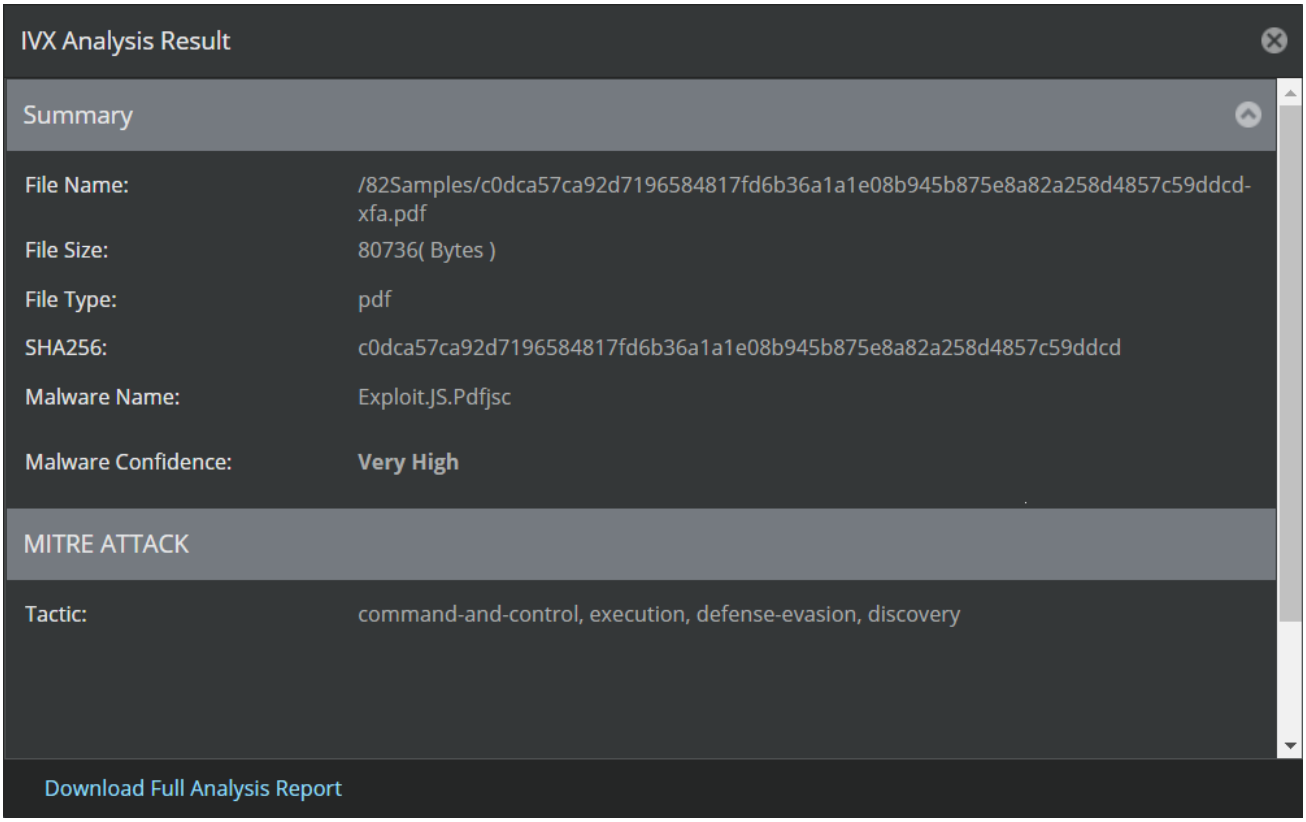


Table 49. Field descriptions

Field	Description
Summary	This section displays the summary of the IVX analysis.
File Name	Displays the file that is identified as malicious
File Size	Displays the file size in bytes
File Type	Displays the file type of the identified file
SHA256	Displays the SHA256 hash value of the file
Malware Name	Displays the name of the malware associated with the identified file
Malware Confidence	The highest malware severity as returned by IVX appliance or IVX Cloud
MITRE ATT&CK	This section displays the tactics utilized by the malware file to carry out the malicious activity.
Download Full Analysis Report	Downloads a file that contains the report for the malware from IVX. If the file is detected by Trellix VX, the downloaded file name will be **<file hash>_ivx_report**. If the file is detected by IVX Cloud, the downloaded file name will be **<file hash>_ivxcloud_report**. This file contains detailed analysis result data and can be opened with any text editor.
Close	Closes the **IVX Analysis Result** window

View the Trellix Intelligent Sandbox specific details for a detected malware

Similar to viewing the specific details for other malware engines, you can also view the specific results returned by Trellix Intelligent Sandbox. In the **Malware Files** page, click next to the confidence level for Trellix Intelligent Sandbox.

Figure 405. Details returned by Trellix Intelligent Sandbox

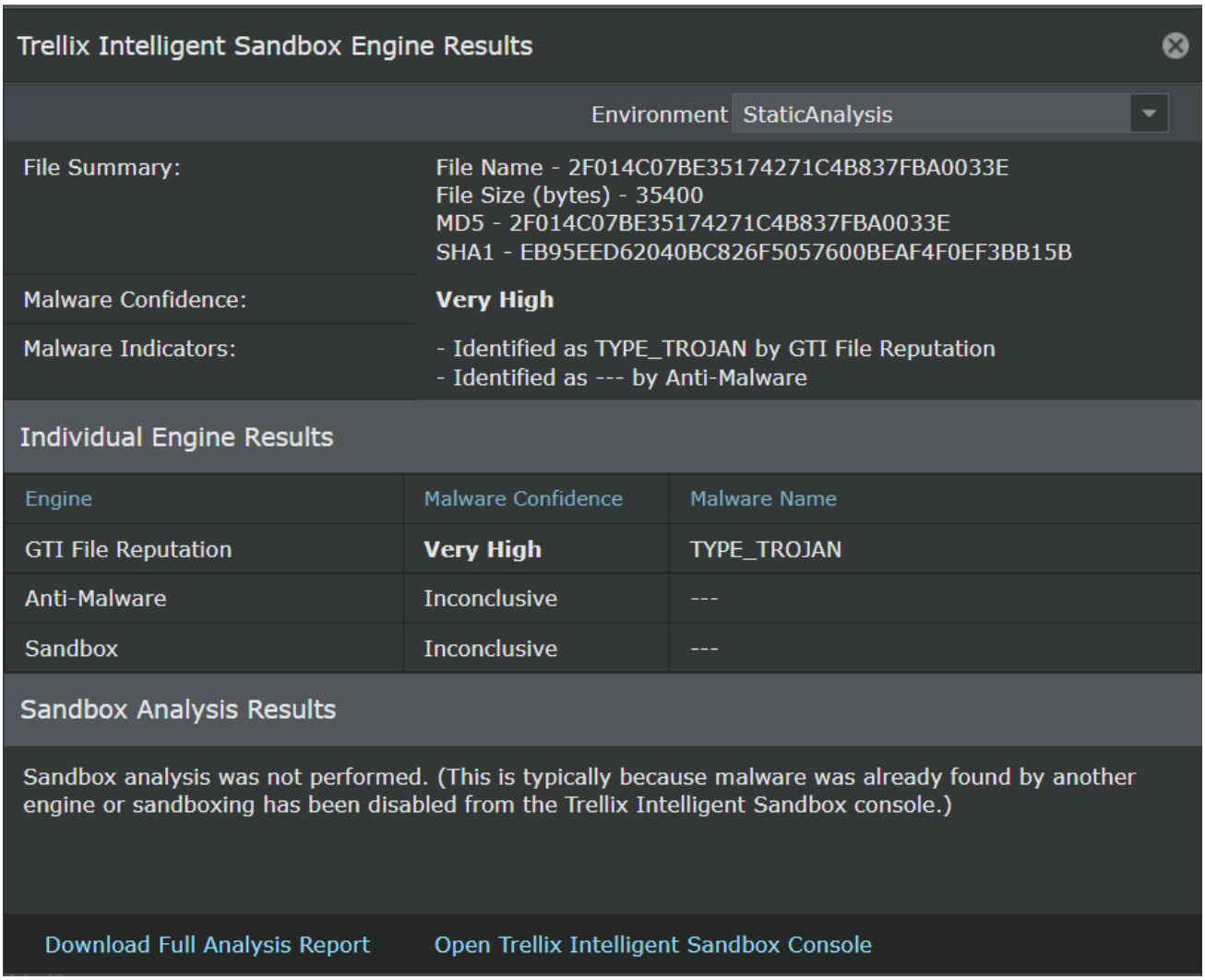


Table 50. Field descriptions

Field	Description
Environment	The VM profile that was used by Trellix Intelligent Sandbox to dynamically analyze the file. This indicates the operating system on which the file was executed.
File Summary	The name of the file, its size, and hash values are displayed.
Malware Confidence	The highest malware severity as returned by the components of Trellix Intelligent Sandbox

Field	Description
Malware Indicators	The summary of the reports from various analysis methods employed by Trellix Intelligent Sandbox
Individual Engine Results	This section lists the analysis methods available in Trellix Intelligent Sandbox. Here, they are referred to as **Engine**. The severity level returned by each method and the name for the malware are also displayed. If a particular method is not used, it indicates that it is not selected in the analyzer profile used for the Sensor.
Sandbox Analysis Results	This section displays the details if the file was dynamically analyzed by Trellix Intelligent Sandbox. This includes the details of the analyzer VM, the time and duration of the dynamic analysis, behavior during dynamic analysis, and so on.
Analysis Environment	This indicates the operating system on which the file was executed along with the build number of Trellix Intelligent Sandbox.
Download Full Analysis Report	Downloads a zip file that contains all the reports for the malware from Trellix Intelligent Sandbox. This is equivalent to downloading the reports zip file from the Trellix Intelligent Sandbox web application. This zip file contains the reports for each analysis. The contents of this zip file are explained beneath this table.
Open Trellix Intelligent Sandbox Console	Click to open the logon page of the Trellix Intelligent Sandbox that analyzed the file.
Close	Closes the **Trellix Intelligent Sandbox Engine Results** window

Download the <file hash>.zip file to the desired location. The files in this zip are created and stored with a standard naming convention. Based on the reports selected in the analyzer profile used for the analysis, the zip contains the following results:

- <file hash>_summary.html (.json, .txt, .xml): This is the same as the Analysis Summary report in the Trellix Intelligent Sandbox web application. There are four file formats for the same summary report in the zip file. The html and txt files are mainly for end-users to review the analysis report. The .json and .xml files provide well-known malware behavior tags for high-level programming script to extract key information.
- <file hash>.log: This file captures the Windows user-level DLL API calling activities during dynamic analysis. You must thoroughly examine this file to understand the complete API calling sequence as well as the input and output parameters. This is the same as the User API Log report in the Trellix Intelligent Sandbox web application.
- <file hash>ntv.txt: This file captures the Windows native services API calling activities during dynamic analysis.
- <file hash>.txt: This file shows the PE header information of the submitted sample.
- <file hash>_detail.asm: This is the same as the Disassembly Results report in the Trellix Intelligent Sandbox web application. This file contains reverse-engineering disassembly listing of the sample after it has been unpacked or decrypted.
- <file hash>_logicpath.gml: This file is the graphical representation of cross-reference of function calls discovered during dynamic analysis. This is the same as the Logic Path Graph report in the Trellix Intelligent Sandbox web application. Use a graph editor, such as yWorks yEd Graph Editor, to view this file.
- log.zip: This file contains all the run-time log files for all processes affected by the sample during the dynamic analysis. If the sample generated any console output text, the output text messages are captured in the ConsoleOutput.log file zipped up in the log.zip file. Use any regular unzip utility to see the content of all files inside the log.zip file.
- dump.zip: This file contains the memory dump (dump.bin) of binary code of the sample during dynamic analysis. This file is password protected. The password is *virus*.

- dropfiles.zip: This is the same as the Dropped Files report in the **Analysis Results** page of Trellix Intelligent Sandbox web application. The dropfiles.zip file contains all files created or touched by the sample during the dynamic analysis. It is also password protected like dump.zip.

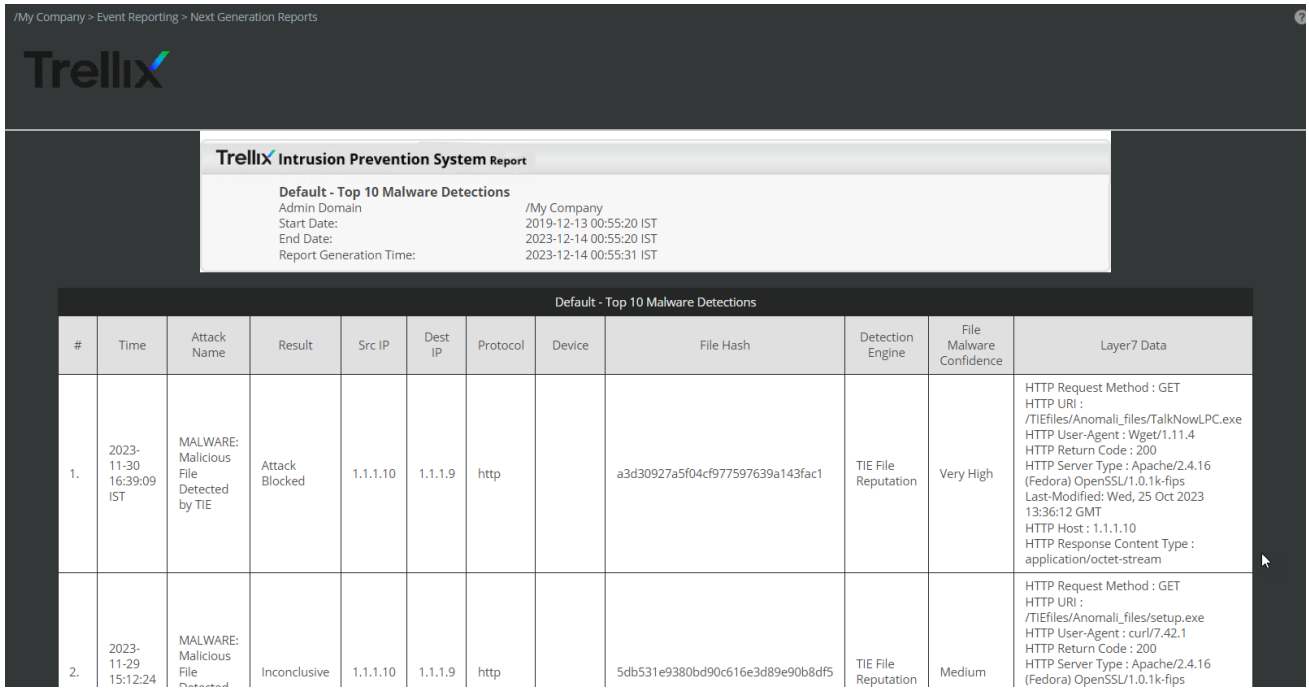
For a detailed explanation of all these files and Trellix Intelligent Sandbox reports, see the [Trellix Intelligent Sandbox Product Guide].

Manager reports for malware detections

A default Next Generation Report called **Top 10 Malware Detections** provides details of the detected malware. For a given time period, this report shows the alerts raised for the top 10 most frequently downloaded malware in your network. Therefore, for a given file, you can view the results from various malware engines. However, these results are dependant on the Advanced Malware policy configuration for the period of the report.

1. In the Manager, select Analysis → Event Reporting → **Next Generation Reports.**
2. From the list of **Saved Reports**, select **Default - Top 10 Malware Detections** and then click **Run.**
3. Specify the time period for which you want to generate the report in the **Date Options** section.
4. Select the output format of the report from the **Report Format** list.
5. Click **Run.**

Figure 406. The default Top 10 Malware Detections report



The generated report is displayed.

Table 51. Column definitions

Column	Definition
Time	The time stamp when a malware engine determined the file to be malicious

Column	Definition
Attack Name	The alert raised by the Sensor for the file
Result	The response action taken by the Sensor for the file. For example, the Sensor could have blocked the file download.
Src IP	The source IP address as seen in the traffic for the malware traffic
Dest IP	The target host that is downloading the file
Protocol	The L7 protocol involved. This could be HTTP or SMTP.
Device	The Sensor that detected the file download
File Hash	The MD5 hash value of the file as calculated by the Sensor
Detection Engine	The malware engine that reported the malware
File Malware Confidence	The malware score reported by the malware engine
Layer7 Data	The L7 data associated with the file

NOTE

The admin domain filter on the main **Analysis** tab (provided in the left pane) has no impact on the reports generated. The admin domain filter criteria selected for the reports show data specific to the admin domain selected.

- For information how to use the Next Generation Reports, see the section [Next Generation reports] in [Trellix Intrusion Prevention System Product Guide].
- You can also generate a User Defined report using all of the above columns. For example, you can generate a User Defined report that reports only very-high severity malware detected by Sensors of a particular domain. You must use **Alert Data** as the **Data Source** when you define the report. For more information on how to generate a User Defined report, see the section [Generate Next Generation user defined reports] in [Trellix Intrusion Prevention System Product Guide].

Malware engine caching

Malware scanning engines like Trellix IPS Analysis, and Gateway Anti-Malware have caching capabilities. By default, the IVX and Trellix Intelligent Sandbox malware engine file results are cached.

Once a file is analyzed by IVX or Trellix Intelligent Sandbox, the file results are cached. If the same file is received by the Sensor, it is not sent to these engines for analysis, and the results are retrieved from the cache.

- The Sensor continues to submit files for analysis to IVX or Trellix Intelligent Sandbox or both (based on malware engines selected) until the file analysis results are complete and stored in the cache.
- The cache can be purged after a specified duration, which can be configured via CLI.
- You can use the CLI commands, **`atdcache autopurge`**, **`set atdcachepurge interval hours`**, and **`clearmalwarecache`** to configure the cache settings. See the [CLI commands] section for details.

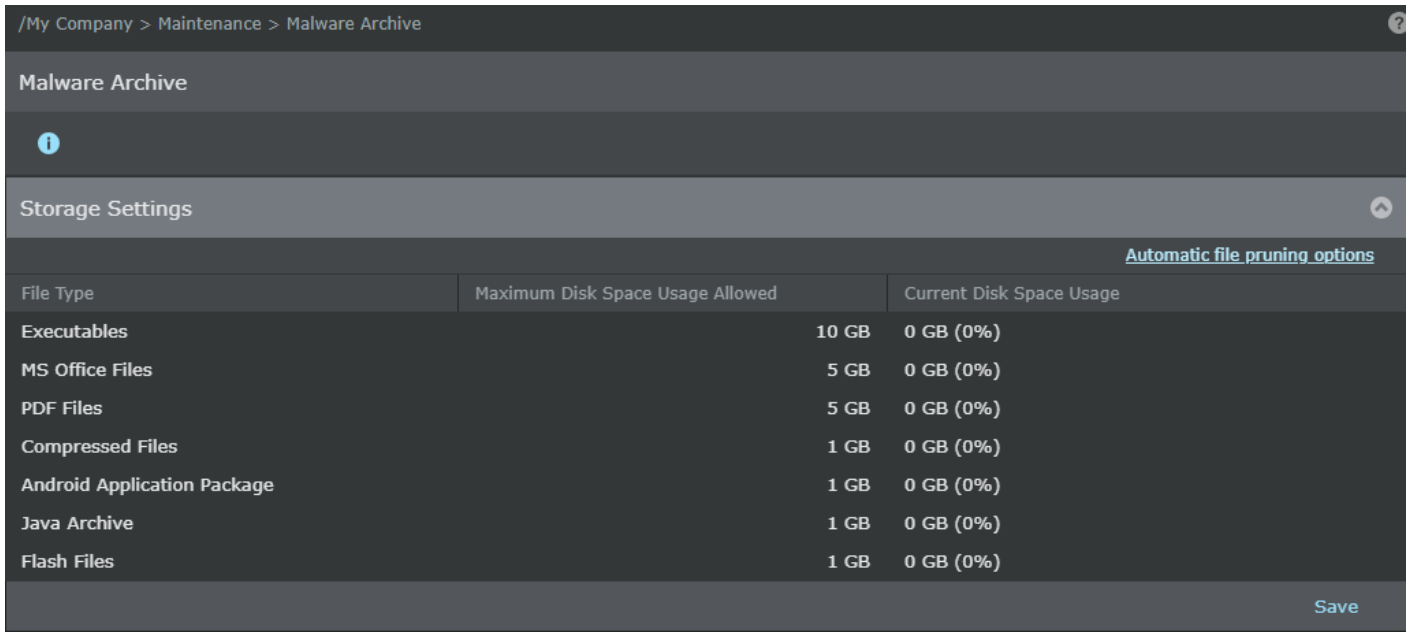
Archive malware files

The malware policy has configuration settings to archive downloaded files based on various characteristics. These downloaded files are archived on the Manager server as encrypted files. You can configure the location and maximum disk space that can be used to store the archives. The configuration for disk usage is defined at the Global Manager level. The Manager also provides configuration to prune files that are stored for more than a specified period of time.

Perform the following steps to maintain the malware files saved to the Manager.

1. Select Manager → <Admin Domain Name> → Maintenance → **Malware Archive**.
2. The **Storage Settings** are displayed for each file type. Click the **Maximum Disk Space Usage Allowed** to modify it as per your requirement.

Figure 407. File storage settings



3. To prune the file storage, click **Automatic file pruning options**.

   File pruning option allows you to determine the interval at which the Manager prunes older data to make sure its file system and database have adequate space for new data.

4. Click **Save**.

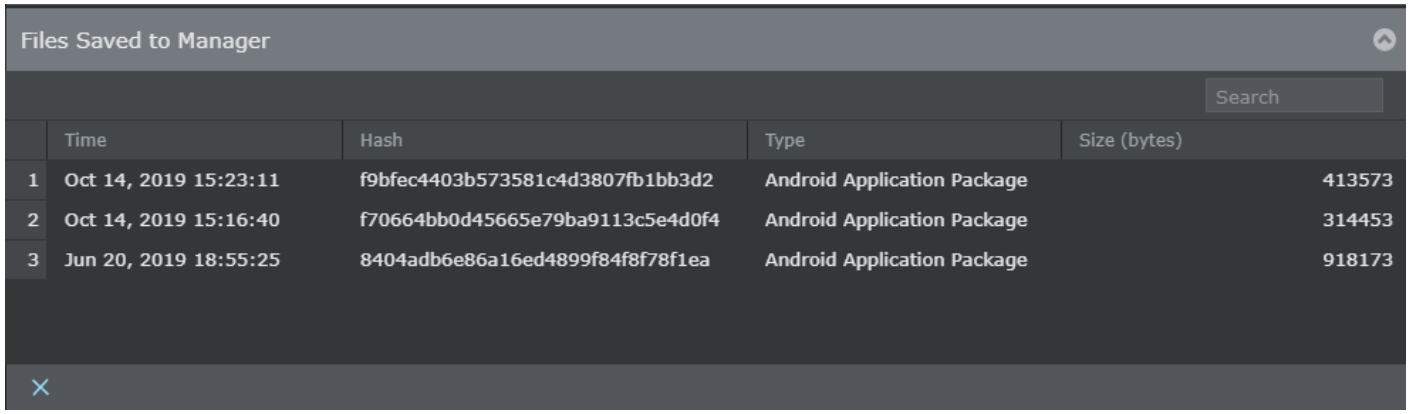
   The Manager warns you when the allocated disk space to a malware file type reaches 70%, 80%, 90%, and 100% of the maximum allowed. When the maximum space limit is reached, new malware files of that type are not stored until space is freed.

   The default location of these files in the Manager server is `%programfiles%\Trellix\IPS Manager\App\temp\tftpin\malware`. The list of files currently archived on the Manager are displayed with the following details.

   - **Time**— Indicates the date and time when the file was saved
   - **Hash** — Displays the MD5 hash of the file
   - **Type** — The type of the saved file

- **Size** — The size of the file saved

Figure 408. Details on stored files



5. To delete the archived files, select the required ones and click ✕

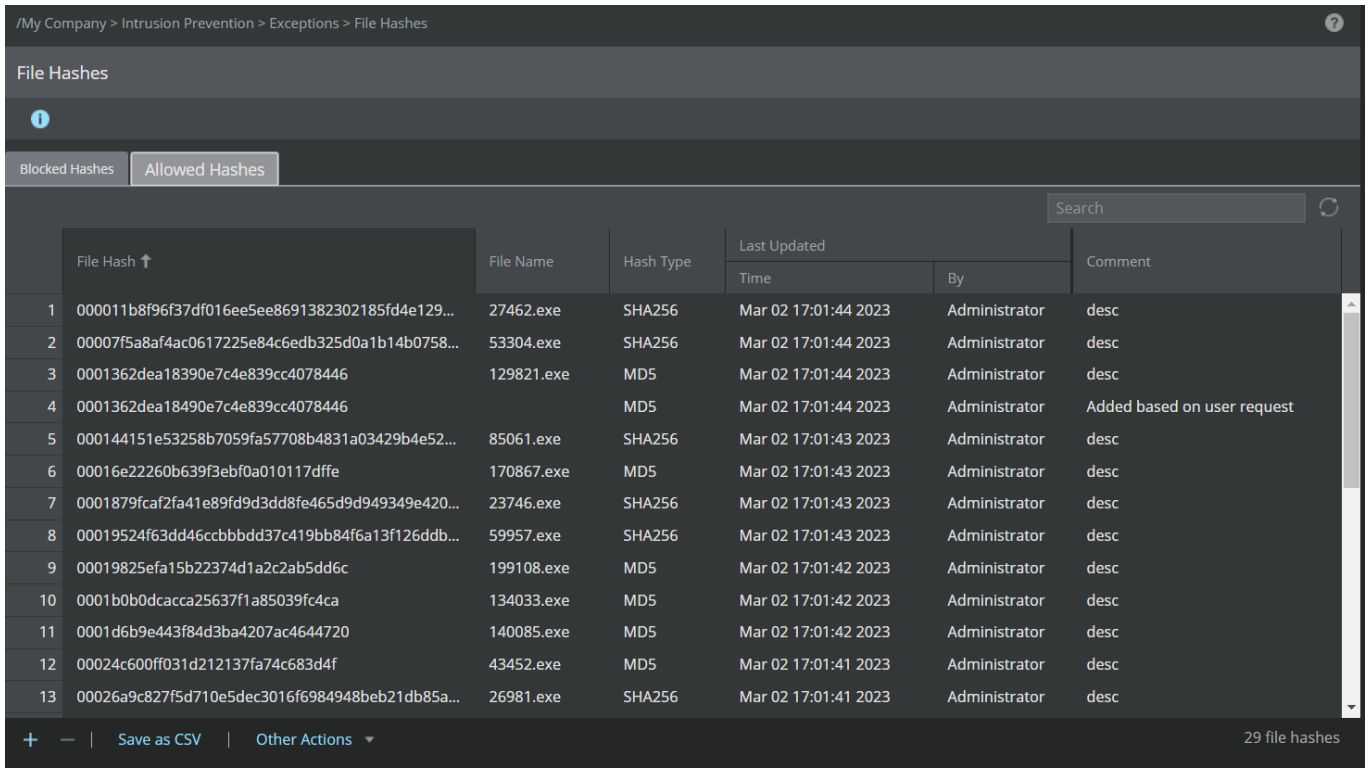
Add hash values to the allow list

You can add a list of allowed fingerprints (MD5 or SHA256 hash values) for files you want to be exempted from malware analysis when found in HTTP or SMTP downloads.

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **File Hashes**.

   You can view the current list of allowed hashes on the **Allowed Hashes** tab of the **File Hashes** page.

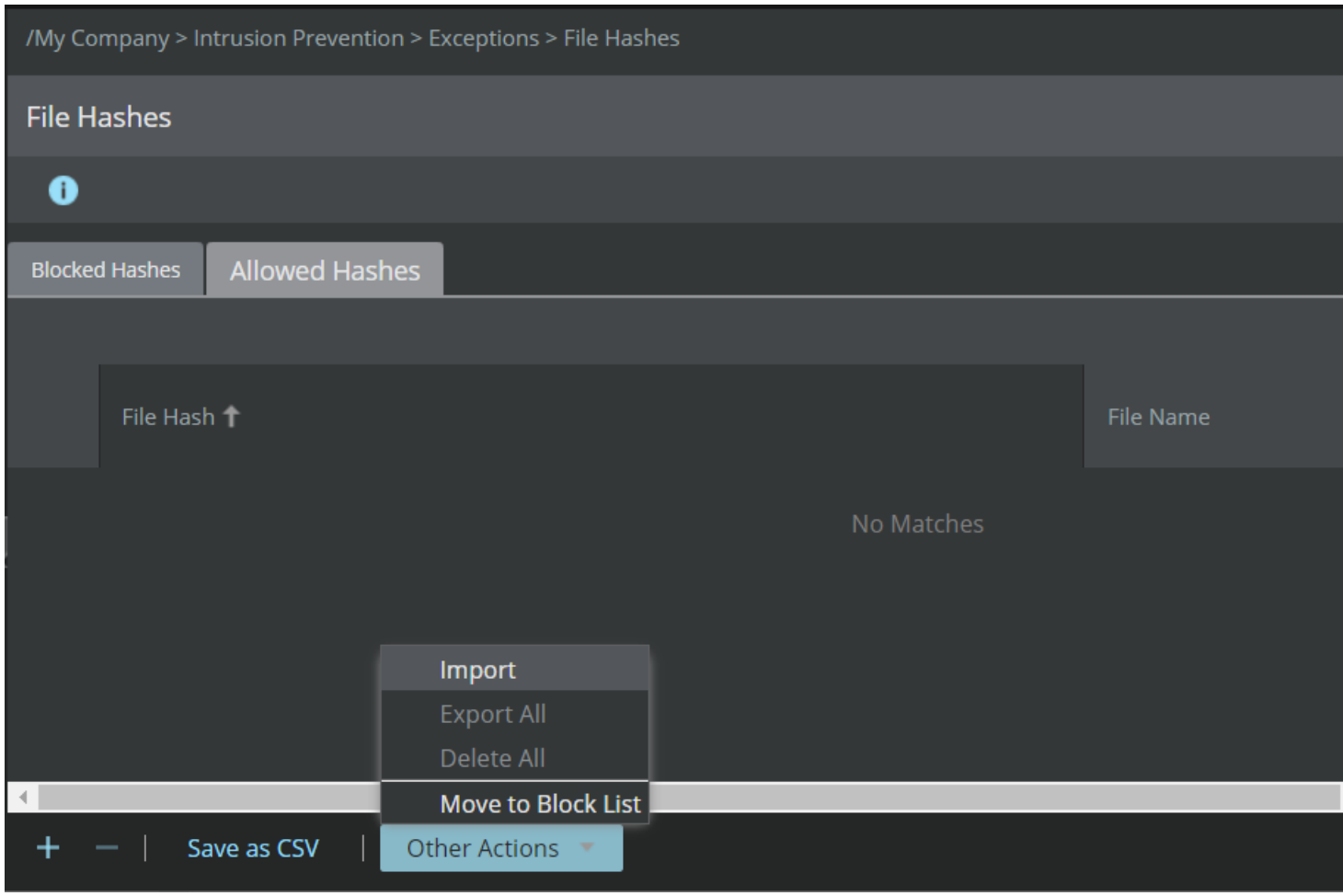
Figure 409. Allowed Hashes



The following table describes the details displayed on the **Allowed Hashes** tab.

Format	Description
File Hash	Specifies the file hash. The **File Hash** should be in MD5 or SHA256 format
File Name	Specifies the name of the file along with the file extension
Hash Type	Specifies the format of the hash. The supported file hash types are MD5 and SHA256.
Last Updated	Displays the following: • **Time**: Specifies the time stamp of the imported allow list • **By**: Specifies the user who imported the allow list
Comment	Any comments about the list

2. File hashes can be added through this page in two ways — using the **Import** option or the + icon. To import a file containing the hash values, click Other Actions → **Import**.



3. **Import from CSV** window appears. Use the **Append** option to add a new list of hashes or to append a list of hashes to an existing list. Use the **Replace** option to remove the existing list of hashes and add a new list from the file being imported.

   The file to be imported should be in the following CSV format.

<Name of the file with extension (like .exe, .com)>,<File size>,<Hash type>,<File hash>,<Description>

Example file format for MD5 hashes: **Application.exe, 1024000, MD5, 30a4edd18db6dd6aaa20e3da93c5f425, textual description**.

Example file format for SHA256 hashes: **Service.exe, 1024000, SHA256, a6279afa088a2e200b3b222c3169e9dce332a08759512800b48bf038e47bf528, textual description**. Also note that if you are adding multiple entries in the CSV file, each entry has to be in a new line.

The following is a sample for a CSV file with multiple file hashes.

	A	B	C	D	E
1	<Optional file name>	524	MD5	2e51d1f45dd1126c9e81b3a293042a82	<Optional comment>
2	Application.exe	628	SHA256	8ff50a5df7d4eca1744552893f19d4ae5af0997999de0af77944f58fef5f5d8b	File related to virus
3	MaliciousService.exe	357	SHA256	098f6bcd4621d373cade4e832627b4f6	File related to trojan

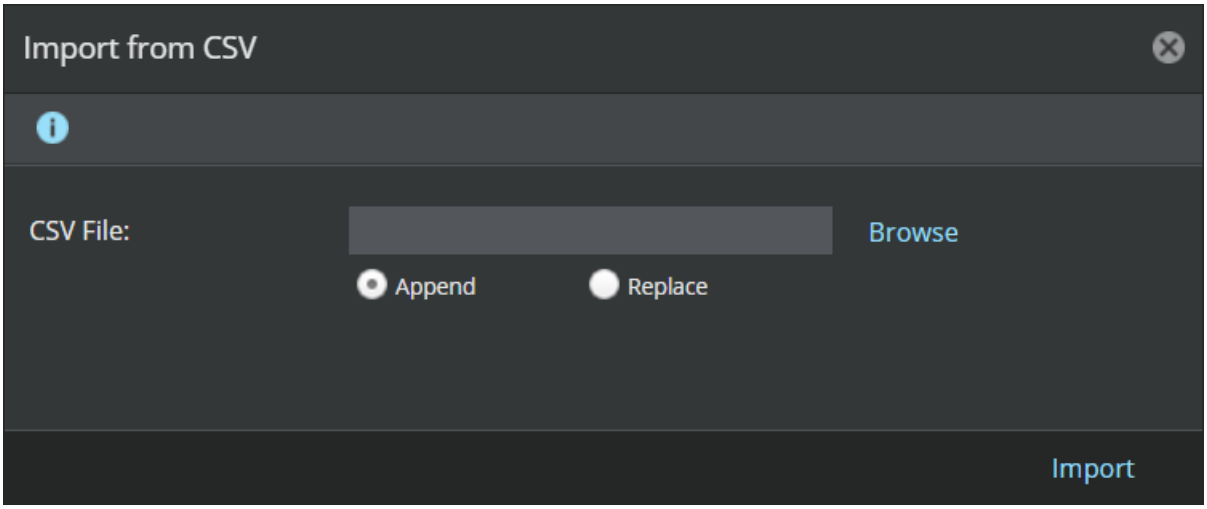
The following table describes the details of the files to be imported in the CSV or XML format.

Format	Description
<Name of the file with extension (like .exe, .com)>	Specifies the name of the file to be imported, along with the file extension. This is an optional value.
<File size>	Specifies the size of the file to be imported. The file size should be a valid integer. **NOTE** File size value is mandatory. It is used by the Sensor as a secondary matching criterion when the same hash has been added to both the block list and allow list. **NOTE** If the file size is unknown, you can add a placeholder value like 1 to the CSV file as this value is mandatory.
<Hash type>	Specifies the format of the hash. The supported file hash types are MD5 and SHA256.
<File hash>	Specifies the hash for the file to be imported
<Description>	Specifies the description of the file to be imported. This is an optional value.

NOTE

If you import the same file hashes to allow list first and then to block list, the hashes in the allow list will be removed and added to the block list. Similarly, if you import the same file hashes to block list first and then to allow list, the hashes in the block list will be removed and added to the allow list.

4. Click **Browse** to locate the CSV file that contains the list of hashes you want to import.

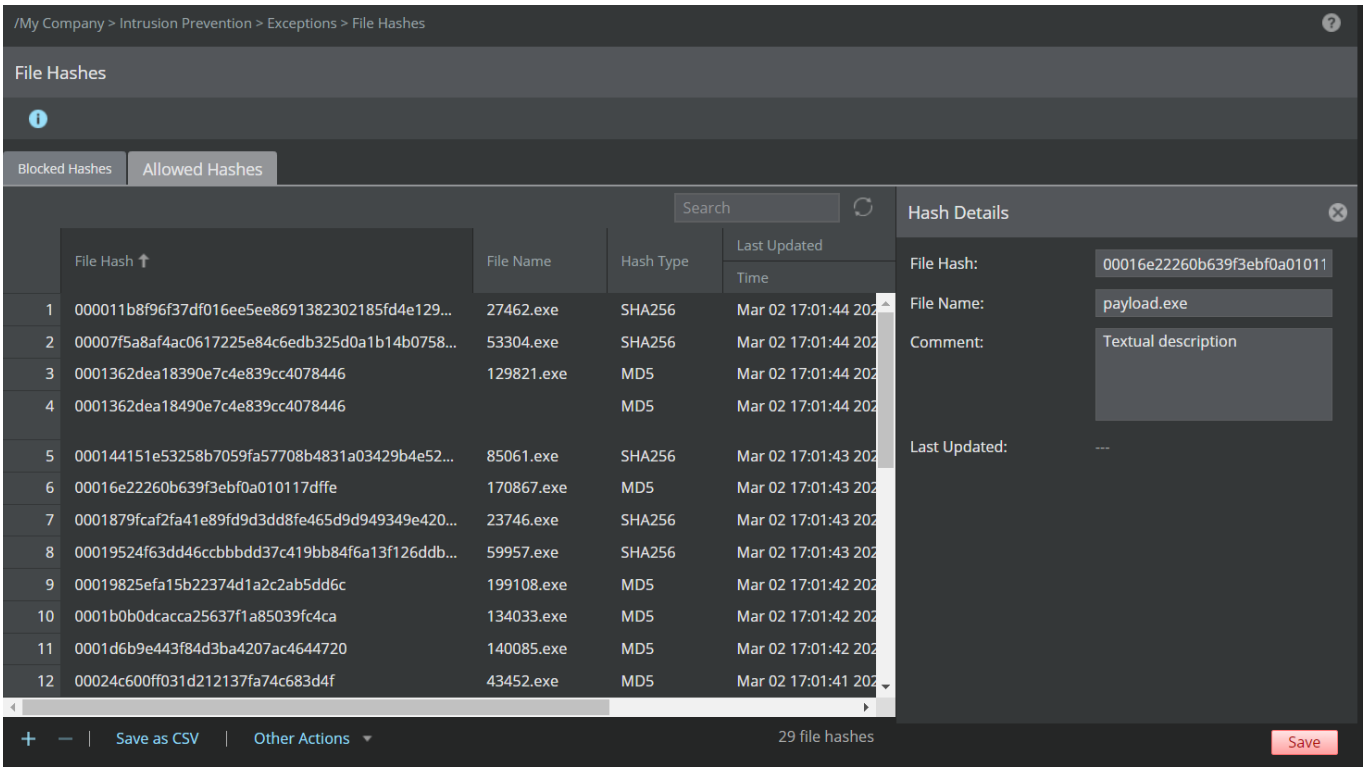


5. Click **Import** upon selecting the CSV file.
6. To add a single file hash to the allowed hashes, click +.

   Click **Save** after entering the values in **File Hash**, **File Name**, and **Comment**. The **Comment** field is optional.

> **NOTE**
>
> The **File Hash** should be a 32 or 64 digit hexadecimal value depending on the hash type.

Figure 410. Add a single allow list file hash value



NOTE

- The Manager running on **11.1 Update 1** or later releases supports addition of up to 400,000 hash entries (allowed and blocked combined) with a limit of 200,000 per each hash type. Manager prior to **11.1 Update 1 release** supports addition of only MD5 hashes up to 100,000 entries (allowed and blocked combined).
- Sensors prior to **11.1 Update 1 release** do not support SHA256 hashes. The maximum number of hashes supported (cumulative of Blocked Hashes and Allowed hashes) by these Sensors is 100,000.
- Sensors running on **11.1 Update 1** or later releases support both SHA256 and MD5 hashes. NS-series Sensors support a maximum of 200,000 hashes for each hash type while the Virtual IPS Sensors support a maximum of 100,000 hashes for each hash type. If the Manager has both NS-series and virtual Sensors, entries over 100,000 in each hash type are pushed only to the NS-series Sensors. The push fails on virtual Sensors and a fault is raised which can be noticed in the **Faults** (Manager → Troubleshooting → Logs → **Faults**) tab.
- In case of heterogeneous environments, if the total MD5 hash entries exceed 100,000:
  - A limit exceed error can be seen in **filetransfer.log** during a bulk (full) update
  - A fault will be raised in the **Faults** tab and error count will be incremented at the Sensor level during an incremental update. Refer to **`show ab stats`** command for more information.

    NOTE

    A Full update is triggered when the total entries are more than 4000; else, an incremental update is triggered to all the Sensors connected to the Manager.
- In case MD5 and SHA256 hashes of the same file are added, the MD5 hash takes precedence over SHA256 hash of the file during analysis.

7. To export the allowed hashes from the Manager to a local system, click Other Actions → **Export All**.
8. To delete specific entries from the allow list, select them by holding the **Shift** or **Ctrl** key and clicking on the required rows. Then click  .

   The deleted hashes are now neither in the allow list nor in the block list.
9. To remove all the entries, select Other Actions → **Delete All**.
10. To move specific entries to the block list, select the entries and then select Other Actions → **Move to Block List**.
    - A manual signature set push is not required each time the allow list or the block list is updated. The Manager updates the Sensor dynamically with the modified entries in the allow list or block list, at an interval of 5 minutes. These updates occur in bulk (the complete list of entries) or increments (added/deleted entries). To view the status of these updates, use the **`show ab stats`** command. For more information, see the [CLI commands] section in the [Trellix Intrusion Prevention System Product Guide].

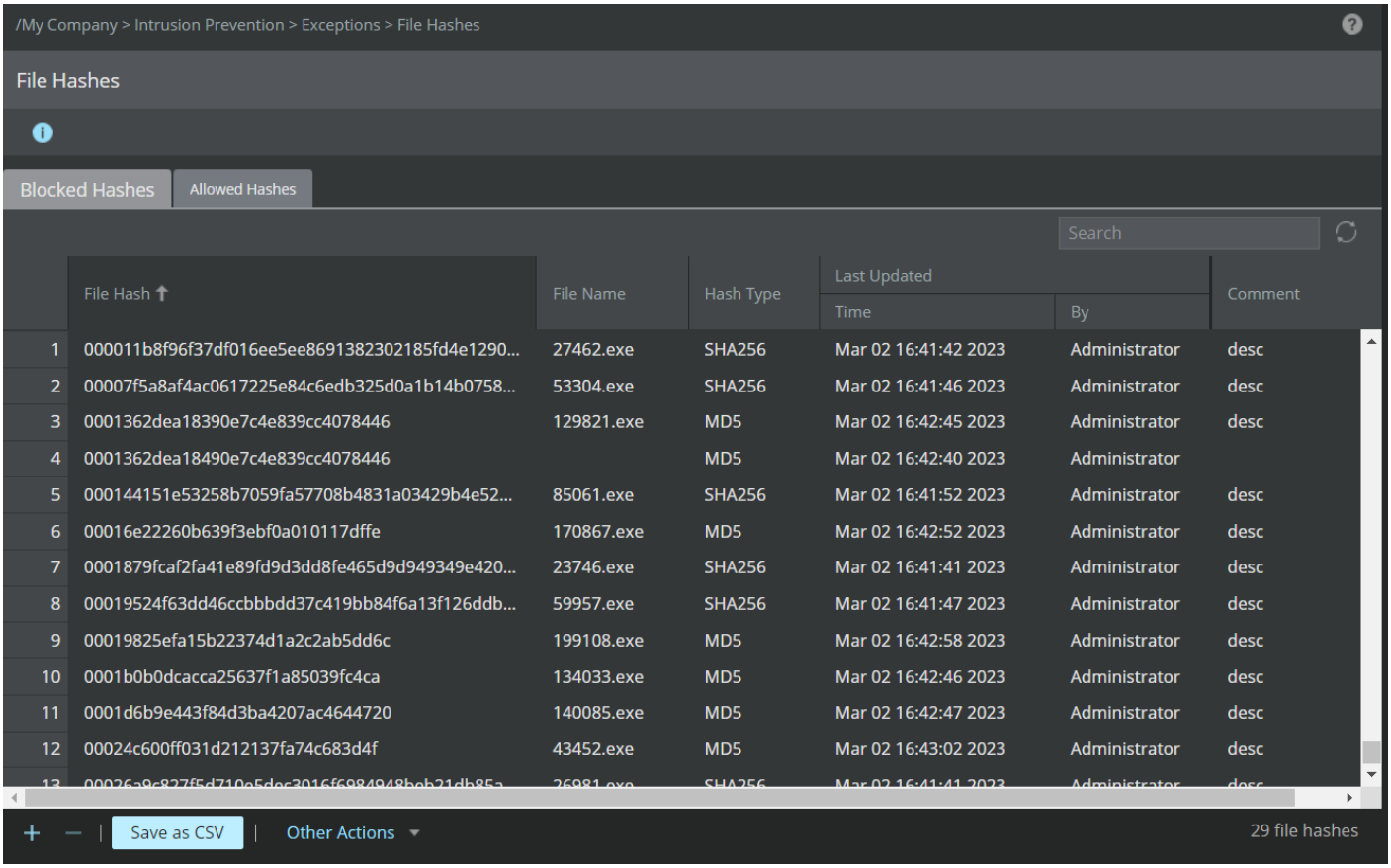
Add hash values to the block list

You can add MD5 or SHA256 hash values of files that you want to be treated as malicious when found in HTTP and SMTP downloads. If a file's hash matches a hash value in the block list, the Sensor treats the file as malicious of *very high* severity.

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **File Hashes**.

   On the **Blocked Hashes** tab, you can add the hash values to be blocked, manage the file types to be checked for the blocked hashes, and view the maximum file size scanned.

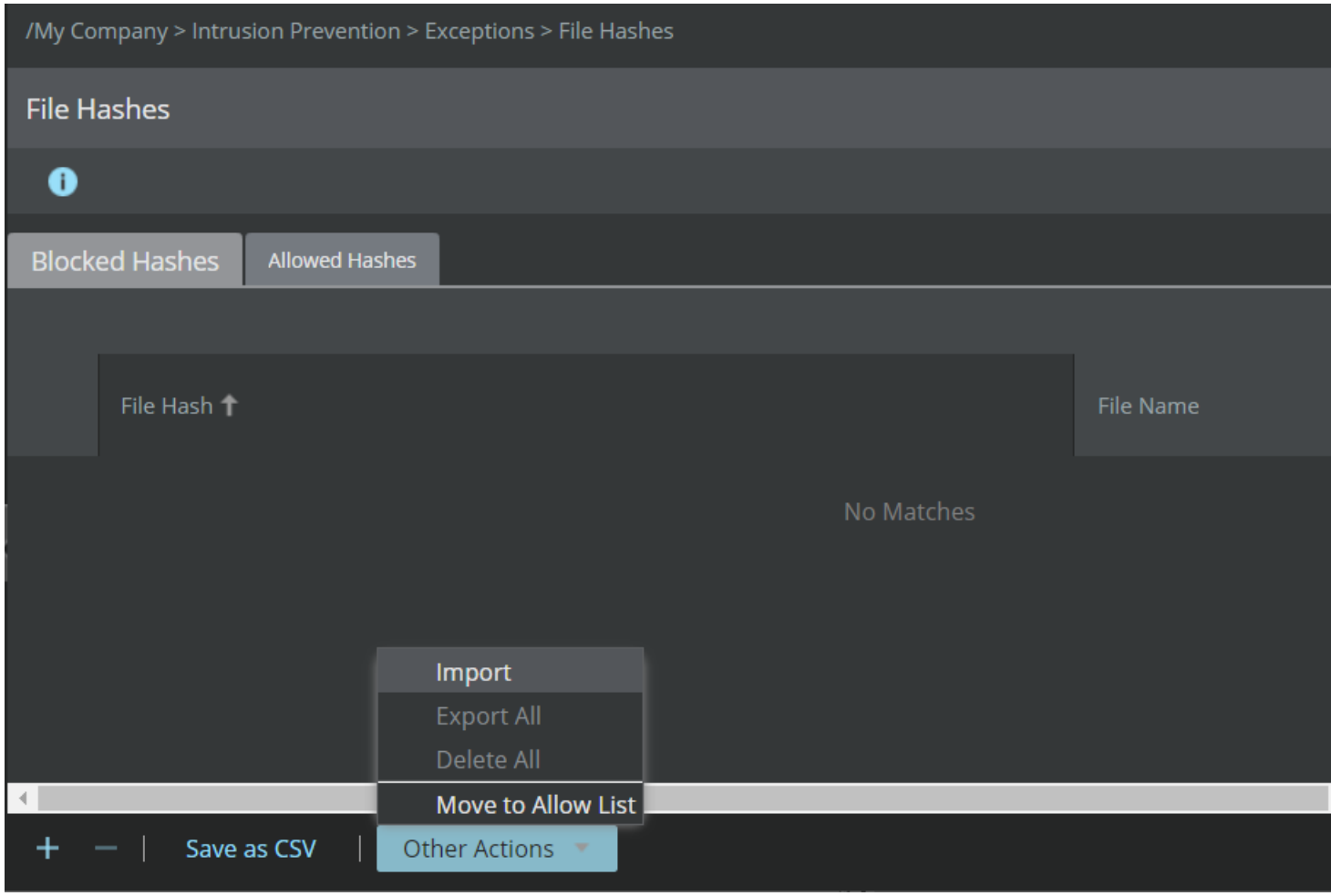
Figure 411. Blocked hashes



The following table describes the details displayed on the **Blocked Hashes** tab.

Format	Description
File Hash	Specifies the file hash. The **File Hash** should be in MD5 or SHA256 format
File Name	Specifies the name of the file along with the file extension
Hash Type	Specifies the format of the hash. The supported file hash types are MD5 and SHA256.
Last Updated	Displays the following: • **Time**: Specifies the time stamp of the imported block list file hash • **By**: Specifies the user who imported the block list file hash
Comment	Any comments about the list

2. File hashes can be added through this page in two ways — using the **Import** option or the + icon. To import a file containing the hash values, click Other Actions → **Import**.



3. **Import from CSV** window appears. Use the **Append** option to add a new list of hashes or to append a list of hashes to an existing list. Use the **Replace** option to remove the existing list of hashes and add a new list from the file being imported.

   The file to be imported should be in the following CSV format.

   `<Name of the file with extension (like .exe, .com)>,<File size>,<Hash type>,<File hash>,<Description>`

   Example file format for MD5 hashes: **`Application.exe, 1024000, MD5, 30a4edd18db6dd6aaa20e3da93c5f425, textual description`**.

   Example file format for SHA256 hashes: **`Service.exe, 1024000, SHA256, a6279afa088a2e200b3b222c3169e9dce332a08759512800b48bf038e47bf528, textual description`**. Also note that if you are adding multiple entries in the CSV file, each entry has to be in a new line.

   The following is a sample for a CSV file with multiple file hashes.

	A	B	C	D	E
1	<Optional file name>	524	MD5	2e51d1f45dd1126c9e81b3a293042a82	<Optional comment>
2	Application.exe	628	SHA256	8ff50a5df7d4eca1744552893f19d4ae5af0997999de0af77944f58fef5f5d8b	File related to virus
3	MaliciousService.exe	357	SHA256	098f6bcd4621d373cade4e832627b4f6	File related to trojan

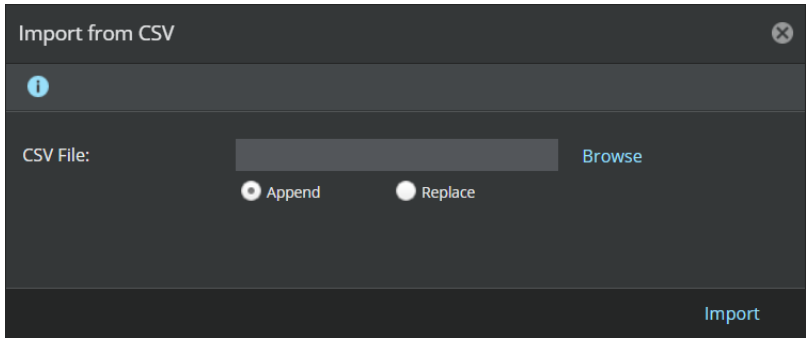
   The following table describes the details of the files to be imported in the CSV or XML format.

Format	Description
`<Name of the file with extension (like .exe, .com)>`	Specifies the name of the file to be imported, along with the file extension. This is an optional value.
`<File size>`	Specifies the size of the file to be imported. The file size should be a valid integer. **NOTE** File size value is mandatory. It is used by the Sensor as a secondary matching criterion when the same hash has been added to both the block list and allow list. **NOTE** If the file size is unknown, you can add a placeholder value like 1 to the CSV file as this value is mandatory.
`<Hash type>`	Specifies the format of the hash. The supported file hash types are MD5 and SHA256.
`<File hash>`	Specifies the hash for the file to be imported
`<Description>`	Specifies the description of the file to be imported. This is an optional value.

NOTE

If you import the same file hashes to allow list first and then to block list, the hashes in the allow list will be removed and added to the block list. Similarly, if you import the same file hashes to block list first and then to allow list, the hashes in the block list will be removed and added to the allow list.

4. Click **Browse** to locate the CSV file that contains the list of hashes you want to import.



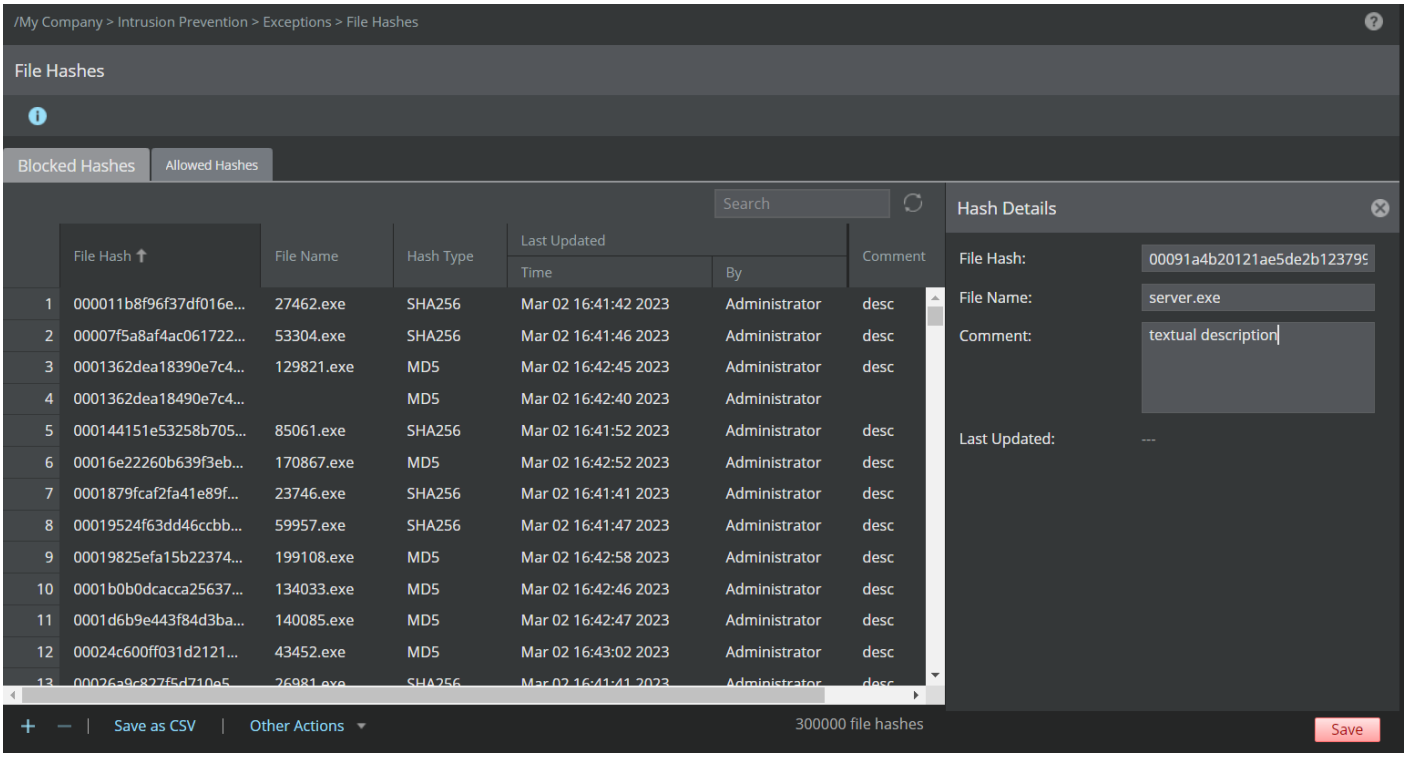
5. Click **Import** upon selecting the CSV file.
6. To add a single file hash to the blocked hashes, click +.

   Click **Save** after entering the values in **File Hash**, **File Name**, and **Comment**. The **Comment** field is optional.

NOTE

The **File Hash** should be a 32 or 64 digit hexadecimal value depending on the hash type.

Figure 412. Add a single block list file hash value



NOTE

- The Manager running on **11.1 Update 1** or later releases supports addition of up to 400,000 hash entries (allowed and blocked combined) with a limit of 200,000 per each hash type. Manager prior to **11.1 Update 1 release** supports addition of only MD5 hashes up to 100,000 entries (allowed and blocked combined).
- Sensors prior to **11.1 Update 1 release** do not support SHA256 hashes. The maximum number of hashes supported (cumulative of Blocked Hashes and Allowed hashes) by these Sensors is 100,000.
- Sensors running on **11.1 Update 1** or later releases support both SHA256 and MD5 hashes. NS-series Sensors support a maximum of 200,000 hashes for each hash type while the Virtual IPS Sensors support a maximum of 100,000 hashes for each hash type. If the Manager has both NS-series and virtual Sensors, entries over 100,000 in each hash type are pushed only to the NS-series Sensors. The push fails on virtual Sensors and a fault is raised which can be noticed in the **Faults** (Manager → Troubleshooting → Logs → **Faults**) tab.
- In case of heterogeneous environments, if the total MD5 hash entries exceed 100,000:
  - A limit exceed error can be seen in **filetransfer.log** during a bulk (full) update
  - A fault will be raised in the **Faults** tab and error count will be incremented at the Sensor level during an incremental update. Refer to **`show ab stats`** command for more information.

    NOTE

    A Full update is triggered when the total entries are more than 4000; else, an incremental update is triggered to all the Sensors connected to the Manager.
- In case MD5 and SHA256 hashes of the same file are added, the MD5 hash takes precedence over SHA256 hash of the file during analysis.

7. To export the blocked hashes from the Manager to a local system, click Other Actions → **Export All**.
8. To delete specific entries from the block list, select them by holding the **Shift** or **Ctrl** key and clicking on the required rows. Then click  .

   The deleted hashes are now neither in the allow list nor in the block list.
9. To remove all the entries, select Other Actions → **Delete All**.
10. To move specific entries to the allow list, select the entries and then select Other Actions → **Move to Allow List**.
    - A manual signature set push is not required each time the allow list or the block list is updated. The Manager updates the Sensor dynamically with the modified entries in the allow list or block list, at an interval of 5 minutes. These updates occur in bulk (the complete list of entries) or increments (added/deleted entries). To view the status of these updates, issue the **`show ab stats`** command. For more information, see the [CLI commands] section in the [Trellix Intrusion Prevention System Product Guide].

File or content mismatch

Attackers sometimes attempt to modify the extension of the file in order to avoid detection. Certain file types which are subject to a more thorough analysis, because of the nature of the content that they hold, have their extensions changed in order to mislead firewalls or conventional security systems from analyzing or blocking them. Once such a file is in the network, it can perform various actions such as contacting a bot server or attaching itself to documents in order to proliferate across a network. A common example is when an executable file is sent with an extension of .sys, but when analyzed, contains a content type value as plain text.

The Sensor is equipped with a specific signature and an underlying mechanism to be able to detect such evasion attempts. When a file appears, the Sensor first extracts the magic number for the file type. Every file type has a magic number that is unique to itself. The Sensor extracts this data and does not rely only on the extension provided in the file name. This method of detection also works when no file extension is provided. The Sensor check the magic number and content type.

NOTE

Magic numbers are not extracted for JAR, APK, and ZIP files since the Sensor cannot differentiate among these three files.

When the Sensor has extracted the magic number, it is able to distinguish between files whose extensions are genuine and those of which have been tampered. If the extension has been tampered with, the Sensor raises a *MALWARE: File Mismatch Detected* alert in the Attack Log. To use this feature, you must confirm that the attack definition, *MALWARE: File Mismatch Detected*, is enabled. It is enabled by default.

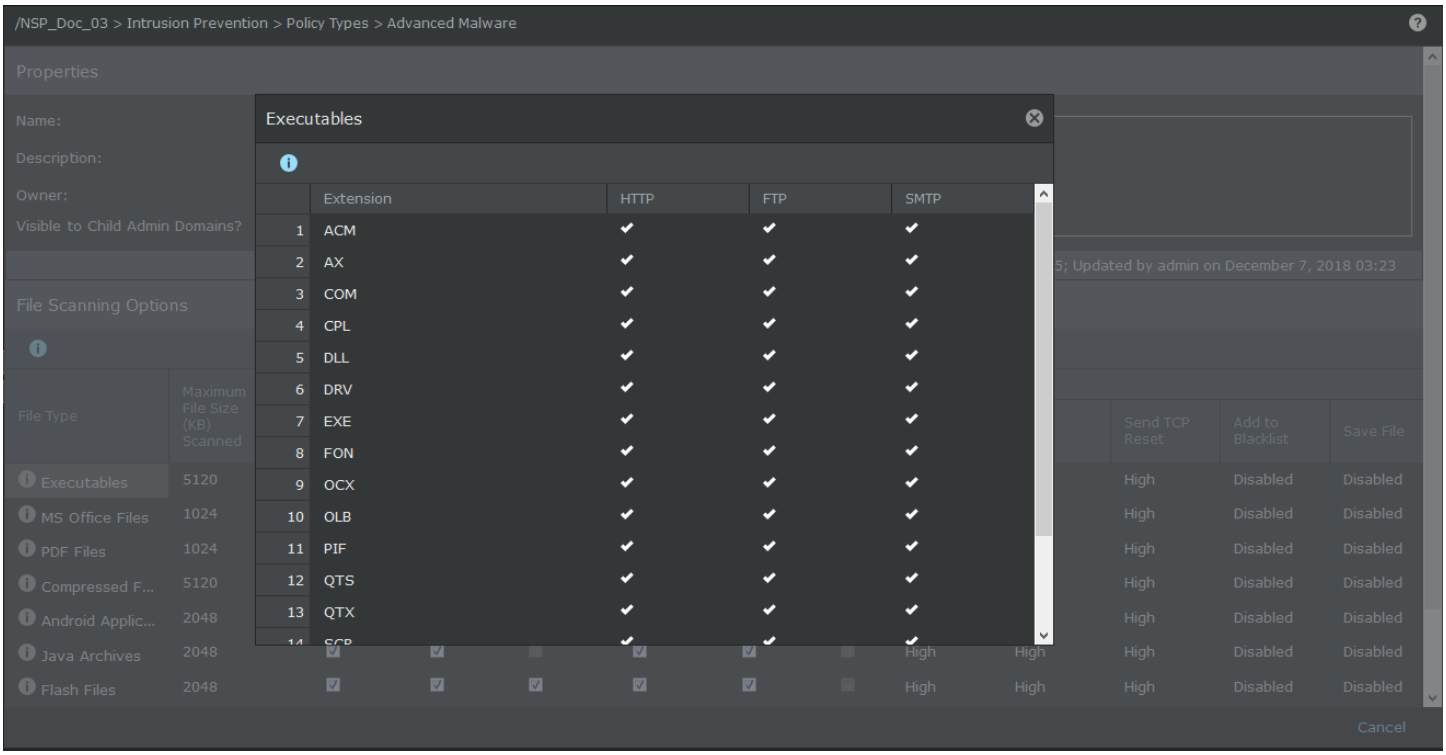
NOTE

This feature is separate from advanced malware policies and requires no additional configuration for a fresh installation. It is available by default.

File types scanned

You can view the file types scanned by clicking on the **info** icon for a given file type under Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **Advanced Malware**.

The following image shows the file types scanned for the **Executables** file type.



Advanced callback detection

Bot is defined as malware running on a compromised system that is designed to participate in a centrally managed network of compromised computers known as a botnet. Single botnets have been known to consist of over a million compromised computers, and are arguably the most significant threats to the global Internet today.

Bot herders are moving away from massive botnets consisting of hundreds of thousands of zombies in favor of smaller and more targeted ones. Also, the IRC protocol for command and control (C&C) is being phased out in favor of more covert protocols, such as HTTP and non-SSL encrypted traffic over port 443.

The bot-like behavior is usually identified in several phases (each identified by a single attack ID), such as exploitation and infection, download of dropper files, download of configuration files, and attack and propagation. Each of the phases is typically carried out in a single network session. In some of the cases, such network sessions might look benign too. Traditionally, an attack signature can detect attack in a single flow except reconnaissance attacks. Trellix IPS supports advanced callback detection by correlating multiple attacks across different flows. Attacks are correlated by observing a host for a given period.

Advanced callback detection provides detailed information retrieved from different attack phases at the end of a successful correlation. Trellix IPS also forwards the attack information to the NTBA Appliance for doing similar correlation.

How the Advanced Callback Detection Framework works

The Advanced Callback Detection framework provides an effective solution to detect and identify bot infected machines in a network. It takes a two-fold approach to detect bots:

- Correlate multiple different attacks being carried out in different network sessions.
- Use a heuristic based approach that detects behaviors of bots.

This approach allows the framework to detect both known and 0-day bots.

0-day botnet detection

The Advanced Callback Detection framework uses a probabilistic 0-day botnet detection approach, targeted toward detection of 0-day bots. It consists of multiple heuristics identified during the research and analysis of various bots. Heuristics cover a wide range of checks such as the following:

- Anomalies in protocols being used for communication such as HTTP and SSL
- Response errors in protocols such as DNS, SMTP
- Suspicious behavior such as port scan and stealth scan
- Cloud based detection such as GTI File Reputation and IP Reputation

The Advanced Callback Detection framework monitors for such heuristics being exhibited by a particular source IP address within a specified amount of time. This allows the framework to determine if the source IP address has been compromised and is exhibiting bot behavior.

The framework has capabilities to correlate attacks across different communication protocols.

The following are some of the currently implemented heuristics:

- **`SSL: Invalid SSL Flow Detected`**

- **SSL: Invalid SSL Flow Detected Due to Wrong Hello Record Type**
- **SSL: Invalid SSL Flow Detected Due to wrong Record Version**
- **SSL: Invalid SSL Flow Detected Due to Wrong Handshake Type**
- **Heuristic DNS: Too Many Type A Query Response Errors Found**
- **Heuristic DNS: Too Many Type MX Query Response Errors Found**
- **DNS: Recursive Query To Root Servers Found**
- **BOT Heuristic: Spam Bot Activity - Multiple Block list Responses from SMTP server**
- **BOT Heuristic: Potential Bot Activity - Multiple Resets from SMTP receiver**
- **Heuristic SMTP: Multiple Emails sent without Authentication**
- **IRC: IRC Client Activity Detected**
- **HTTP: Executable Files Found in Zip Files**
- **HTTP: Password Protected Zip File Found**
- **HTTP: Invalid Flow Detected**
- **Bot: Potential Stealth Scanner Detected**
- **Malware: Potential Malicious File Transfer Detected by GTI File Reputation (Artemis)**
- **BOT: HTran Connection Bouncer Error Message Detected**

0-day botnet detection examples

This section describes the detection of some popular and well known bots like Aurora, Kraken and Pushdo with heuristics support. Specific traits and techniques implemented by these bots are detected.

Heuristics detected on Aurora and Pushdo bot traffic

The following are observed:

- SSL Unix-Timestamp too old or too long into the future (**SSL: Client Hello Invalid Unix Timestamp**)
- Invalid SSL Flow (**SSL: Invalid SSL Flow Detected**)

The framework raises a medium confidence heuristic correlation bot alert, **BOT: Potential Bot Detected - Medium Confidence Heuristics Correlation**.

Heuristics detected on Kraken bot traffic

The following are observed:

- SMTP 5xx errors from servers (**SMTP: Unexpected Server Rejection**)
- E-mails sent without authentication (**BOT Heuristic: Potential Bot Activity - Multiple Resets from SMTP receiver**)

The framework raises a medium confidence heuristic correlation bot alerts, **BOT: Potential Bot Detected - Medium Confidence Heuristics Correlation**.

The Advanced Callback Detection framework which consists of all the above listed heuristics has proved effective in detecting the following categories and traits exhibited by bots.

- Spam bots (bots designed to assist in sending spam emails)
- Domain Flux (bots that implement domain-generation algorithms to generate domains on the fly to stay active and undetected)
- IRC bots (bots that use IRC protocol to carry out malicious activities)
- HTran (bots that use HTran a connection bouncer to redirect TCP traffic destined for one host to an alternate host to hide the primary C&C server)
- Suspicious scan activity (bots that usually scan to look for open ports and services on the system)

Known botnet detection

The Advanced Callback Detection framework also uses a deterministic botnet detection approach, targeted toward detection of known bots. As mentioned earlier, a bot lifecycle can be divided into exploitation, infection and the attack/propagation phases. Each phase has a corresponding attack signature to detect the phase. The framework monitors per source IP address the specified sequence of these attack IDs within a specified time to trigger a correlated attack. This provides a precise bot detection.

Consider the example of Kraken botnet. Kraken bot is known to have the following phases:

1. Connectivity test to[mx.google.com].
2. Download Test: Front pages of popular news websites – [www.nytimes.com], [www.cbsnews.com], [www.cnn.com], and [www.google.com].
3. Peer Lookup: DNS Queries for randomly generated URI based on dynamic DNS domains.
4. Peer Connect & Update: Connect to peer bot (UDP dport 447/TCP dport 80/TCP dport 443) and download update.
5. Download Payload (Spam template, Spam Payload, MX server addresses and so on).
6. Send Spam.

Phases 1 and 2 are not malicious by themselves. However, when correlated with phases, 3,4,5 and 6, Kraken botnet can be detected effectively.

Known botnet detection example

Virut botnet detection

A machine infected with Virut bot can be detected by co-relating the component attacks. The framework raises the alert, **`BOT: Virut Bot Activity Detected`**.

Bot Command and Control server activity detection

Detection of bot Command and Control server (C&C server) activity along with the callback traffic is a key feature of the advanced botnet detection(advanced callback detection). Trellix IPS monitors networks for bot callback activities and protects the network by updating the reputation of the newly identified C&C servers in the Update Server.

The C&C server that communicates with the infected endpoint directs instructions to the malware, which then sends back information and gets instructions in the form of callback traffic. Blocking the callback activity prevents communication between the C&C servers and the malware. The following detection and blocking mechanisms for callback activity are provided by Trellix IPS:

- Multiple signatures are provided in the Default Prevention policy for detecting the callback activity.
- Heuristic detection capabilities that correlate individual bot (callback) behaviors across flows, detecting complex patterns of behavior.

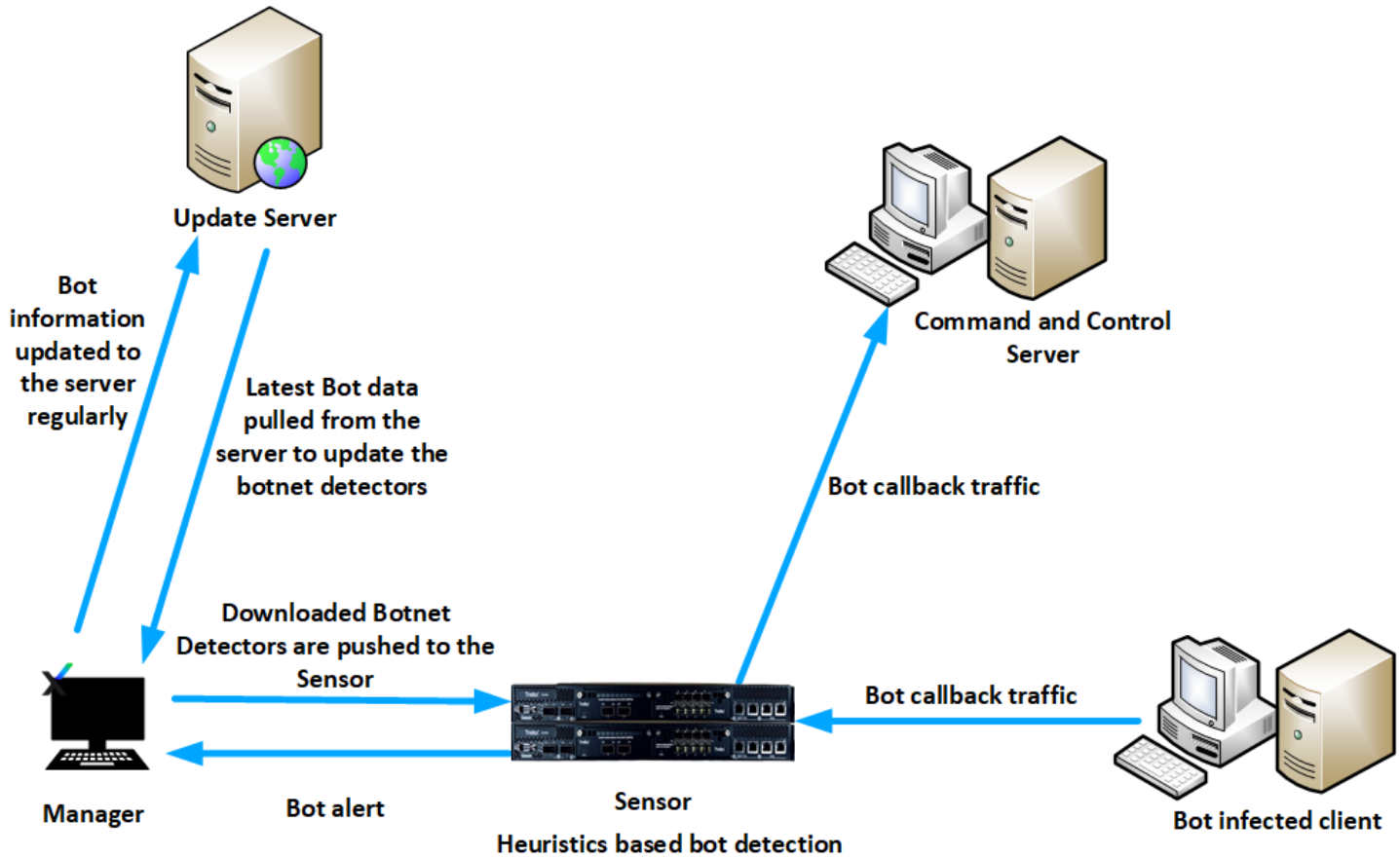
- Trellix provides bot (callback) intelligence that includes a bot Command and Control database consisting of known Command and Control URLs, server domain names, and IP addresses. The Manager pulls this information from the cloud in the form of callback detectors, and downloads to the Sensors a series of indicators of compromise to detect callback activities. The Manager also periodically queries the cloud servers for DAT file updates to the callback detectors.

How callback detectors work?

The callback detectors are generated by Trellix. The callback detectors contain information regarding the IP addresses, domains, and URLs of the malicious bot Command and Control servers. Each of these is categorized based on at least one or more relevant callback IDs (botnet IDs). The callback detectors also contain the relevant ports and protocols that are monitored by Trellix IPS.

For enhanced callback detection (botnet detection), download the latest callback detectors or schedule automatic download and deployment of the callback detectors. The Manager downloads the callback detectors and pushes them to the Sensor. The bot C&C server communicates in the form of callback activities that are detected by the Sensor using the information in the callback detectors. The Sensor inspects all traffic against the malicious IP addresses and port numbers, domains and URLs in the callback detectors and triggers alerts based on them. The Sensor sends an alert to the Manager indicating the callback ID detected along with the Layer 7 information (if Layer 7 data collection is configured). The Manager uses the callback-ID information in the alert to associate the information present in the callback detector. This information can be drilled down and viewed in the **Dashboard** and **Attack Log** of the Manager.

Figure 413. Callback detection



Trellix IPS allows you to analyze bots using the **Top Callback Activity** dashboard. The dashboard allows you to drill down into each piece of detected bot callback activity. The **Callback Activity** page provides you with more details of the detected bot activity.

The Manager provides both automatic and manual import of the callback detectors.

Inspection of DNS response packets for advanced callback detection

Sensors can inspect DNS response packets to detect known and zero-day callback activities.

- For the known botnets, Sensors inspect the DNS response packets for C&C server domains according to the callback detectors.
- For the detection of zero-day callback activities, Sensors perform complex heuristic analyses of DNS response traffic. This way, Sensors can detect the following types of callback activities:
  - IP addresses and domains related to a Fast Flux Service Network (FFSN).
  - Domain names generated by bots infected with Domain Generation Algorithm (DGA).

NOTE

You can edit the attack definitions related to DNS inspection in the required IPS policies. Alternatively, you can edit the attack definitions in **Master Attack Repository** to affect all IPS policies.

Detecting command & control server domains

Callback Detection Exclusions List

You can configure Sensors to perform detailed heuristic analyses of DNS packets for callback activities such as FFSN and DGA. However, such complex analyses consume considerable Sensor resources. Therefore, you can exclude domains, which you know are definitely safe from further analysis.

IMPORTANT

Trellix strongly recommends that you add your organization's public and internal domain names to the **Callback Detection Exclusions List**. Excluding such domains from analysis preserves Sensor resources to analyze unknown domains.

You create the callback detection exclusions list by importing the list of exclusion domains into the Manager. The Sensor checks for these callback detection exclusions first in the DNS packets before checking for the C&C server domains defined in the callback detectors.

NOTE

In case you want to allow traffic to C&C server domains by the callback detectors, you can add them to the **Callback Detection Exclusions List**.

When the Sensor detects an excluded domain name in the DNS traffic, it excludes that DNS traffic from any further DNS-based callback detection. However, the Sensor inspects the subsequent L7 traffic from the same endpoint to the excluded domain for threats.

NOTE

By default, checking the **Callback Detection Exclusions List** is enabled when you enable any feature for advanced callback detection.

Inspection of DNS traffic for C&C server domains

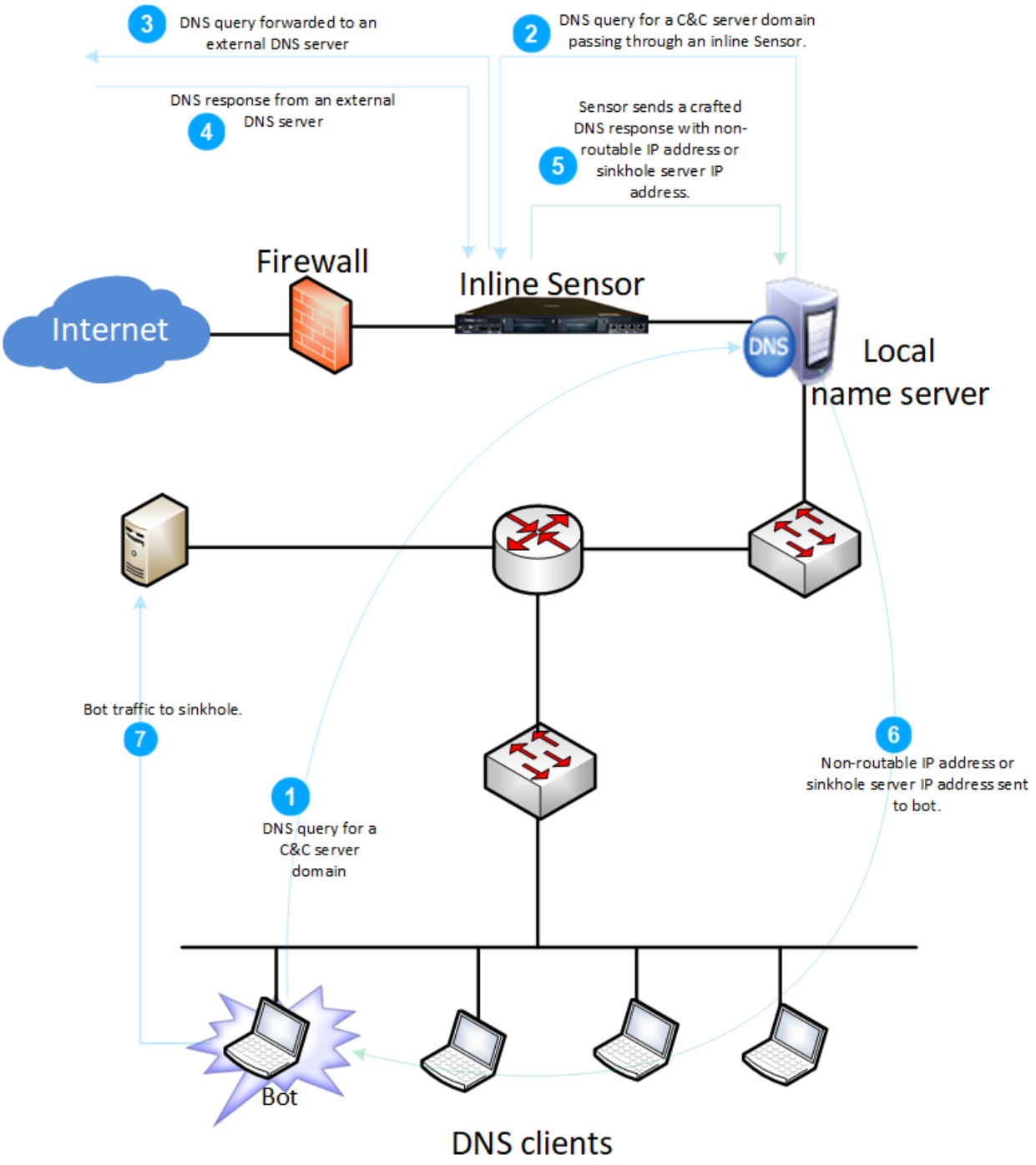
The Sensor blocks the DNS traffic if the DNS response packet contains a C&C server domain according to callback detectors. If a host attempts to reach a C&C server domain, it is most likely infected and is now a bot. So, the Sensor sends a crafted DNS response back to sinkhole this bot traffic. The concept of sinkholing is explained in detail in the subsequent sections of this chapter.

NOTE

Even if the callback detectors file is present in the Sensor, you must configure the Sensor for inspecting DNS responses for C&C server domains.

How the Sensor detects domain name exceptions and C&C server domains?

The high-level flow of how the Sensor detects domain name exceptions and C&C server domains in the DNS traffic is explained in this section.



For the sake of explanation, assume the following:

- Inline Sensor monitoring ports are upstream to the local (recursive) name servers. Therefore, all traffic from the name servers pass through the Sensor.
- You have configured the network of the name server as the inside network. The Sensor inspects DNS response packets for known C&C server domains. So, you must enable the following options on the **Advanced Callback Detection** tab of **Inspection Options** policy.

- **Callback Detectors and Heuristic Callback Discovery** — Enable this option in the outbound direction.
- **DNS Sinkholing** — Enable this option. The Sensor checks the DNS packets for C&C server domains. If the Sensor detects a C&C server domain, it sends a crafted DNS response packet to the corresponding bot.
- **Domain Name Exclusion List Processing** — Enable this option. The Sensor checks the DNS packets for user-defined **Domain Name Exceptions**.

> **NOTE**
>
> Recall that the Sensor inspects the DNS response packet for the C&C server domains. If the Sensor inspects a response packet, you must enable the corresponding feature in the direction of the request packets. In the scenario discussed here, the DNS requests are outbound since the DNS server and clients are defined as inside network. So, for this scenario, you enable the above-mentioned feature for outbound.

- You have downloaded the latest callback detector in the Manager and deployed it on the Sensor as well.

1. In step 4 of the above diagram, the Sensor receives the DNS response packet. The Sensor checks if the source or destination IP address in the DNS response is part of the **CIDRs Excluded from Advanced Callback Detection** list. If true, the Sensor exempts the DNS flow from inspection for callback activities. If not, the Sensor parses the DNS response as follows.
2. The Sensor checks the domain name in the DNS response against the **Callback Detection Exclusions.** If present, the Sensor forwards the packet and does not perform any other DNS-based analysis (for FFSN and DGA). However, the Sensor subjects the subsequent L7 traffic to IPS as applicable.
3. If the domain name is present in the callback detector's C&C server, the Sensor performs the following:
   a. If the DNS response contains A records, the Sensor crafts a DNS response with 127.0.0.1 as the resolved IP address and 720 minutes as the TTL for this record. The Sensor sends this crafted DNS response through the peer monitoring port. When the corresponding host (bot) receives this loopback address as the resolved IP address, it routes the traffic to itself. This way, you can restrict the malicious bot traffic to the infected host. For the next 12 hours, the recursive name server provides this loop back address to any host trying to resolve the corresponding C&C server domain.

      This loopback IP address and TTL are default values. You can configure them in the **Protocol Settings** page for the Sensor (Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **Protocol Settings**). So, if you want to redirect the bot traffic to a specific server, you can provide the IPv4 address in the **Protocol Settings** page with a TTL value of up to 720 minutes. For example, you might want to sinkhole the bot traffic to a Linux server with socat and packet sniffer installed. Redirecting the bot traffic to a separate server enables you to analyze the bot traffic instead of simply sinkholing the traffic.

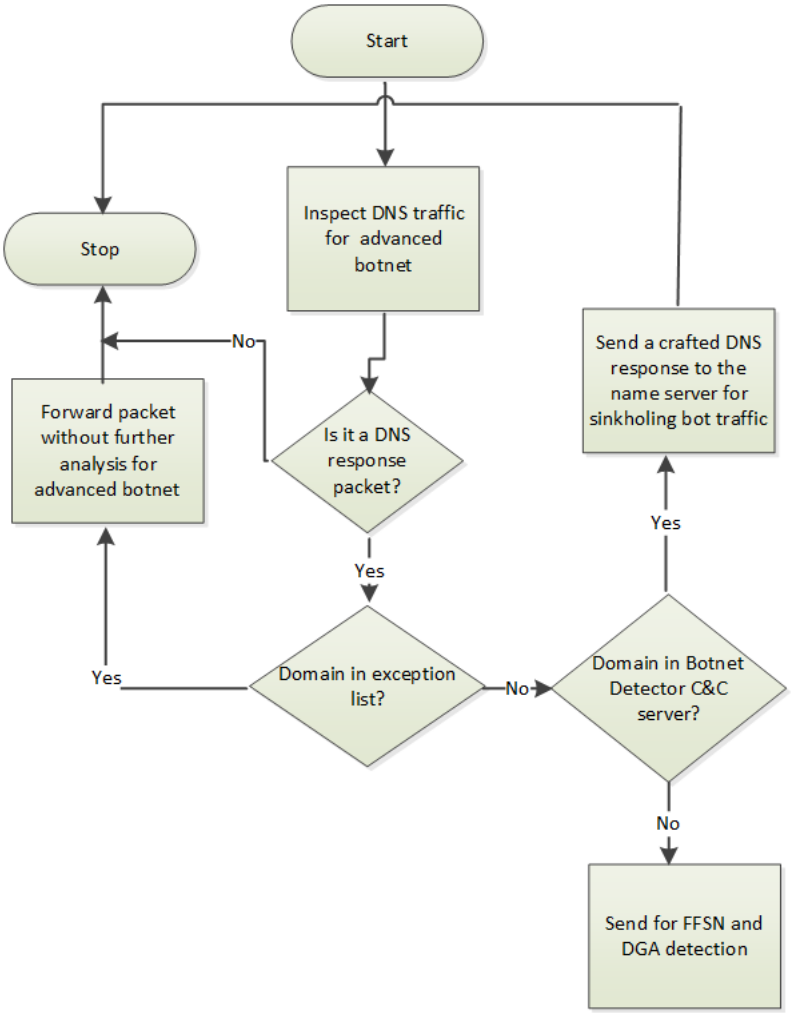
   b. If the DNS response contains AAAA records, the Sensor crafts a DNS response with ::1 as the IP address with the TTL value as configured in the **Protocol Settings** page.

      > **NOTE**
      >
      > For AAAA records, you cannot configure a different sinkhole IP address. Only the default ::1 loop-back IP address is allowed.

   If the Sensor is inline between the DNS clients and the recursive name server, the Sensor sends the crafted DNS response to the bot through the monitoring port. Therefore, depending upon the operating system, the bot might or might not cache the sinkhole IP address according to the TTL in the **Protocol Settings** page.

4. If the domain is not present in the botnet detector's C&C server, the Sensor parses the DNS response for FFSN and DGA detection. If you configure both FFSN and DGA, the Sensor analysis the DNS packets concurrently for both.

Figure 414. DNS-based detection of excluded and C&C server domains



When the Sensor detects a C&C server domain, it raises the *Callback Detectors: High Confidence C&C Server Name Match* alert.

Note the following for interfaces in SPAN and tap modes:

- You must enable **Callback Detectors and Heuristic Callback Discovery** in inbound and outbound direction. That is, you must enable C&C server detection in both the directions.
- The Sensor might not be able to block the DNS traffic related to C&C server domains. As a result, sinkholing of bot traffic might not be possible.
- Even if an interface is in SPAN or tap mode, it can still reduce the load on the FFSN and DGA heuristic engines by identifying the domain name exceptions and C&C server domains.

Configure DNS-based domain name exceptions and C&C server domain detection

Follow these high-level steps to configure the Sensor to detect domain name exceptions and C&C server domains in the DNS response packets.

1. Import the **Domain Name Exceptions** into the Manager. See Manage domain name exceptions (page 996).
2. Make sure that the latest callback detector file is deployed on the required Sensors. See Manage Botnet Detectors (page 1024).
3. Optionally, configure the TTL for the crafted DNS response packet as well as the sinkhole IPv4 address. See Configure TTL and IP address for DNS sinkholing (page 1003).
4. Enable **Domain Name Exceptions** detection, **DNS Sinkholing**, and other advanced callback detection options in the inspection option policies. See Define Advanced Botnet Detection in a Protection Option policy (page 1015).
5. Apply the inspection option policies to the Sensor resources. See Assign a protection option policy to Sensor resources (page 1023).

Domain Name Exceptions

You can launch **Domain Names** page from the Manager by navigating to Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Domain Names**. The **Domain Names** page provides the following options:

- **Callback Detection Exclusions**: Displays domains whose traffic are excluded from callback detection. This list is blank by default. To manage the Callback Detection list of exclusions, refer to Manage domain name exceptions (page 996).
- **IPS Inspection Exclusions**: Displays domains whose traffic is excluded from all IPS inspection

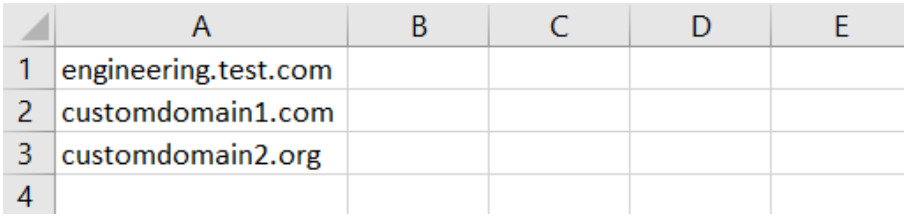
Manage domain name exceptions

Make sure that you have write access to the root admin domain.

You might want to exclude certain domains from DNS-based analysis for callback detection. Include all such domains in the domain name exceptions list in the Manager. You can also use the domain name exceptions list to exclude C&C server domains by the callback detectors.

1. Create a .csv file, which contains all domains to be included in the domain name exception list.

   Figure 415. Sample .csv file

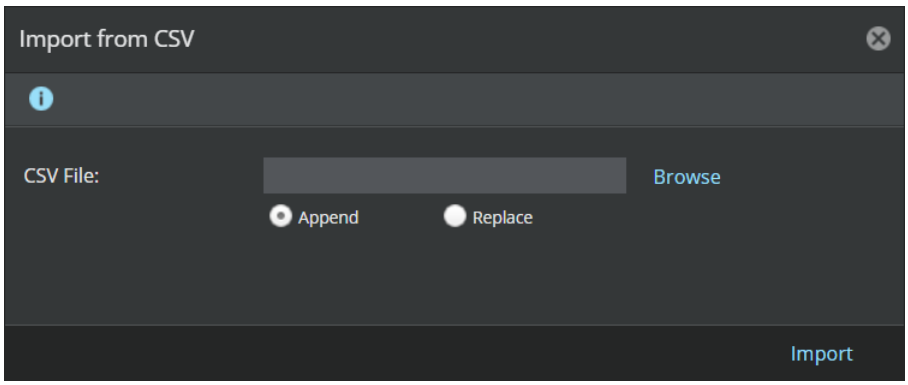
   The domain names, which you include in the domain name exceptions can contain any number of levels. However, for levels above the second level, the domain name in the DNS response must exactly match to be exempted.

   - For example, if the domain name exceptions contain *.org*, all domain names for which the top-level domain is *.org* are exempted.
   - If the domain name exceptions contain ntp.org, all domain names ending with ntp.org are exempted. For example, 1.pool.ntp.org is exempted.
   - If the domain name exceptions contain pool.ntp.org, the domain name in the DNS response must exactly be pool.ntp.org to be exempted. That is, 1.pol.ntp.org is not exempted.

- If the domain name exceptions contain ntp.org and 1.pool.ntp.org, 2.pool.ntp.org is also exempted. If you have ntp.org in the domain name exceptions, you need not include 1.pool.ntp.org in the domain name exceptions.
- As a best practice, make sure that you add all your organization's public and internal domain names to the exceptions list. If *Trellix* is an example, you add **`trellix.com`** to the exception list. Add the last two domain levels for such exceptions. That is, instead of **`www.trellix.com`**, add **`trellix.com`**. This ensures that Sensor resources are not spent on analyzing DNS traffic of known domains.

2. In the Manager, select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Domain Names.**
3. To manage **Callback Detection Exclusions**:
   a. To import the domain names from the .csv file, click Other Actions → **Import** on the **Callback Detection Exclusions** tab.
   b. **Import from CSV** window appears. Browse the .csv file. Use the **Append** option to add a new list of domains or to append a list of domains to an existing list. Use the **Replace** option to remove the existing list of domains and add a new list from the file being imported. Click **Import** in the **Import from CSV** window.

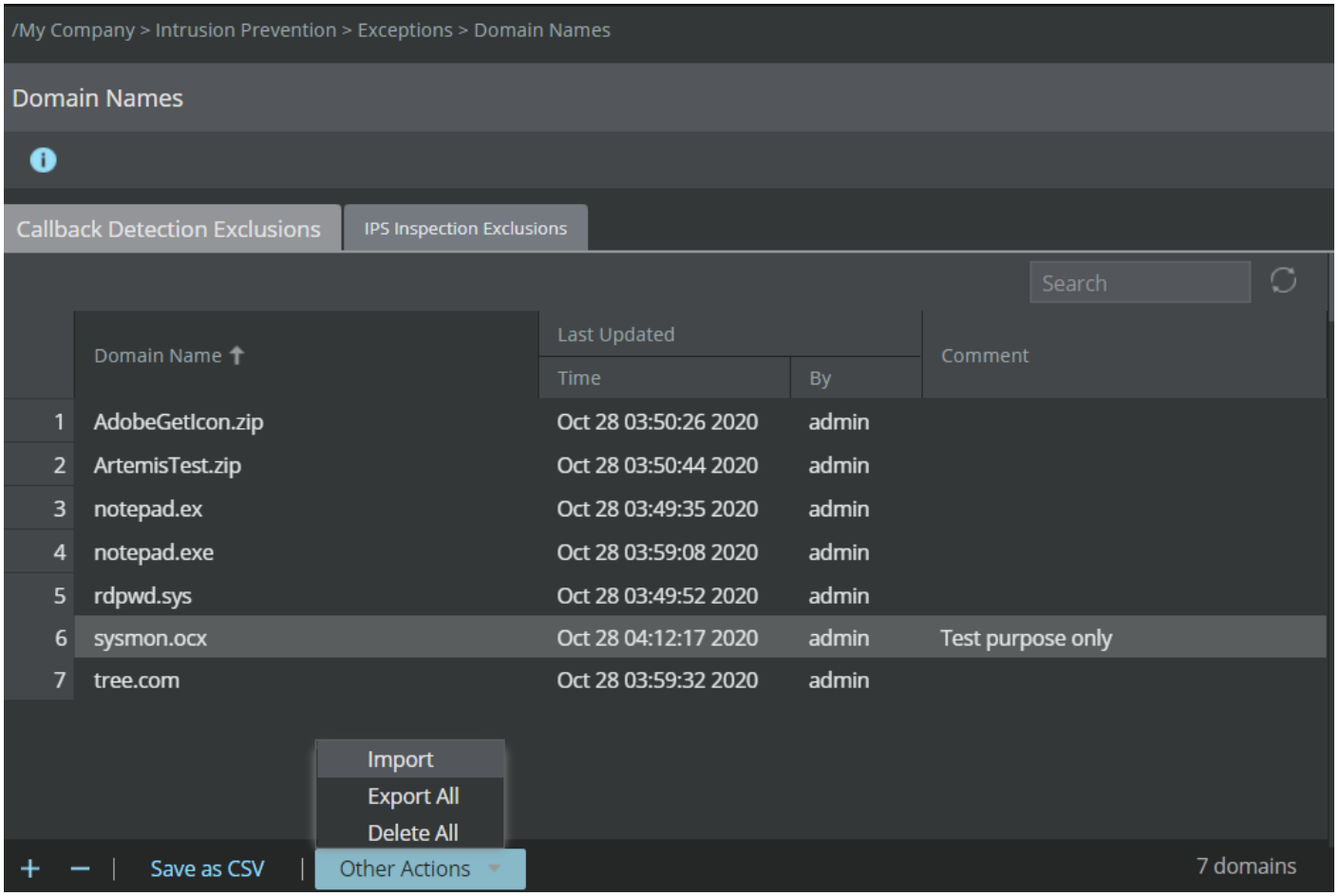
Figure 416. Import Domain Names from a CSV file



The domain names are displayed under the **Callback Detection Exclusions** tab.

- **Domain Name** — Name of the domain imported
- **Last updated** — Automatically populates the **Date** and **Time** when a domain name was imported and the user who imported it
- **Comment** — Enter a comment for the required record names. Double-click the **Comment** column for a record and type in the comment.
- You cannot include the comments in the .csv file when the domain names are imported. You can manually enter them in the **Domain Names** page.

Figure 417. Imported domain names

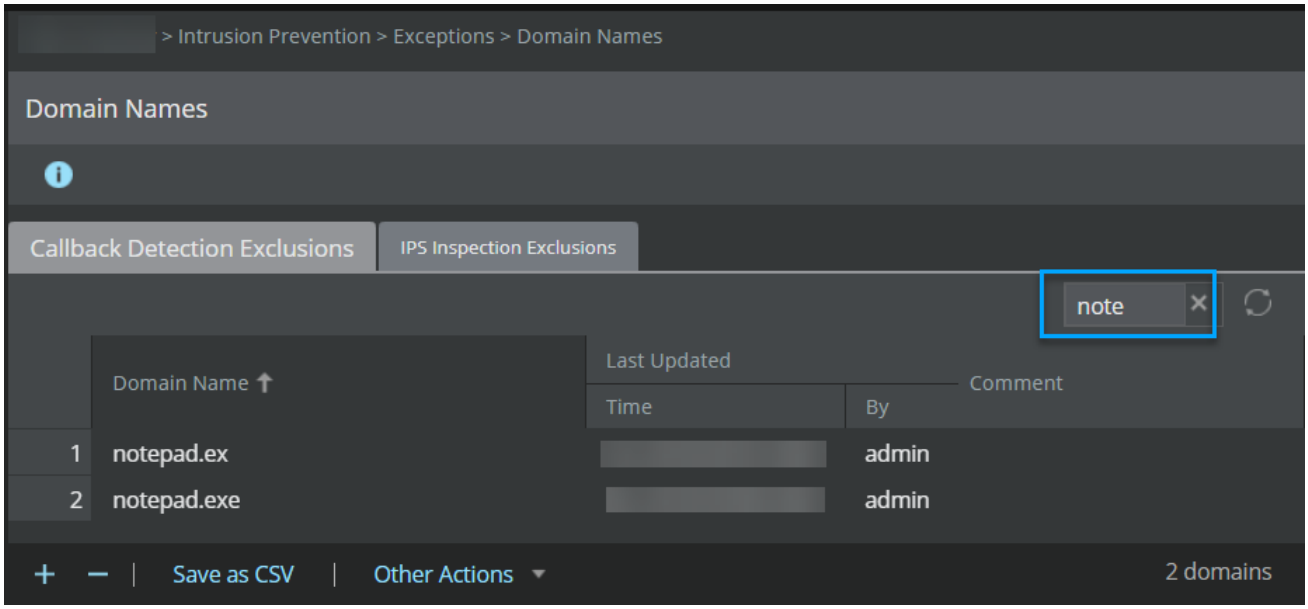


c. To add a single domain to the exclusion list, click +.

d. To locate records in the **Domain Names** page, enter a string in the **Search** box.

   All records containing the entered string in any of the columns are listed.

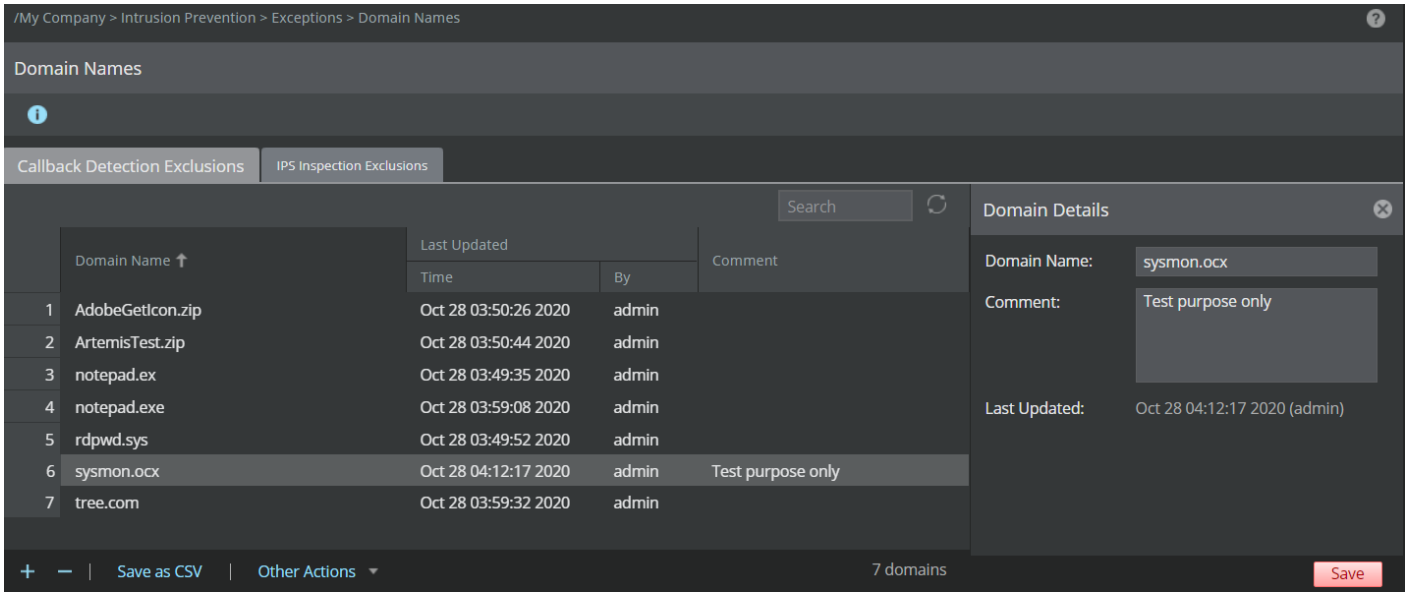
Figure 418. Search records



e. To edit any record, double-click the domain.

You can edit the domain in the **Domain Details** pane. Click **Save**.

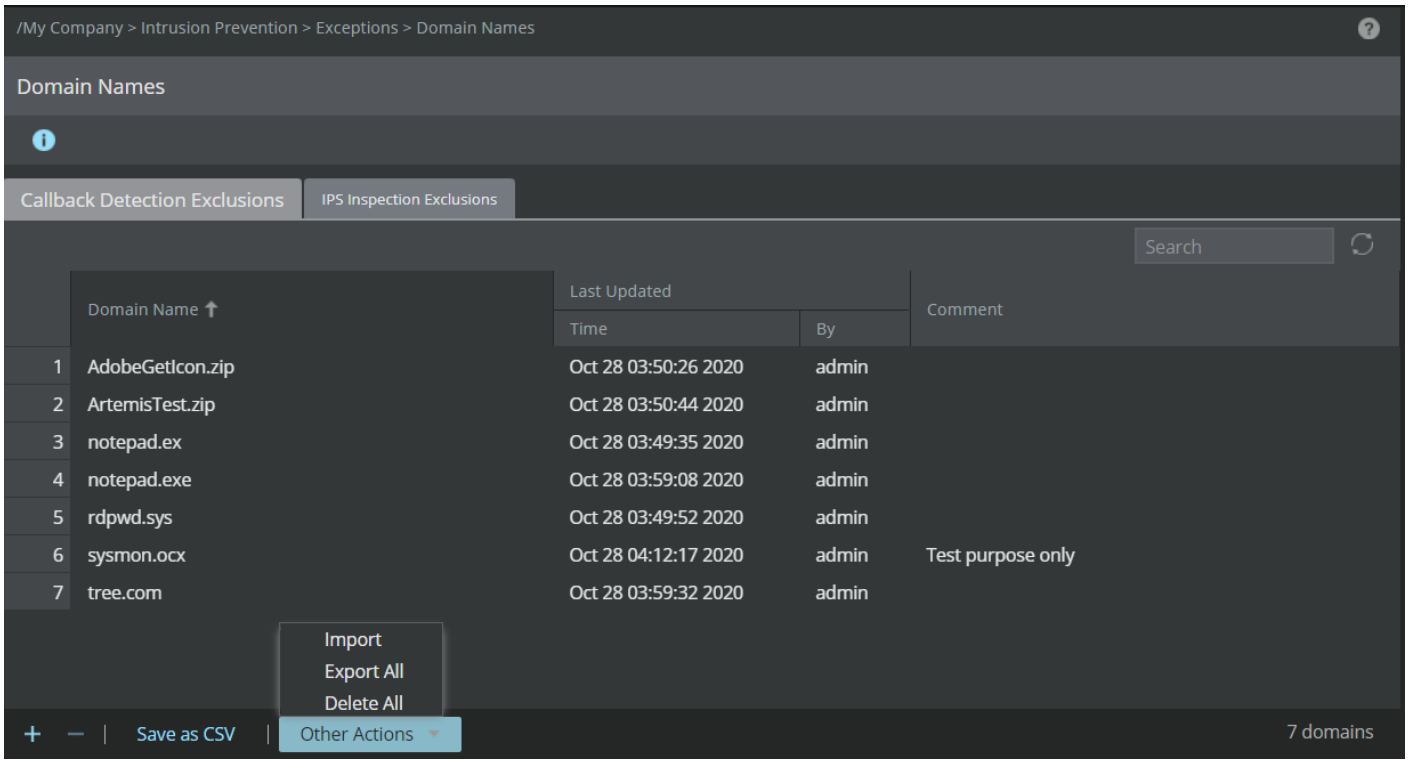
Figure 419. Edit record



f. To delete records, select the domain name(s) and click −.

To delete all the records, click Other Actions → **Delete All**.

Figure 420. Delete records



g. To export the current list of domain name exceptions to a .csv file, click Other Actions → **Export All** and save the file.

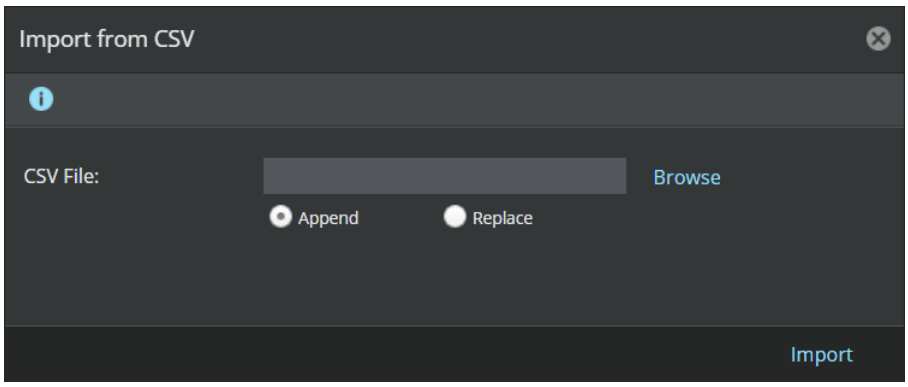
You can also save all the existing domains. Click **Save as CSV** to save the existing list.

4. To manage **IPS Inspection Exclusions**:

a. To import the domain names from the .csv file, click Other Actions → **Import Custom** on the **IPS Inspection Exclusions** tab.

b. **Import from CSV** window appears. Browse the .csv file. Use the **Append** option to add a new list of custom domains or to append a list of custom domains to an existing list. Use the **Replace** option to remove the existing list of custom domains and add a new list from the file being imported. Click **Import** in the **Import from CSV** window.

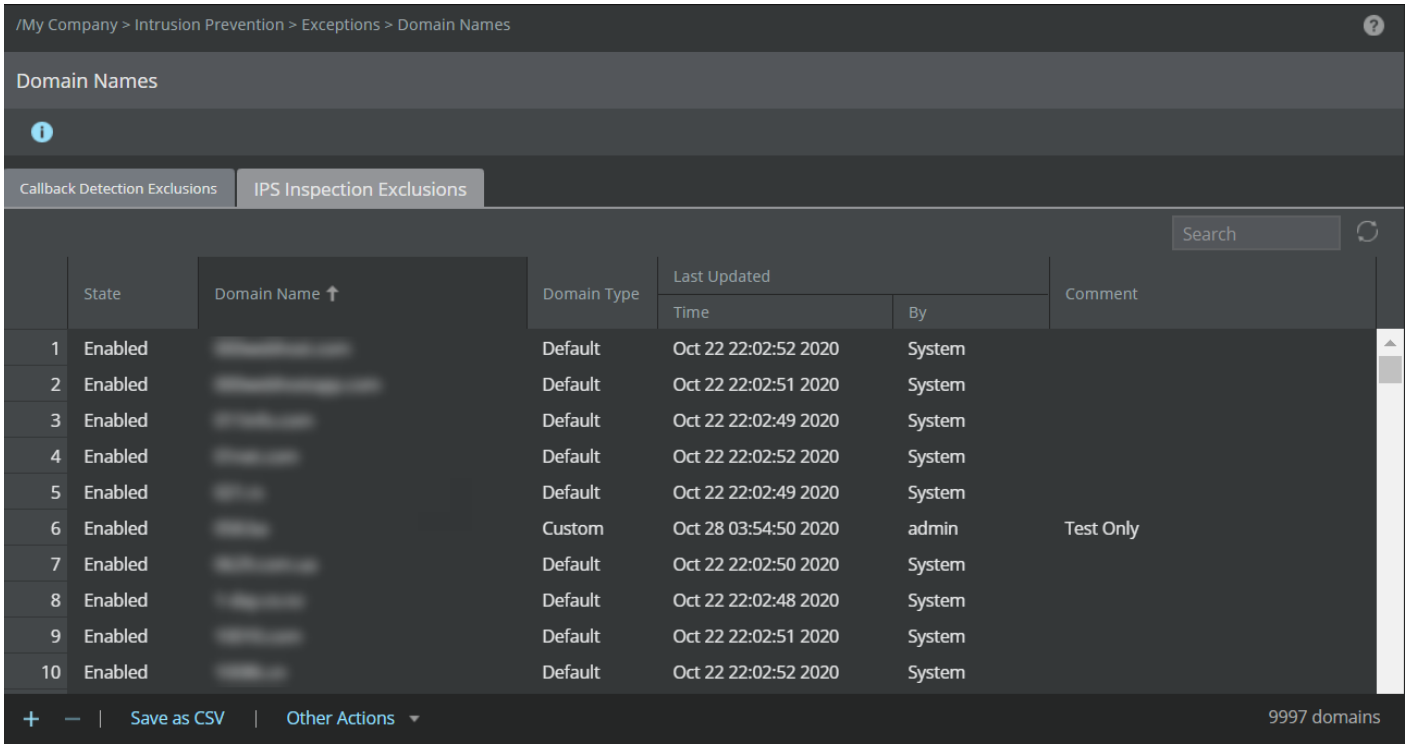
Figure 421. Import Domain Names from a CSV file



The domain names are displayed under the **IPS Inspection Exclusions** tab.

- **State** — Current state of the domain - **Enabled**/**Disabled**
- **Domain Name** — Name of the domain imported
- **Domain Type** — The type of domain - **Default**/**Custom**
- **Last updated** — Automatically populates the **Date** and **Time** when a domain name was imported and the user who imported it
- **Comment** — Enter a comment for the required record names. Double-click the **Comment** column for a record and type in the comment. The comment is automatically saved when you click outside the column.
- You cannot include the comments in the .csv file to be included when the domain names are imported. You can only manually enter them in the **Domain Names** page.

Figure 422. Imported domain names

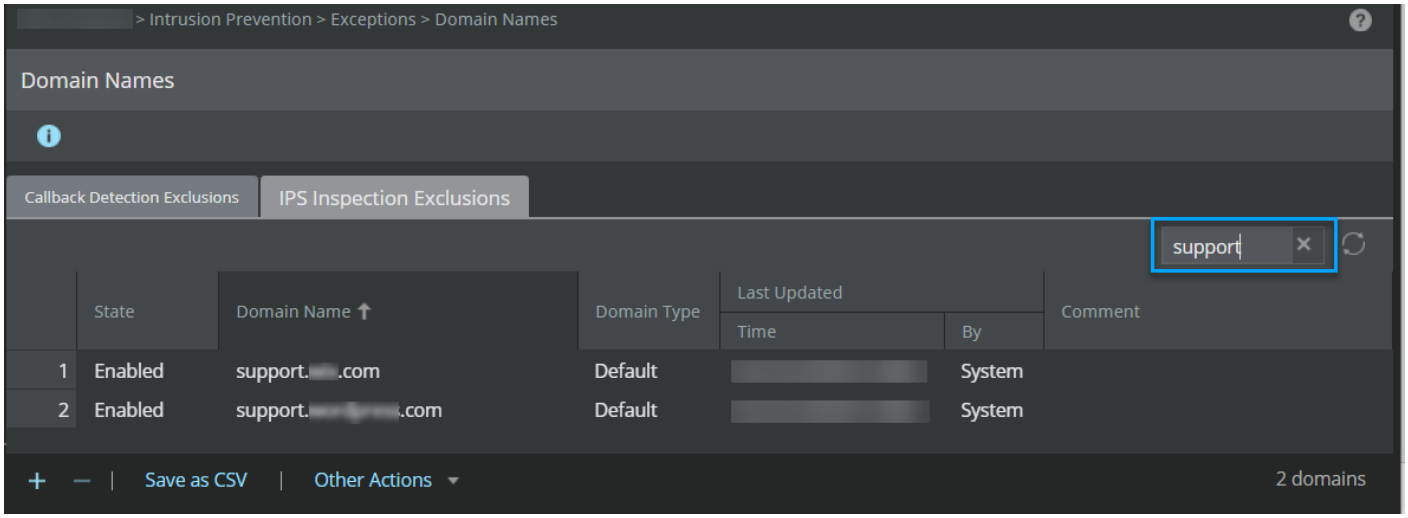


c. To add a single domain to the exclusion list, click +

d. To locate records in the **Domain Names** page, enter a string in the **Search** box.

All records containing the entered string in any of the columns are listed.

Figure 423. Search records



e. To edit any record, double click the domain.

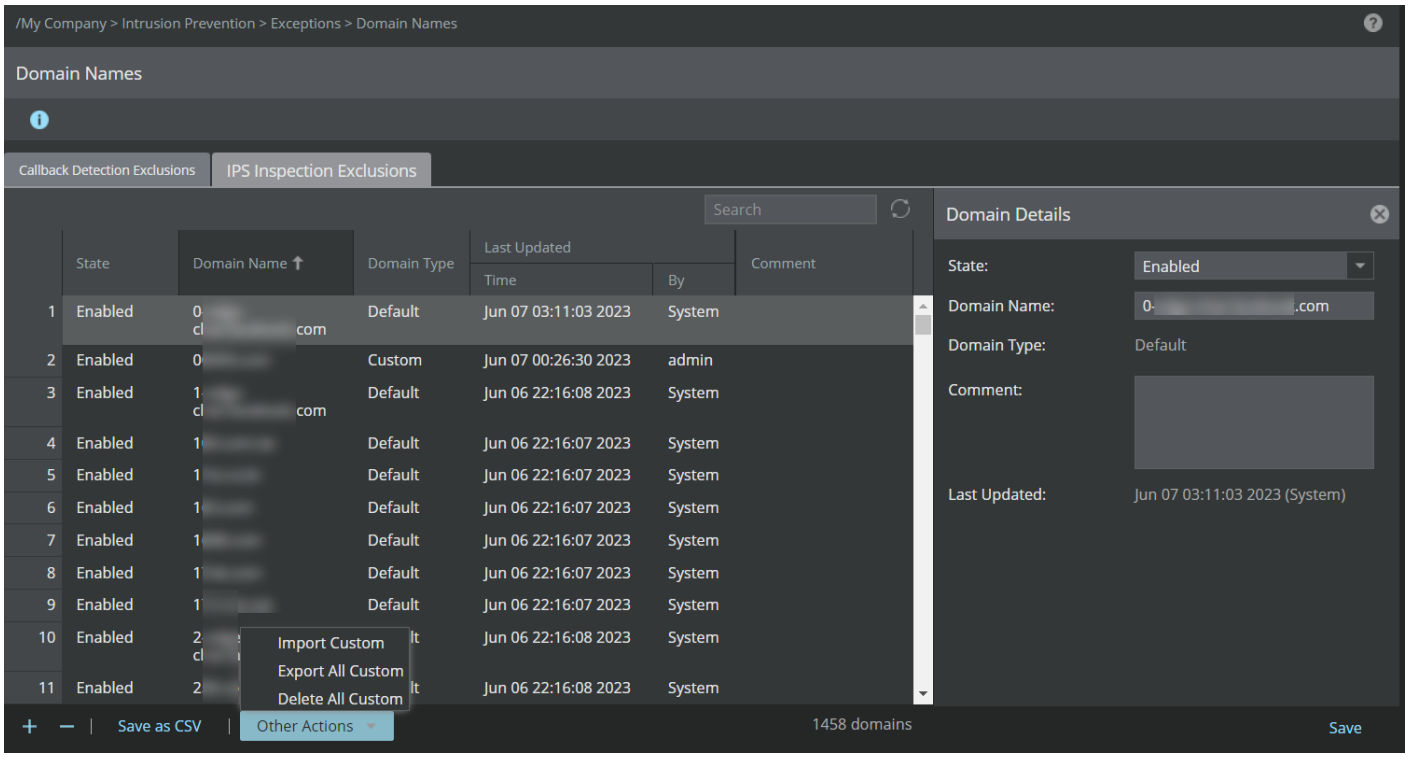
You can edit the domain in the **Domain Details** pane.

> **NOTE**
>
> You cannot edit the **`Domain Name`** for a default domain. You can either enable or disable a default domain name by selecting the domain and selecting the **Enabled** or **Disabled** option in the **State** drop-down list in **Domain Details** pane.

f. To delete records, select the domain name and click −.

To delete all custom records, click Other Actions → **Delete All Custom**.

Figure 424. Delete records



g. To export the current list of custom domain name exceptions to a .csv file, click Other Actions → **Export All Custom** and save the file.

You can also save all the existing domains. Click **Save as CSV** to save the existing list.

NOTE

When the datapath processors on the Sensor are experiencing a high number of queued packets to be processed, the traffic from domains in the whitelist is skipped for inspection.

Configure TTL and IP address for DNS sinkholing

When a Sensor detects a C&C server domain in a DNS response packet, the Sensor crafts a DNS response. You can configure the TTL for this crafted DNS response. The TTL value applies for both A and quad-A records. For A records, you can also configure the sinkhole IPv4 address.

1. In the Manager, select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **Protocol Settings.**
2. In the **Protocol Settings** page, scroll down to the **DNS** section.
3. For **DNS Sinkholing Time-To-Live (TTL)** field, enter the TTL you want to include in the crafted DNS response packets sent by the Sensor.

   The default and the maximum values are 720 minutes.
4. Click **Update** to save the changes in the Manager database.

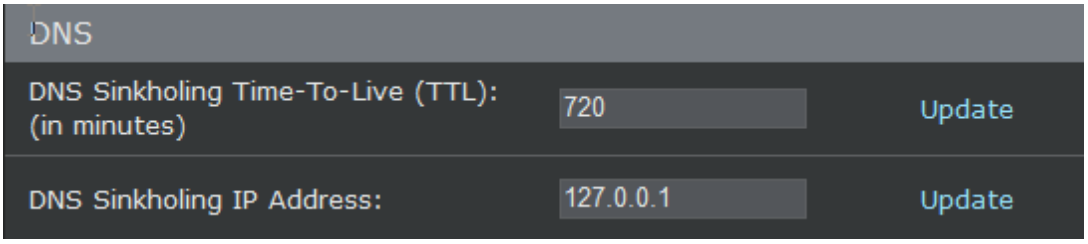
5. The **DNS Sinkholing IP Address** field indicates the IP address to which the bot traffic is sinkholed.

   The default value is the loop back IP address (127.0.0.1 for A records and ::1 for quad-A records present in the actual DNS response). You can configure an IPv4 address for the bot to send the bot traffic to that server. You cannot configure an IPv6 address as a sinkhole server IP address.

6. Click **Update** to save the changes in the Manager database.

> **NOTE**
>
> The Manager sends any changes in the **Protocol Settings** page immediately to the Sensor through SNMP without the need for a manual configuration update.

Figure 425. DNS settings



7. To restore all the fields in the **Protocol Settings** page to their default values and deploy the changes to the Sensor, click **Restore**.

> **IMPORTANT**
>
> **Restore** applies to all the fields in **Protocol Settings** page and not just the **DNS** section.

Fast Flux Service Network detection

As part of advanced callback protection, Sensors can protect your network from attacks effected through a Fast Flux Service Network (FFSN). Typically, an FFSN is used for DDoS, spam, phishing, advanced malware attacks. Sensors use a heuristics-based detection mechanism to identify domains and IP addresses related to FFSN. Once Sensors identify the FFSN domains, they can detect the bots in your network, when they communicate with those FFSN domains.

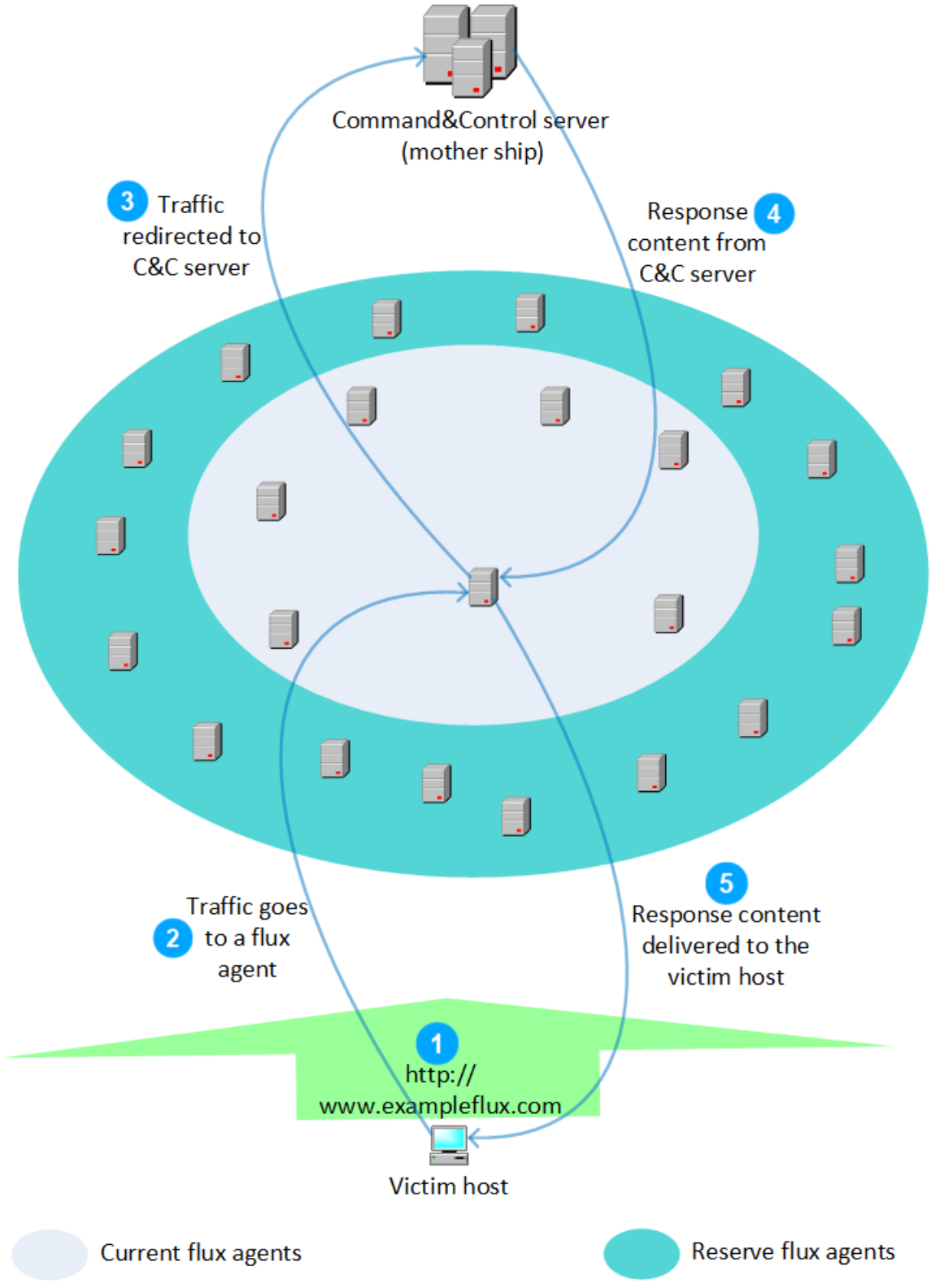
> **NOTE**
>
> Because it is a heuristics-based detection mechanism, FFSN detection is equally effective in SPAN, tap, and inline modes.

What is a Fast Flux Service Network?

Generally, a Fast Flux Service Network consists of hundreds of compromised hosts commanded and controlled by a server (C&C server). The C&C server acts as the *mother ship* for the network. The compromised hosts are referred to as *flux agents*. These flux agents are hosts with public IP addresses, such as home computers. When a host in your network is infected, it attempts to access the malicious content on the C&C server. For this purpose, the FFSN has a registered domain name.

The main objective of an FFSN is to ensure high-availability of the malicious content on the C&C server as well as to prevent the C&C server from being identified and subsequently blocked. To achieve this goal, attackers exploit the way DNS functions. The FFSN strategy has dual approaches to it.

Figure 426. An FFSN network



- Firstly, the DNS records for the FFSN domain are configured such that it resolves to the IP addresses of the flux agents. That is, the flux agents act as the front end for the FFSN domain. So, a flux agent acts as a reverse proxy between the victim host and the C&C server. This prevents the C&C server from being exposed to security applications and law-enforcement agencies.
- Secondly, attackers make sure that the IP addresses resolving to the FFSN domain continually change. That is, the IP addresses associated with the domain are in a flux. This is achieved by configuring a very low time to live (TTL) for the DNS A records. At one point in time, only a batch of the flux agents are advertised. Attackers keep rotating the pool of flux agents that are currently in use.

  This technique of keeping the IP addresses in a flux, ensures high availability of the FFSN domain. Even if some of the flux agents are not available (probably powered off by the legitimate owners) or if the domain IP addresses are blocked by a security application, the domain is still available.

Typical characteristics of an FFSN

- The number of A records is high.
- The TTL of FFSN IP addresses is very low.
- With each DNS query, the FFSN domain is likely to resolve to newer IP addresses. Therefore, the DNS results reaching your local name server is different from the previous.
- The flux agents belong to different networks and usually are from different geographical locations.
- The IP addresses in the A records do not belong to the same Autonomous System Number (ASN).
- The traffic between an victim host and the C&C server is typically HTTP. As this traffic is redirected through a flux agent, there is a relative delay observable at the victim host for this HTTP traffic.
- The C&C server rotates the flux agents based on round-robin to distribute the load and for high-availability. There could also be factors such as availability of the flux agents.
- Analyzing a flux agent usually does not provide much information on the served malicious content or the C&C server.

Differentiating benign DNS traffic and FFSN traffic

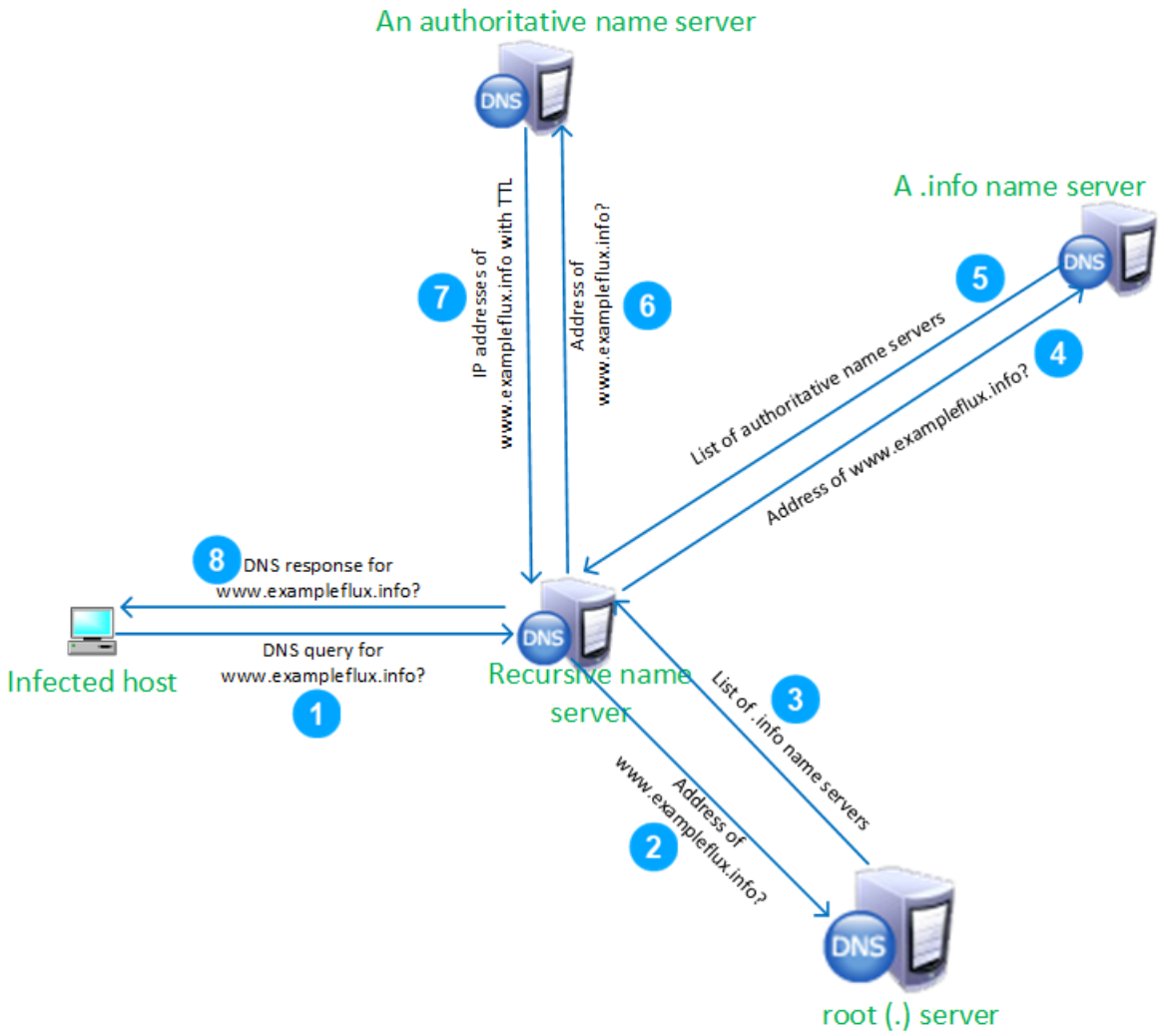
There are some similarities between how an FFSN functions and certain cases of normal DNS traffic.

- For example, to load-balance Web service requests, name servers resolve domains to servers based on round-robin.
- In the case of Content Delivery Networks (CDNs), the domain resolves to servers based on their availability and proximity to the client. So, the domain might resolve to IP addresses belonging to different networks and geographical locations.
- For the purpose of load-balancing, such benign DNS results also have a low TTL.

Though FFSNs can exhibit similar behavior as some benign DNS traffic, the Sensor is capable of differentiating these traffic from FFSN traffic.

DNS traffic flow

Because FFSN is based on DNS, the Sensor inspects the DNS response traffic to detect FFSN domains and flux agents. To understand how the Sensor detects FFSNs, review how DNS traffic flows when an victim host attempts to access an FFSN domain.



1. Consider a victim host in your network attempts to access an FFSN domain, for example `www.exampleflux.info`. The host sends the DNS request to the recursive (local) name server.
2. Assume that name resolution details are not available in the recursive name server's cache. So, it sends a request to the root name server.
3. The root name server responds with the list of name servers for the .info top-level domain (TLD).
4. The recursive name server queries a .info name server for `www.exampleflux.info`.
5. The .info name server provides the list of authoritative name servers for `www.exampleflux.info`.
6. The recursive name server queries one of the authoritative name servers for `www.exampleflux.info`.
7. The authoritative name server responds with the IP addresses of the current flux agents.
8. The recursive name server passes on this list of flux agents to the victim host.

How Trellix IPS detects FFSN?

At a high-level, Trellix IPS detects FFSN as described in this section.

For the sake of explanation, assume the following:

- Sensor monitoring ports are inline between the protected hosts (DNS clients) and the local (recursive) name server. Therefore, all DNS requests and responses pass through the Sensor.
- You have configured the DNS clients as the inside network. That is, the name server is in the outside network. The Sensor inspects DNS response packets for FFSN. So, you must enable **Fast Flux Detection** in the outbound direction. Enabling **Fast Flux Detection** in the outbound enables the Sensor to track the DNS response with the corresponding request.

1. The Sensor filters out the DNS traffic, which need not be inspected for FFSN. The DNS traffic is exempted from FFSN inspection, if any of the following conditions are met. The Sensor checks the DNS response packets in the following sequence.
    a. The source or destination IP address in the DNS response packet belongs to **CIDRs Excluded from Advanced Callback Detection** list.
    b. The domain is exempted according to the user-defined domain name exceptions. Assume that you have imported the domain name exceptions in the Manager and enabled **Domain Name Exclusion List Processing** in the inspection option policy.
    c. The domain is blocked according to the callback detectors. Assume that you enabled **Callback Detectors and Heuristic Callback Discovery** in the inspection option policy. Then, the Sensor sends a crafted DNS response packet to sinkhole the corresponding callback traffic.

       If you disabled **Callback Detectors and Heurisitc Callback Discovery**, the Sensor inspects the DNS traffic for FFSN even for C&C server domains.
    d. The domain is already analyzed for FFSN and found to be benign.

    NOTE

    If a requested domain name resolves to an IP address of a reserved CIDR, such as the private network CIDRs in RFC 1918, the Sensor does not consider that IP address for FFSN suspect processing.

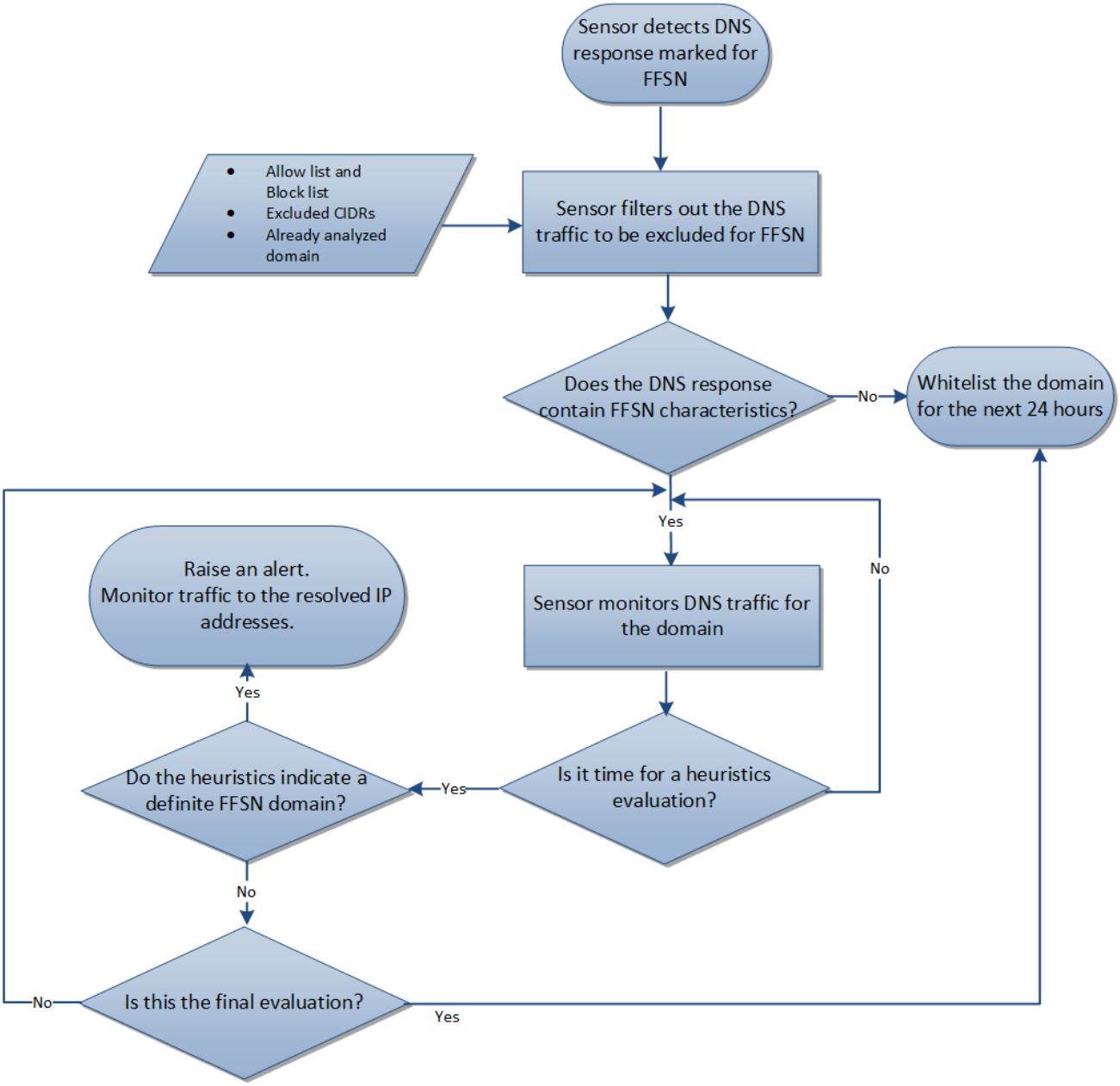
2. The Sensor identifies the domains to be monitored for FFSN. For each domain, it checks the DNS response packets for any FFSN characteristics.

   If the Sensor finds any FFSN characteristics in the DNS responses, it considers the domain for heuristics-based inspection for FFSN.

   - The Sensor might take anywhere between 10 seconds to 12 hours to complete this heuristic analysis for a suspected domain.
   - If the heuristics parameters indicate that the domain belongs to an FFSN, the Sensor raises the *Botnet: Heuristic Detection of Fast Flux DNS* alert. Because *Botnet: Heuristic Detection of Fast Flux DNS* is a component attack, quarantining the host is not applicable.

     The Sensor adds all IP addresses which resolved for this domain in its watch list for the next 12 hours. When any hosts communicate with any of these IP addresses, the Sensor raises the *Botnet: Connection to Fast Flux Agent Detected* alert. This alert enables you to identify other victim hosts in your network.
   - Sensor does not consider DNS responses for FFSN, if they contain IPv6 addresses.

Figure 427. FFSN detection flow



When the Sensor detects an FFSN domain, it includes the following information in the alert:

- The IP addresses in the A records
- Reverse DNS result for the IP addresses
- Monitor interval
- Number of IP addresses in the A records
- Geo-diversity of the IP addresses
- IP address of the last victim host to query for the FFSN domain

NOTE

For interfaces in SPAN and tap mode, you must enable FFSN detection in both inbound and outbound direction.

Domain Generation Algorithm detection

As part of advanced callback detection, Sensors can protect your network from attacks effected through Domain Generation Algorithm technique. DGA is triggered for an infected host (bot) to communicate with the command and control (C&C) server. Some infamous malware which are known to use the DGA technique are Conficker, Pushdo, and Gameover ZeuS.

Sensors use a heuristics-based detection mechanism to identify the following:

- Bots employing DGA technique
- The IP address of the C&C server of the DGA botnet
- Hosts attempting to communicate with the C&C server domain

Because it is a heuristics-based detection mechanism, DGA detection is equally effective in SPAN, tap, and inline modes.

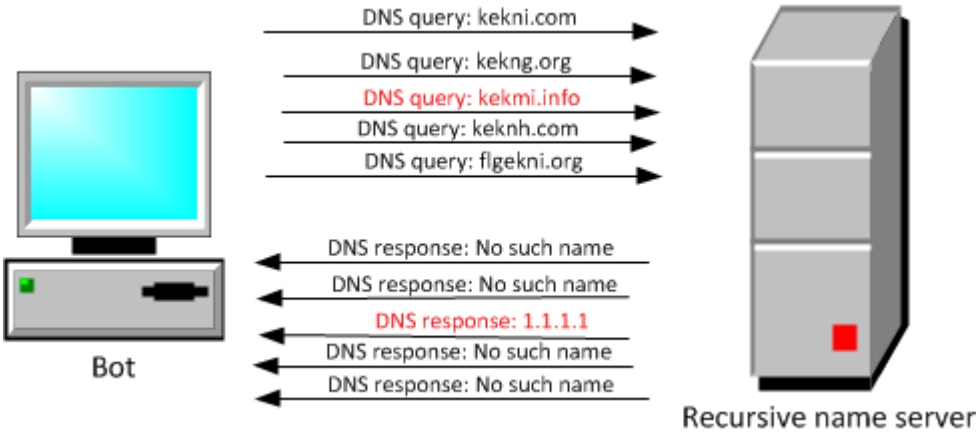
How DGA-based botnet works?

For a botnet to be active, the bots must be able to communicate with the C&C server. For example, bots transfer the results of previous operations as well as seek further instructions. As a counter-measure, security applications find ways to break this communication channel between the bots and the C&C server. One of the ways of breaking a botnet is to identify the IP addresses and domains of C&C servers based on signatures to block them, or use a central reputation system to identify known C&C server domains and IP addresses. So, for a botnet, it is critical that the C&C server details are concealed so that they are highly available for the bots and avoid any legal action.

Some hackers use DGA to keep the C&C infrastructure concealed but available to the bots. DGA uses a seed, such as date or time, and generates random C&C server domain names. The bot contacts the local name server to resolve these domain names. DGA generates a high number of such domain names over a short period.

The attacker registers one of the random domain names generated by the DGA. So, the bot is now able to access the C&C server. Attackers register DGA domains for short periods. This just-in-time registration makes it difficult for security applications and reputation systems to block the domain.

Figure 428. DGA traffic from a bot



Malware might use DGA as the primary or secondary method to contact the C&C domain. For example, some malware such as Conficker use DGA as the mechanism to contact its C&C domain. Some Zeus variants employ DGA as a secondary mechanism. That is, the DGA code is triggered only when a bot is unable to reach the hardcoded C&C domains.

How Trellix IPS protects against DGA botnet?

A Sensor has a specialized heuristic engine to detect DGA-generated domains. Sensors perform the following tasks as part of DGA detection:

1. Sensors identify the bots as they attempt to resolve C&C domains.
2. When a bot successfully resolves a DGA-generated domain, Sensors attempt to identify and expose the C&C infrastructure of that DGA-based botnet.
3. Post-detection of the C&C infrastructure, Sensors look for any subsequent communication between the C&C server and hosts on your network. This identifies the other bots on your network.

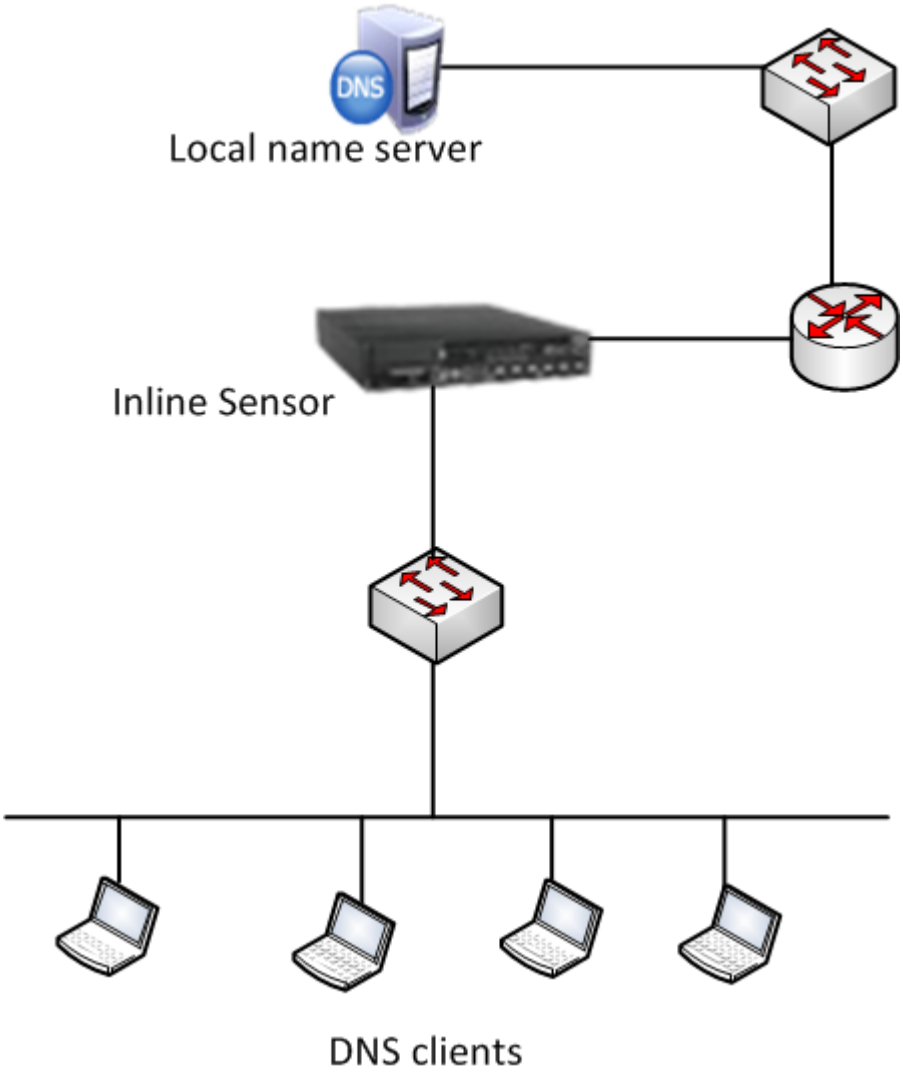
NOTE

For interfaces in SPAN and tap mode, you must enable DGA detection in both inbound and outbound direction.

At a high-level, Trellix IPS detects DGA-related information as described in this section.

For the sake of explanation, assume the following:

Figure 429. Sensor between DNS clients and the name server



- Sensor monitoring ports are inline between the protected hosts (DNS clients) and the local (recursive) name server. Therefore, all DNS requests and responses pass through the Sensor.
- You have configured the DNS clients as the inside network. That is, the name server is in the outside network. The Sensor inspects DNS response packets for DGA. So, you must enable **Domain Generation Algorithm Detection** for outbound in the inspection option policy. This enables the Sensor to track the DNS response with the corresponding request.

NOTE

For DGA, a Sensor does not inspect AAAA records.

1. The Sensor first detects an infected host.
    a. The Sensor starts its DGA heuristic analysis, if it suspects DGA involvement in the monitored DNS traffic.

b. The Sensor filters out DNS packets, which need not be inspected for DGA. The Sensor excludes the suspicious DNS traffic from DGA analysis, if any of the following conditions are met. The Sensor checks the DNS response packets in the following sequence.

   i. The source or destination IP address in the DNS response packet belongs to **CIDRs Excluded from Advanced Callback Detection** list.

   ii. The domain is exempted according to the user-defined domain name exceptions. Assume that you have imported the domain name exceptions in the Manager and enabled **Domain Name Exclusion List Processing** in the inspection option policy.

   iii. The domain is blocked according to the callback detectors. Assume that you enabled **Callback Detectors and Heuristic Callback Discovery** in the inspection option policy. Then, the Sensor sends a crafted DNS response packet to sinkhole the corresponding callback traffic.

   If you disabled **Callback Detectors and Heuristic Callback Discovery**, the Sensor inspects the DNS traffic for DGA even for C&C server domains.

> **NOTE**
>
> If a requested domain name resolves to an IP address of a reserved CIDR, such as the private network CIDRs in RFC 1918, the Sensor does not consider that IP address for DGA C&C suspect processing.

c. The Sensor mines the information in the DNS packets and runs them through its heuristic engine. If the heuristic analysis indicates that the domains are DGA-generated, the Sensor does the following.

   - The Sensor raises the *Botnet: DGA Heuristic Detection of Botnet Zombie* alert.

     The possible Sensor actions for this alert are to quarantine and remediate the victim host and send an alert to the Manager. Capturing the packets is not applicable.

   - For a specific time period, the Sensor tracks the subsequent DNS traffic to and from the bot to detect the C&C domain.

> **NOTE**
>
> If the same host is infected by different malware family using a different DGA, the Sensor raises an alert separately for each unique DGA.

2. After detecting a bot, the Sensor attempts to identify the C&C domain and the corresponding IP addresses.

   a. The Sensor monitors the DNS traffic for all bots detected for a specific time period to discover the current C&C domain name.

   b. Some DGA deliberately query for legitimate domain names to mislead security products. Also, the user logged on to the bot might query for a legitimate domain name. So, the Sensor performs a detailed analysis to accurately identify the C&C domain.

   c. When the C&C domain is detected, the Sensor raises the *Botnet: DGA Heuristic Detection of C&C Server in DNS Response* alert.

3. If any of the monitored hosts in your network attempt to communicate with the C&C IP addresses, the Sensor raises the *Botnet: DGA Heuristic Detection of Connection to C&C Server* alert. This alert enables you to identify all hosts in your network, which are part of the botnet.

Define callback activity detection in an inspection option policy

You configure callback activity options in an inspection option policy. You create inspection option policies at the domain level. Then, you can apply the inspection option policy to the required Sensor interfaces owned by that domain.

You can define the following callback activity features in an inspection option policy:

- Define the CIDRs to be excluded from inspection for callback activity.
- DNS-based detection of exempted domains according to domain name exceptions.
- DNS-based detection of C&C server domains according to callback detectors.
- DNS-based detection for FFSN and DGA.
- HTTP-based detection of command and control servers according to callback detectors and multiple heuristic analysis for zero-day botnets.

When the Sensor begins its inspection for callback activity, it first verifies if the traffic is to be excluded from inspection for callback activity:

1. Regardless of the protocol, the Sensor checks if the source or destination of the traffic belongs to an excluded CIDR. If yes, the Sensor excludes that flow from inspection for callback activity.
2. If the protocol is DNS, the Sensor checks for domain name exceptions first and then C&C server domains.
3. If the protocol is DNS and the domain is not for a known C&C server, the Sensor inspects for FFSN and DGA.
4. If the protocol is HTTP, the Sensor checks if the HTTP request contains any IP addresses, domains, or URLs of C&C servers in callback detectors.
5. The Sensor checks for anomalies such as protocol anomalies and response errors in protocols and performs heuristic analysis to detect zero-day botnets.

1. In the Manager, select Policy → <Admin Domain Name> → Intrusion Prevention → **Inspection Options**.

   The inspection option policies available for the admin domain are listed.
2. Complete the following to create an inspection option policy.
   a. Click +
   b. Specify the details on the **Properties** tab and click **Next.**

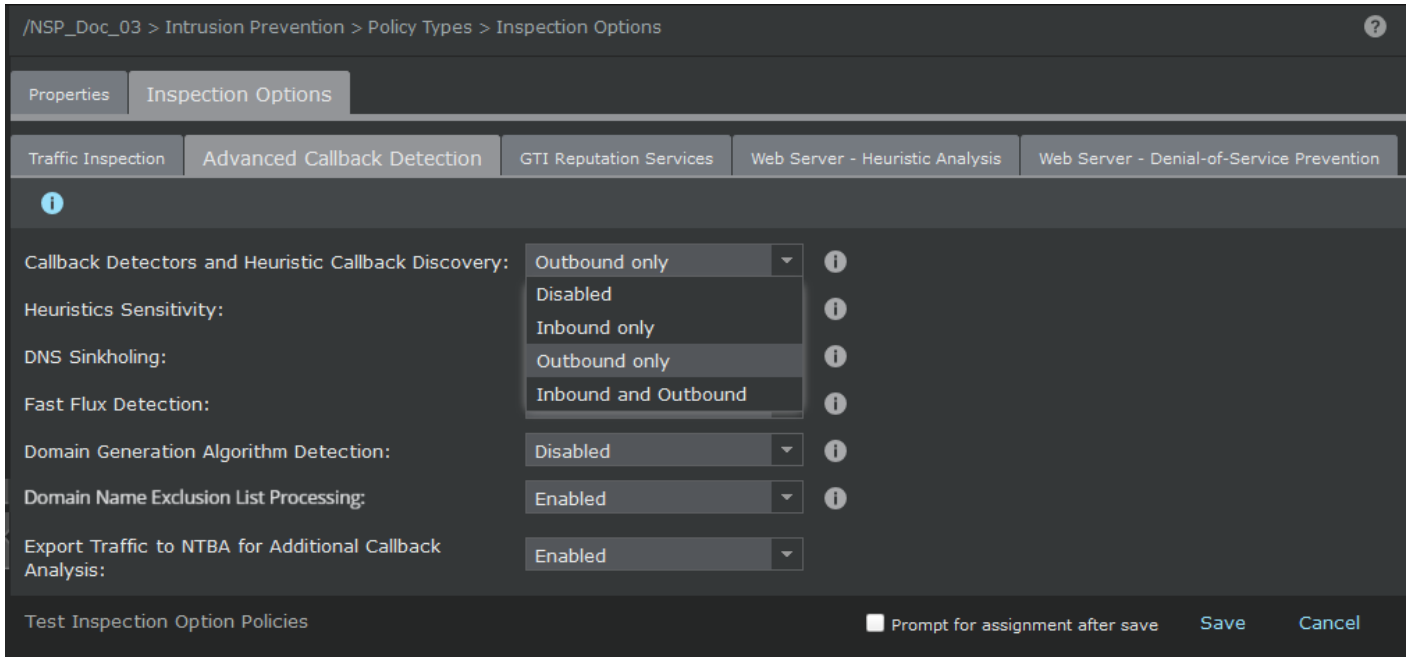
Option	Definition
Name	Enter a relevant name for the inspection option policy.
Description	Enter the details for the policy.
Owner	Indicates the admin domain in which you are creating this policy.
Visibility	• **Owner and child domains** — Select this option to make the policy available to the child admin domains of the current domain. You can apply this policy to the interfaces owned by the child domains, but cannot modify or delete the policy from the child domains. • **Owner domain only** — Select this option to restrict the policy to the current admin domain.

Option	Definition
Editable Here	Indicates whether you can edit the policy in the current admin domain. If the policy is editable, it indicates that the current domain owns the policy.
Statistics	**Last Updated** — The date and time when the policy was last updated. **Last Updates By** — Name of the user who last modified the policy **Assigments** — Number of interfaces the policy is assigned to.
Prompt for assignment after save	Select if you want to be prompted to assign the policy to Sensor interfaces and sub-interfaces when you save the policy.

3. To use an existing inspection option policy, select an editable policy in the **Inspection Options** page and click

4. Select Inspection Options → **Advanced Callback Detection**.

Figure 430. Advanced Callback Detection tab



5. Complete the following steps to configure HTTP-based detection of command and control server information (IP addresses, domains, and URLs of command and control servers in the callback detectors) as well as multiple heuristic analysis for zero-day botnets.

> **NOTE**
>
> These heuristic analyses considers factors such as protocol anomalies and response errors in protocols. It does not include DNS-based heuristic analyses for FFSN and DGA detection.

   a. From the **Callback Detectors and Heuristic Callback Discovery** drop-down list, select the required option. Additional options are displayed when you select an option other than **Disabled**.

NOTE

In case of HTTP traffic, you must enable HTTP response scanning in the same direction to protect your clients.

- **Disabled** — Select to disable HTTP-based detection of IP addresses, domains, and URLs of C&C servers in the callback detectors as well as heuristic analyses for zero-day botnets. You can still enable DNS-based detection of FFSN, DGA, and exporting of traffic to NTBA for callback analysis.

  NOTE

  If you wish to disable **Layer 7 Data Collection** option in **Traffic Inspection** ensure that **Callback Detectors and Heuristic Callback Discovery** option is also disabled.

- **Inbound only** — Select this option to inspect traffic in the inbound direction. For example, select this option to protect the servers in your inside network.

  In case of HTTP traffic, the Sensor inspects the HTTP request traffic for callback activity. So, the Sensor inspects the HTTP traffic to the servers for callback activity. To also inspect the HTTP traffic to the clients for callback activity, you must enable HTTP response traffic scanning as well in the inbound direction in the same inspection option policy. The **HTTP Response Traffic Scanning** option is available on the **Traffic Inspection** tab.

- **Outbound only** — Select this option to inspect traffic in the outbound direction. For example, select this option to protect the servers in your outside network or the clients in your inside network.

  To inspect the HTTP traffic to the clients, you must also enable HTTP response traffic scanning in the outbound direction in the same inspection option policy.

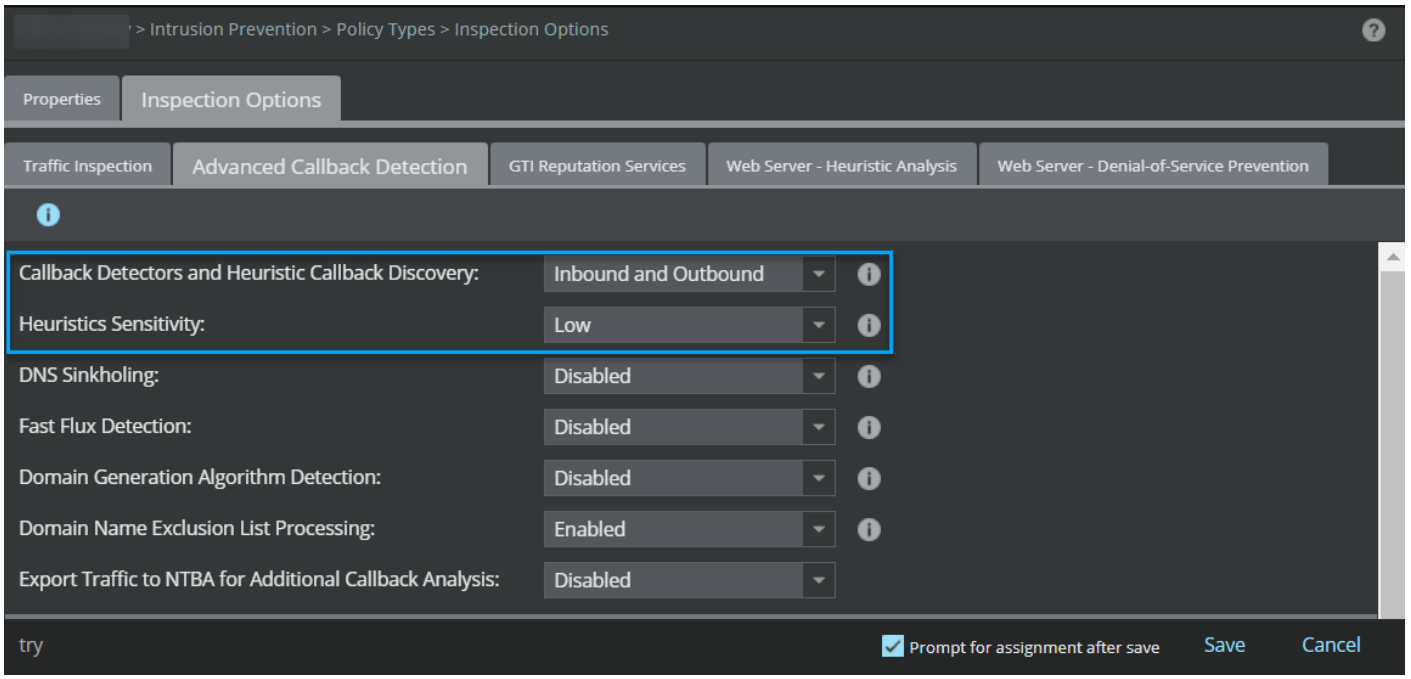
- **Inbound and Outbound** — Select this option to inspect traffic in either direction. This option might impact Sensor performance more than the options described above. In case of HTTP traffic to clients, you must also enable HTTP response traffic scanning in inbound and outbound.

b. Select **Low**, **Medium**, or **High** sensitivity level from the **Heuristics Sensitivity** drop-down.

The sensitivity level determines the level of confidence the heuristic engine must have for the analysis. For example, if you select low, the Sensor's heuristic engine must have a very high confidence that it is botnet traffic for it to raise the alert.

- Low sensitivity level is selected by default.
- This sensitivity setting does not apply to **Fast Flux Detection** and **Domain Generation Algorithm Detection** heuristic engines.

Figure 431. C&C detection (HTTP-based) and heuristic analysis



6. Complete the following steps to configure DNS-based detection of C&C server domains.

   For this feature, the Sensor parses the DNS response traffic to detect C&C server domains according to the callback detectors.

   NOTE

   The DNS-based detection of C&C server domains is controlled by **Callback Detectors and Heurtisitc Callback Discovery** option as in the previous step.

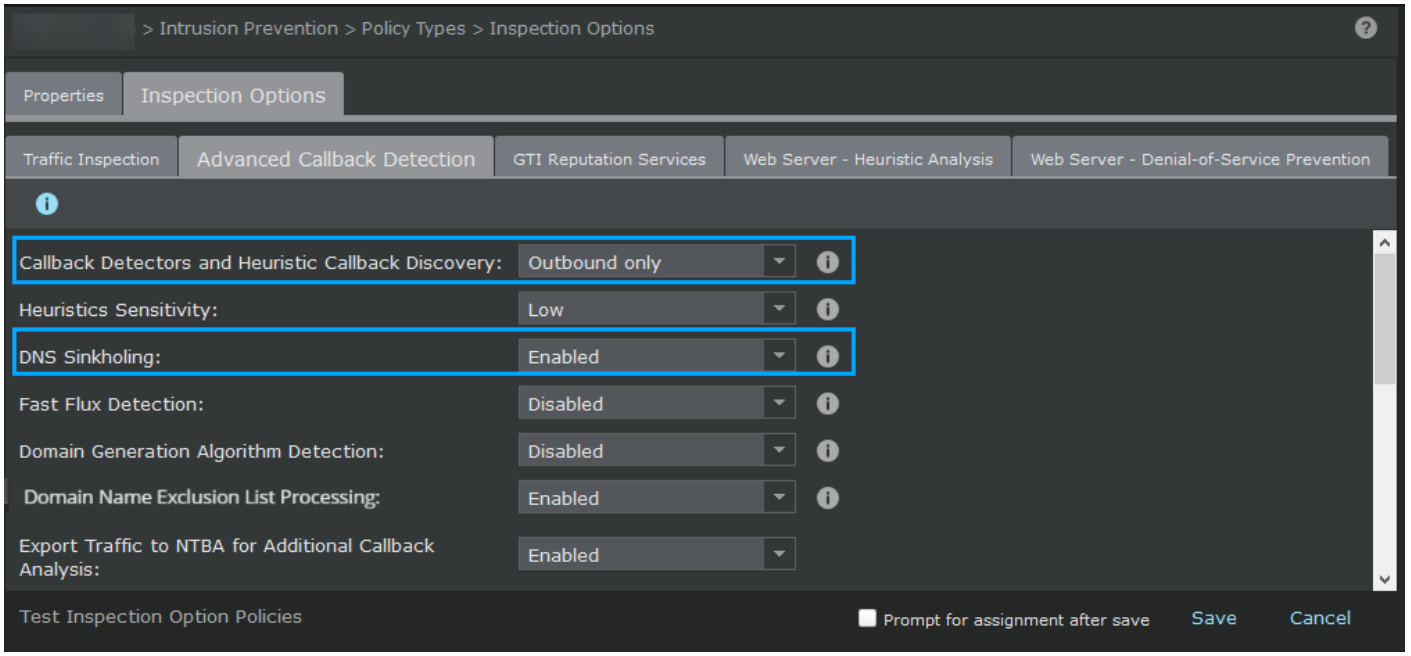
   a. From the **Callback Detectors and Heurtisitc Callback Discovery** drop-down list, select the required option. Additional options are displayed when you select an option other than **Disabled**.

      - **Disabled** — Select to disable DNS-based detection of C&C server domains. You can still enable DNS-based detection of FFSN, DGA, and exporting of traffic to NTBA for callback analysis.
      - **Inbound only** — Select this option if the name servers are in the inside network and the clients are in the outside network. The Sensor inspects the DNS response traffic in the outbound direction only.
      - **Outbound only** — Select this option if the name servers are in the outside network and the clients are in the inside network. The Sensor inspects the DNS response traffic in the inbound direction only.
      - **Inbound and Outbound** — Select this option if you want the Sensor to inspect DNS response packets regardless of the direction. This option has a greater impact on Sensor performance when compared to the other options described above.

   b. Optionally, enable **DNS Sinkholing**.

      For this feature, the Sensor parses the DNS response traffic. The Sensor checks if the domain name in the DNS response is C&C server in the callback detectors file. If so, the Sensor drops the DNS response and forwards a crafted DNS response with the TTL and IP address as per the DNS settings in the **Protocol Settings** page.

Figure 432. DNS-based C&C server domain detection

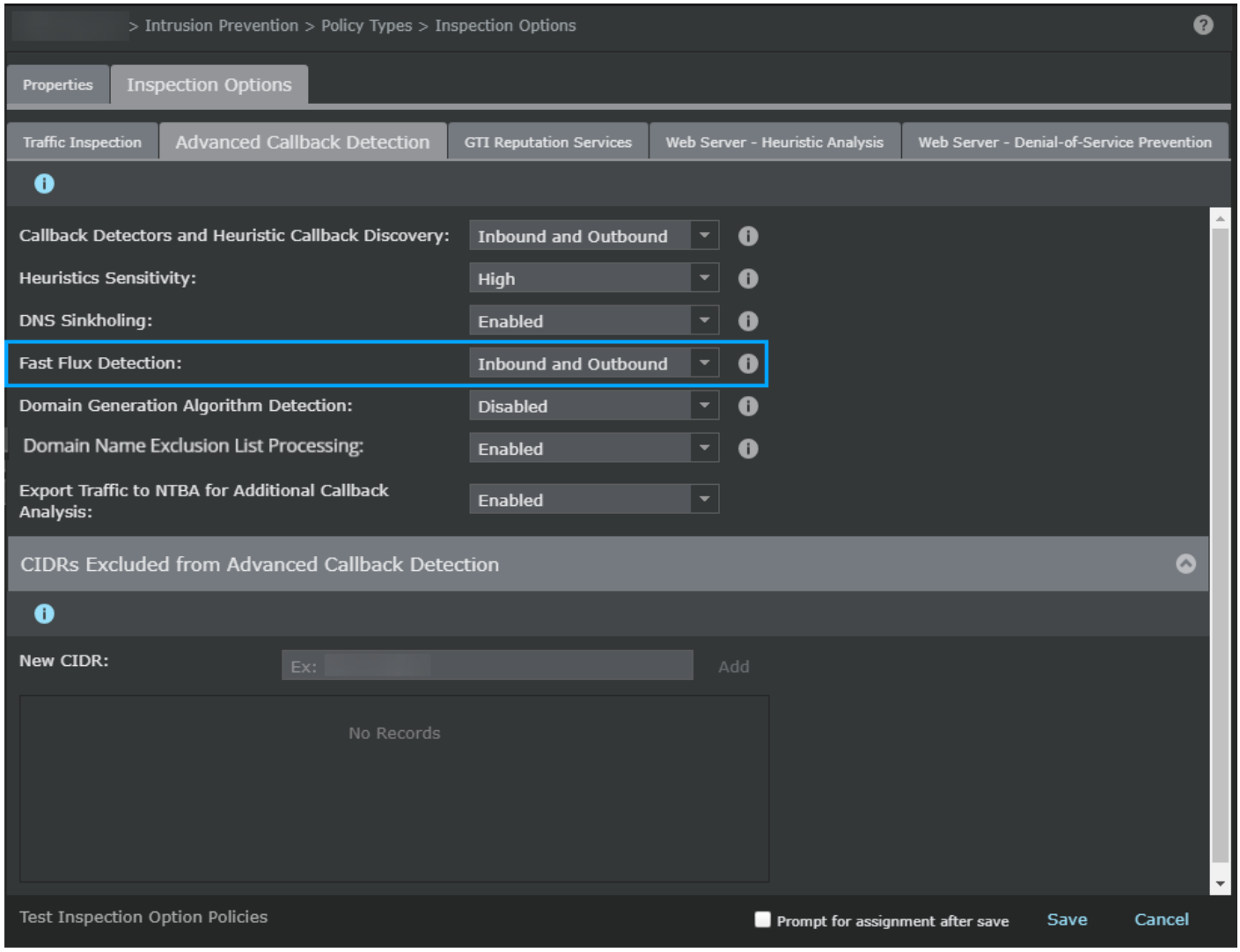


7. Enable **Fast Flux Detection** in the required direction.

   The Sensor parses the DNS response traffic to detect FFSN involvement.

   - **Disabled** — Select to disable FFSN detection by the Sensor.
   - **Inbound only** — Select this option if the name servers are in the inside network and the clients are in the outside network. The Sensor inspects the DNS response traffic in the outbound direction only.
   - **Outbound only** — Select this option if the name servers are in the outside network and the clients are in the inside network. The Sensor inspects the DNS response traffic in the inbound direction only.
   - **Inbound and Outbound** — Select this option if you want the Sensor to inspect DNS response packets regardless of the direction. This option has a greater impact on Sensor performance when compared to the other options described above.

Figure 433. FFSN detection



8. Enable **Domain Generation Algorithm Detection** in the required direction.

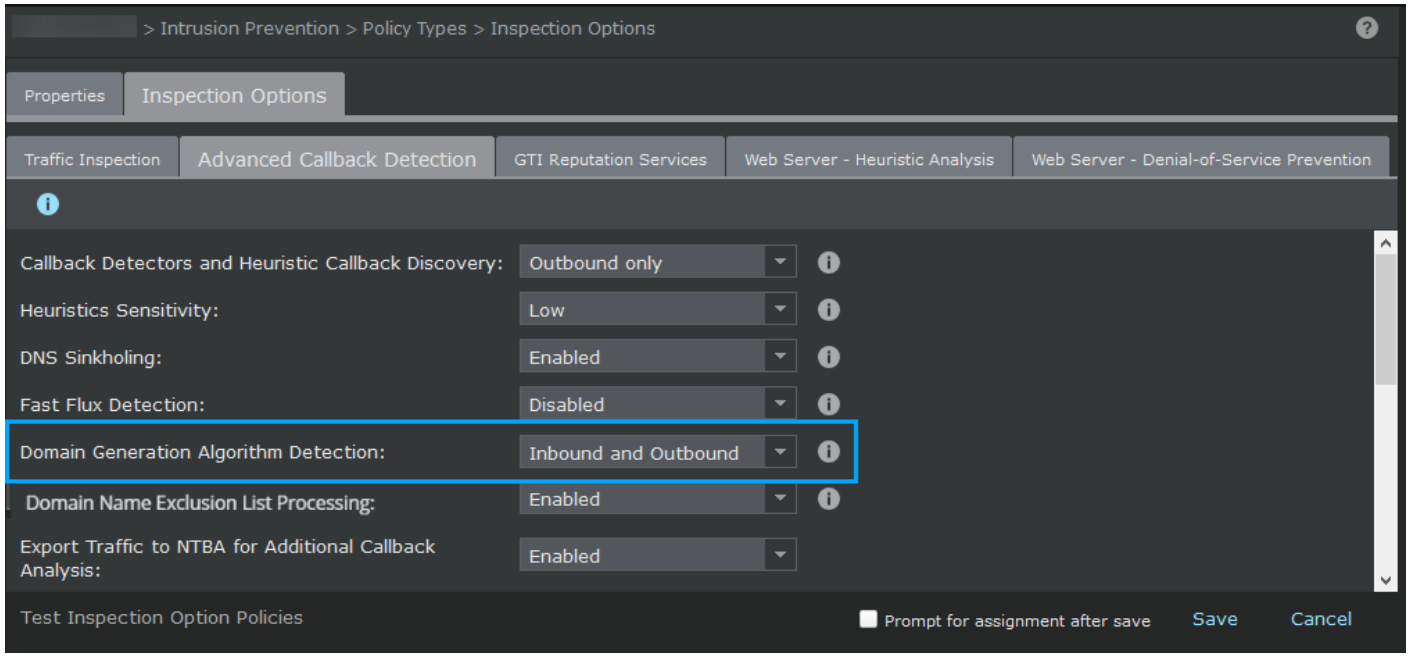
   The Sensor parses the DNS response traffic to detect DGA involvement.

   - **Disabled** — Select to disable DGA detection by the Sensor.
   - **Inbound only** — Select this option if the name servers are in the inside network and the clients are in the outside network. The Sensor inspects the DNS response traffic in the outbound direction only.
   - **Outbound only** — Select this option if the name servers are in the outside network and the clients are in the inside network. The Sensor inspects the DNS response traffic in the inbound direction only.
   - **Inbound and Outbound** — Select this option if you want the Sensor to inspect DNS response packets regardless of the direction. This option has a greater impact on Sensor performance when compared to the other options described above.

NOTE

The **Fast Flux Detection** and **Domain Generation Algorithm Detection** heuristic engines operate in parallel for a given DNS response packet and are independent of each other. That is, the Sensor might raise an alert for FFSN and DGA for the same DNS traffic.

Figure 434. DGA detection



9. Enable **Domain Name Exclusion List Processing** .

   Before analyzing DNS traffic, the Sensor checks if the domain name in the DNS response is exempted according to **Domain Name Exceptions** list. If so, the Sensor forwards the DNS response without any further DNS-based analysis for botnet.

   - The **Domain Name Exclusion List Processing** option applies to all DNS-based of callback activity-C&C server domains, FFSN detection, and DGA detection. So, for the domain name exceptions, the Sensor checks the DNS response in the same direction as **Callback Detectors and Heurtistic Callback Discovery**, **Fast Flux Detection**, and **Domain Generation Algorithm Detection**.
   - As a best practice, make sure you add your organization's public and internal domain names to the exceptions list. If Trellix is an example, you add **`trellix.com`** to the exception list. Add the last two domain labels for such exceptions. That is, instead of *www.trellix.com*, add **`trellix.com`**. This ensures that Sensor resources are not spent on analyzing traffic related to known domains.
   - Except for purposes such as troubleshooting, always enable **Domain Name Exclusion List Processing** to preserve Sensor resources.

10. If required, enable **Export Traffic to NTBA for Additional Callback Analysis** to send the botnet events to NTBA for further analysis.

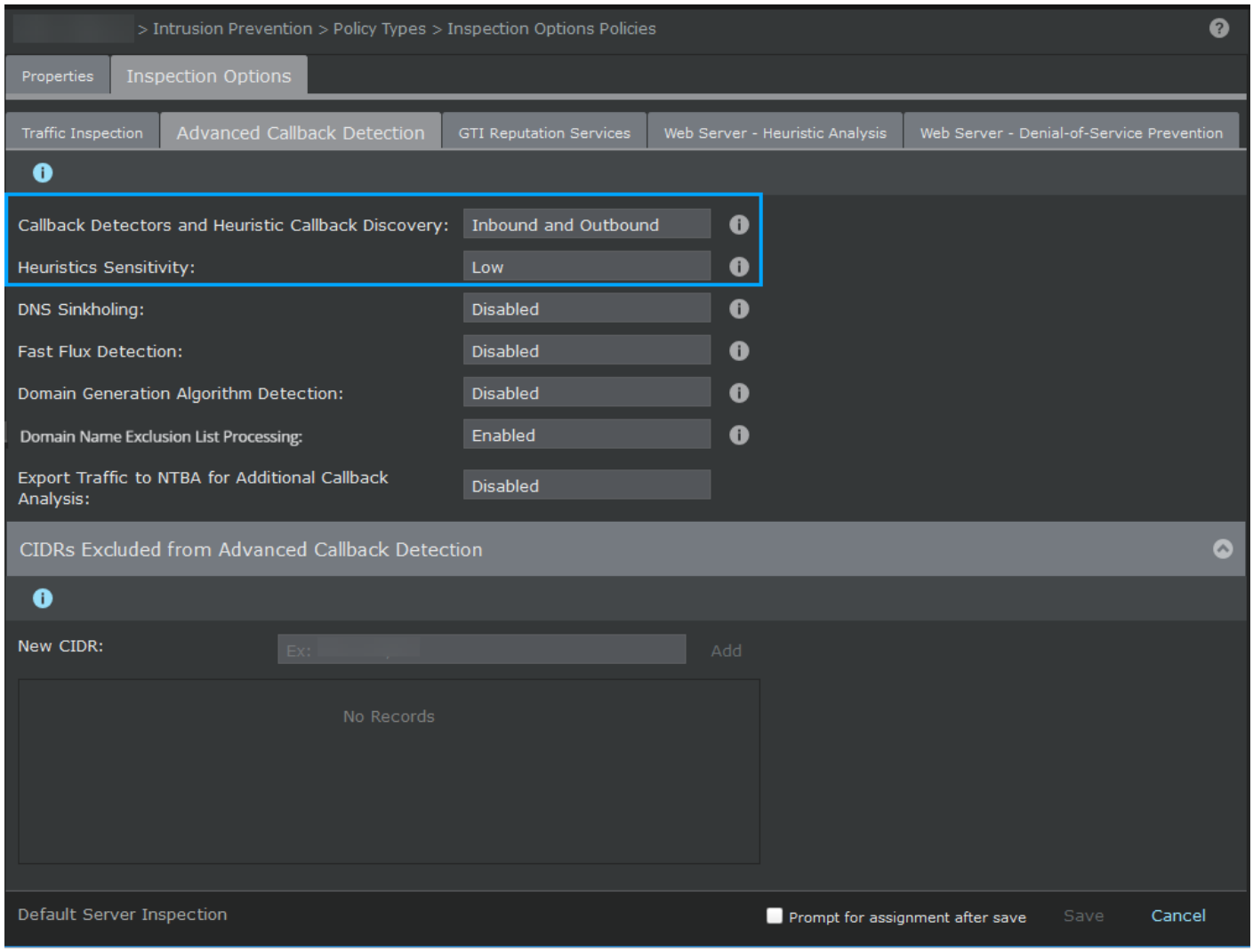
    Heuristic detection correlates different bot activities and raises an alert when a specific condition is met. The sensitivity level determines the level of confidence the heuristic engine must have for the analysis. For example, when a low

sensitivity level (default) is selected, the engine must have high confidence that it has detected a bot before raising an alert.

NOTE

Events can be sent to NTBA even when the local detection is disabled.

Figure 435. Callback Activity Detection configuration



11. Define the IPv4 CIDRs to be excluded from callback detection.
    - To add a CIDR, enter a valid CIDR notation and click **Add.** For example, enter 10.1.1.0/24 to exclude the hosts from 10.1.1.1 through 10.1.1.254 from callback detection.
    - To remove a CIDR from the list, click on the adjacent **X** icon.
    - If the traffic is from or to a defined CIDR, the Sensor exempts that traffic from the following callback detection features.
        - DNS-based detection

- HTTP-based detection for IP addresses of C&C server domain alone is exempted. The Sensor performs HTTP-based detection for IP address and URL, domain, domain and URL of C&C server domain.
- Other advanced callback heuristics

12. Click **Save**.

    If you select **Prompt for assignment after save**, you are prompted to assign the inspection option policy to the Sensor resources owned by the corresponding domain.

Assign an inspection option policy to Sensor resources

Prerequisite: Make sure you have created an inspection option policy with advanced callback configuration.

If you apply a policy to a subinterface that is different than the interface policy, the policy enforced at the interface level protects all traffic not specific to the subinterface. Thus, interface rules only apply to interfaces, and subinterface rules only apply to subinterfaces.

NOTE

In case of inspection option policy, you don't assign policies separately for inbound and outbound. You specify the direction for each inspection option in the policy.

Steps:

1. Select Intrusion Prevention → Policy Manager → **Interfaces.**
2. Enter a string in the text box next to **Clear All Filters** to quickly locate the required interface.

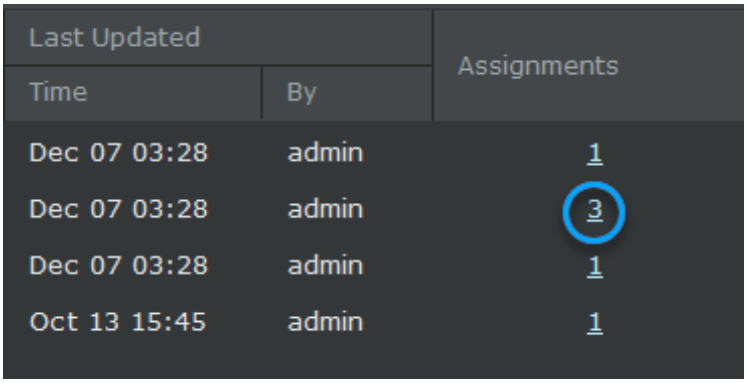
   For example, enter *IPS* to display the records containing this string in any of the columns.
3. Double-click the required record and in the right-side pane, scroll down to the **Inspection Options** section.
4. Select the required inspection option policy from the **Policy** list and click **Save**.
5. Do a configuration update for the Sensor to enforce the policy.

Alternative method to assign an inspection option policy

You can assign inspection option policies from the **Inspection Options** page. If you select the **Prompt for assignment after save** option in the policy, you are prompted to assign the policy to the relevant interfaces and sub-interfaces.

1. Select Intrusion Prevention → **Inspection Options.**
2. Click the **Assignments** value of the policy that you want to assign.

   The **Assignments** window displays.



3. Assign the IPS policy to the required interfaces and subinterfaces.

Option	Definition
Search Interfaces	To filter the list of available interfaces, enter a string that is part of the **Available Interfaces**.
Available Interfaces	Lists the interfaces and subinterfaces of the Sensors in the admin domain. The Sensor interfaces to which you have already assigned this IPS policy are displayed under **Selected interface**. **NOTE** In case of Sensors in failover, the ports used for interconnection of the Sensors are not displayed. If you assign an IPS policy to an interconnect port, the assignment is automatically removed when you create the HA pair. Select a resource and click » to move it to **Selected Interface**.
Current Policy	The inspection option policy that is currently assigned to an interface or sub-interface. To replace that policy with the policy that you are currently assigning, move the interface or sub-interface to **Selected Interface**.
Selected Interface (Policy Group)	Lists the Sensor interfaces to which you have assigned the selected inspection option policy.
Reset	Reverts to last saved configuration.
Save	Saves the changes to the Manager database.
Cancel	Closes the **Assignments** window without saving the changes.

4. Do a configuration update for the corresponding Sensors to enforce the policy.

Manage callback detectors

For Manager deployments that have access to the Internet, the Manager automatically downloads callback detectors from the CDN server. For Manager deployments that do not have access to the Internet, you can download callback detectors manually.

Callback detectors

You can download callback detectors and push it to the Sensor.

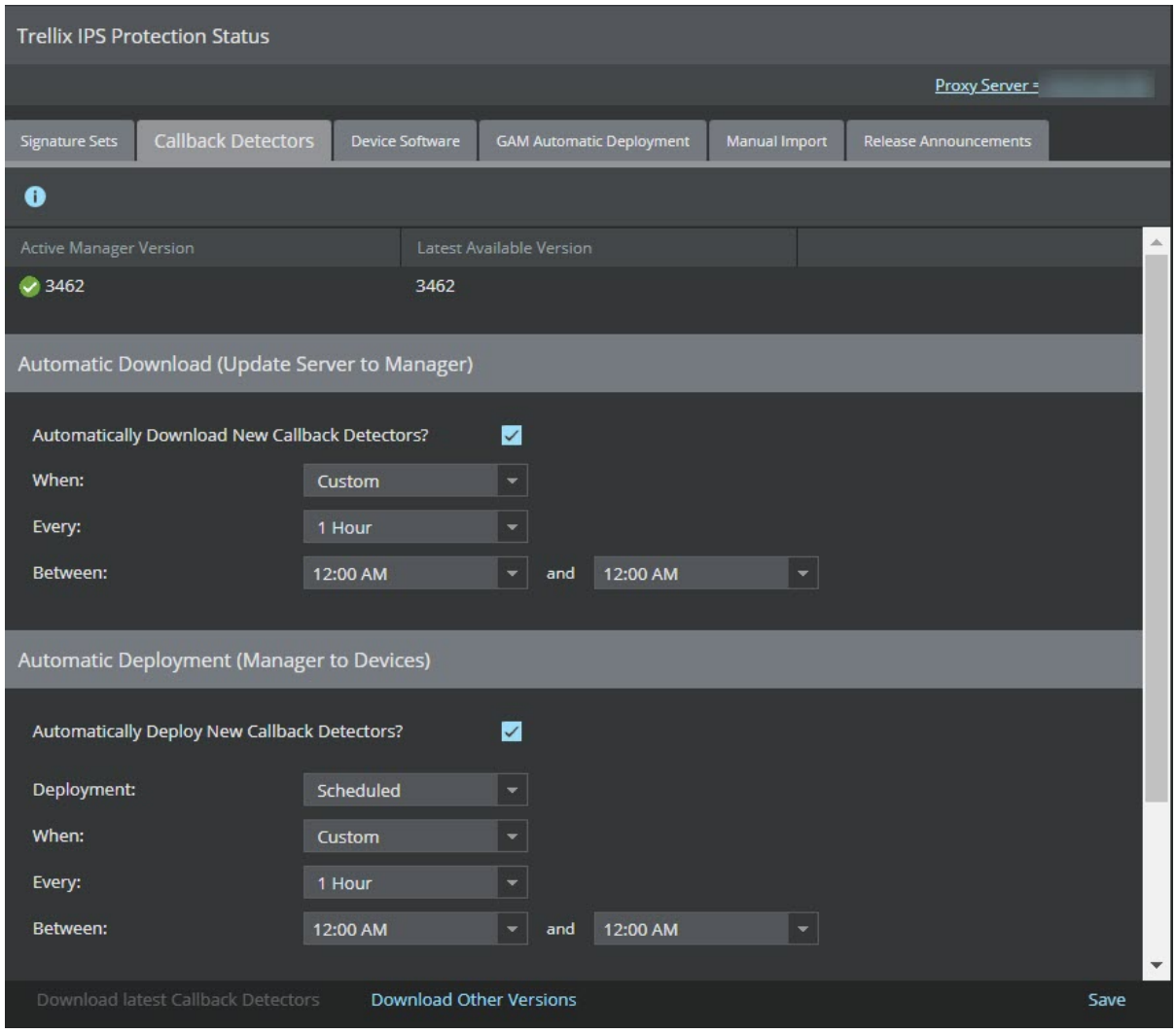
Steps:

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Callback Detectors** tab. The **Callback Detectors** tab is displayed.

   - The **Active Manager Version** displays currently available version.
   - The **Latest Available Version** displays the latest available version for you to download.

   NOTE

   You can also change the display settings to meet your requirements from the filter option.



2. To download the latest callback detectors, select **Download Latest Callback Detectors**.

   A **Confirmation** dialog box appears, select **OK**. A status window opens to process the signature download.

3. To download other versions of callback detectors, select **Download Other Versions**.

   The latest 10 versions are available for you to download. It displays the update details such as the **Release Date** and **Size (MB)** for that particular **Version**.

4. Select the version required and click **Download**.

   The selected callback detectors become the active callback detectors on the Manager.

   To automatically download the callback detectors, refer to Automatic download of callback detectors (page 76).

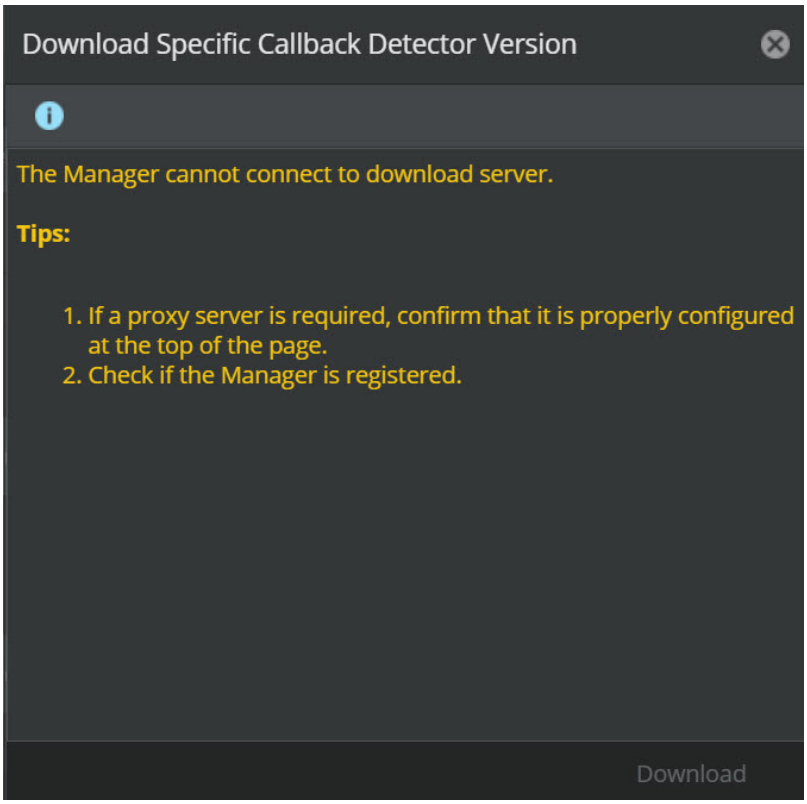
   You can also view the active and latest callback detectors version in the **Manager Summary** monitor of the Manager Dashboard. In the **Device Summary** monitor, you can view the callback detectors version on specific devices.

   - If the active manager version is the latest available version, **Download Latest Callback Detectors** is disabled.
   - A icon is displayed beside the **Active Manager Version** if the active callback detector version matches the latest callback detector version.
   - A icon is displayed beside the **Active Manager Version** if the active callback detector version is older than the latest callback detector version.

   NOTE

   In an air-gap network, unregistered, or proxy server disabled Manager:

   - The **Latest Available Version** is displayed as **---**.
   - A icon is displayed beside the **Active Manager Version**.
   - When you select **Download Other Versions**, the **Download Specific Callback Detector Version** does not display available versions of callback detectors.



Automatically updating signature sets and callback detectors

The Manager allows you to schedule the download of the signature set and callback detectors. Once configured, the scheduler downloads the signature set and callback detectors from Trellix IPS Update Server to the Manager. For example, every one hour, the Manager verifies the Trellix IPS Update Server and downloads the new file uploads.

The success/failure of the import process is indicated through fault notifications, emails, and SNMP traps.

Once the new signature set and callback detectors are available on the Manager, they can be scheduled to be deployed on your devices.

A proxy server is provided for all internet communications. You can manage the proxy server and know the proxy details from the scheduler page.

For more information on automatically updating signature sets, refer to Automatic download of signature sets (page 70).

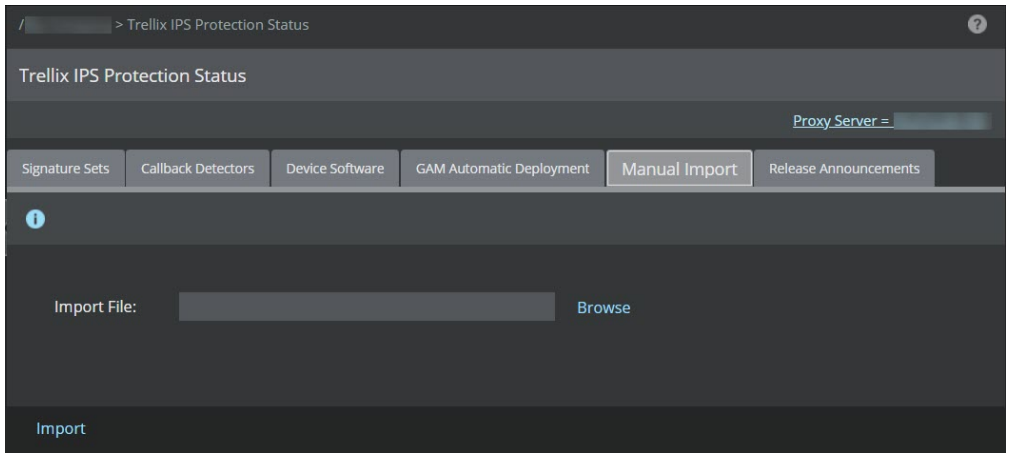
For more information on automatically updating callback detectors, refer to Automatic download of callback detectors (page 76).

Manually import device updates

The Manager allows you to manually import the following device updates from the file system if your Manager deployment has no access to internet.

- Device software (.jar)
- Signature set (.ivu or .jar)
- Callback detectors (.zip)
- Gateway antimalware updates (.upd)

1. Select Manager → <Admin Domain Name> → **Trellix IPS Protection Status**. Then, select **Manual Import** tab. The **Manual Import** tab is displayed.



2. Click **Browse** and choose the file on your system or a network location and click **Import**.

   Later, do a configuration update for the corresponding Sensors.

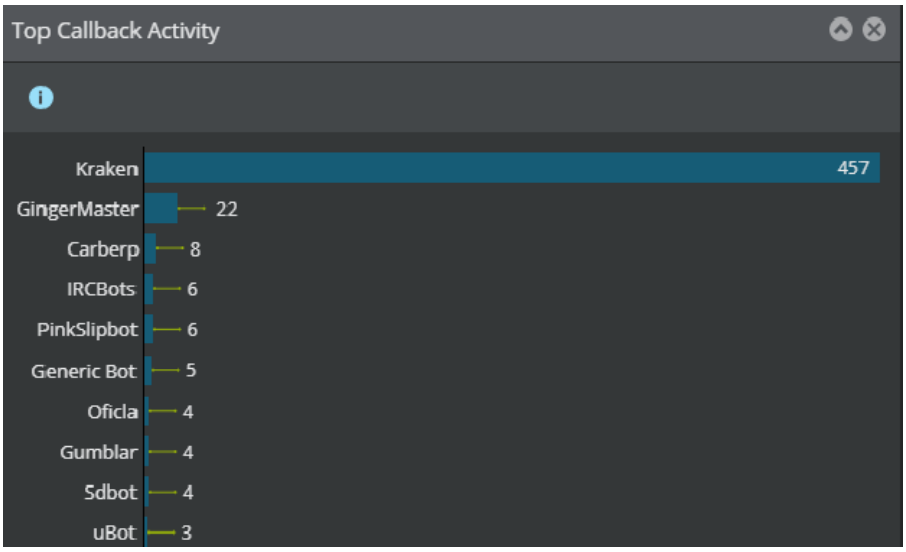
   The Manager audits the import process. The success or failure can be verified in the audit messages.

Analyze Callback Activities

You can leverage the analysis technique provided by the Trellix IPS to perform an in-depth analysis of the callback activity in your network. The Manager provides you with a complete view of the bot events and threats on your network for further analysis and

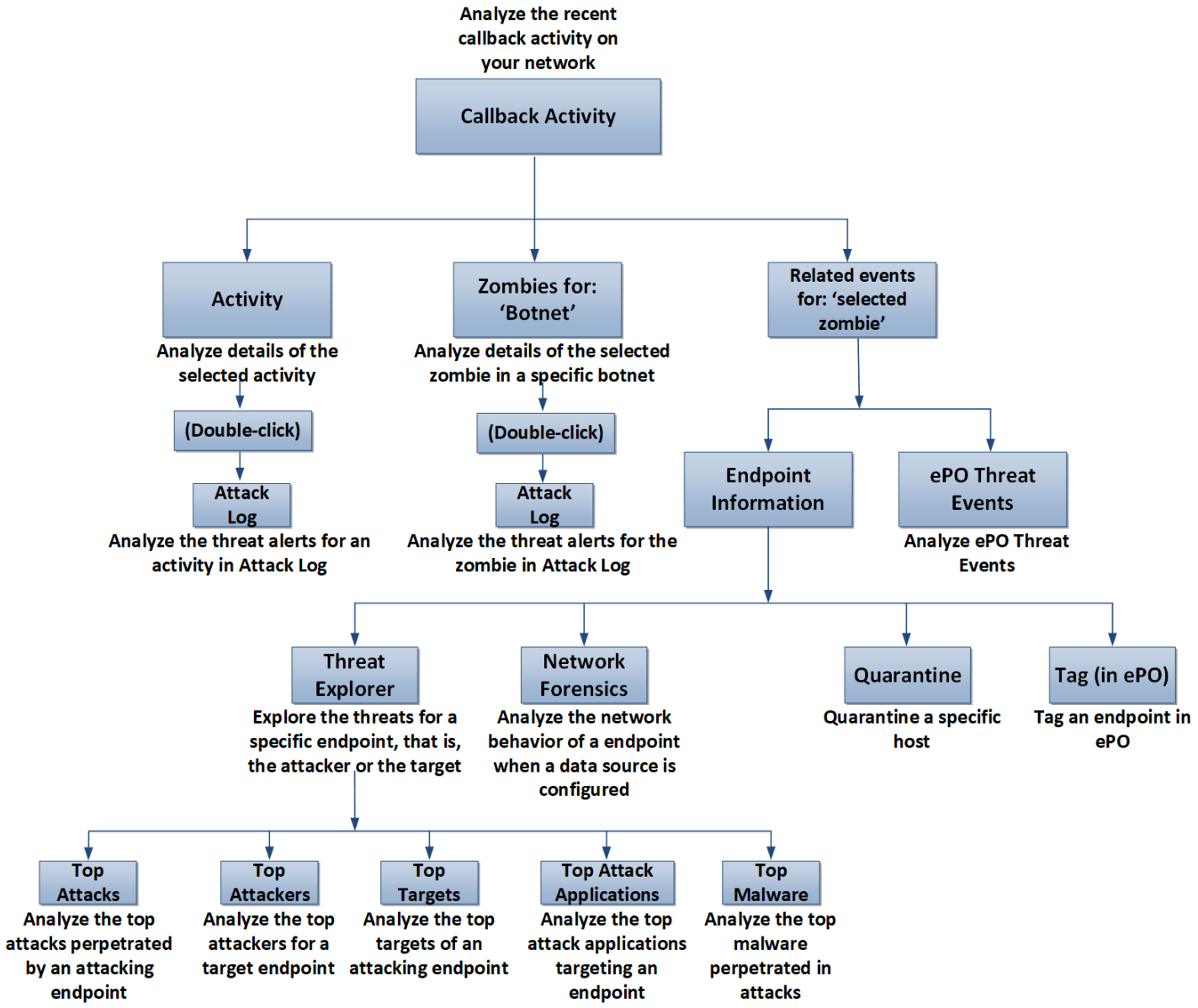
actions, thus providing a comprehensive view of the threat landscape in your network. You can view the **Top Callback Activity** dashboard. This dashboard is populated when bot activity is detected in your network. The dashboards display the callback activity name and the number of bots (zombies) in your network for the corresponding callback activity. The **Dashboard** page security monitors are displayed as bar charts.

Figure 436. Dashboard-Top Callback Activity



If you want to drill down further on a specific bot activity, click the bar, and you'll be redirected to the Analysis → **Callback Activity** page, which displays additional details on that activity. This page provides you with the flexibility of filtering and sorting the information displayed based on your choices. In addition to these filtering/sorting options, you can also view the alerts that match the filter criteria by opening the **Attack Log** page. You can view the callback activities specific to admin domains by selecting the required admin domain from the **Domain** drop-down list. Summarized data for callback activities, which includes data from the child domains, also can be viewed. If you have integrated the Manager with products like ePolicy Orchestrator - On-prem, Intelligent Sandbox, or Trellix Virtual Execution, you can view the host name, operating system, open ports, known vulnerabilities.

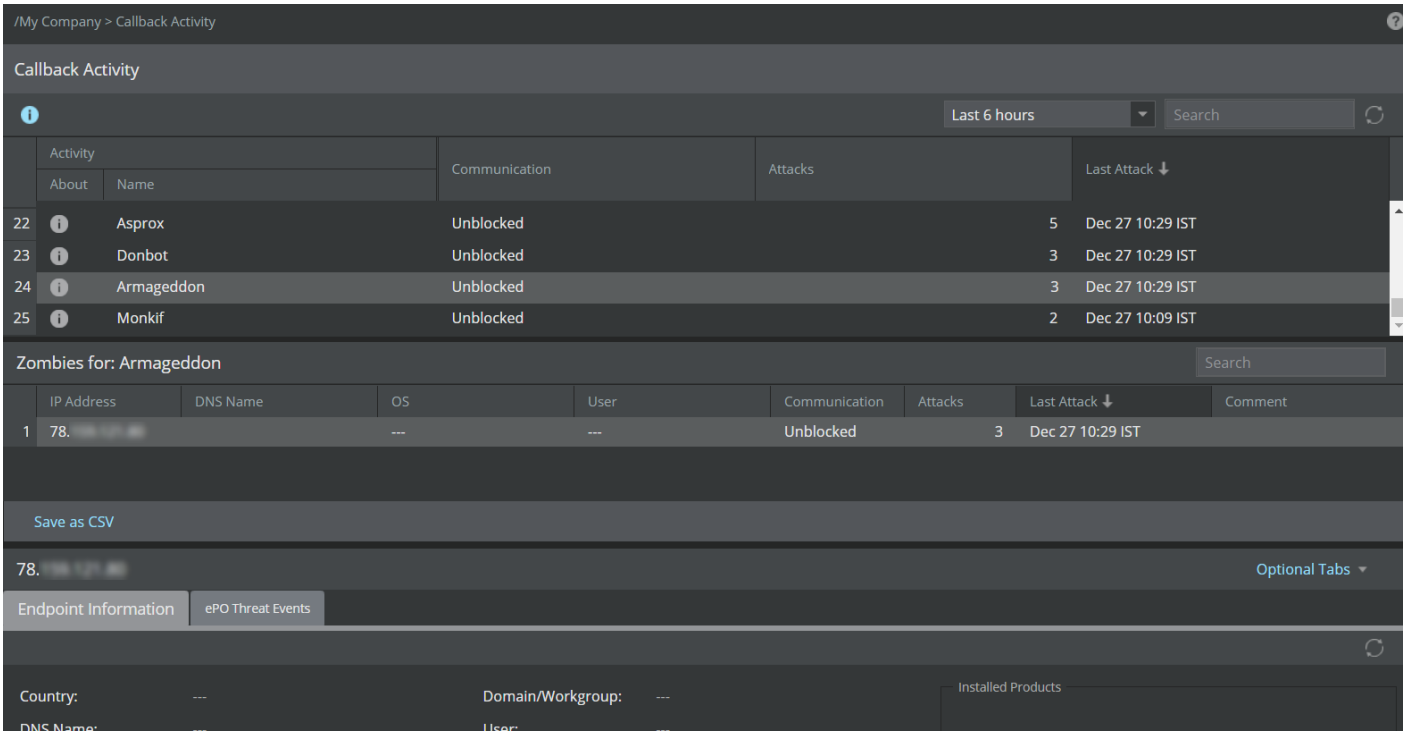
Figure 437. Callback activity analysis



You can analyze details of the callback activities, such as the callback activity name, status of the Command and Control Server communication, number of events and the details of the last event occurrence.

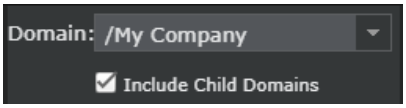
You can further analyze the details of all the zombies in the activity. For each zombie you can view its IP address, DNS name, operating system, user details, status of the Command and Control Server communication, number of events and the details of the last event occurrence.

Figure 438. Analyze callback activities



Filters can be applied at the admin domain levels which provide bot data for the selected admin domains. Data from the child domains are included in the data provided. The **Include child domains** checkbox is selected by default. Deselect the checkbox to view data only for the selected admin domain.

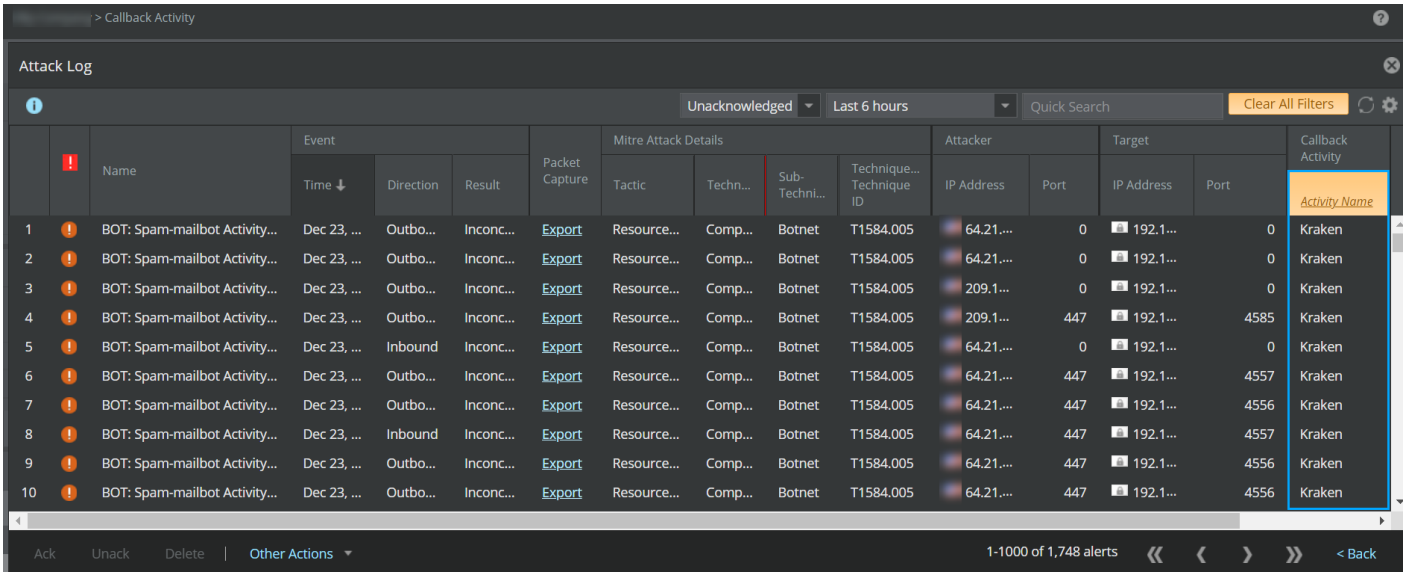
Figure 439. View data specific to admin domain



Attack Log

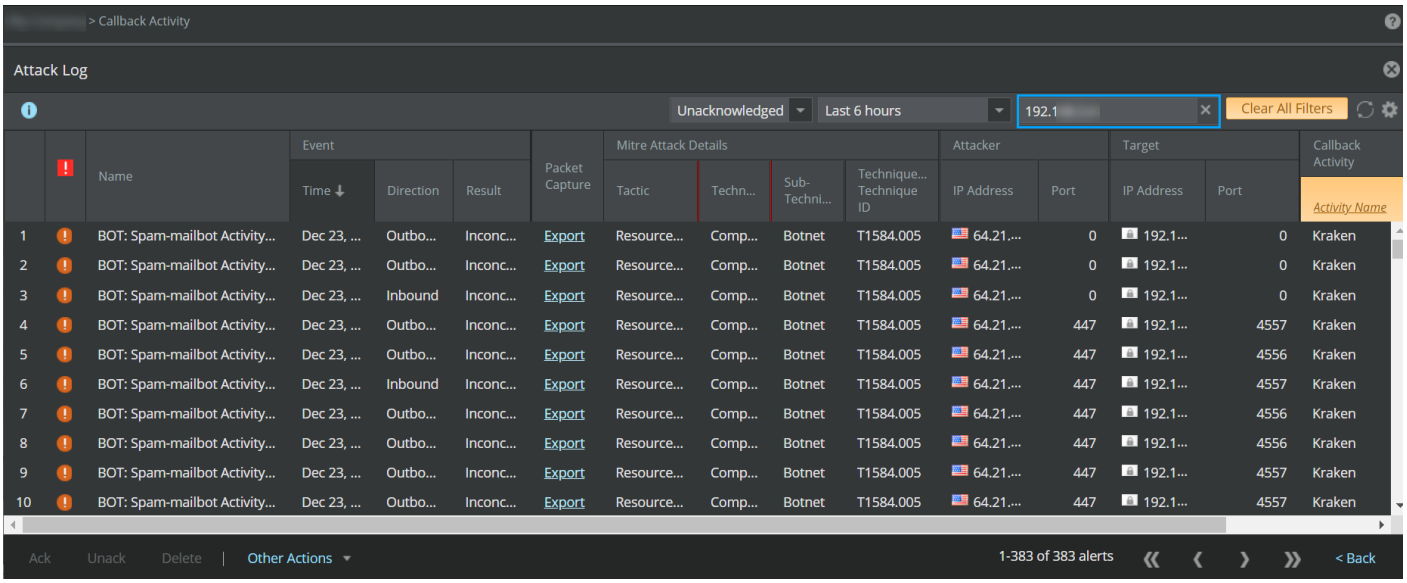
Upon double-clicking any callback activity under the **Activity** section, the **Attack Log** opens where you can view and analyze the alerts related to the callback activity.

Figure 440. Callback Activity related alerts in Attack Log



Double-click the IP address under the **Zombies for: <Activity>** section to view alerts related to the IP address and callback activity.

Figure 441. IP address related alerts in Attack Log



To close the attack log, click **Back** or icon.

Activity

This tab displays the following details of the selected activity.

Option	Definitions
About	Click to view the detailed **Activity Description**. This comprehensive activity report provides information, such as the activity description, symptoms of the bot, bot prevention methods, and bot removal tips.
Name	The name of the callback activity family
Communication	The status of the bot's communication with the Command and Control server, whether blocked or unblocked
Attacks	The number of attacks executed by all the bots listed under the callback activity family
Last Attack	The date and time of occurrence of the last attack

Zombies for: <activity>

This tab displays the details of the selected zombie for a particular activity.

Option	Definitions
IP address	IP address of the attacker
DNS name	DNS name of the endpoint to resolve the names to IP addresses
OS	Operating system platform of the endpoint
User	Operating system user name of the endpoint.
Communication	The status of the bot's communication with the Command and Control server, whether blocked or unblocked
Attacks	The number of attacks executed by a selected bot/IP address
Last Attack	The date and time of occurrence of the last attack
Comment	Additional comments on the activity can be added

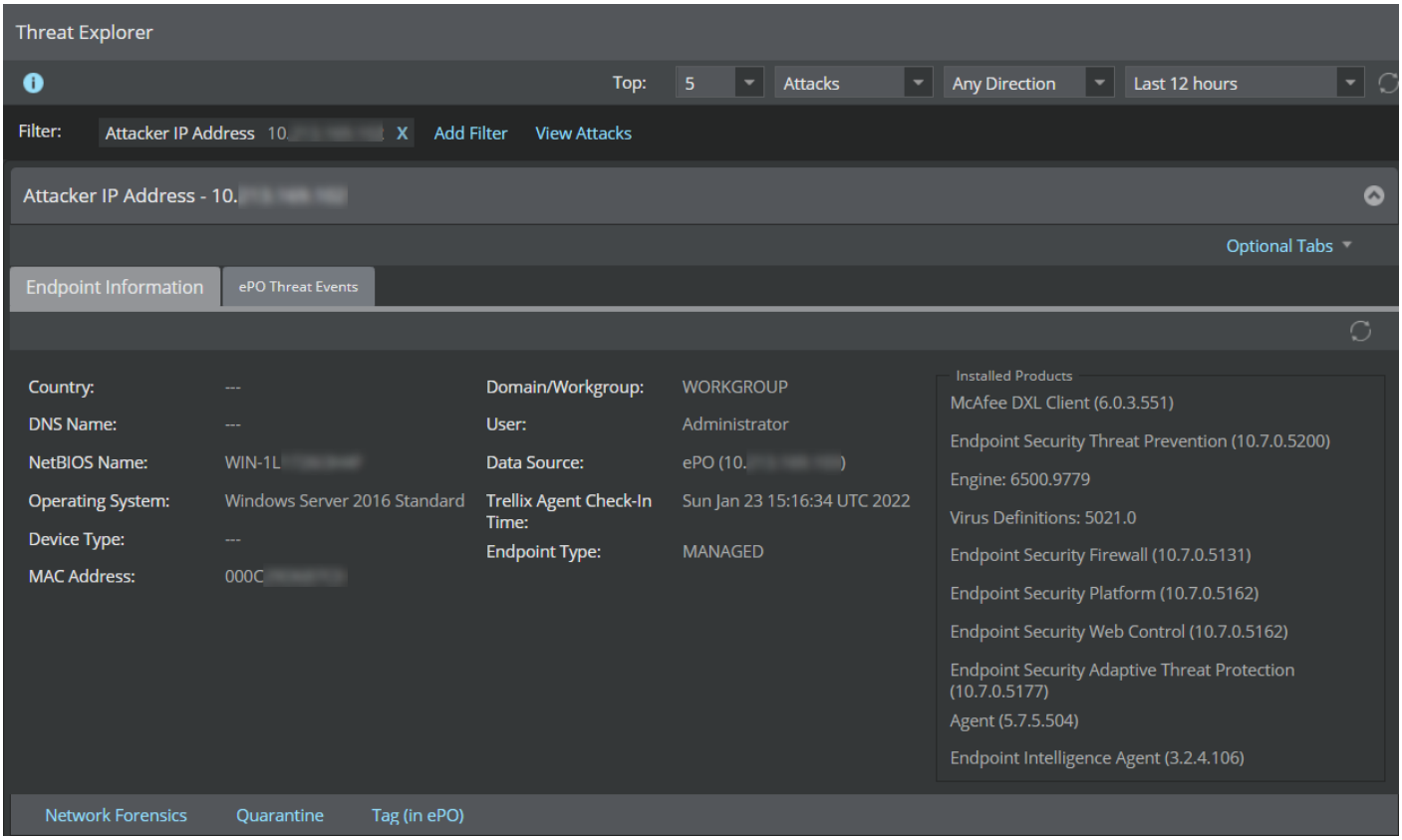
'Zombie IP address'

This tab displays various events related to a specific zombie.

- **Endpoint Information**

  The **Endpoint Information** sub-tab shows the following details specific to the endpoint.

Figure 442. Analyze Endpoint Information

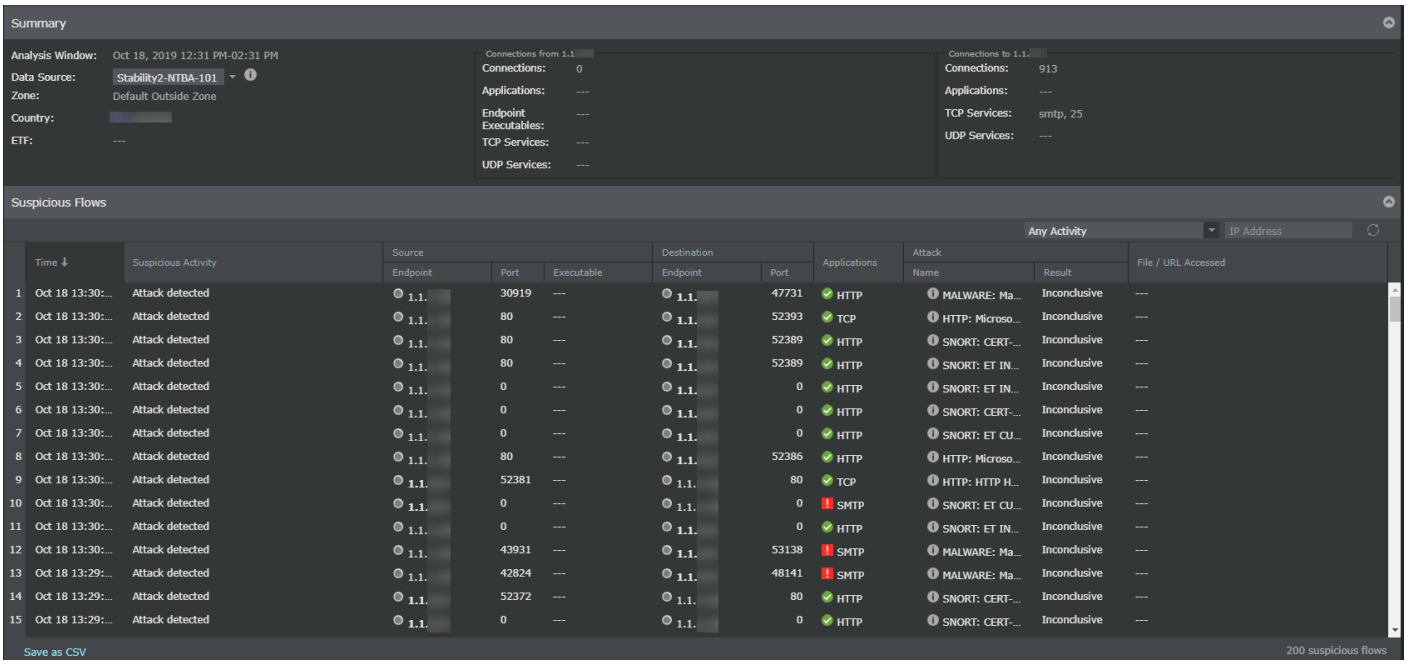


Option	Definitions
Country	Country of the endpoint
DNS Name	DNS name of the endpoint to resolve the names to IP addresses
NetBIOS Name	NetBIOS name of the endpoint to access the endpoint machines
Operating System	Operating system platform of the endpoint
Device Type	Device type of the attacker/target
MAC Address	MAC address of the endpoint
Domain/Work-group	Domain or workgroup of the endpoint
User	Operating system user name of the endpoint
Data Source	Point product (Trellix ePO - On-prem) from where information is retrieved
Trellix Agent Check-In Time	Check-in time of the Trellix Agent that communicates with the same Trellix ePO - On-prem server integrated with the admin domain

Option	Definitions
Endpoint Type	Type of the endpoints: • UNMANAGED (No Agent) — This indicates that there is no Trellix Agent installed on the endpoint. • UNMANAGED (MANAGED) — This indicates that the endpoint has a Trellix Agent but there is no active communication channel between the Agent and Trellix ePO - On-prem server integrated with the admin domain. • MANAGED — This indicates that the endpoint has a Trellix Agent and there is active communication channel between the Agent and Trellix ePO - On-prem server integrated with the admin domain. The endpoint is managed by the agent.
Installed products	List of the installed products

- **Threat Explorer**
  - **Explore as attacker IP** — Explore the threats where the endpoint is the source IP address.
  - **Explore as target IP** — Explore the threats where the endpoint is the destination IP address.
- **Network Forensics** — Click this tab to analyze the network behavior of the endpoint when NTBA is configured.

Figure 443. Network Forensics page

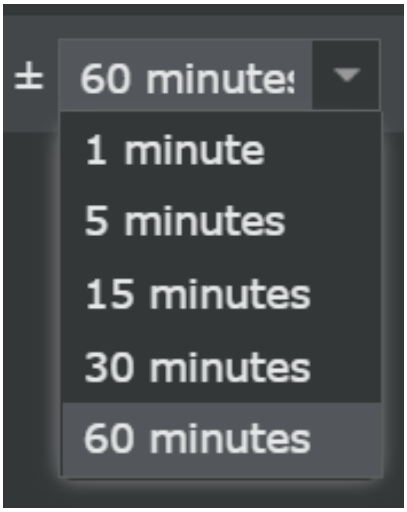


You can filter your view by choosing the time and date of your choice.

Figure 444. Date and time options in Network Forensics page

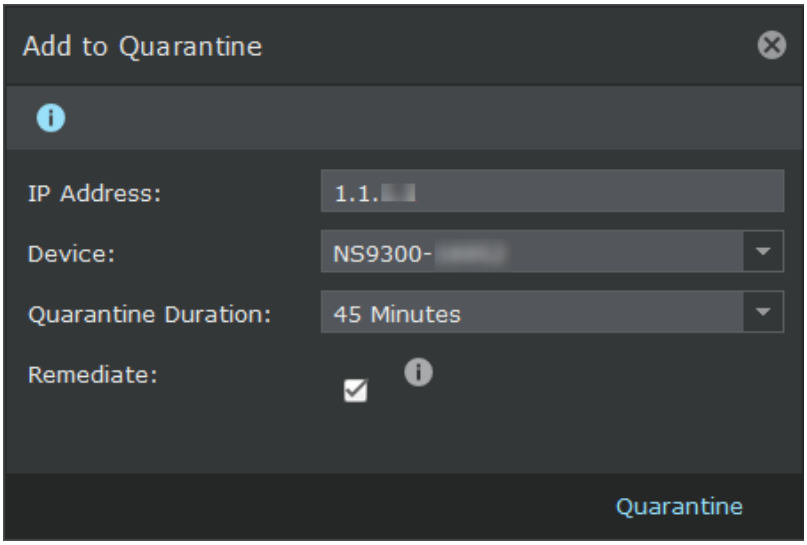
You can view the data according to your time preference by selecting the time period from the drop-down list. You can use the ± icon to view the details before and after any event/attack.

Figure 445. Show option



- **Quarantine** — Use this option to block all the traffic originating from the specified IP address seen on the selected device for the selected time.

Figure 446. Quarantine Endpoint dialog



To quarantine endpoints to block all the traffic originating from the specified IP address:

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal**. Remediation cannot be configured for IPv6 address. The checkbox and the information icon for remediation are not displayed if you enter an IPv6 address in the **IP Address** field.

Click **Quarantine**. The endpoint is added and displayed in the **Quarantine** page.

- **Tag (in ePO)** — Use this option to assign a tag to the selected endpoint in Trellix ePO - On-prem.

  You are able to assign tags only to endpoints whose **Endpoint Type** denotes MANAGED. This means that the endpoint runs a suitable version of Trellix Agent and is managed by Trellix ePO - On-prem.

  To assign a tag:

  1. Select a tag from the drop-down list. If the tag you are looking for does not appear in the list, click the refresh button.
  2. Click **Tag**.

If the tagging is successful, you receive a message stating its success. If not, you receive a failure notification.

- **ePO Threat Events**

  The **ePO Threat Events** sub-tab displays the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for a selected endpoint. The information displayed under this sub-tab includes the date and time at which the threat event was generated, the ID associated with the event, the event description, event category, action taken on the event, and the type of the threat that triggered the event.

  You can click the icon to refresh the list and view the latest **50 Threat Events** listed in the ePolicy Orchestrator - On-prem for the selected endpoint. The **Search** text field allows you to search for a specific event based on the **Event Received Time**, **Event ID**, **Event Category** and **Threat Type**. For example, to view all events associated with the Event ID 1095, type **`1095`** in the **Search** field.

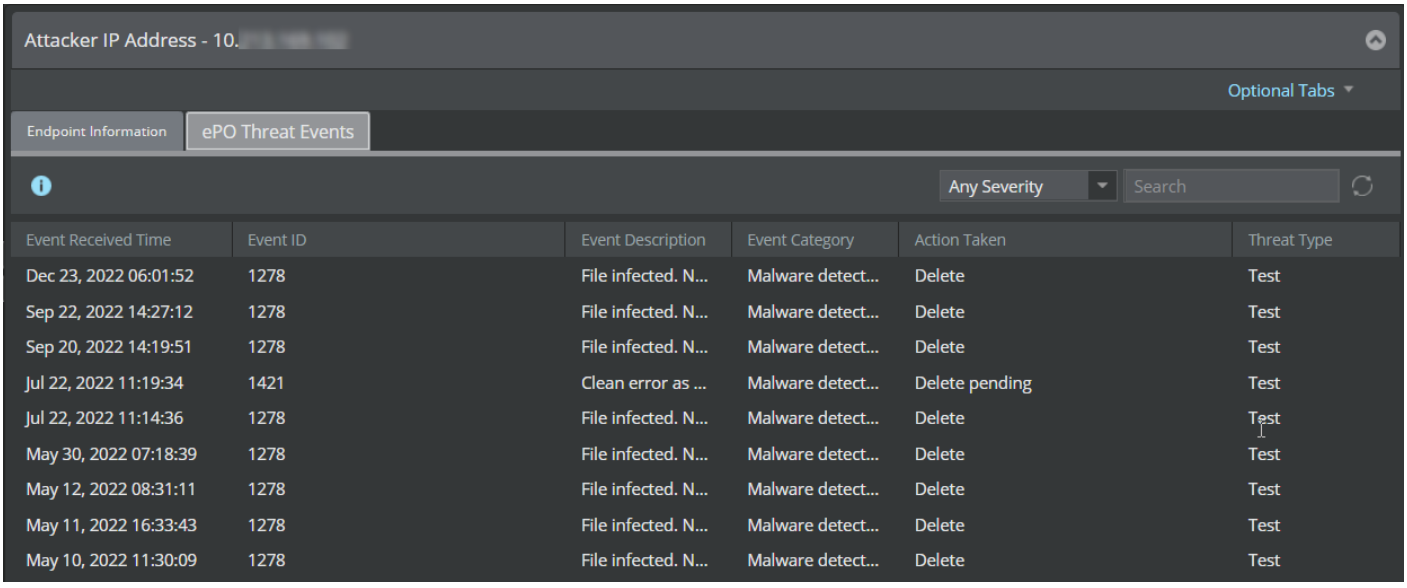
  NOTE

  The sub-tab has **Any Severity** filter selected by default. With this filter selected, the sub-tab displays all types of events including those which are informational and/or of low-severity. Such events act as noise and impede one's ability to find true threats. To exclude these events, select the **Warning+ Severity Only** filter from the drop-down menu. This displays only those events with Critical, Alert and Warning severity.

  NOTE

  Ensure that the ePO server has the latest Trellix IPS Extension file installed. For information on how to download and install the Trellix IPS Extension, see section [Install Trellix IPS extension file in Trellix ePO - On-prem] in [Trellix Intrusion Prevention System Integration Guide].

Figure 447. ePO Threat Events sub-tab



CLI commands related to Advanced Callback Detection

The following are the CLI commands related to **Advanced Callback Detection**.

Normal mode command

- **`show botnet-alertstats`**: This command displays the alert statistics related to advanced callback detection.

Debug mode commands

- **`show botnet-usage`**: This command displays the usage statistics related to advanced callback detection.
- **`dumpdgastats`**: This command dumps DGA-related diagnostic data to a debug file.

For the details of these commands, see the [CLI commands] section.

Denial-of-Service attacks

In a Denial-of-Service (DoS) attack, attackers take advantage of many hosts across the Internet, which they had previously compromised, to launch a brute-force attack that starves the target of its essential resources.

The objective of a DoS attack is to deprive organizations of access to the services or resources. If a website is hit by a DoS attack, millions of users are denied access to the website. As such, DoS attacks do not aim at intruding a network or information theft. By preventing authorized and legitimate access, DoS attacks cause aggravation and cost to the target customer. Distributed Denial-of-Service (DDoS) uses multiple compromised systems to launch an attack. This amplifies the effect of an attack.

Some of the DoS attacks are hard to defend because DoS packets appear to be normal packets. Most DoS attacks use spoofing and flooding techniques to impact network infrastructure.

The degraded service and lost business from a DoS attack leads to staggering costs both during and after an attack. For an e-commerce site like eBay or Buy.com, one day of disruption due to a DoS attack can result in huge revenue loss. The SQL Slammer worm, a DoS attack that made mission-critical Microsoft® SQL servers inaccessible, cost corporations billions of dollars worldwide. Beyond the immediate costs, the lasting effects of a successful DoS attack include lost customers, loss of faith in the service's dependability, and damage to the corporate brand.

What is a Denial-of-Service attack?

A DoS attack is a malicious attempt to render a service, system, or network unusable by its legitimate users. Unlike most other hacks, a DoS does not require the attacker to gain access or entry into the targeted server. The primary goal of a DoS attack is instead to deny legitimate users access to the service provided by that server.

Attackers achieve their DoS objective by flooding the target until it crashes, becomes unreachable from the outside network, or can no longer handle legitimate traffic. The actual volume of the attack traffic involved depends on the type of attack traffic payload used. With crafted payload such as malformed IP fragments, several such packets might be sufficient to crash a vulnerable TCP/IP stack; on the other hand, it might take a very large volume of perfectly conforming IP fragments to overwhelm the defragmentation processing in the same TCP/IP stack. Sophisticated attackers might choose to use a mixture of normal and malformed payloads for a DoS attack. DoS attacks can vary in impact from consuming the bandwidth of an entire network, to preventing service use of a single targeted host, or crashing of a single service on the target host.

Most DoS attacks are flood attacks; that is, attacks aimed at flooding a network with TCP connection packets that are normally legitimate, but consume network bandwidth when sent in heavy volume. The headers of malicious packets are typically forged, or spoofed, to fool the victim into accepting the packets as if they are originating from a trusted source.

What is a Distributed Denial-of-Service attack?

A Distributed Denial-of-Service (DDoS) is a type of DoS attack that is launched from compromised hosts distributed within or across networks. A DDoS attack is coordinated across many systems, all controlled by a single attacker known as a master. Prior to the attack, the master compromises a large number of hosts, typically without their owners' knowledge, and installs software that will later enable the coordinated attack. These compromised hosts called zombies are then used to perform the actual attack. Zombies are also called daemons, agents, slaves, or bots. When the master is ready to launch the attack, every available zombie is contacted and instructed to attack a single victim. The master is not a part of the attack; hence tracing the true origin of a DDoS attack is very difficult. As with a DoS attack, packets sent from each zombie might be spoofed to fool the victim into accepting data from the trusted source. DDoS allows the attackers to utilize the network to multiplex low-volume sources into a high-volume stream to overwhelm the targets. Through the master-zombie communication, the real attackers can potentially hide their identities behind the zombies.

Evolution of Denial-of-Service attacks

In the recent past, DoS attacks were performed by individuals, using the physical resources of one or a handful of computers. This was primarily because of a lack of technical know-how to perpetrate large scale attacks. Gradually, easy-to-use utility programs evolved which made performing DoS attacks easier. This lead to an increase in the occurrences of DoS attacks. The surge in DoS attacks was especially notable with many web-based companies being targeted. These included major websites such as Amazon, Ebay!, and Microsoft.

DoS attacks evolved further with the usage of tools, which perpetrate attacks generated by malware. Once installed, the malware would direct the infected machine to attack specific targets. If multiple infected computers targeted the victim simultaneously, the effects of the attack were greatly amplified.

The next evolution of DoS saw the attackers develop botnets, which are a centrally managed network of compromised computers. This followed the upsurge in DDoS attacks. In a DDoS attack, an attacker uses multiple machines to launch an attack. The internet saw the invention or refinement of techniques to bring computers under the attackers' control and to produce powerful attacks. DoS attacks are the most significant threat in the online world today, especially for businesses which depend on web-based transactions.

How a Denial-of-Service attack works

In most DoS attacks, the legitimate users are denied access to an online resource, a website, or a server. This is achieved by exhausting the physical resources of the victim or by disrupting network connections to it. There are also some specific DoS attacks which exploit a flaw in the target. These are known as vulnerability attacks. However, the result is the same — disruption of the network services. The two most common methods of perpetrating a DoS attack is targeting physical resources and network connections.

Targeting physical resources

Targeting physical resources of a victim is often an effective tactic because it is a violation of how the internet works. The virtual world of the internet is a web of interconnected physical resources, such as, bandwidth, processors, memory and so on. These resources are limited. For example, at any given time, a website processes a number of requests. Once this number is achieved, all the current requests are processed before handling new ones. If a DoS attacker continues to flood the website with requests, new requests are prevented from being fulfilled. The legitimate user requests are also denied access, thus creating a DoS attack.

Targeting network connections

The Internet depends on network connection, such as connections established between a website and a user's computer. The number of connections that can be established with a website are limited. Additionally, the connections should conform to certain protocols. An attacker disrupts these connections by using invalid or an exhaustive number of connection requests to flood the victim. This results in a DoS attack.

Attacked systems see an upsurge in network traffic. If the system does not crash from the attacks, its network capacity is exhausted. Some attacks generate traffic at the rate of several gigabits per second, which far exceeds the capacity of most Internet sites. The increase often results in the Internet service being significantly slowed or completely disconnected. Attempts to form new connections, or reconnect, might not be processed at all.

DoS attacks defended against by Trellix IPS

In Trellix IPS, DoS attacks are classified into two main categories based on their design.

Volume-based attacks are largely bandwidth attacks. When a DoS attack is launched, it is detected as a significant change in the statistical composition of the network traffic. For example, a typical network might consist of 70 percent TCP and a 30 percent mix of UDP and ICMP. A significant and unusual variation in the statistical mix is a signal of a new attack.

In a flood attack, server or network resources are exhausted by a flood of packets. Since a single site perpetrating a flood attack can be identified and isolated easily, a more sophisticated approach, a DDoS attack, is used for many flood attacks.

Attacks, such as SYN floods, use packets to exhaust critical server resources to prevent legitimate clients from connecting to the server. A DDoS attack utilizes a number of machines in a coordinated manner. These machines, known as zombies, are machines that have been compromised and are under the attackers' control. By deploying zombies, hackers can stage large coordinated attacks. As attacks originate from a large number of PCs spread across a wide network, it is extremely difficult to separate legitimate traffic from attack traffic.

The sophistication required and barrier to launch these DDoS attacks has been greatly reduced through the availability of packaged tools that are freely available on the Internet. Some examples of these packaged tools are Tribe Flood Network and Stacheldraht.

Volume-based Denial-of-Service attacks

Volume-based DoS attacks are statistical anomalies in the traffic monitored by a Sensor. In other words, with insight into the normal distribution and volume of traffic, the Sensor looks for significant changes in these levels, which can indicate malicious behavior.

TCP SYN attack

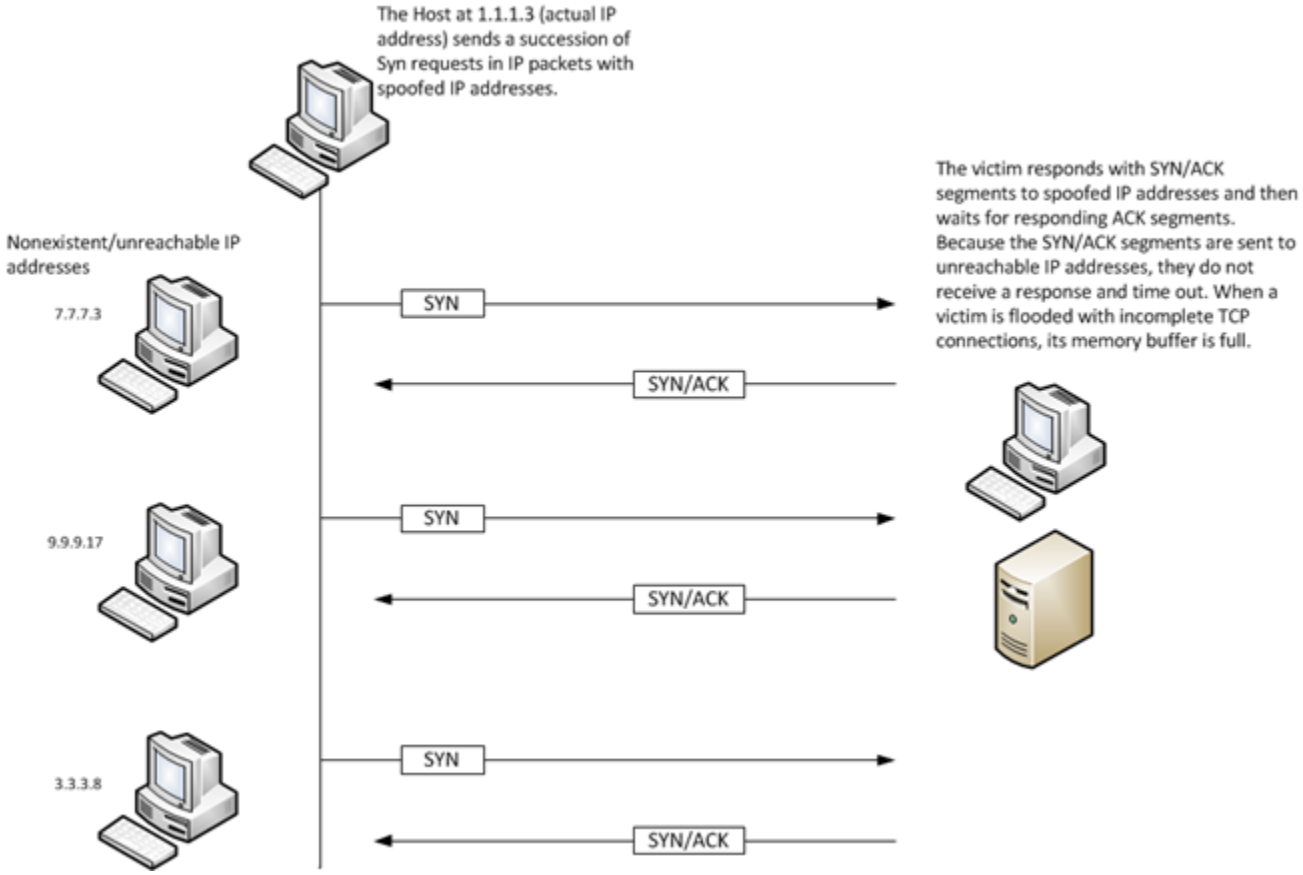
A TCP SYN attack takes place when the attacker sends a large volume of TCP SYN packets using spoofed IP addresses to the target host. This fills up data structures on servers and creates a DOS condition.

Consider the following example. Two hosts establish a TCP connection using the three-way handshake — A sends a SYN segment to B; B responds with a SYN/ACK segment; A responds with an ACK segment. A SYN flood attack occurs when a site is inundated with SYN segments containing spoofed IP source addresses such as nonexistent or unreachable addresses. B responds with SYN/ACK segments to these addresses and then waits for responding ACK segments. Because the SYN/ACK segments are sent

to nonexistent or unreachable IP addresses, they never elicit responses and eventually time out. When a host is flooded with incomplete TCP connections, a DoS condition is created.

Once this buffer is full, the host can no longer process new TCP connection requests, even the legitimate ones. The attack disables the victim and its normal operations.

Figure 448. A TCP SYN flood



TCP full-connect attack

A TCP full-connect attack is an attack that has a valid source IP address and goes though the full TCP hand-shake process. The attacker uses real PCs with real IP addresses to generate a TCP full-connect attack. This is typically done using botnets. Sending TCP full-connect attacks from several botnets ties down server resources and creates a DoS condition. TCP full-connect usually is a DDoS attack launched from botnets in distributed systems.

A bot is defined as malicious software running on a compromised system that is designed to participate in a centrally managed network of compromised computers known as a botnet. Single botnets have been known to consist of over a million compromised computers, and are arguably the most significant threats to the global Internet today.

Multiple systems access a single Internet or service in a way that appears legitimate. This makes the detection of botnet-based DoS attacks difficult as it is hard to distinguish legitimate requests from those coming from a botnet. In the past, social networking site, Twitter is known to have experienced a DoS attack from a botnet.

TCP ACK/FIN attack

A TCP ACK/FIN attack takes place when the attacker sends a large volume of TCP ACK/FIN packets intentionally to the target host. This consumes bandwidth and creates a DoS condition.

TCP RST attack

A TCP RST attack takes place when the attacker sends a large volume of malicious, mimicked TCP RST packets aimed to prematurely terminate active TCP sessions.

In TCP RST attacks, the network is constantly monitored for TCP connection requests sent to the victim. As soon as such a request is found, the attacker sends a spoofed TCP reset packet to the victim and obliges it to terminate the TCP connection.

Consider the following example. Computer A crashes while a TCP connection is in progress. Ccomputer B, on the other end, interacting with computer A continues to send TCP packets since it does not know computer A has crashed. When computer A restarts, it receives packets from the pre-crash connection. Computer A has no context for these packets and sends a TCP reset to computer B. This reset lets computer B know that the connection is no longer working. The user on computer B tries another connection. However, a third computer or computers (DoS attackers) monitoring the TCP packets on the connection, might send premature forged or mimicked TCP reset packets to one or both endpoints to terminate active TCP connections.

This attack consumes system resources that receive, check, and discard the packets, thus causing a DoS condition.

DNS flood attack

Sending a flood of DNS requests to a server constitutes a DNS flood attack. Since DNS uses UDP, no hand-shake process is involved. A flood of DNS requests can tie down the resources of a DNS infrastructure and create a DoS condition.

DNS servers like other Internet resources are prone to DoS attacks. DNS uses UDP queries for name resolution; so a full circuit is never established (as contrasted with TCP), thus making DoS attacks difficult to trace and block. DNS flood works by sending a flood of rapid DNS requests from multiple machines, thereby giving the server more traffic than it can handle and resulting in slower response time for legitimate requests.

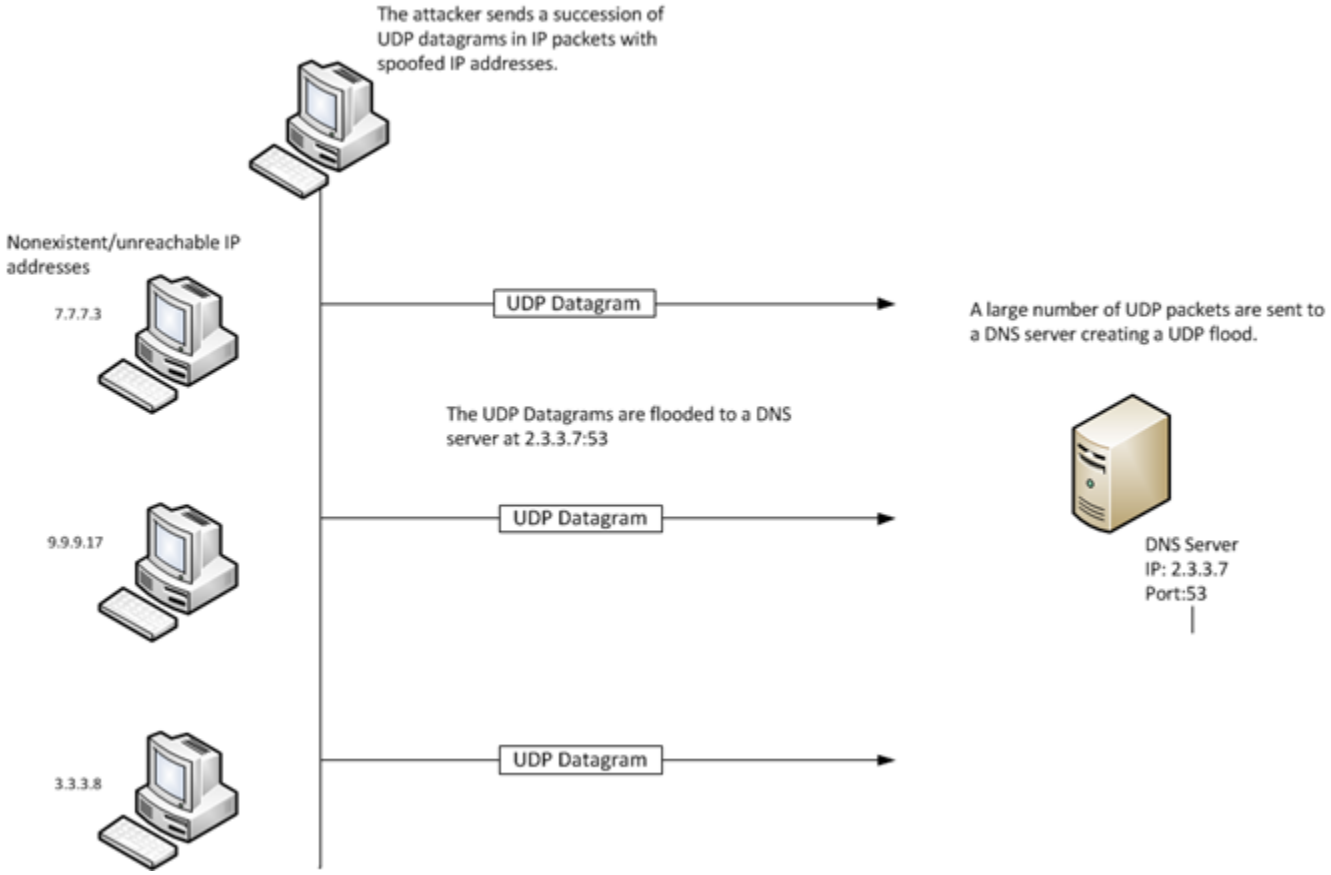
Consider the following example where a DNS flood is run from one machine and the DNS server queried from another machine. The attacking machine sends different types of DNS packets, each with a different spoofed source port to the target. To assess the impact of this attack on the victim's performance, the attacker first clears his local cache from another machine and then queries the target name server. Clearing the local cache ensures the resolver gets the information from the server and not locally. The attacker then stops the attack and queries the target name server once again from another machine, after clearing the cache. The queries during the attack and after the attack prove a significant performance impact on the victim server. If this attack was multiplied from a number of machines, the impact would be even greater.

UDP flood attack

Sending a flood of UDP attacks to a targeted system constitutes a UDP flood attack. When communication is established between two UDP services, an UDP flood attack is initiated by sending a large number of UDP packets to random ports of the targeted system. The targeted system is forced into sending many *Destination unreachable* UDP packets, thus consuming its resources and leading to DoS. As UDP does not require any connection setup procedure to transfer data, anyone with network connectivity can launch an attack; no account access is needed.

Another example of UDP flood is connecting a host's *chargen* service to the *echo* service on the same or another machine. All affected machines might be effectively taken out of service because of the excessively high number of packets produced. In addition, if two or more hosts are so engaged, the intervening network might also become congested and deny service to all hosts whose traffic traverse that network.

Figure 449. UDP flood



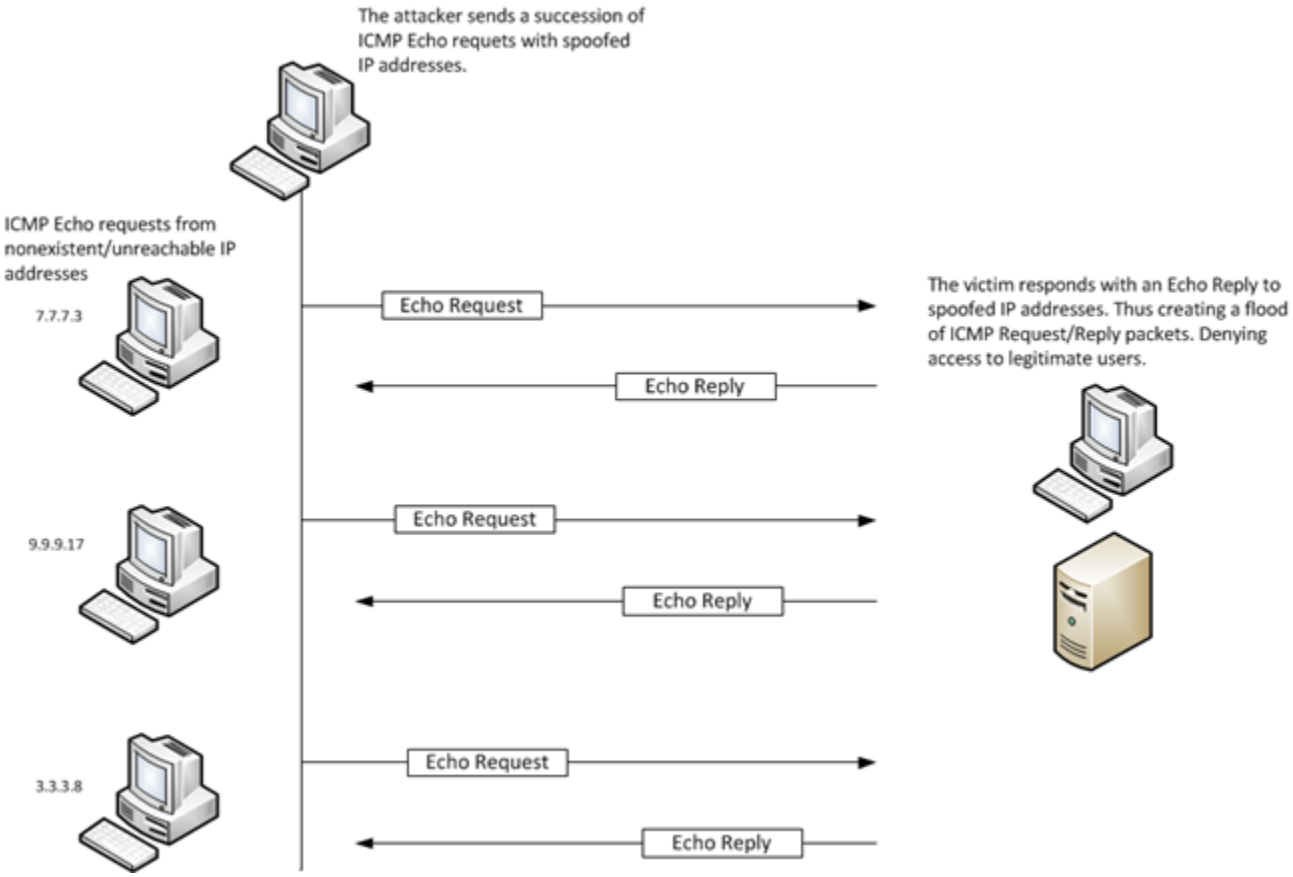
ICMP flood attack

This attack involves flooding the network with ICMP echo request or reply packets. A flood of echo requests to a target system makes the system busy responding to the requests. If there is a flood of reply packets, it is very likely that the remote attacker has forged an IP address from within your network and is sending ICMP echo request packets to another network. That network replies to the address in the requests, thus starting a request/reply flood between the two networks.

In such an attack, the attackers send large numbers of IP packets with the source address forged to appear to be the address of the victim. The network's bandwidth is consumed, preventing legitimate packets from getting through to their destination.

A variation of an ICMP flood is also known as the smurf attack, named after a program capable of generating this attack. In such an attack, an ICMP echo request is sent to a broadcast network address, acting as an amplifying agent. The source address of the victim is spoofed. The result is a flood of replies from that network which takes the victim's network down.

Figure 450. ICMP flood attack



Non TCP/UDP/ICMP flood attack

This involves flooding the network with packets other than TCP, UDP, or ICMP. Packets involved in this attack might include IPSec and malformed IP packets (such as IP with bad checksums and inconsistent length).

Application level flood

Attackers often use expensive queries to slow down servers causing resource exhaustion and denial of service. Traditional denial of service detection techniques might not identify the attack because the volume of queries can be too small.

Vulnerability-based DoS attacks

Unlike volume-based DoS attacks, vulnerability-based or exploit-based DoS attacks are generally single requests that can result in a DoS condition. Vulnerability-based DoS attacks exploit vulnerabilities in the network and its systems. The following table describes some well-known examples of vulnerability-based DoS.

Attack name	Description
TearDrop attack	This involves fragmented ICMP packets with overlaps among the fragments. Such fragments cause certain implementations of the IP stack to crash or go into an infinite loop, thus leading to a DoS condition.
Ping of Death attack	This involves sending packets that exceed the maximum authorized size (65,536 bytes) to a system with a vulnerable TCP/IP stack, causing it to crash.
Land attack	This involves using IP-address spoofing with the same IP address and port number in the source and destination fields, causing vulnerable systems to become unstable.

Distributed Denial-of-Service attack tools

DDoS attacks can be launched by using tools that are built to generate DDoS attacks.

There are many DDoS attack tools. Some well-known tools are listed below:

- **Trinoo** — It is an attack tool that installs agent programs on compromised hosts and uses the agents through a master program to attack one Trinoo, or more target hosts by flooding them with UDP packets. Communication between the master and agents is password protected.
- **Tribal Flood Network (TFN)** — TFN uses an attack approach similar to Trinoo, can generate multiple attacks, and use spoofed IP addresses. ICMP echo request flood, TCP SYN flood, and UDP flood are some of the attacks that can be launched by TFN.
- **TFN2K** — TFN2K is an advanced version of TFN with features that makes it more difficult to detect. TFN2K uses multiple protocols including UDP, TCP, and ICMP.
- **Stacheldraht** — Stacheldraht, which means *barbed wire* in German, has features that include those of Trinoo and TFN. Stacheldraht has features like encrypted communication between agents and the master program.
- **Shaft** — Shaft is a tool similar to Trinoo that can launch packet-flooding attacks.
- **Trinity** — Trinity is a flood attack tool that uses chat programs such as Internet Relay Chat (IRC).
- **MStream** — MStream is a tool based on *stream.c* attack in which access to the handler is password protected.

DoS attack detection mechanism

Trellix IPS provides an integrated hardware and software solution, which delivers comprehensive protection from known, first strike (unknown), DoS, and DDoS attacks from several hundred Mbps to multi-gigabit speeds.

The Trellix IPS architecture employs a combination of threshold-based, self-learning, profile-based detection techniques to detect DoS and DDoS attacks.

With threshold-based detection, you can configure data traffic limits to ensure your servers will not become unavailable due to overload. These thresholds are selected based on coverage of different DDoS attacks and on the availability of statistics that will help the users to configure them. Meanwhile, self-learning methodologies enable Trellix IPS to study the patterns of network usage and traffic over time; thus understanding the wide variety of lawful, though unusual, usage patterns that might occur during legitimate network operations. The learning algorithm takes into account sudden bursts that is common in all network traffic, and differentiates it from the real onset of DDoS traffic. In addition to learning the intensity behavior, it also learns the

correlational behavior of different types of packets, which reliably captures TCP/IP protocol behavior, route configuration, and so on. Highly accurate DoS detection techniques are essential because popular websites and networks do experience legitimate and sometimes unexpected traffic surges during external events, or for a particularly compelling new program, service, or application.

The combination of these two techniques yields the highest accuracy of detection for the full spectrum of DoS and DDoS attacks, when hundreds or even thousands of hosts are co-opted by a malicious programmer to strike against a single victim.

Once DoS/DDoS attacks have been detected, Trellix IPS offers methods to block various types of DoS Attacks.

Volume-based DoS attack detection

Trellix IPS detects volume-based DoS attacks through threshold-based and statistical anomaly-based (learning-based) methods. Often a combination of these two methods is used.

Threshold-based mode

In the threshold mode, the Sensor monitors the network traffic for packet floods, such as too many IP fragments, transmitting through from a source to a destination as detected within a Sensor interface or subinterface. When configuring the DoS policy or customizing at the interface or subinterface level, you must specify the count and interval rate in seconds, for the threshold attacks you want to detect. The Sensor sends an alert, if configured to do so in the DoS policy, when the traffic exceeds the customized thresholds for an enabled attack. You can also enable a notification for an attack if it warrants special attention. For threshold-based attacks, a Sensor monitors both inbound and outbound traffic.

This method requires that you to fully understand your typical traffic pattern to pick *good* threshold values; otherwise it can produce false alarms due to traffic fluctuations, such as *flash crowds* — for example, everyone logging on the network at 9 a.m.— or other legitimate increased traffic.

NOTE

Although default values are provided for thresholds and intervals, you must configure the actual thresholds and intervals for each DoS threshold mode attack you want to detect. Customization of DoS thresholds works best after researching the current levels to be defended for each DoS threshold. This helps you to determine exactly what counts and intervals are best for protecting your network.

The threshold method involves specifying the count and interval thresholds while configuring a DoS policy in the Manager. When the threshold is crossed, the DoS attack is detected.

Threshold value and interval can be customized in the Manager for threshold attacks, such as:

- Inbound Link Utilization (Bytes/Sec) Too High
- Too Many Inbound ICMP Packets
- Too Many Inbound IP Fragments
- Too Many Inbound Large ICMP packets
- Too Many Inbound Large UDP packets
- Too Many Inbound Rejected TCP Packets

- Too Many Inbound TCP Connections
- Too Many Inbound TCP SYNs
- Too Many Inbound UDP Packets

Learning-based (statistical anomaly-based) mode

A new Sensor runs for its first 48 hours in learning mode. After 48 hours, the Sensor automatically changes to detection mode, having established a baseline of the *normal* traffic pattern for the network, or a long-term profile. The assumption is that there are no DoS attacks during those first 48 hours.

After moving to detection mode, the Sensor continues to gather statistical data and update its long-term profile. In this way, the long-term profile evolves with the network. The Sensor also builds short time profiles with a time window of a few minutes.

Learning mode profiles can be managed in the **DoS Data Management** page of the Manager. DoS profile learning can be rebuilt (re-learned) or reloaded at this level. To access the **DoS Data Management** page:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Troubleshooting → Denial of Service → **Data Management.**

Subinterfaces and individual CIDR hosts within a VLAN tag or CIDR block can be created and protected against DoS attacks with specific learning-mode settings. This is useful in preventing a server in your DMZ or other location from being shutdown by a DoS attack. A separate profile is created for each resource.

The statistical method uses statistical data gathered over a time window to create normal short-term and long-term profiles. DoS attacks are detected when there are anomalies between the traffic pattern in normal profiles and network traffic. Statistical anomalies in traffic are monitored by the Sensor with reference to learned data on normal traffic.

The Sensor uses the following checks and counter checks to ensure accuracy of detection:

- Counter profile contamination
- Source IP address classification

NOTE

If there is a change in the routing scheme, Trellix recommends instructing the Sensor to relearn the network so that it can create a new baseline.

Countering profile contamination

The goal behind the long-term profile is to define normal traffic levels. The Sensor can identify anomalous spikes in traffic with reference to the defined normal levels. The Sensor also uses the gathered statistical data to calculate short-term profiles, that is statistical data averaged over a time window of a few minutes.

If a short-term profile, which includes DoS attack data, is used to update the long-term profile, it contaminates the long-term profile. Trellix IPS uses the following counter measures to help prevent contamination:

- When in detection mode, the Sensor temporarily ceases updating the long-term profile if too many statistical anomalies are seen over a short period.
- The Sensor uses percentile measure. A few large spikes in the short-term data will probably upset a simple average, but are less likely to affect a percentile measure. For example, imagine a group of four students taking an exam with percentile measure ranges of 0-29, 30-49, 50-69 and 70-100 for judging the effectiveness of the exam. Let us say three of the students receive grades of 95 percent, 93 percent, and 92 percent and the fourth receives a grade of 0 percent. The average score is only 70 percent but three of the four students are still in the 70-100 range. The teacher can therefore use the percentile ranges as a valid measure for judging the effectiveness of the exam.

Source IP address classification

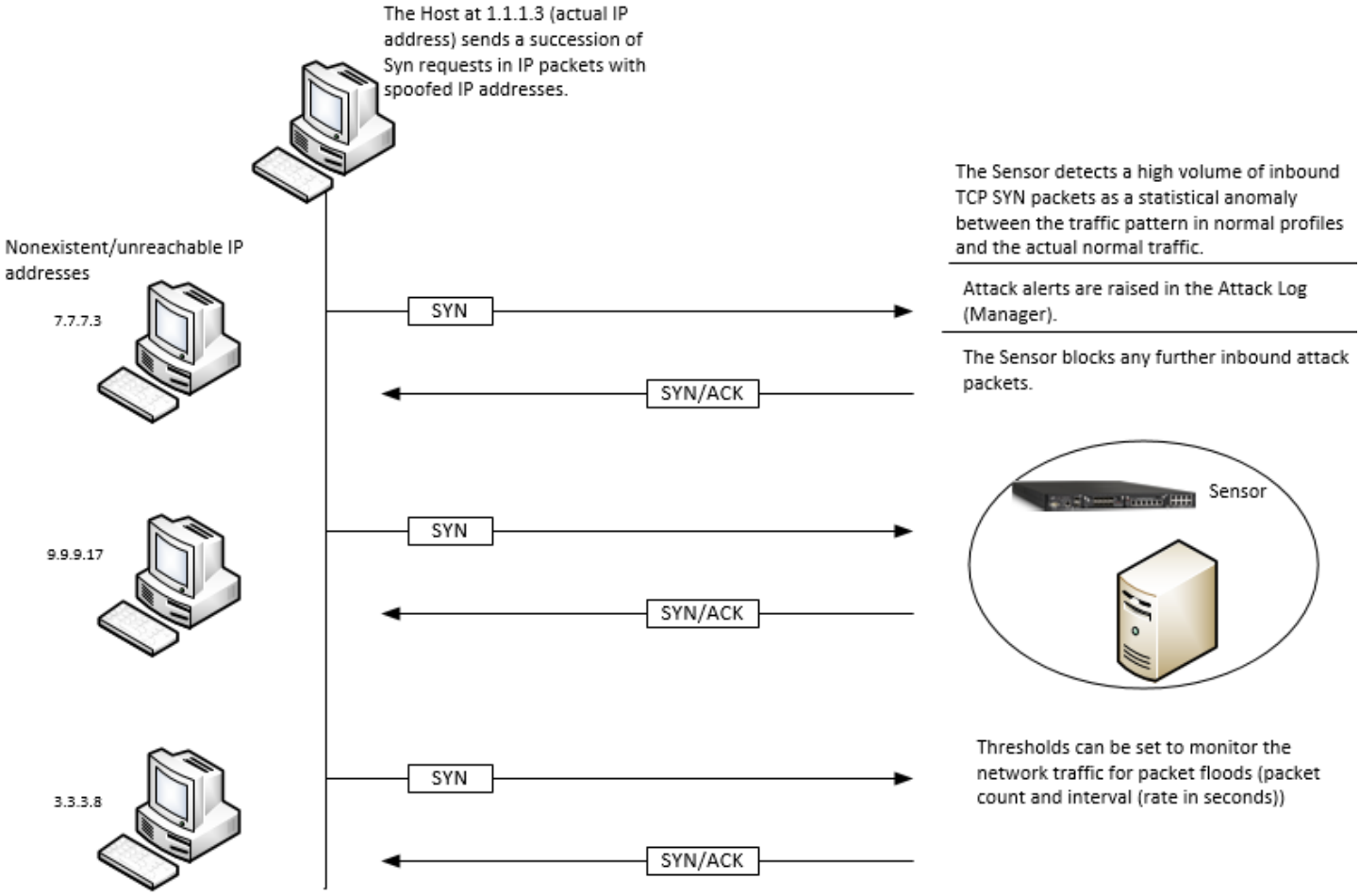
The Sensor builds unique source IP address profiles; one profile for each tracked packet type in each direction.

How the DoS attack detection mechanism works

The Sensor is deployed inline in the host network; having established the baseline of the *normal* traffic pattern for the network in the first 48 hours of deployment (learning mode), and built a long-term profile for the statistical data on the SYN segments in the TCP connection. Consider that the Sensor is in the detection mode. It continues to gather statistical data and update its long-term profile. The learning mode uses statistical data gathered over a time window to create normal short-term and long-term profiles.

Consider the following example of a TCP SYN flood attack.

Figure 451. TCP SYN flood attack



- There is a flood of TCP SYN packets using spoofed IP addresses to the target host.
- The Sensor detects a high volume of inbound TCP SYN packets. This upsurge in the packets is regarded as an anomaly between the traffic pattern in normal profiles and the actual network traffic. The Sensor monitors statistical anomalies in traffic with reference to learned data (DoS profiles) on normal traffic. Refer to the section [Statistical anomaly]. The following is a sample DoS profile. Bin 2 indicates a lower percentage of long-term traffic when compared to the short term, and hence traffic is blocked.

  ```
  0: 0.0.0.0/6 AS=1.563% LT=49.969% ST=100.00% stR=1.000
  1: 128.0.0.0/2 AS=25.000% LT=0.021% ST=0.00% stR=0.000
  *2: 64.0.0.0/2 AS=25.000% LT=1.615% ST=100.00% ltR=2357.098 stR=148966.400
  3: 192.0.0.0/2 AS=25.000% LT=0.021% ST=0.00% stR=0.000
  4: 32.0.0.0/3 AS=12.500% LT=0.000% ST=0.00% stR=0.000
  5: 16.0.0.0/4 AS=6.250% LT=0.000% ST=0.00% stR=0.000
  6: 8.0.0.0/5 AS=3.125% LT=0.000% ST=0.00% stR=0.000
  7: 4.0.0.0/6 AS=0.000% LT=11.752% ST=0.00% ltR=16885.654 stR=0.000
  ```

- Based on the configured DoS policy settings, alerts are raised in the Attack Log. The learning mode can be customized on the Manager for inbound, outbound, or bidirectional traffic. The severity of the attack and Sensor response is also configurable. Refer to the section [Configure the Learning mode].
- The alerts in the Attack Log display the SYN packet rate data relating to the violated learning mode measure, the violated measure's packet rate for the last minute when the alert was raised, and the ranges of IP addresses, both source and destination, that were involved in the DoS attack.
- The Sensor blocks any further inbound attack packets. The blocking of packets can be enabled while configuring the learning mode or from the Attack Log once an alert is raised.
- Additionally, thresholds can also be set to monitor the number of packets per second.

  In the threshold mode, the Sensor monitors the network traffic for packet floods, transmitting through from a source to a destination as detected within a Sensor interface or subinterface. When configuring the DoS policy or customizing at the interface or subinterface level, the count and interval (rate in seconds) for the threshold attacks to be detected.

NOTE

Combining threshold and learning methods greatly improves reliability of detection.

DoS policy applies to inbound, outbound, and bidirectional traffic. Inbound traffic is that traffic received on the port designated as *outside* (that is, originating from outside the network) in inline or tap mode. Typically, inbound traffic is destined to the protected network, such as an enterprise intranet.

Outbound traffic is that traffic sent by a system in your intranet, and is on the port designated as *inside* (that is, originating from inside the network) in inline or tap mode.

When GTI is enabled, IP Reputation is applicable only for inbound connections. When GTI is enabled and Connection Limiting rules are configured, you can block the malicious traffic received on the inbound connections. For example, you can deploy a Sensor in front of a web server, and enable GTI along with Connection Limiting policies and Advanced Malware policies to limit access to the server and prevent DoS attacks.

Configure the threshold mode

The threshold method provides administrators with a way to trigger alerts if a preconfigured traffic volume threshold is exceeded.

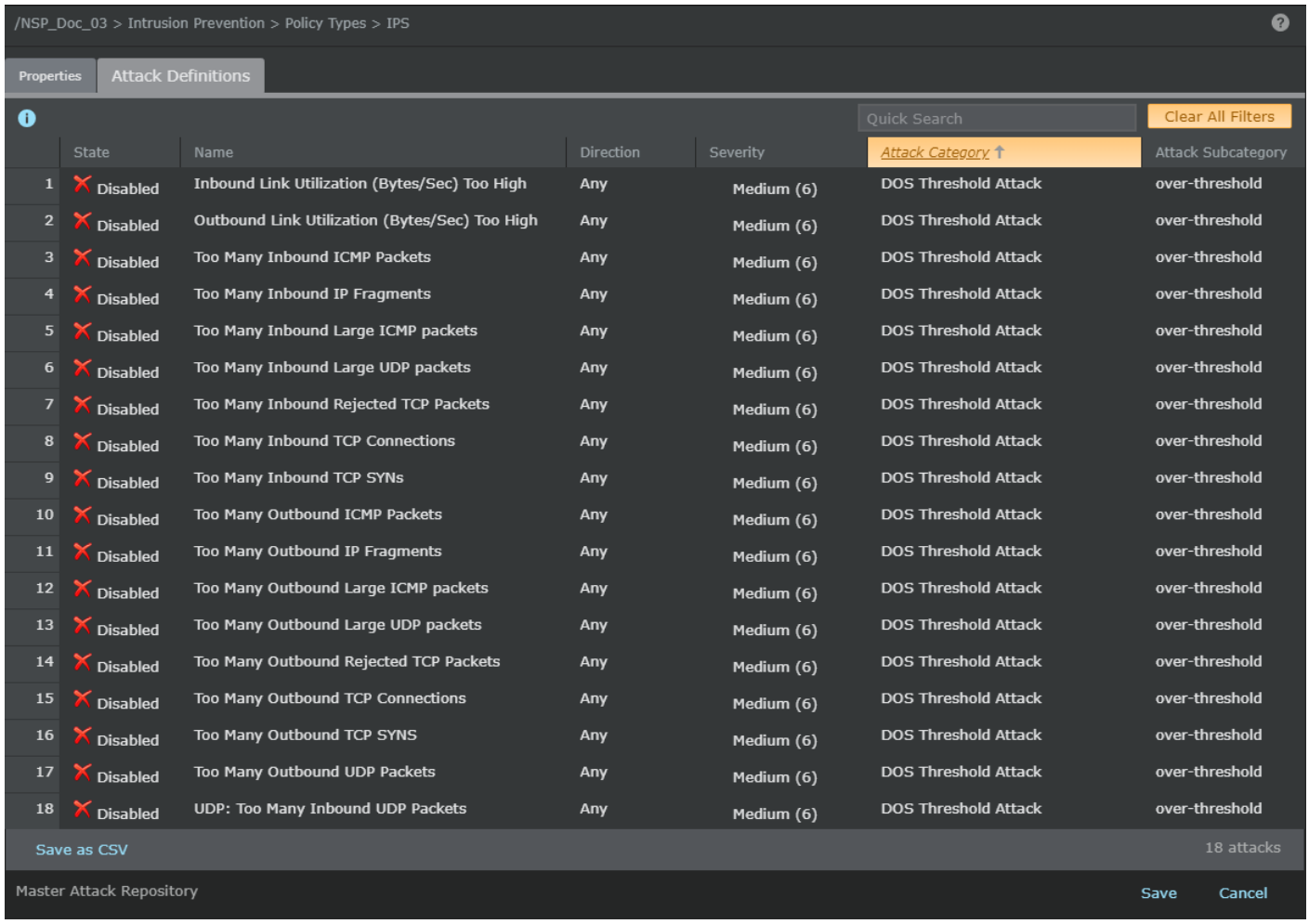
The key to successfully using thresholds is to have an understanding of the normal traffic levels on the network. In most cases, an external device such as a sniffer is used to baseline the network, and the initial levels are set according to that data. Once a baseline has been established, the administrator can enable the relevant threshold for an attack and configure each with values that make sense for a particular network.

Follow the tasks below to set threshold values for DoS attack definitions using **Master Attack Repository**. Note that the changes that you make through **Master Attack Repository** feature affects the corresponding attack definitions in all the IPS policies.

1. Click the **Policy** tab.
2. Select the root admin domain from the **Domain** drop-down list.
3. Select Intrusion Prevention → Policy Types → **IPS**.

   The **IPS** page is displayed.

4. Double-click on the row of **Master Attack Repository** column. The **Attack Definitions** page of the **Master Attack Repository** is displayed.



	State	Name	Direction	Severity	Attack Category	Attack Subcategory
1	Disabled	Inbound Link Utilization (Bytes/Sec) Too High	Any	Medium (6)	DOS Threshold Attack	over-threshold
2	Disabled	Outbound Link Utilization (Bytes/Sec) Too High	Any	Medium (6)	DOS Threshold Attack	over-threshold
3	Disabled	Too Many Inbound ICMP Packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
4	Disabled	Too Many Inbound IP Fragments	Any	Medium (6)	DOS Threshold Attack	over-threshold
5	Disabled	Too Many Inbound Large ICMP packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
6	Disabled	Too Many Inbound Large UDP packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
7	Disabled	Too Many Inbound Rejected TCP Packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
8	Disabled	Too Many Inbound TCP Connections	Any	Medium (6)	DOS Threshold Attack	over-threshold
9	Disabled	Too Many Inbound TCP SYNs	Any	Medium (6)	DOS Threshold Attack	over-threshold
10	Disabled	Too Many Outbound ICMP Packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
11	Disabled	Too Many Outbound IP Fragments	Any	Medium (6)	DOS Threshold Attack	over-threshold
12	Disabled	Too Many Outbound Large ICMP packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
13	Disabled	Too Many Outbound Large UDP packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
14	Disabled	Too Many Outbound Rejected TCP Packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
15	Disabled	Too Many Outbound TCP Connections	Any	Medium (6)	DOS Threshold Attack	over-threshold
16	Disabled	Too Many Outbound TCP SYNS	Any	Medium (6)	DOS Threshold Attack	over-threshold
17	Disabled	Too Many Outbound UDP Packets	Any	Medium (6)	DOS Threshold Attack	over-threshold
18	Disabled	UDP: Too Many Inbound UDP Packets	Any	Medium (6)	DOS Threshold Attack	over-threshold

5. Double-click on the row of the attack category **DOS Threshold attack**.

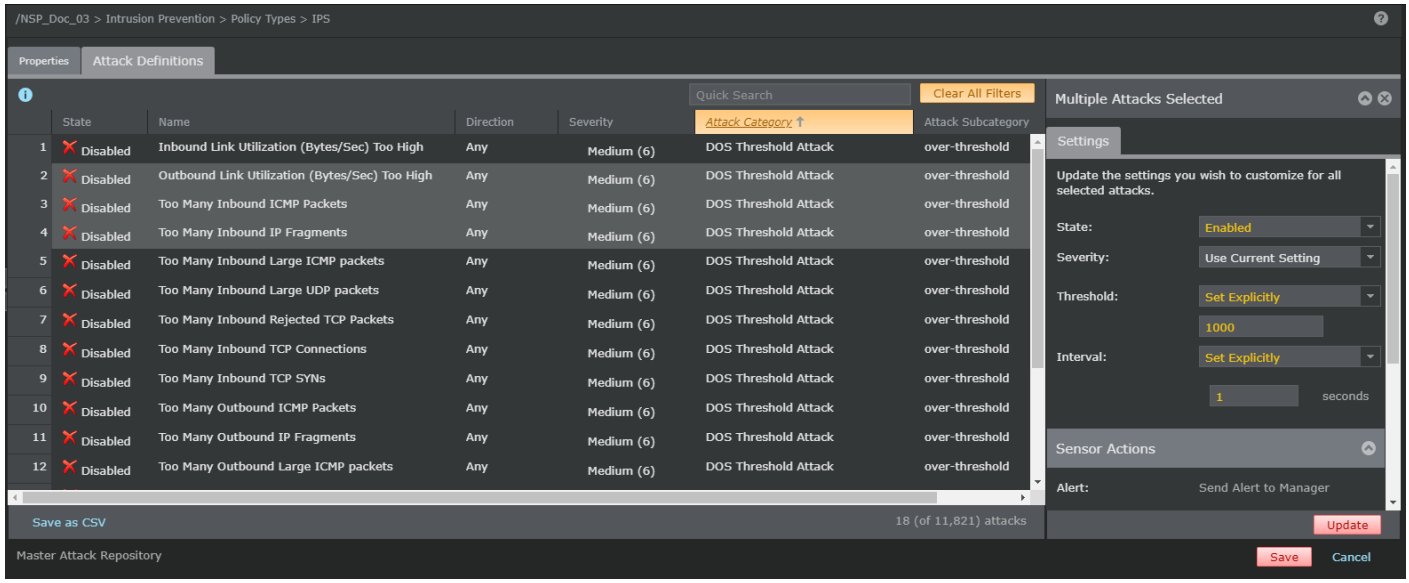
   The **Settings** tab for the attack is displayed.

6. In the **Threshold** field set the attack threshold.

   For example, for the **Threshold** and **Interval** fields, select **Set Explicitly** and type 1000 and 1 respectively as values for these selections. Such a setting will enable an alert to be sent if a Sensor sees 1000 or more Inbound Link Utilization within a 1-second interval.

7. In the **Attack Definitions** page, select the required DoS Threshold attack from the list.

   Press **Shift** key (for continuous selection) or press **Ctrl** key (for discontinuous selection) and then select the attacks.



> **NOTE**
>
> The Threshold method can be configured only to send alerts; traffic meeting or exceeding the pre-defined thresholds cannot be blocked.

The Threshold method is used mostly for troubleshooting. The administrator might want to be notified if bandwidth utilization goes above a pre-defined limit.

In contrast to the threshold method, the learning-based method automatically establishes a baseline and if configured, can alert or block if that baseline is exceeded in such a way that it constitutes an attack.

8. After you complete the customizing the attacks, click **Update** to update the changes to the attacks. Click **Save** and deploy the configuration changes to the corresponding Sensors.

Configure the learning mode

You can customize the learning mode for DoS attack definitions using **Master Attack Repository.** Note that the changes that you make through **Master Attack Repository** feature affects the corresponding attack definitions in all the IPS policies. You can also edit DoS attack definitions per IPS policy.

Steps:

1. Click the **Policy** tab.
2. Select the root admin domain from the **Domain** drop-down list.
3. Select Intrusion Prevention → Policy Types → **IPS**.
4. Double-click on the row of the IPS policy you want to edit. The **Attack Definitions** page of the **Master Attack Repository** is displayed.
5. Double-click on the row of the attack category **DOS Learning attack**.

   The **Settings** tab for the attack is displayed.

6. In the **Severity** checkbox select a different severity level from the drop-down list, if you want the attack to be of a higher or lesser priority.
7. In the **Manager Actions** area, select the options in the following fields:

   To customize notifications,

   - **Syslog**
   - **SNMP**
   - **E-Mail**
   - **Pager**
   - **Script**
   - **Auto-Acknowledgement Alert**
8. After you complete the customizing the attacks, click **Update**. Click **Save** and deploy the configuration changes to the corresponding Sensors.

Alerts for DoS attacks

DoS related alerts are raised when a Sensor detects volume-based DoS attacks, vulnerability based DoS attacks, and attacks by DDoS attack tools. Trellix IPS uses attack signatures to detect communication between many known DDoS attack tools, and also to detect vulnerability-based attacks. Alerts are raised in the Attack Log when such attacks are detected.

In the case of volume-based attacks, Sensor looks for statistical anomalies in short-term and long-term profiles. The Sensor compares the short-term profile against the long-term profile. If there is a significant difference in the traffic levels, an alert is generated, and the Sensor blocks traffic with statistical anomalies if configured to do so.

The Sensor raises an alert when it detects one of two varieties of statistical anomalies:

- Categorical or *imbalance* anomalies
- Volume anomalies

NOTE

Statistical anomalies are the result of an attack when the long-term profiles accurately reflect the normal traffic for a given network. However variations in network traffic, due interventions such as changes in the routing scheme, can cause anomalies. In such cases you must rebuild the profile from scratch using the **Rebuild the DoS Profiles (start the learning process from scratch)** option in the **DoS Data Management** page.

Follow these steps to go to the **DoS Data Management** page:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Troubleshooting → Denial of Service → **Data Management.**

Categorical (or imbalance) anomalies

Certain types of packets are intrinsically related. Without ICMP echo reply, for example, ICMP echo request would be of little use. Similarly, without FIN and RST, you would be able to begin a TCP connection, but not end it.

Trellix IPS detects two types of categorical anomalies:

- ICMP echo anomalies (echo request and echo reply)
- TCP control segment anomalies (SYN, SYN ACK, FIN, and RST)

Trellix IPS records the distribution of these types of packets in its long-term profile. A significant change in the distribution of these packet types in the short term is a reliable indication of malicious behavior.

For example, Network A might have 50 echo replies for every 50 echo requests, whereas Network B might have only 40 replies for 60 requests. In this case, the distribution would be 50 percent / 50 percent and 40 percent / 60 percent, respectively. In practice, distribution differs from network to network, but usually maintains a relatively consistent average over an extended period. A sudden and drastic (short-term) change in the distribution of ICMP echo packets or TCP control packets is historically indicative of malicious behavior, if not an outright attack.

Volume anomalies

Trellix IPS also tracks rapid increases in the volume, or intensity, of traffic.

To simplify the analysis of volume anomalies, the self-learning algorithm categorizes all packets into one of the following eight types:

- IP fragment
- ICMP echo (request and reply)
- All other ICMP
- UDP
- TCP SYN and FIN
- TCP RST
- Non-TCP/UDP/ICMP

Percentiles

One of the methods that the Trellix IPS uses to deal with volume anomalies is to establish thresholds based on packet rate and burst size for different packet types. Changes to these established thresholds indicate threats and are dealt with accordingly.

To measure volume changes over time, Trellix IPS establishes two percentiles for each of the packet types. For a given packet type, the Sensor looks at the distribution of the following:

- Short-term packet rate
- Traffic burst size

The Sensor analyzes these distributions to establish thresholds that the short-term averages must not typically exceed. For example, Trellix IPS might determine that, for a given packet type, 95 percent of the short-term profiles averaged a rate of X packets per second or fewer, and a packet size of Y bytes or smaller. When the average rate exceeds X packets per second and the pocket size exceeds Y bytes, Trellix IPS analyzes the significance of change. If the change is significant and matched a threat perception, an alert is raised.

NOTE

Only one statistical anomaly alert is sent per attack every two minutes.

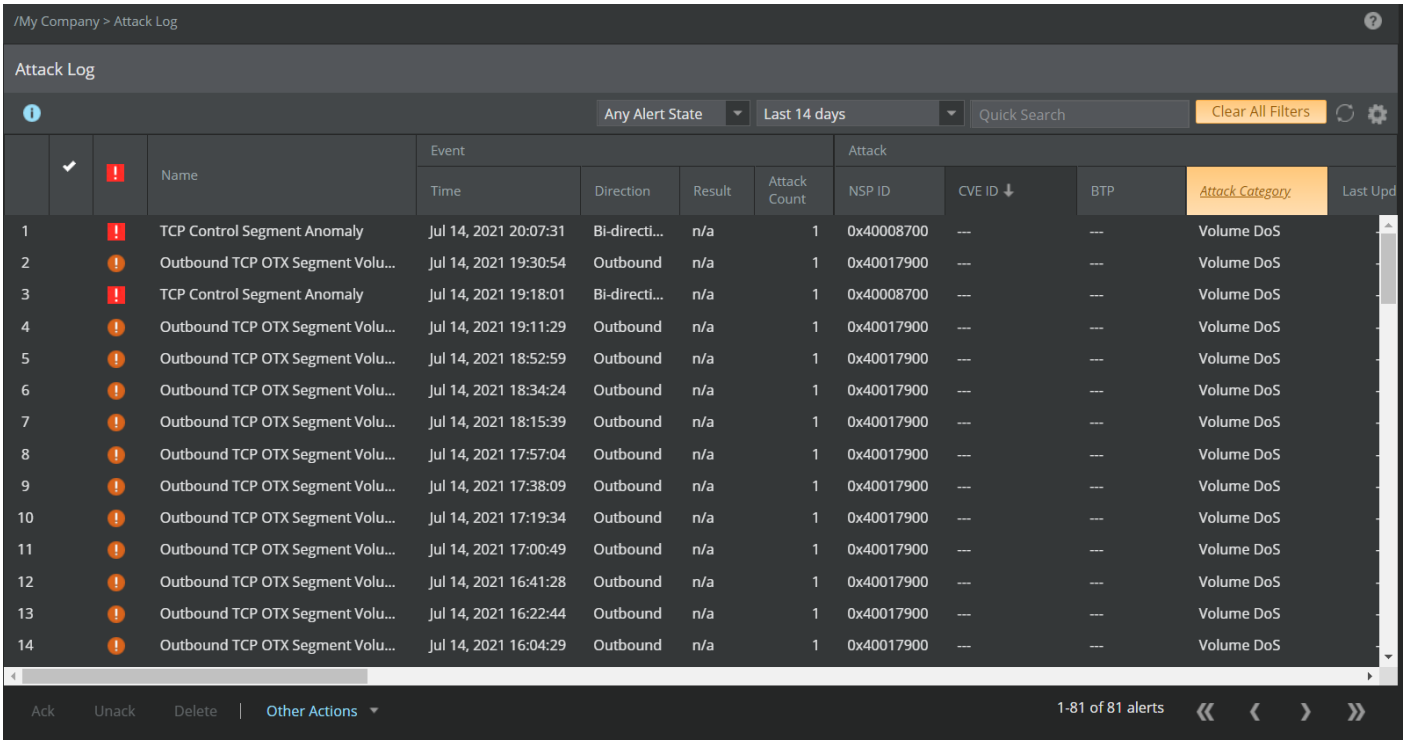
Alert details

DoS related alerts are listed in the **Attack Log** page under the **Analysis** tab. DoS related alerts are either alerts relating to threshold violations or statistical attacks.

- Simple threshold alerts are those in violation of DoS threshold mode settings.
- Statistical attacks are those in violation of DoS learning mode settings.

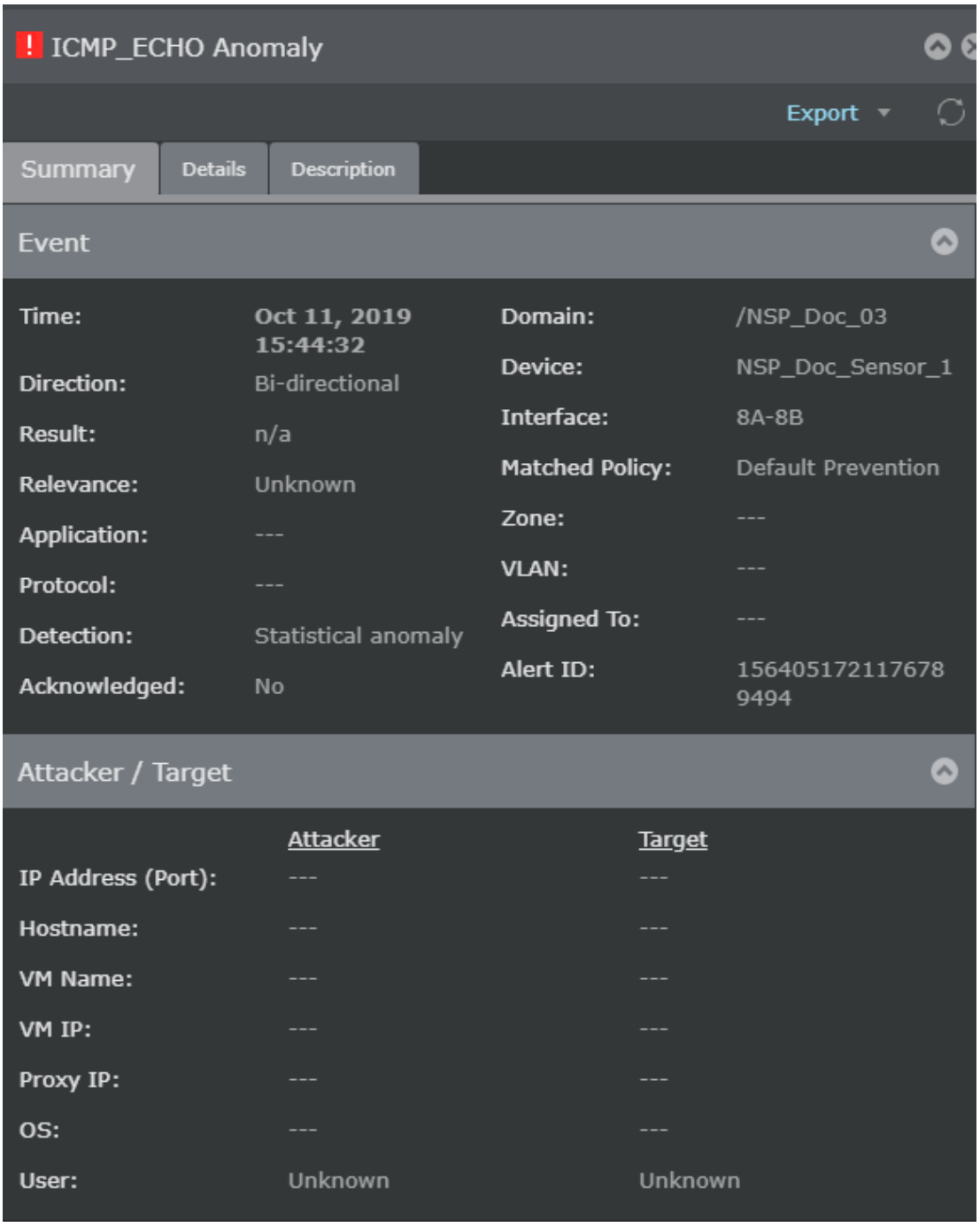
To view details of a specific alert, double-click an alert. The alert details panel opens on the right side.

Figure 452. All Alerts page of Attack Log



The alert details panel gives a clearer picture of the key information related to the attack. The information can then be used to augment your policy settings and/or to initiate a response action.

Figure 453. Alert Details panel



The alert details panel displays alert details that are specific to a type of attack. Hence, the information displayed varies from one type of attack to another.

Some alert details relating to DoS attacks are:

Simple Threshold Alerts

Simple Threshold alerts are those in violation of DoS threshold mode settings.

- **Threshold ID** — This ID corresponds to where this threshold attack is listed in the **DoS Threshold Mode** catalog.
- **Observed Value** — The number of times the instance occurred. Since an alert was sent, this value is larger than the threshold value.
- **Threshold Duration** — The time limit value set within DoS threshold mode customization for the attack instance. This complements the **Threshold Value**. This duration is run to the end to capture all instances within the time limit rather than stopping after the first value over the threshold is detected.
- **Threshold Value** — The limit set within DoS threshold mode customization for the attack instance and complements the **Threshold Duration**.

Statistical Alerts

Statistical attacks are those in violation of DoS learning mode settings.

- **Packet Rate Distribution** — Displays bar graphs with packet rate data related to the violated learning mode measure. The violated measures are displayed with the corresponding packet rate over the last 1 minute. The graph displays the learned long-term rate (as established by the DoS profiling process) against recent activity, or short-term rate. The short-term rate is for the most recent 1 minute approximately. When the short-term rate is greater than the long-term rate and exceeds the specified response sensitivity (low, medium, or high - from **DoS Learning Mode** settings), an alert is generated.

  The percentage value represents the percentage of all traffic for which the noted measure accounted. For example, if the *normal* percentage for IP fragments is approximately 2.5 percent, then IP fragments make up 2.5 percent of all traffic through the monitored segment. If the percentage of fragmented IP packets in the traffic during an interval was significantly higher than the established long-term percentage, it indicates an IP fragment flood attack.

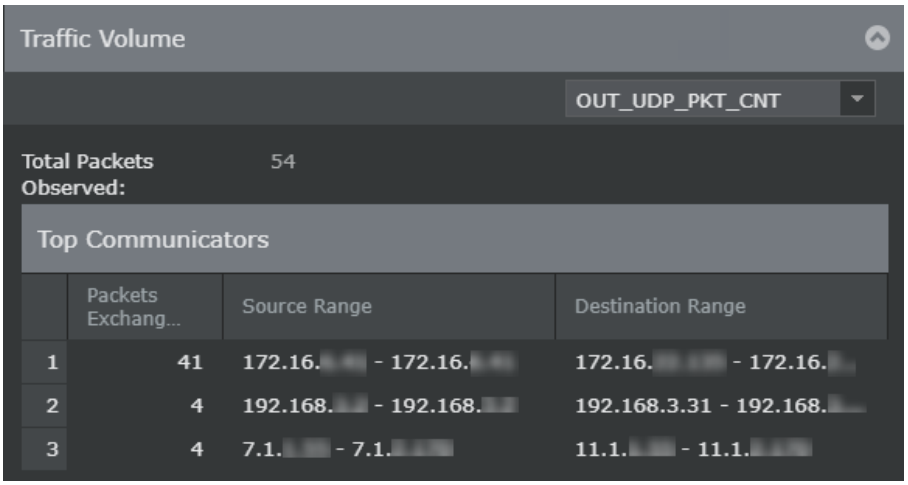
Figure 454. DoS packet rate distribution graph

- **Packet Rate** — Displays the violated measure's packet rate for the last minute when the alert was raised. Packet rates are shown in five-second intervals.

Figure 455. DoS packet rate graph

- **Traffic Volume** — Displays the ranges of IP addresses, both source and destination that were involved in the DoS attack.
  - The packet type and total number of packets that were a part of the attack are also noted.
  - **Total Packets Observed** is the number of DoS packets seen from the given source and destination range. This includes both benign and attacking packets. All packets of various packet types, such as TCP SYN, destined to the particular network are displayed in the alert.

Figure 456. DoS IP range dialog



The first DoS alert shows packets counts received for 5 seconds before the alert. The subsequent suppressed alerts show the number of packets received since the last alert.

If you choose to drop packets, the Sensor drops only the *bad* packets. Thus, the Sensor might not always drop packets from what is determined as a *good* source IP address.

Blocking DoS attacks

A Sensor can be configured to block traffic when statistical anomalies occur. Blocking DoS traffic is more involved than blocking normal exploits because the source is often unclear. For example, the success of a distributed attack might depend on the quantity of compromised hosts generating traffic together, rather than a single host generating a significant volume on its own. This complicates the blocking process because a Sensor cannot merely block hosts that individually generate large volumes of traffic. Moreover, DoS attack tools typically generate traffic with spoofed IP addresses, so attempting to block them gains nothing and wastes resources.

Instead, Trellix IPS classifies source IP addresses as IP profiles to differentiate between good and bad hosts. It then uses these IP profiles to determine a blocking scheme for the Sensor .

NOTE

- The Sensor must be in detection mode to detect and block attacks.
- You can block DoS attacks only when the Sensor is deployed in the inline mode.

How blocking works for DoS attack traffic

A DoS policy applies to inbound, outbound, and bidirectional traffic. *Inbound* traffic is that traffic received on the port marked *outside*, that is, originating from outside the network, in inline mode. Typically inbound traffic is destined to the protected network, such as an enterprise intranet. *Outbound* traffic is that traffic sent from a system in your intranet, and is on the port marked *inside,* that is, originating from inside the network, in inline mode.

Bidirectional attacks reflect changes in the distribution of ECHO requests and replies in both inbound and outbound. For example, if the Sensor normally sees 50 percent inbound replies and 50 percent outbound replies, but then the distribution changes to 70 percent / 30 percent, the change might raise an alert.

NOTE

There are also learning mode attacks that do not have a directional association, specifically ICMP ECHO anomaly and TCP control anomaly. Note that Sensors can only raise an alert in case of ICMP echo anomaly and TCP control anomaly attacks but cannot block them, even when in inline mode.

The Sensor applies the outbound or inbound DoS policy depending on the traffic direction, which is determined through the Sensor cabling and port configuration. The *drop attack packets* response action must be enabled by traffic type (protocol type) within the DoS policy.

When the Sensor detects an attack traffic condition, the block action will persist until the attack condition ends and will repeat whenever the attack condition is present.

Block DoS attacks in Attack Log

All attacks, except ICMP echo anomaly and TCP control anomaly, can be configured to be blocked from within the Attack Log.

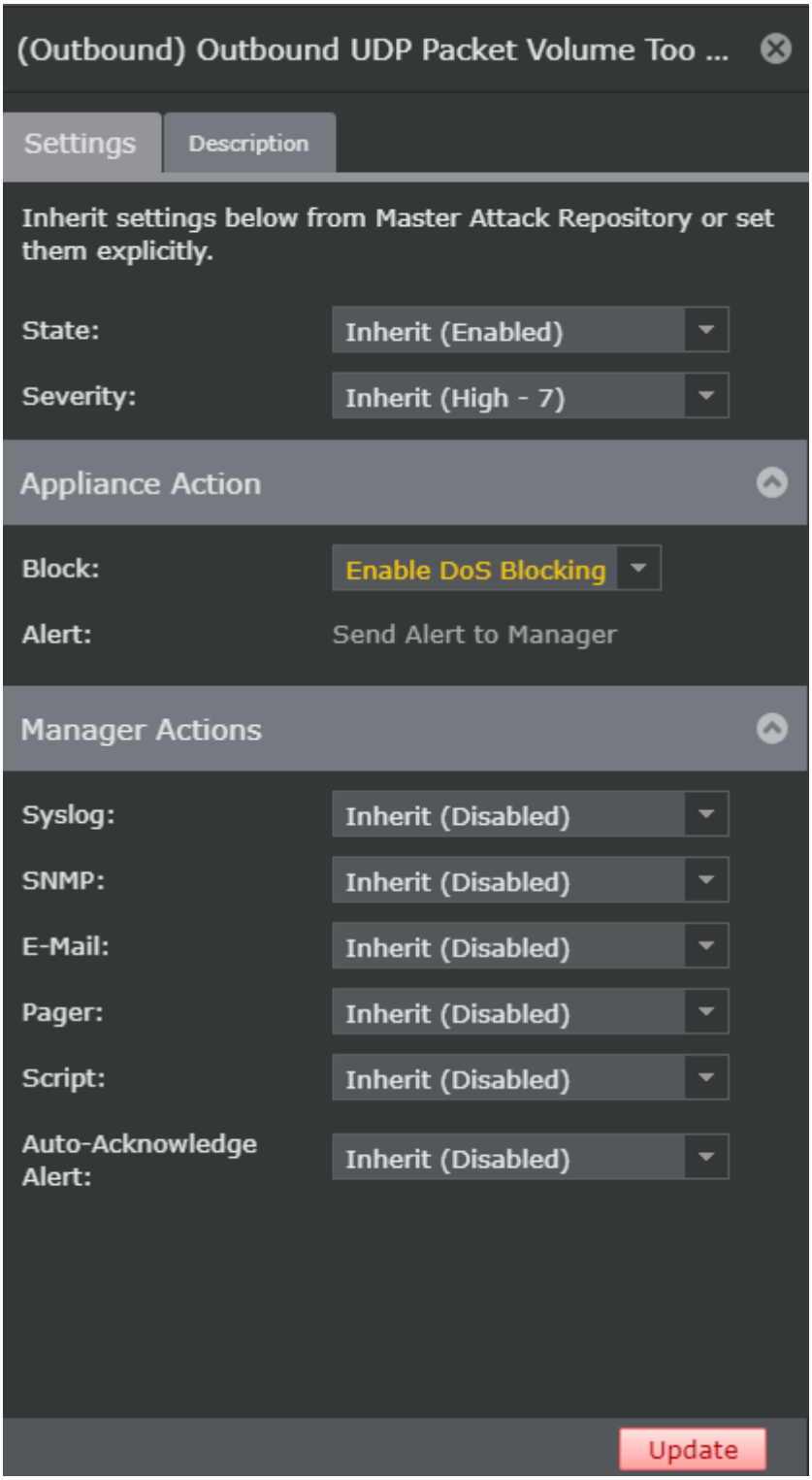
Steps:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the DoS alert for which you want to enable blocking and click **Other Actions**.
3. Select **Update Policy**, and click **(Domain IPS) /<Admin Domain Name>/<Policy Name>** or **(Interface IPS) /<Admin Domain Name>/<Device Name>/<Interface>**.

   The **<Attack Name>** panel opens.
4. Under the **Appliance Action** section, select **Enable DoS Blocking** for **Block**.
5. Click **Update**.

   The respective policy is updated with the DoS blocking for the attack selected.

Figure 457. Blocking attacks in Attack Log



Verify blocked DoS attacks using Attack Log

Alerts reflecting a DoS condition continue to be sent to the Attack Log for the duration of the attack. In the Attack Log, the result status displays **DoS Blocking Activated** for the attack condition.

To apply **DoS Blocking Activated** filter to the **Results** column, do the following:

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Click on drop-down icon in the **Results** column, and select Filters → **DoS Blocking Activated**.

Exploit-based DoS attack detection

Exploit or vulnerability-based attacks are manifested in attack signatures, which Trellix IPS uses to detect specific exploit attacks.

A signature is a profile of an attack. Detection of specific attacks is possible through signatures. Trellix IPS also uses exploit signatures for DoS attacks that are not caused by traditional means such as volume overload. For example, the *HTTP: Microsoft IIS...SLASH... DenialofService* exploit identifies a single request that prevents older IIS servers from responding to clients until they are restarted.

The Sensor uses signatures to perform different levels of traffic processing and analysis. Trellix IPS signatures operate on a framework of flows, protocol parsing, and packet searches to detect vulnerability-based DoS attacks and attacks using DDoS attack tools. For example, Trellix IPS's detection mechanisms enable a signature to identify every HTTP traffic flow, every HTTP traffic flow using the GET mechanism, every HTTP traffic flow using GET with `/cgi-bin/calendar.pl` as the path and even every GET with that path and a parameter named `month` with a value of `February`.

Trellix IPS supports the aggregation of multiple signatures into every attack. Each signature within an attack can be more or less specific to identify everything from generic network activity that affects a given platform in a particular way to a specific piece of code that has very specific and identifiable effects. Based on their specificity and severity, signatures are assigned different confidence and severity values.

Flows

At the highest level, the Trellix IPS addresses UDP and TCP traffic based on the concept of a flow. Flows are defined by their protocol (either UDP or TCP), source and destination ports, and IP addresses of their endpoints. UDP does not contain the concept of *state* that TCP does, so the Sensor implements a timer-based flow context for UDP traffic. After dividing traffic into flows, the Sensor makes use of port mapping, or in the case of traffic running on non-standard ports, intelligent protocol identification, to pass each flow to the appropriate protocol parsing mechanism.

It is also worth noting that Trellix IPS provides you with the ability to specify whether your signature will look at the complete flow, one direction of the flow, or restrict itself to data occurring within single packets of the flow. Precise control of this detection window is necessary for accurate detection of attacks.

Protocol parsing specifications

Protocol specifications (Trellix IPS's protocol parsing mechanisms) parse through network flows to validate traffic and divide it into protocol fields, which might then be actively tested against Trellix IPS-supplied attack definitions or Custom Attack Definitions. By dividing protocol traffic into the appropriate fields, Trellix IPS can perform matches against the most specific field or sub-field pertinent to an effective attack, thus supporting signatures with very low false-positive rates. Since the parsing process is fully stateful, it allows detection of anomalies in the protocol's behavior. Additionally, this parsing makes it possible to

provide an additional benefit to signature writers in the form of qualifiers. Qualifiers are tests that are embodied in the name of a particular protocol field. For example, rather than specifying that an HTTP request method must be **GET**, the Trellix IPS system allows the use of **http-get-req-uri** as the name of the field, saving the requirement of providing that test in the signature, and the Sensor from having to perform an extra pattern match.

Packet searches

Traffic flows that are not identified as belonging to any particular protocol are passed to the Packet Search Protocol Specification Engine for further parsing. Trellix IPS presents each direction of the flow to Trellix IPS-defined attacks and to any Custom Attack Definitions. Tests against packet search traffic typically take the form of specific ordered pattern matches to prevent false positives and performance problems.

Where signatures fit

Signatures tie together elements of flows, protocol parsing, and packet search framework to derive specific *fingerprints* for network traffic from smaller building blocks. In essence, signatures are like DNA tests. They can identify both specific people and relatives of that person. In the intrusion-detection case, the relatives might be a collection of buffer overflow attacks against a certain piece of software, and the particular person would be a specific piece of exploit code.

While the two are not greatly different, Trellix IPS adopts a convention of differentiating between anomaly-based attack signatures (not to be confused with anomaly-based detection for DoS attacks) and signatures pertaining to a specific attack. The main difference is that while anomaly-based signatures examine the network for unexpected or non-conforming behavior, signatures pertaining to specific attacks will often look for a very particular indicator, such as a flag with a particular value, or a specific string's presence. Signature-based anomaly attacks know what to expect in normal traffic, and trigger when they get something else. Normal attack signatures look for specific misbehavior. When defining attacks to detect and protect from vulnerabilities, a blended set of signatures are often defined which check for behavioral anomalies as well as specific exploit strings. Using this mechanism, all possible attempts to exploit the vulnerability can be detected.

Layer 7 DoS protection for web servers

Trellix IPS provides protection from DoS attacks at various TCP/IP levels, including DoS protection at layer 3, connection-limiting policies at layer 4, and web server protection at layer 7.

A layer 7 DoS attack is difficult to detect when compared to DoS attacks at other layers because such an attack is often perpetrated through the use of an upsurge of HTTP requests, where the attacker looks like a legitimate connection, and is therefore passed on to the web server. There are multiple HTTP requests at the same time, and these legitimate HTTP requests are mixed in with the attack.

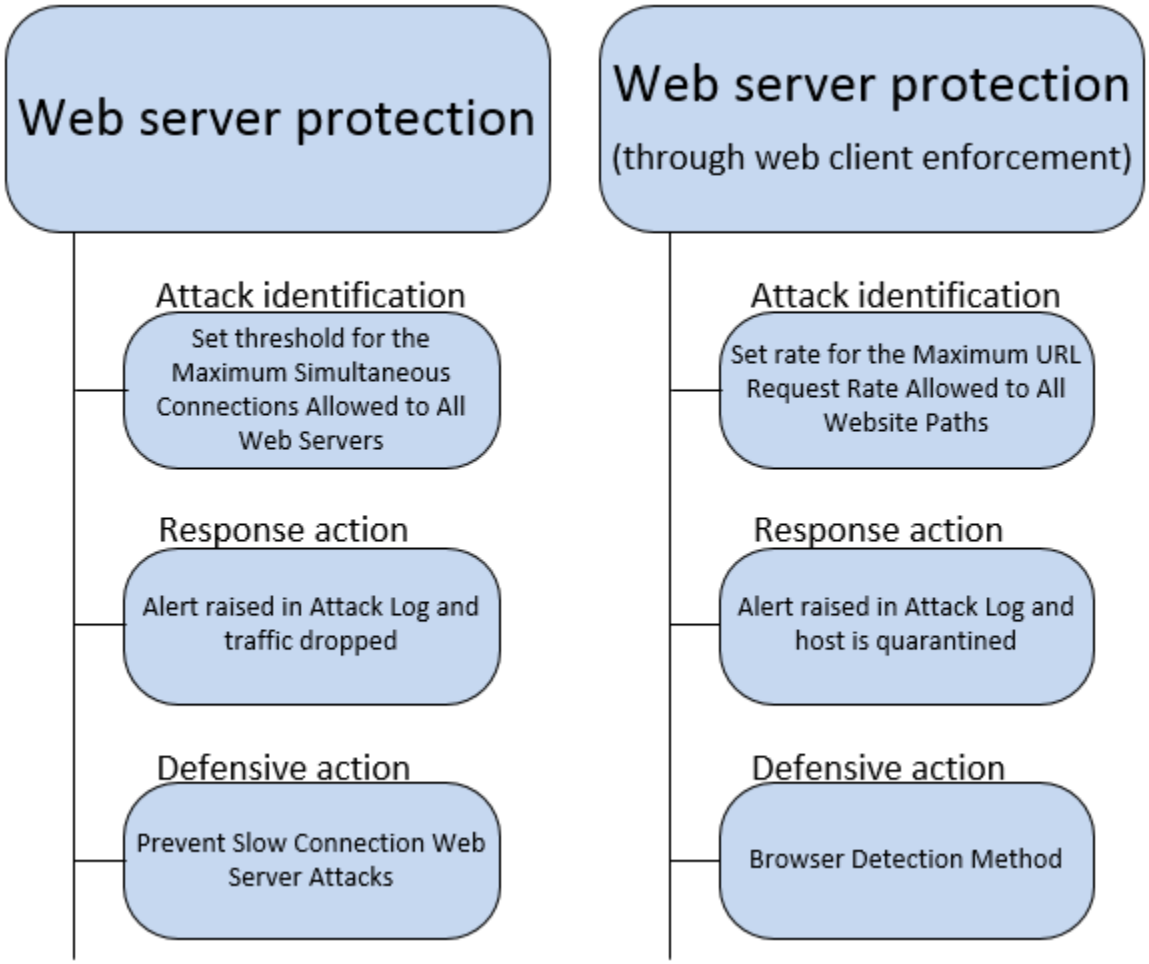
With the growth in bots, HTTP application-level DoS attacks have become more common and even more difficult to detect. bots can be programmed to launch DoS attacks against a particular domain or URL, and these requests appear as normal HTTP requests originating from a browser, thereby making it difficult to differentiate bot traffic from normal traffic.

Multiple types of DoS attacks range from attacking web server infrastructures to targeting a particular URL/path resulting in huge file downloads and slowing down the web servers. Since bot traffic pattern is different depending on the botnet technology and the attack classes, Trellix IPS aims at allowing users to customize different response actions based on configured thresholds.

Defending against Layer 7 DoS attacks usually involves a mechanism to configure different HTTP response actions based on traffic volume anomaly. Trellix IPS deals with DoS attacks in layer 7 by employing the HTTP challenge-response approach based

on the traffic volume anomaly with different threshold methods. A three-pronged protection approach is used consisting of attack identification, response action, and the defensive action.

Figure 458. DoS protection at layer 7



You can view the status of L7 DoS using the **`show l7ddosstat`** command.

Using the Manager, the layer 7 DoS protection for web servers allows you to configure inspection options on the web server side as well as the web client side.

This feature is available on the following Sensor models:

- NS9500, NS9300, NS9200, and NS9100
- NS7600, NS7500, NS7350, NS7250, and NS7150
- NS7300, NS7200, and NS7100
- NS5200 and NS5100
- NS3600, NS3500, NS3200 and NS3100

Web server protection settings

The Sensor provides the ability to define threshold values to limit the maximum simultaneous connections to web servers, minimizing connection-based DoS attacks on your network. The number of active HTTP connections coming to the server that are less than or equal to the defined threshold value are allowed, whereas the connections exceeding the threshold are dropped.

The connections to the web servers are limited based on the defined threshold value. The threshold value is defined as maximum simultaneous connections.

After the threshold is defined, the Sensor limits the maximum connections based on the configured values. An alert is sent each time the connections exceed the defined threshold value and excess connections are dropped. This ensures that the web servers do not become unavailable due to overload.

The Sensor provides you with a defense mechanism to recover from a DoS attack. You can configure the option to prevent slow connection web server attacks.

The logic behind this option is that the HTTP protocol is designed for short connections. Five minutes is assumed to be a long time and a connection alive for more than five minutes is assumed to be a slow connection. When this option is enabled, the Sensor sends a TCP reset to clear the 10 percent (of the configured threshold) of the oldest active connections, alive for more than five minutes. This option works only when your web resources are under a DoS attack. For example, if the configured threshold is 10000, then 1000 active connections are closed. If the Sensor finds that there are only 500 connections alive for more than five minutes, then only 500 are closed. This leads to some amount of recovery from a connection flood. The client receives no indication of a connection drop. It appears to be a connection timeout.

NOTE

Trellix recommends that if your environment requires long term HTTP connections, do not use this option.

To understand the working of the DoS inspection options on the web server side, consider the following scenario where the Sensor is deployed in the inline mode.

- Configure the threshold for **Maximum Simultaneous Connections Allowed to All Web Servers** with a value of 10000.
- Enable **Slow-Connection Attack Prevention**.
- Push the configuration changes to the Sensor.
- The Sensor monitors the connection requests to the web servers and detects an upsurge of connection requests. Once the connection threshold is reached, the Sensor raises an alert. All connections beyond the configured threshold of 10000 are dropped. You can view the alert details in the Attack Log.
- The Sensor scans the active connections and identifies the connections alive for more than five minutes as slow.
- The Sensor sends a TCP reset to clear 10 percent of the oldest active connections, that is, 1000 active connections.
- Use the **`show l7ddosstat`** command to verify the connection details.

Web client protection settings

You can use the URL rate limiting technique to control the rate of URL requests to all website paths per second per IP address. The Sensor permits rate limiting of URL requests by limiting the number of the requests that go to the web. URL requests that are less than or equal to the specified rate are allowed, if the requests exceed the configured rate, an alert is raised.

You can configure to protect specific websites or apply protection to all websites. When you configure specific websites to protect against DoS attacks, the Sensor considers only those HTTP requests that contain these paths. Specifying paths optimizes the performance of the feature.

The Sensor provides you with a defense mechanism to detect the web client browser. You can use the browser detection method. This option mitigates DoS attacks originated from bots. With this option, you can send a challenge back to the user to determine if the HTTP requests are originating from valid browsers or bots. You can configure an HTML or a Javascript challenge.

The logic behind this option is that bots have limited browser functionalities. When the Sensor sends a challenge, the browser should send a legitimate response. If the response is legitimate, it is assumed that the request is originating from a valid browser. The Sensor processes the response and communicates back to the server.

If the request originated from bots, they might not understand the challenge sent by the Trellix IPS and drop the connection request. When this happens, the Sensor quarantines the host.

To understand the working of the DoS inspection options on the web client side, consider the following scenario where the Sensor is deployed in the inline mode.

- Configure the threshold for **Maximum HTTP Requests/Second Allowed to Any Website Path** with a value of 50.
- Enable **Client Browser Detection**.
- Select the **Browser Detection Method** as **JavaScript Challenge**. JavaScript based challenge/response mechanism is used to detect a valid client browser.
- Select all **Website Paths to Protect**.
- Push the configuration changes to the Sensor.
- The Sensor monitors the URL requests to websites and detects an upsurge of URL requests. Once the URL request rate is reached, the Sensor raises an alert.
- Excess connections from the same host, exceeding any URL/second threshold, are validated by Javascript challenge mechanism. If the challenge response/refresh is successful, Sensor forwards the request to server. If the challenge response/refresh is unsuccessful by attempting 3 times, Sensor drops the request, resets the server and quarantines the host.
- Use the **`show l7ddosstat`** command to verify the counters.

Configure Web Server - Denial-of-Service Protection at the admin domain node and interface level

The Layer 7 DoS protection settings for web servers are disabled by default. You can configure the Layer 7 DoS inspection options in the parent domain at a global level and inherit these options in the child admin domains (interfaces and subinterfaces). You can modify the inherited settings at the child admin domains. You can also modify the setting at the interface level.

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Navigate to Intrusion Prevention → Policy Types → **Inspection Options**.
4. To create a new policy, click  . To edit an already existing policy, double click on the policy. If you are creating a new policy, proceed to step 5. If you are editing an already existing policy, proceed to step 6.

   The following substeps have to be followed when configuring Layer 7 DoS protection at an interface level:

   a. In the **Policy** tab, after selecting the **Domain**, navigate to Intrusion Prevention → **Policy Manager**.

   b. On the **Interface** tab, double-click the interface to enable Layer 7 DoS protection.

The **<Device name/Interface>** panel opens.

c. In the **Inspection Options** section, select the policy from the **Policy** drop down list.

To create a new policy, click the + icon or click the ✎ icon to edit an already assigned policy.

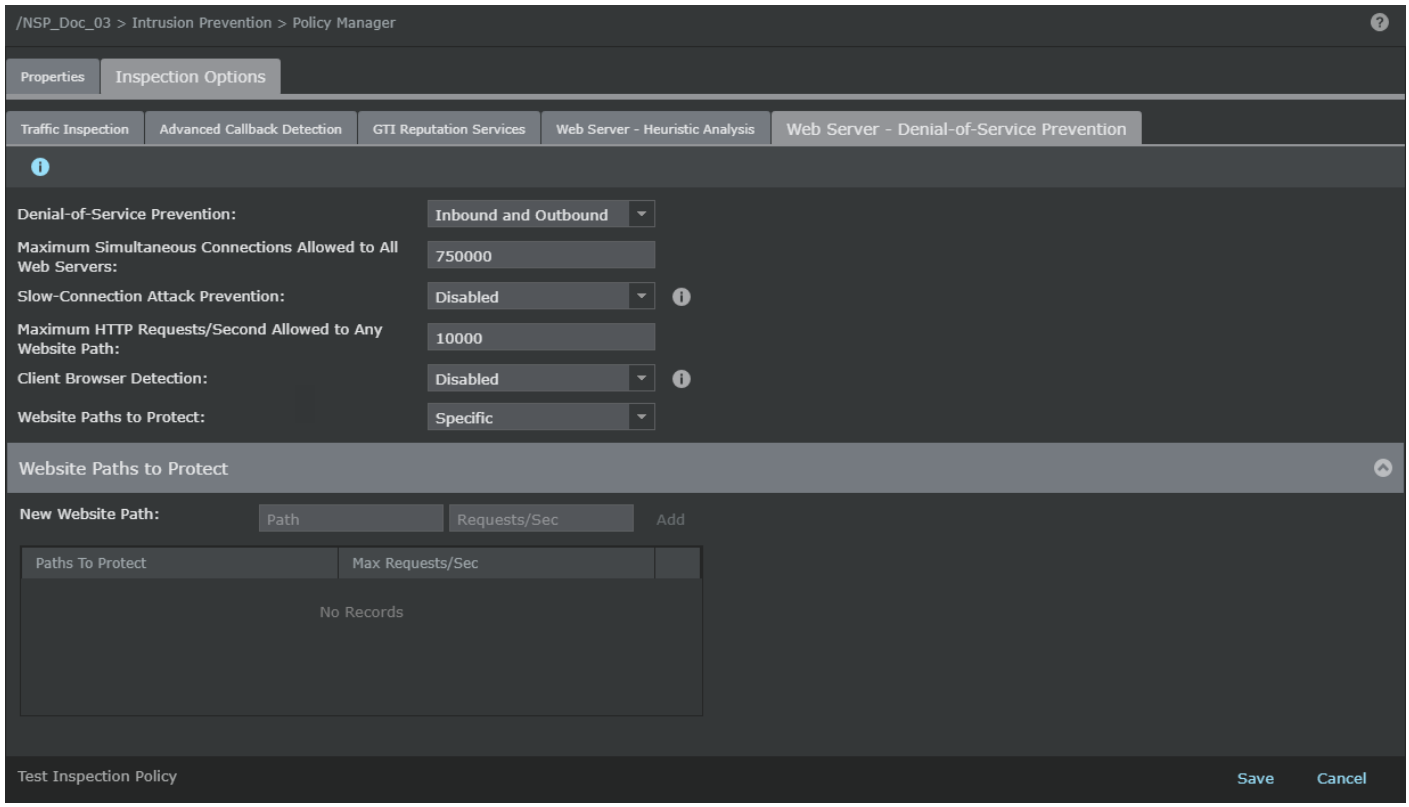
You can also assign a policy to an interface by selecting the **Prompt for assignment after save** option in the **Inspection Options** page.

If you are creating a new policy proceed to step 5. If you are editing an existing policy proceed to step 6.

5. The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and click **Next**.

The **Inspection Options** page opens.

Figure 459. Configuration of Web Server-Denial of Service



6. Configure the following DoS protection settings.

Table 52. Web Server - option definitions

Option	Definition
Denial-of-Service Prevention	Select the direction of traffic for which you would like to configure the DoS prevention.
Maximum Simultaneous Connections Allowed to All Web Servers	Specifies the threshold for maximum connections allowed to all web servers from a host. When connection limiting rules are created, whichever has smaller threshold raises an alert first.

Option	Definition
Slow-Connection Attack Prevention	Enable this option to close 10% of the oldest slow open connections. This option is disabled by default.
Maximum HTTP Requests/Second Allowed to Any Website Path	Specifies the threshold for maximum HTTP requests allowed to all website per second
Client Browser Detection	Enable this option to send a challenge back to the user to determine if the HTTP requests are originating from valid browsers or Bots.
Browser Detection Method	The detection methods use the challenge/response mechanism to detect a valid client browser. The options are **HTML Challenge** and **JavaScript Challenge**. This option is not supported in span and tap modes.
Website Paths to Protect	Specify website paths to which the HTTP requests are sent, to be protected. You can protect **All** or **Specific** paths. A maximum of 64 website paths per Sensor and 8 website paths per interface can be protected.
Website Paths to Protect	
New Website Path	Enter the website paths that you want to protect in **New Website Path** and click **Add**. For example, if you specify /trellix.com as a path, then the Sensor inspects only those requests that contain /trellix.com. • **Path** — Specify the website path you would like to protect. • **Requests/Second** — Specify the maximum HTTP requests allowed to the protected website path. • To delete a website path, hover over the path and click the **X** icon.

7. Click **Save**.

Manage DoS attack definitions for an interface and a subinterface

All of the provided IPS policies include protection against DoS attacks. There is no separate policy for DoS attacks. You can customize the DoS attack definitions just like you customize any of the exploit attack definitions in the IPS policies. For a given signature set, the same DoS attack definitions with the same configuration is included in all the pre-defined IPS policies. DoS customization is key to protecting a specific host or server from a concentrated DoS attack.

Trellix IPS enables extremely granular DoS protection: you can customize DoS attack definitions for the Sensor, interface, and sub-interface separately. At the Sensor level, customize the attack definitions in the baseline IPS policy. At the interface and subinterface levels, customize the local IPS policy. Therefore, you can apply customized DoS attack definitions that is exclusive for a given VLAN or CIDR traffic for a specific interface.

Customize DoS attack definitions for an interface or subinterface

At the interface and subinterface levels, the DoS attack definitions are inherited from the IPS policy applied at the Sensor level. This includes the DoS learning attack definitions as well as the DoS threshold attack definitions. Any customization in the assigned IPS policy applies automatically at the interface and subinterface levels. You can further customize these attack definitions in the **Interface-Specific Customization** section exclusively for the interface or subinterface. Just like any other customization in an IPS policy, these are applicable only to that interface or subinterface. Also, note that the customization done at an interface is not inherited by the corresponding subinterfaces, unlike the customization at the Sensor, which are inherited at the interfaces and subinterfaces.

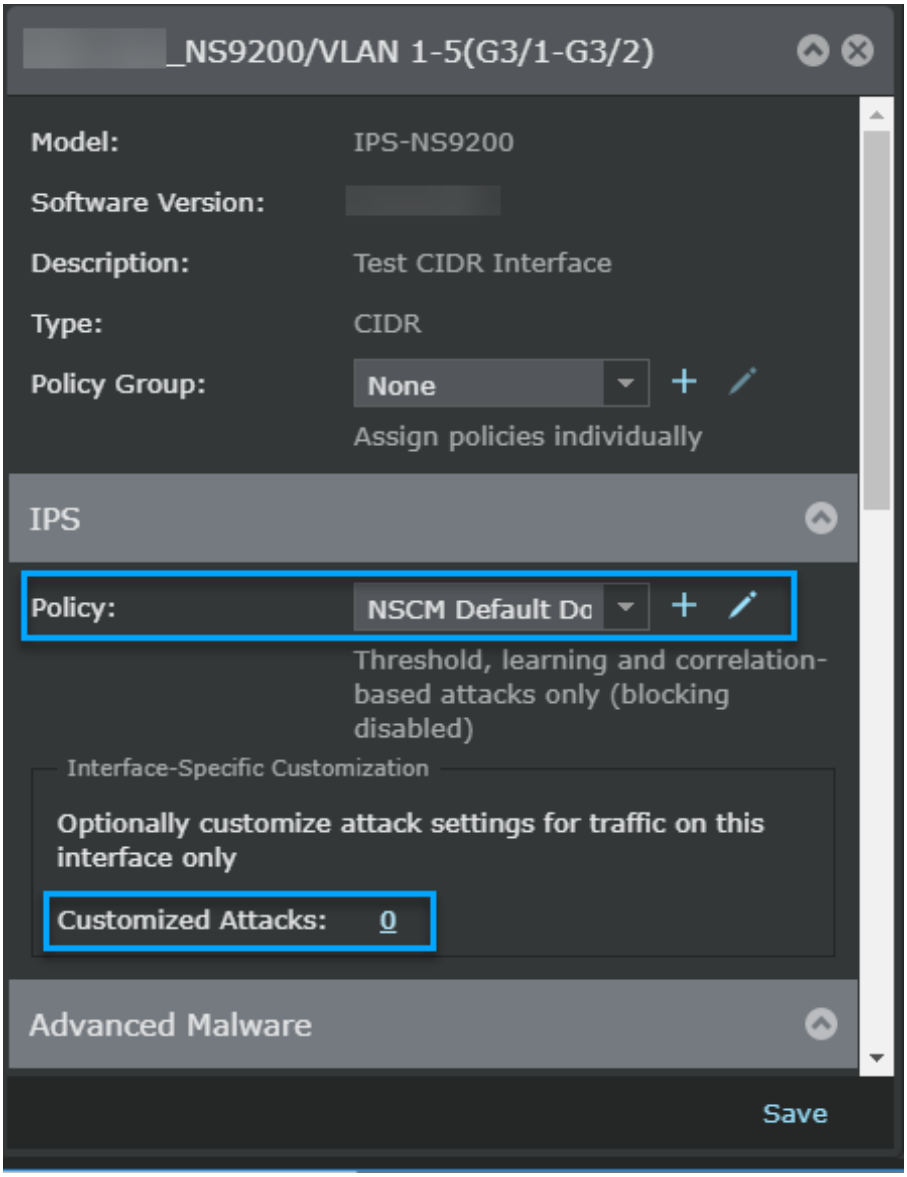
The process of customizing attack definitions at interfaces and subinterfaces are similar.

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Navigate to Intrusion Prevention → **Policy Manager**
4. Double-click the interface to which you would like to customize the DoS learning attack.

   The **<Device Name/Interface>** panel opens on the right side.

   Under the **IPS** section, you can view the applied IPS policy.

Figure 460. The applied IPS policy

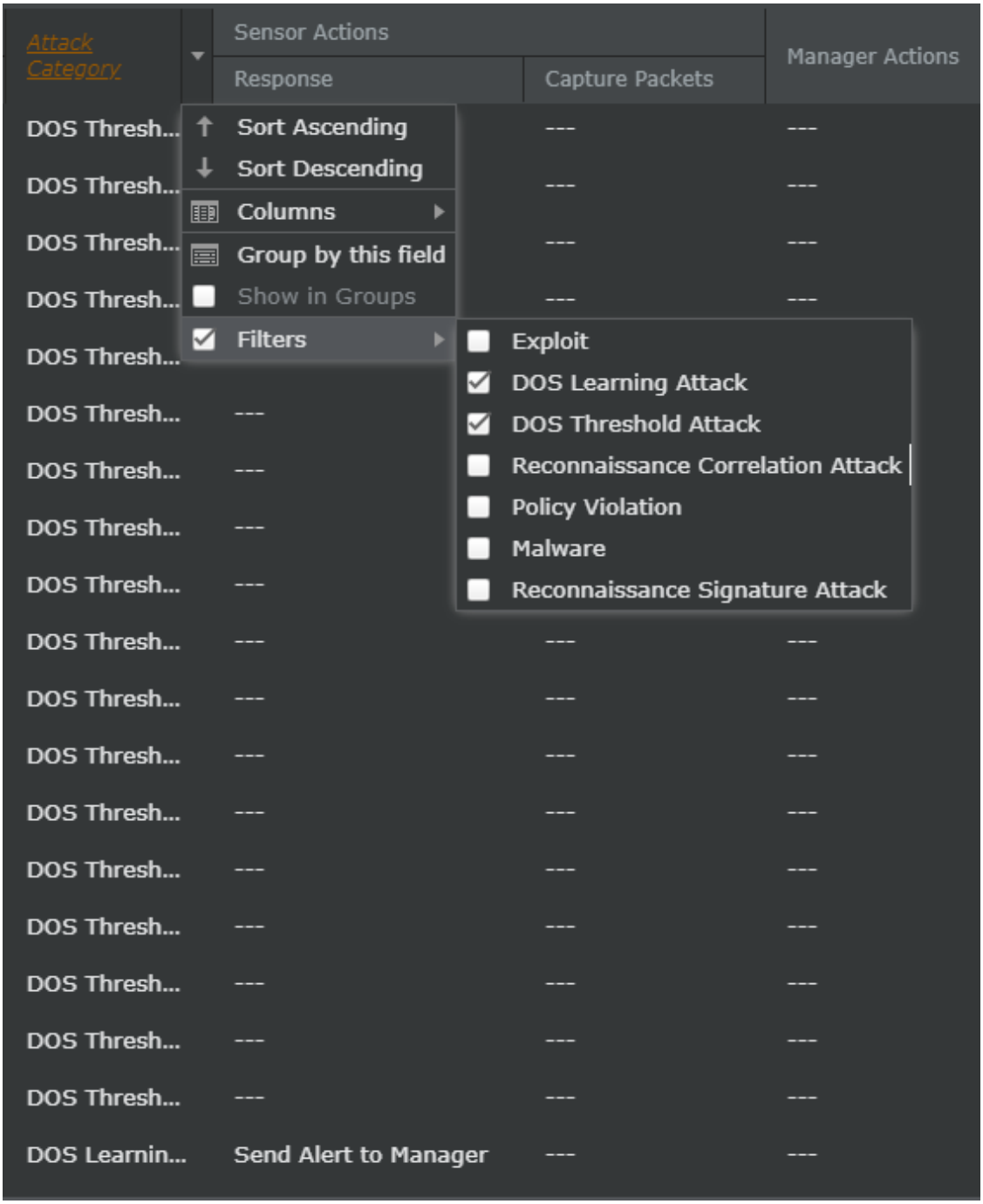


5. Click on "0" next to the **Customized Attacks** field under **Interface-Specific Customization**.

   The **Attack Definitions** window opens.

6. Select the filter from the **Attack Category** column to view the **DOS Learning Attack** or **DOS Threshold Attack** based on the DoS attacks that you want to customize.

Figure 461. Number of attack definitions by Attack Categories



The attack definitions belonging to the DoS attack category you selected are listed. This includes inbound, outbound, and bidirectional attack definitions.

NOTE

DOS Learning Attack and **DOS Threshold Attack** are the categories that correspond to DoS attack definitions.

7. Double-click on the attack that you want to customize. The **<Attack Name>** panel opens on the right side.

   You can also select multiple attacks by using the **Ctrl** key to select multiple attacks. For the sake of explanation, assume that you are customizing a single attack.
8. Customize the DoS attack definition on the **Settings** tab of the **<Attack Name>** panel.
9. Click **Update**.
10. After you have customized all the required attack definitions, click **Save**.

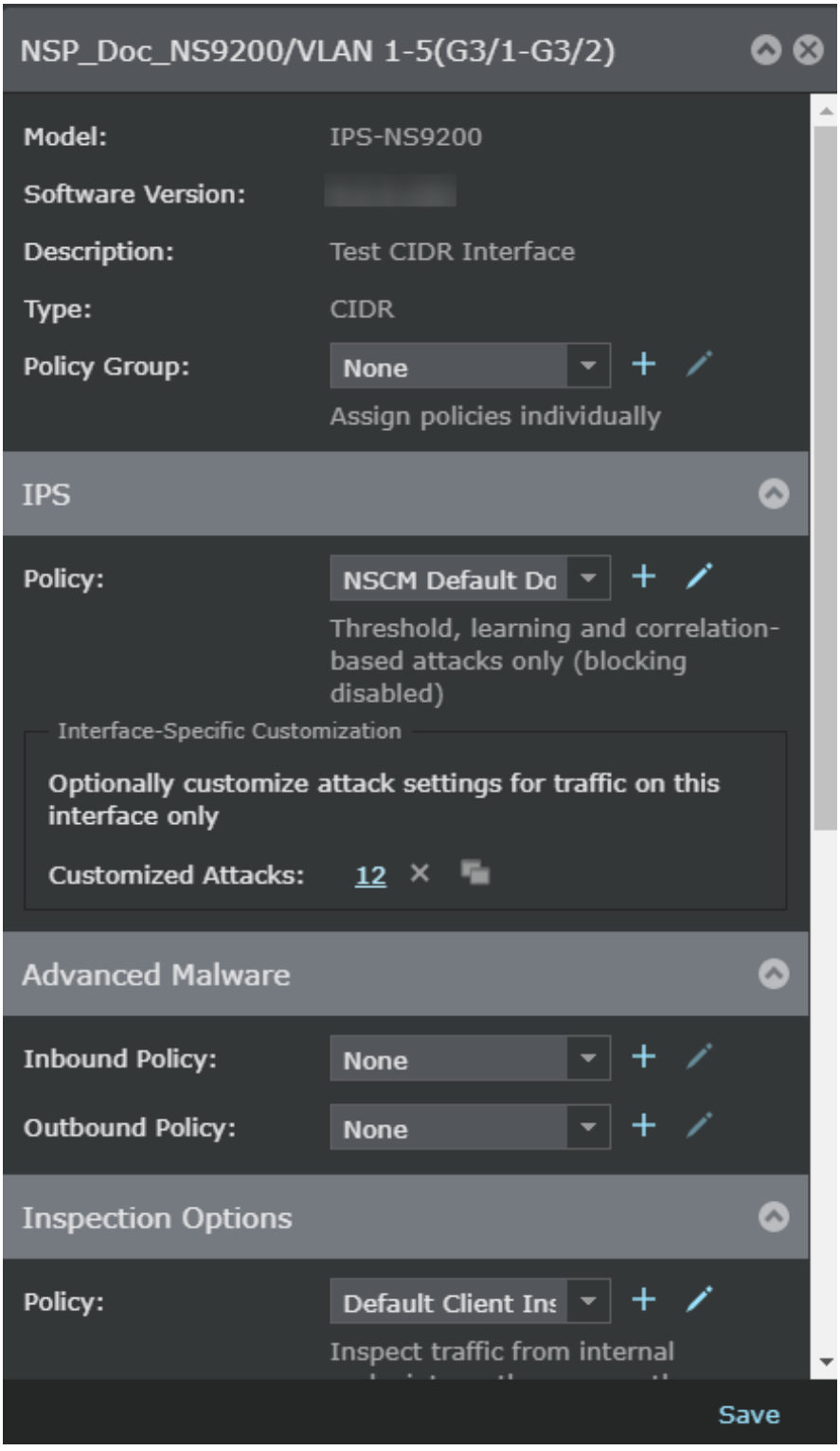
    A **Save Confirmation** dialog opens. Click **Confirm** to save the changes. Click the "x" icon to exit the window without saving the changes.
11. Click the **Save** button in the **<Device Name/Interface>** panel to save all the changes.

    The **Customized Attacks** field shows the integer value of the number of attacks customized for that policy.

    In the **<Device Name/Interface>** panel, you have the following options:

    -  (merge) — Merges the customized policy with the assigned IPS policy. After a successful merge, the **Customized Attacks** field shows the integer value as "0".
    -  (delete) — Deletes any customized attacks before it is merged with the assigned IPS policy.

Figure 462. Customized attacks merge



12. Deploy the configuration changes to the required Sensors for the changes to take effect.

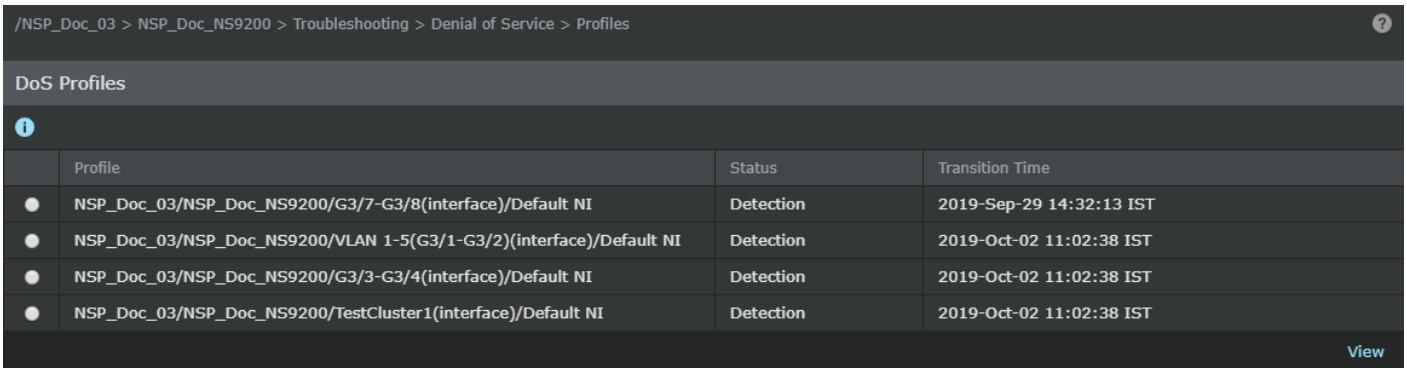
View the applied DoS profiles at a Sensor resource

The **DoS Profile** page of an interface details the current status of DoS learning mode policies applied to an interface. DoS policy was inherited from the domain upon Sensor addition, but might have changed due to one of the following:

- Application of a different policy.
- Creation of one or more custom DoS IDs for an interface.

> **NOTE**
>
> At the Interface-x level, you cannot see status for DoS IDs created within a subinterface. The view at this level is strictly for the parent and direct child relationship. For more information on *child* DoS policies of a subinterface, refer to [Viewing the applied DoS policies of a sub-interface] section.

Figure 463. View DoS Profile



In the DoS learning mode, a profile is built over a 48-hour period to determine the normal traffic pattern. Once the initial learning is complete, the Sensor detects traffic that is outside of the normal parameters while continuing to take measurements of network traffic and adjusting the profile accordingly. Activity outside of the normal parameters raises an alert.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Troubleshooting → Denial of Service → **Profiles**. The fields are as follows:

Table 53. Option definitions

Option	Definition
Profile	The subinterface or VLAN/CIDR ID where a DoS profile was applied. **Default NI** refers to all traffic that is not a part of an interface subdivision, that is, subinterface, VLAN tag, or CIDR block.

Option	Definition
Status	Lists whether the policy is currently learning the network behavior or actively detecting. **Learning** means the initial traffic profile is being created by determining a normal traffic baseline. This learning period requires 48 hours. **Detection** means the profile has finished the initial learning period and traffic checking for abnormal levels is in progress.
Transition Time	The exact time when the learning profile started analysis or when the active detection for the learning profile began. The **Status** field indicates which process is currently operating.

6. Optionally, select a DoS ID and click **View** to display rate data for the measures in the DoS profile applied to the selected DoS ID.

   You can change the measure by toggling the direction and measure drop-down list. To return to the **DoS Profiles** page, click **Close**.

Figure 464. DoS Detection Status sub-tab

View the applied DoS policies of a subinterface

The **DoS Profile** page of a subinterface provides operational details on the custom DoS policies applied to a subinterface. DoS policy was inherited from the interface upon subinterface creation, but might have changed due to one of the following conditions:

- Application of a different policy for the subinterface.
- Creation of one or more custom DoS policies for a subinterface. This was achieved by performing the **Manage Custom** action for an entire subinterface, for individual VLAN/CIDR IDs within a subinterface, or for a CIDR addresses within a VLAN or CIDR ID.

In DoS learning mode, a profile is built over a 48-hour period to determine the normal traffic pattern. Once the initial learning is complete, the Sensor detects traffic that is outside of the normal parameters while continuing to take measurements of network traffic and adjusting the profile accordingly. Activity outside of the normal parameters raises an alert.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Denial of Service → **Profiles**.

Table 54. Option definitions

Option	Definition
Profile	The subinterface where DoS policy was applied. **Default NI** refers to all traffic that is not a part of a subinterface subdivision, that is, DoS ID for a VLAN tag or CIDR address within a subinterface.
Status	lists whether the profile is currently learning or detecting. **Learning** means the initial learning profile is being created to determine the normal traffic baseline. This learning period requires 48 hours. **Detection** means the profile has finished the initial learning period and traffic checking for abnormal levels is in progress.
Transition Time	The exact time when the learning profile started analysis or when the detection for the learning profile began. The **Status** field indicates which process is currently operating.

2. Optionally, select a DoS ID and click **View** to display rate data for the measures in the DoS profile applied to the selected DoS ID.

   You can change the measure by toggling the direction and measure drop-down list. To return to the **DoS Profiles** page, click **Close**.

Customized DoS policy in a network

The following table summarizes the rules for creating custom DoS policies in a network.

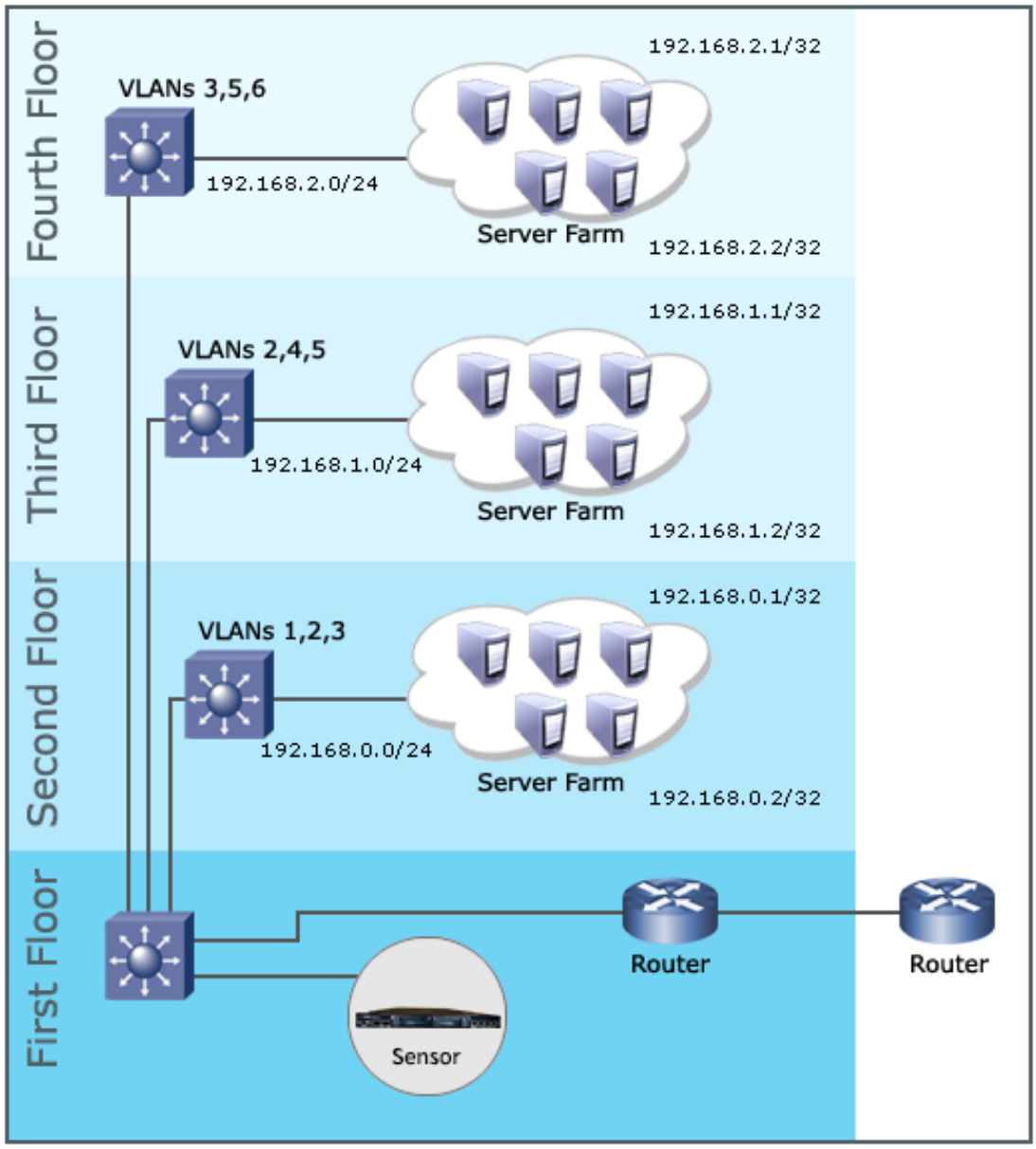
If you customize DoS:	Then...
At the Interface level, for the entire interface or for a VLAN or CIDR ID (and a subinterface has not been created)	You cannot create subinterfaces for the interface.
At the SubInterface level, for the entire subinterface or for a VLAN or CIDR ID within the subinterface	You cannot customize DoS at the interface level.

For a VLAN interface with multiple VLAN tags, you can do one of the following:

- Customize the inherited DoS policy and create multiple DoS policies for each of your VLAN tags. If you create DoS policies for your VLAN tags at the interface node, you cannot create subinterfaces for your VLAN tags.
- Customize the inherited DoS policies and create multiple subinterfaces which can then have custom DoS policies. If you created subinterfaces for your VLAN tags, you cannot create custom DoS policies for any VLAN tags at the interface level.
- For a CIDR interface with multiple CIDR-based addresses, you can do one of the following:
  - Customize the inherited DoS policies and create multiple DoS profiles for each of your CIDR addresses
  - Customize the inherited DoS policies and create multiple subinterfaces which can then have custom DoS policies. If you created subinterfaces for your VLAN tags, you cannot create custom DoS policies for any VLAN tags at the interface level.

In this example, suppose a Sensor is in SPAN mode, monitoring the traffic transmitting between the floors of a building. Sensor port G0/1 is the interface number.

Figure 465. DoS policy customization example



The above displays various custom DoS implementations. The traffic type scenarios that follow explain DoS policy customization options for each of the three interface types.

Customize DoS policy for a dedicated interface

Suppose port G0/1's traffic type is dedicated. In this situation, you can:

- Customize the inherited DoS settings for all of the traffic the interface monitors.
- Create multiple DoS policies for multiple CIDR networks. You can create three unique DoS policies for 192.168.0.0/24, 192.168.1.0/24, and 192.168.2.0/24. Once these unique DoS instances have been created, the rest of the interface traffic is protected by the inherited DoS settings.

Customize DoS policy for a VLAN

Suppose instead that Port G0/1's traffic type is VLAN, and that you have added VLAN IDs 1-6 to your interface. In this situation, you can:

- Create multiple DoS policies for each VLAN ID in the network. In this instance, you can create unique DoS policies for VLAN 2, VLAN 4, and VLAN 5. All other traffic in the interface is protected against DoS by the inherited DoS policy settings; the inherited settings can be customized.
- Create a subinterface. You combine VLANS 2, 4, and 5, and call the subinterface VLAN-245.
- Create a DoS instance for an individual VLAN ID and the entire subinterface for all other traffic, for example, just VLAN 2 and the entire VLAN-245. You can later create DoS instances for VLANs 4 and 5.

Customize DoS policy for a CIDR

Suppose that port G0/1's traffic type is CIDR. You can do one of the following:

- Create multiple DoS policies for each CIDR network ID and the rest of the interface's traffic. In this instance, you can create unique DoS policies for 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, and the entire G0/1.
- Create a subinterface. You combine 192.168.0.0/24 and 192.168.1.0/24, and call the subinterface CIDR-0010.
- Create a DoS instance for an individual CIDR ID and the entire subinterface for all other traffic, for example, just 192.168.0.0/24 and the entire CIDR-0010.

Denial-of-Service profile advanced scanning

What is a DoS profile?

A DoS profile is an analysis of network traffic with reference to the normal traffic flow captured during the learning period of a Sensor. A DoS Profile displays the current status of DoS learning mode policies applied to a Sensor, as well as its interfaces and subinterfaces. In DoS learning mode, a profile is built to determine a normal traffic pattern. Once this profile is learned, the Sensor alerts for traffic that is outside of the normal parameters. The profile is continually being built, thus baseline levels adjust over time.

The Manager displays the learning mode status values for the Sensor and each interface, respectively. This is particularly useful if you have changed policy application per interface and you want to determine if the new profile is being built or if it is actively detecting abnormal traffic conditions.

DoS profiles of the selected Sensor are displayed in the **DoS Profiles** page.

NOTE

DoS parameters are configured within each IPS policy or by creating a custom DoS policy at the interface or subinterface level.

View the DoS profiles of a Sensor

The DoS profiles show a comparative display of short-term and long-term distribution for the selected profile.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Troubleshooting → Denial of Service → **Profiles**.

   The **Dos Profiles** page details the current status of DoS learning mode policies applied to an interface or sub-interface. DoS policy was inherited from the domain upon Sensor addition but might have changed due to the application of a different policy at the interface or sub-interface level.

Figure 466. DoS Profiles tab

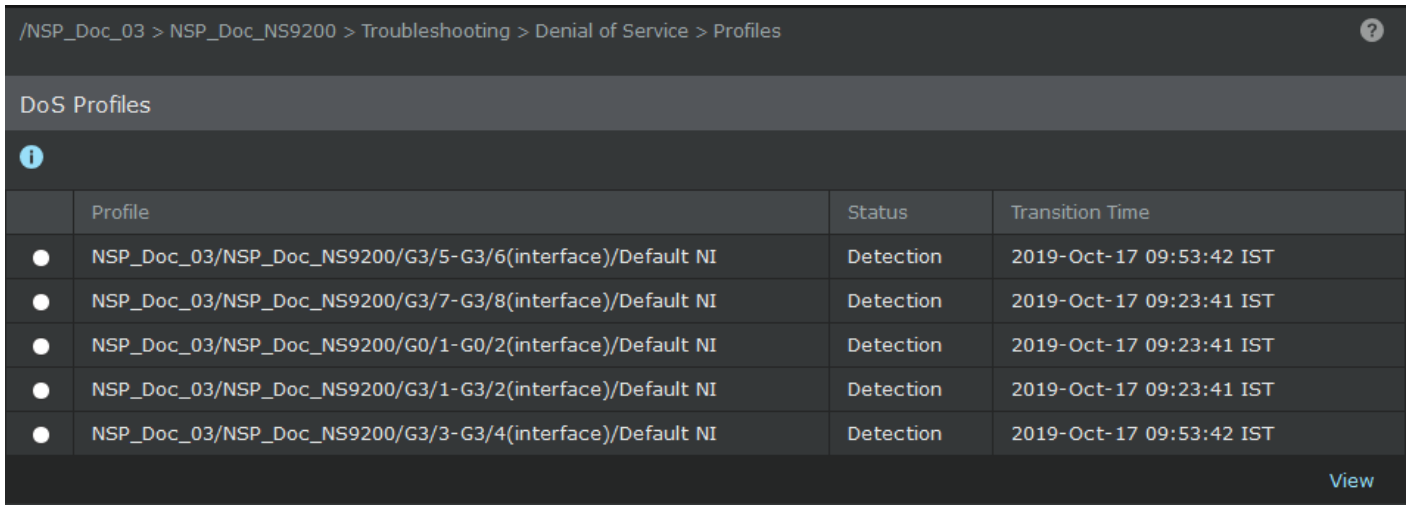


Table 55. Option definitions

Option	Definition
Profile	The sub-interface or VLAN/CIDR ID where a DoS profile was applied. **Default NI** refers to all traffic that is not a part of an interface subdivision, that is, sub-interface, VLAN tag, or CIDR block.
Status	Lists whether the profile is currently learning or detecting. **Learning** means the profile baseline is being built. **Detection** means the learning profile has finished and traffic is being checked against the baseline.
Transition Time	The exact time when the learning profile started analysis or when the active detection for the learning profile began. The **Status** field indicates which process is currently operating.

6. Select a DoS profile and click **View**.

Figure 467. DoS profile - Advanced Scanning

7. Optionally, select the direction (Example: Inbound) and a measure (example: tcp-control) to display rate data for the measures in the DoS profile applied to the selected interface.

   When reading the chart, it is helpful to remember that:

   - The long-term profile is the compilation of the short-term profiles.
   - The horizontal axis contains buckets of the various packet rates.
   - The vertical axis indicates the percentage of those rates falling into each bucket.

8. Click **Close** to go back to the **DoS Profiles** page.

Configure Denial-of-Service profile limits

The limit to the quantity of DoS profiles that can be configured per Sensor is unique for each Sensor model.

The details are as follows:

NS-series — Maximum DoS profiles supported

NS9500 stack - 100 Gbps throughput	NS9500 stack - 60 Gbps throughput	NS9500 stack - 40 Gbps throughput	NS9500 stand-alone - 30 Gbps throughput	NS9500 stand-alone - 20 Gbps throughput	NS9500 stand-alone - 10 Gbps throughput	NS9300/ NS9200/ NS9100
5,000	5,000	5,000	5,000	5,000	5,000	5,000

NS7600 - 15 Gbps throughput	NS7600 - 10 Gbps throughput	NS7600 - 5 Gbps through-put	NS7500 - 7.5 Gbps throughput	NS7500 - 5 Gbps through-put	NS7500 - 3 Gbps through-put
5,000	5,000	5,000	5,000	5,000	5,000

NS7350/ NS7250/ NS7150	NS7300/ NS7200/ NS7100	NS5200	NS5100
5,000	5,000	5,000	300

NS3600 - 5 Gbps throughput	NS3600 - 3 Gbps throughput	NS3600 - 1 Gbps throughput	NS3500	NS3200/ NS3100
5,000	5,000	5,000	128	128

Virtual IPS — Maximum DoS profiles supported

IPS-VM600	IPS-VM5000
300	300

DoS data management

Using the **DoS Data Management** page, you can configure the DoS learning mode profile to restart or load from a previous profile. DoS attacks interrupt network services by flooding a system or host with spurious traffic, which can overflow your system buffers and force you to take the system offline for repairs.

Since a DoS profile can be configured for both learning and threshold modes, the Sensor keeps statistics for both modes. For learning mode, the Sensor monitors the network traffic and develops a normal baseline profile, called a *long-term profile*, by collecting statistics on a number of traffic measures over time. The initial learning time for the profile is typically 48 hours. After that time, the system constantly updates this profile, which is kept on the internal Sensor flash, to keep an updated picture of the network. The Sensor develops a short-term profile, which is a two minute slice of the network traffic. The short-term profile is compared to the long-term profile and an alert is raised if the short-term statistics indicates a traffic surge that deviates too much from the long-term behavior.

For threshold mode, the Sensor keeps track of the threshold limits you enabled for specific attacks. Together these two modes create one profile, which is saved to your Sensor's flash and can be uploaded to the Manager for future re-use. You can upload this saved profile later if you feel the baseline that had previously been created was more effective than a current profile.

Manage DoS profiles

The **DoS Data Management** page enables you to manage the DoS learning mode policies on a Sensor.

Steps:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.

5. Select Troubleshooting → Denial of Service → **Data Management**.

   The last DoS profile uploaded from the Sensor to Manager is listed under **DoS Profiles on Manager**.

6. Select one action from one of the following headings:

   DoS Profile Learning

   - **Rebuild the DoS Profiles (start the learning process from scratch)** — Starts the learning process from scratch. The profile that has just been learned is erased, and a new profile is built. To start the learning process, select this option and click **Update**.

     Typically, this is only required when:

     - It is known that a DoS attack occurred during the initial learning phase, contaminating the long-term profile.
     - There has been a significant change in network traffic, for example, an overhaul to the routing infrastructure.

     NOTE

     When a port runs in learning mode, it does not analyze traffic for DoS attacks. You can infer whether DoS attack has occurred during the initial phase or not by reading situations specific to your network.

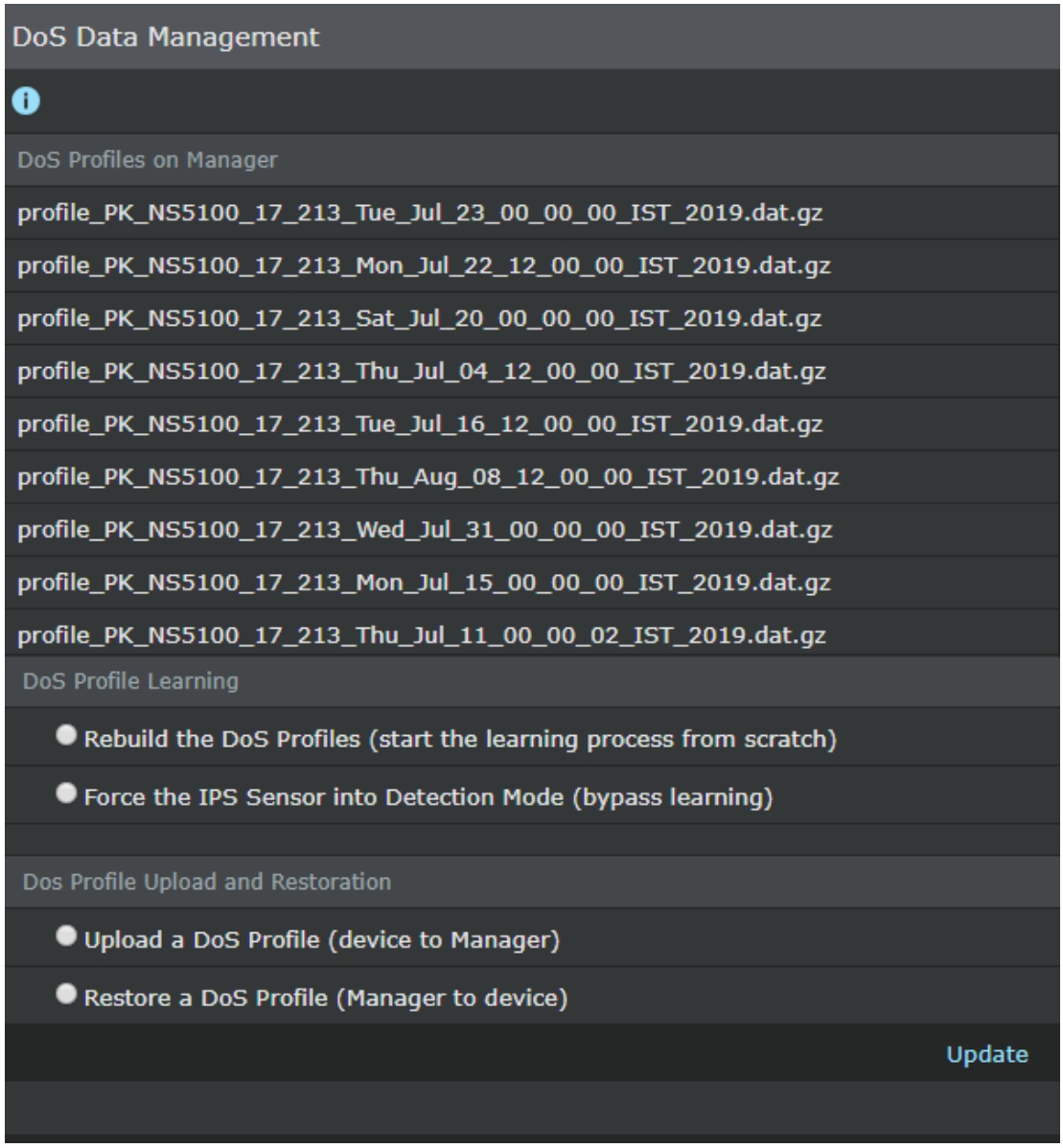
   - **Force the IPS Sensor into Detection Mode (bypass learning)** — You can force a Sensor into detection mode before the normal 48-hour minimum learning period. This option must be reserved for testing and troubleshooting.

     TIP

     Trellix recommends performing a *re-learn profile* when there is a network change, for example if you moved Sensor from a lab environment to a production environment. Re-learning a profile is also recommended if there is a configuration change, that is you changed the CIDR block of a subinterface that causes a significant sudden traffic change to an interface or subinterface for which a profile has already been established (or in the process of initial learning). Without doing so, the Sensor might give false alarms or fail to detect attacks during a time period when it is adapting to the new network traffic conditions.

   There is no need to re-learn a profile when network traffic increases or decreases naturally over time (for example, an eCommerce site that is getting more and more customers; thus its web traffic increases in parallel) since the Sensor can automatically adapt to it.

Figure 468. DoS Data Management area



DoS Profile Upload and Restoration

In most circumstances, there is no need to upload and restore profiles. The exceptions include:

- The Sensor fails to detect an attack. In this case, the Sensor mistakenly learns the bad traffic pattern as good. A previous profile can be restored to replace the contaminated one, if one was saved.
- The Sensor is used for testing that skews the long-term profile. To bring the Sensor back in good standing, a profile is saved, the testing is performed, and the previously saved profile is restored.
- A change to the quantity of interfaces/subinterfaces is made, but the change needs to be reversed. For example, you add a new subinterface, which also changes the quantity and makeup of DoS profile. You then decide to back out of the change. Restoring a profile eliminates the requirement to go through the re-learning phase.

NOTE

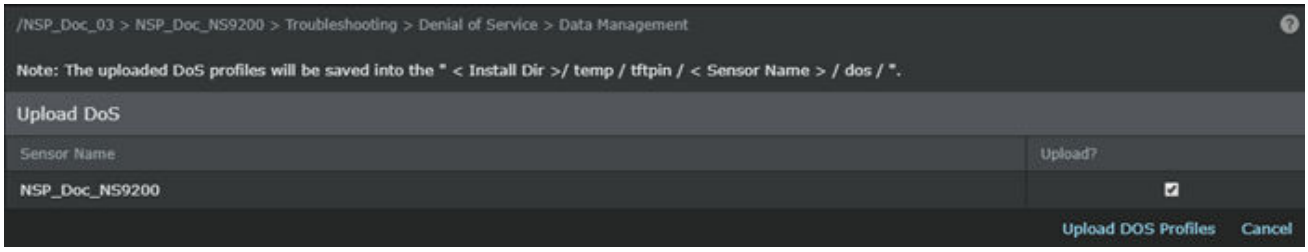
Rebooting a Sensor does not return it to learning mode. A Sensor stores long-term data and picks up where it left off when the reboot started.

- **Upload a DoS Profile (device to Manager)**: Uploads all of the learned profiles on a Sensor's flash to Manager. To upload a Sensor's DoS profiles to Manager, do the following:
  - Select **Upload a DoS Profile (device to Manager)**.
  - Click **Update**. The **Upload DoS** screen opens with the **Upload?** field checked by default.
  - Click **Upload DoS Profiles**. A pop-up displays upload status.
  - Click **Close Window** to close the status window after upload finishes.
  - Click **Data Management** to return to the main screen to view your uploaded file. One file is uploaded for all interfaces, subinterfaces, or DoS IDs of a Sensor. This file is listed in the **DoS Profiles on Manager** section (top) of the table.

NOTE

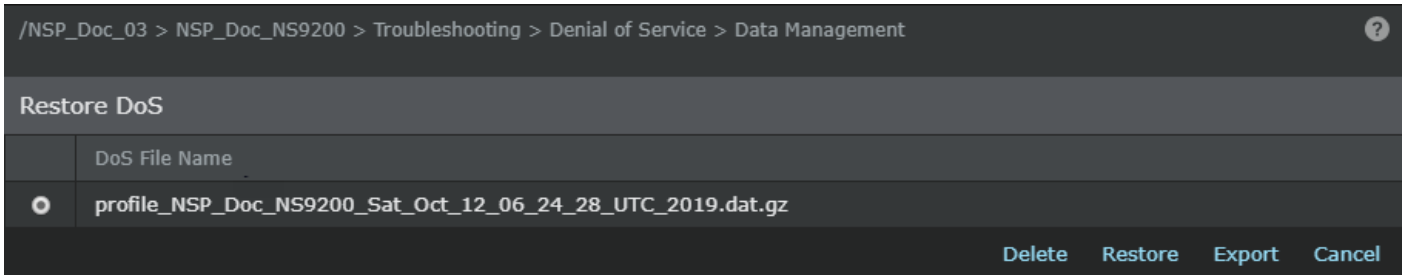
You will have to wait at least 48 hours for the first learning profile to finish before you can download a profile.

Figure 469. Uploading a DoS profile from a Sensor to the Manager



- **Restore a DoS Profile (Manager to device)**: Downloads a DoS profile to the Sensor that has been previously uploaded (saved) to Manager using the **Upload a DoS Profile (device to Manager)** option. The uploaded profile is listed under the **DoS Profile Upload and Restoration** section. To restore a DoS profile, do the following:
  - Select **Restore a DoS Profile (Manager to device)**.
  - Click **Update**.
  - Select a DoS profile and click **Restore**.
  - (Optional) Select a DoS profile and click **Delete** to delete the profile.
  - (Optional) Select a DoS profile and click **Export** to export and save the profile to a client that is not Manager server.

Figure 470. Restoring a DoS profile



DoS filter management

You can view and modify the drop/block packets responses that have been initiated for the DoS learning mode profiles applied for all network identifiers (NIs) within a Sensor. A *DoS filter*, or blocking rule, is similar to a firewall deny rule in that subsequent traffic that matches the filter parameters is blocked from transmitting further through your network. A *network identifier* is a Trellix IPS term relating to interface, subinterface, and DoS ID resources. DoS filters are applied exclusively to DoS learning mode attacks.

A DoS filter can be initiated for any DoS learning mode attack, namely the measures within each attack. Each enabled learning mode attack is a combination of traffic flow rate measures, such as the rate of TCP control packets or UDP packets. When a learning mode profile has completed learning the normal traffic behavior, the long-term measure volumes in this profile are matched against short-term volume calculations for each measure. If the short-term volume is outside of the long-term volume, a statistical attack type alert is raised. Once a statistical alert has been raised, the Sensor can initiate an automatic or manual response to block all subsequent packets of the violated measure.

- For automatic dropping and blocking, you configure a DoS policy with the *drop packets* response enabled for one or more measures and apply the policy to a Sensor interface in inline mode. Automatic filters last as long as the short-term volume continues to violate the long-term volume.
- For manual blocking, you must initiate the response from IPS Policies for an attack. For more information, see [Blocking DoS attacks].

Steps:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Troubleshooting → Denial of Service → **Filters**.

   Do one of the following:

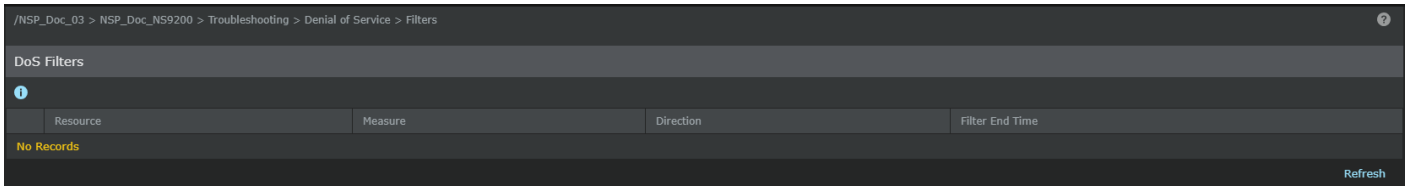
   - To delete a filter, select a filter and click **Delete**.
   - To refresh a filter, select a filter and click **Refresh**.
   - To extend a filter, do the following:

   a. Select a filter and click **Extend**. The **Add DoS Filter Time** dialog opens.

b. Type the number of seconds to add to the **Filter Time**.

c. Click **Save**; click **Cancel** to abort.

Figure 471. Add DoS Filter



DoS attack prevention methods

Once DoS attacks have been detected, Trellix IPS offers the following methods to block various types of DoS Attacks.

Table 56. DoS attack prevention recommendations

Attack	Recommendation	Comments
TCP SYN	SYN Cookies Statistical Anomaly	You can configure SYN cookies in the Manager to accurately block all attack traffic, while allowing all legitimate traffic. TCP SYN or TCP FIN inbound or outbound attacks can be blocked by configuring the policy to block the **TCP SYN or FIN Volume too high** attack in both inbound and outbound directions. When used within an enterprise, Firewall access rules can be configured in the Manager to allow traffic only from known sources. Configuring SYN cookies is more effective and deterministic compared to statistical anomaly.
TCP Full Connect	Connection Limiting with Trellix GTI Integration enabled Statistical Anomaly	You can define a threshold value to limit the connection rate or the number of active connections from each source. In addition to this, you can also define rules to limit access based on the connection rate, external hosts' reputation, and geo-location. Statistical anomaly is based on data learnt over a time window. For immediate prevention of connection based DoS attacks, Connection Limiting would be more effective. When used within an enterprise, Firewall access rules can be configured in the Manager to allow traffic only from known sources.

Attack	Recommendation	Comments
TCP ACK/FIN /RST	Stateful TCP Statistical Anomaly	This attack can be blocked by setting the TCP Flow Violation to **DENY_NO_TCB** in the Manager. TCP SYN or TCP FIN inbound or outbound attacks can be blocked by configuring policy to block the **TCP SYN or FIN Volume too high** attack in both inbound and outbound directions. TCP RST attacks can be blocked by configuring the policy to block the **TCP RST Volume too high** attack in both inbound and outbound directions. Alternatively, TCP RST flood can be blocked by setting the TCP Flow. Trellix recommends that you use stateful TCP to prevent these attacks.
DNS Flood	DNS Protect Connection Limiting with Trellix GTI Integration enabled Statistical Anomaly	You can mitigate DNS flood attacks by using DNS spoof protection feature that can be enabled through CLI commands on the Sensor. You can define a threshold value to limit the connection rate or the number of active connections from each source. In addition to this, you can also define rules to limit access based on the connection rate, external hosts' reputation and geo-location. UDP flood attacks can also be blocked by configuring the policy to block the **UDP Packet Volume too high** attack in both inbound and outbound directions. Statistical anomaly is based on data learnt over a time window. If performance with TCP is acceptable, use DNS Protect, which is more deterministic. For immediate prevention of connection based DoS attacks, Connection Limiting would be more effective.
UDP Flood	Connection Limiting with Trellix GTI Integration enabled Statistical Anomaly	You can define a threshold value to limit the connection rate or the number of active connections from each source. In addition to this, you can also define rules to limit access based on the connection rate, external hosts' reputation and geo-location. UDP Flood attacks can be blocked by configuring the policy to block the **UDP Packet Volume too high** attack in both inbound and outbound directions. Statistical anomaly is based on data learnt over a time window. For immediate prevention of connection based DoS attacks, Connection Limiting would be more effective. Firewall access rules can be configured in the Manager to block UDP traffic that is not expected to be seen with the network.

Attack	Recommendation	Comments
ICMP Flood	Connection Limiting with Trellix GTI Integration enabled	You can define a threshold value to limit the connection rate or the number of active connections from each source. In addition to this, you can also define rules to limit access based on the connection rate, external hosts' reputation, and geo-location.
	Statistical Anomaly	ICMP Flood attacks can be blocked by configuring the policy to block the **ICMP Packet Volume too high** and **ICMP Echo Request or Reply Volume too high** attacks in both inbound and outbound directions. Statistical anomaly is based on data learnt over a time window. For immediate prevention of connection based DoS attacks, Connection Limiting would be more effective. Firewall access rules can be configured in the Manager to block ICMP traffic that is not expected to be seen with the network.
Non TCP/UDP/ICMP Flood	Statistical Anomaly	Non TCP/UDP/ICMP attacks can be blocked by configuring the policy to block the **Non-TCP-UDP-ICMP Volume too high** attack in both inbound and outbound directions.
Exploit DoS attacks	Trellix IPS Signatures	Exploit attacks can be blocked by configuring policies to block the exploit attacks (more than 3000) listed in the IPS Policies, for both inbound and outbound traffic.
Application Level Flood	Custom Reconnaissance Attack Definition	Use correlated attack definition, which is based on the individual attack definitions. For example, custom attacks that check for URI can be further correlated to test for multiple occurrences in a defined time interval to raise a correlated attack.

Trellix IPS uses specific methods to prevent DoS attacks. These methods work independently but can also be applied in combination.

Statistical anomaly

Trellix IPS uses binning to detect statistical anomalies and prevent DoS attacks.

The Sensor builds a profile for each tracked packet type in each direction. Within each source IP profile, the entire IP address space is divided into a maximum of 128 mutually exclusive IP address blocks, or bins, much in the same way CIDR addressing divides the address space. Each bin is uniquely identified by a prefix and prefix length (from 2 to 32 bits). An IP address falls into a bin when the first 'n' number of bits of the address matches the bin's prefix. The Sensor then associates each source IP address with a particular bin in the appropriate profile.

Each bin has the following two properties:

- The percentage of long-term good traffic originating from the source IP addresses that belongs to this bin.
- The percentage of the overall IP address space that the IP range in this bin occupies.

With the source IP addresses properly classified, the Sensor can protect a network from DoS attacks. When a statistical anomaly occurs, the Sensor takes the following actions on the source IP profile in question:

- The Sensor blocks all packets with source IP addresses in the bins that occupy a large percentage of the IP space, but represent a small percentage of the long-term traffic. This combats attacks that are generated with random, wide-ranging, spoofed source IP addresses.
- The Sensor blocks all packets with source IP addresses in the bins that occupy a large percentage of the short-term traffic together with a significantly higher percentage of short-term traffic than historically seen. This combats attacks that are initiated from a handful of networks with authentic source IP addresses.
- The Sensor does not block packets with source IP addresses in the bins that occupy a small percentage of the IP space and represent a high percentage of the long-term traffic. This protects against blocking hosts that are known to be good.

The exception to the third criterion is when the traffic also meets the second criterion. In other words, source IP addresses from the good bins are blocked if their short-term traffic level is significantly higher than their peak long-term level. This combats attacks that are initiated from good hosts that have recently been compromised.

Source IP addresses classification is more effective than using devices such as firewalls that limits the rate of SYN packets on the network to block DoS attacks. The key difference in such an approach and Trellix IPS is that a rate-limiting device blocks traffic randomly. Good traffic has the same probability of being blocked as attack traffic. On the other hand, source IP address classification used by Trellix IPS attempts to differentiate good traffic from attack traffic, so attack traffic is more likely to be blocked.

NOTE

The statistical anomaly method is effective in preventing most attacks; however, there are some chances of false positives.

Advanced malware and callback detection

Using the Advanced Malware policies, you can prevent DoS attacks that involve malware execution. An Advanced Malware policy is a set of rules that scans the traffic across your network, and determines how to respond to malware detected in the network. An effective policy is one that is customized to the network environment being monitored.

To prevent DoS attacks through botnet, Trellix IPS provides heuristics based Advanced Callback Detection feature to protect customer networks from both known and 0-day bots. This can be enabled per VIDS for a Sensor. Enable the heuristics based Advanced Callback Detection feature, which detects bot activity by correlating multiple attacks across different flows. Attacks are correlated by observing a host for a given period of time.

In addition to what is explained above, malicious bot command and control servers' activity can be detected. Detecting bot command and control server activity is a key feature of the Advanced Callback Detection. Trellix IPS monitors networks for bot attacks and protects the network by updating the reputation of the newly identified bot masters in the cloud, using Trellix GTI.

For more information on Advanced Malware and Callback Detection features, see the chapters [Advanced Malware Detection] and [Advanced Callback Detection] respectively.

SYN cookie

In a SYN flood attack, server resources are targeted to consume TCP memory by sending SYN, and after the server responds with a SYN+ACK, force the server to hold state information while waiting for the client's ACK message. As the server maintains state for half-open connections, server resources are constrained. The server might no longer be able to accept TCP connections, resulting in a DoS condition.

Trellix IPS uses a specific choice of initial TCP number as a defense against SYN flood attacks. The SYN cookie feature is a mechanism to counter SYN flood attacks. This feature is an adjunct to the existing statistical anomaly-based DoS detection. In cases where a DoS attack is already underway and there is no time for learning a long-term profile, Trellix IPS provides the ability for the Sensor to proxy all inbound three-way handshakes.

You can enable SYN cookies for both inbound and outbound traffic.

The Sensor supports a configurable threshold for SYN arrival rate, above which the Sensor begins using SYN cookies to avoid reserving connections during the three-way handshake. The SYN cookie feature has a threshold configured for inbound and outbound. Threshold value indicates the number of half-open connections on the Sensor, that is the connections where the three-way handshakes are not yet complete. If it goes beyond the configured threshold, the Sensor changes to SYN cookie mode. When this happens, the Sensor triggers an alert indicating **IP: syncookie proxy <direction> activated**. Similarly, when the number of half-open connections comes down below the threshold value, the Sensor triggers another alert indicating **IP: syncookie proxy <direction> deactivated**. You can view the alert details in the Attack Log.

In SYN cookie mode, the Sensor acts as a TCP proxy, that is it responds to SYN requests received from the client with a SYN+ACK that includes the cookie. The SYN+ACK also contains an Initial Sequence Number (ISN), uniquely generated for every packet, using the information present in the incoming SYN packet, and a secret key. A valid ACK is received only if the connection request is from a legitimate host, after which the Sensor initiates a three-way handshake with the server. If the connection request is not from a legitimate host, a TCP session is not created, and a potential DoS condition is averted. After the three-way handshake is established, the Sensor proxies all further data packets.

The Sensor does not maintain a counter for the number of half-open connections. Hence, there are no capacity limitations for the number of half-open connections.

The Manager provides an interface for the user to enable and disable the SYN cookie feature. It also provides a user the ability to configure threshold values for such SYN cookies. The recommended threshold value is 10% of the supported flows. For example, you can check the number of half-open connections on the Sensor over a normal period of time, and based on that set a threshold that is 2 to 3 times the number of connections. The threshold value assigned is applicable to all interfaces and not to specific interfaces.

Following are few points to be noted when you enable the SYN cookie feature:

- Sensors using SYN cookie settings must be in inline mode. If you do not have any ports in inline mode, configure at least one port pair to be inline.
- When the Sensor is in SYN cookie mode, it acts as a proxy for the TCP connection between the host and the server. When using VLAN-tagged traffic, based on the placement of the VLAN router, there is a possibility that the packets from the host passes through the same interface pair of the Sensor twice to reach the server. In such cases, a separate sub-interface must be configured for each VLAN to ensure that a packet is not seen more than once.

Figure 472. Packets seen twice by the Sensor

- Do not enable SYN cookies when passing MPLS traffic through a Sensor. SYN cookie cannot be supported on MPLS traffic because there is no specific MPLS tag to use in the return direction when the Sensor proxy code responds to the SYN packets. When there is a combination of a SPAN port with MPLS traffic and an inline port without MPLS traffic, the SYN cookie still prevents SYN flood as it parses the normal traffic through the inline port pair.

You can view the number of invalid SYN connections received by the Sensor under the **`show flows`** CLI command. For more information on the CLI command, refer to the [CLI Commands] section.

Stateful TCP engine

Sensor has a built-in TCP stack that follows the state required for TCP protocol. Sensor uses the TCP state to prevent out of context packets and packets without a valid state. The TCP stateful engine can be used effectively to drop spoofed TCP RST, TCP FIN, TCP ACK floods.

DNS protect

DNS protect feature in Sensor can be used to protect DNS servers from DoS spoof attack by forcing the DNS clients to use TCP instead of UDP as their transport protocol. Since TCP uses three-way-handshake, it is comparatively tough to launch spoofed attacks when TCP is used.

You can set the DNS protection mode, add to, or delete existing DNS spoof protection IP addresses from the protected server list using CLI commands.

set dnsprotect

This command, when executed, sets the DNS protection mode.

Syntax

`set dnsprotect <inbound/inbound-outbound/ip-based/off/outbound>`

Parameter	Description
<inbound>	sets the DNS protection mode to 'inbound'
<inbound-outbound>	sets the DNS protection mode to 'inbound-outbound'
<ip-based>	sets the DNS protection mode to 'ip-based'
<off>	turns off the DNS protection mode
<outbound>	sets the DNS protection mode to 'outbound'

NOTE

The list of protected destination IP addresses can be edited irrespective of this setting.

dnsprotect

This command, when executed, performs the following tasks:

- Adds new DNS Spoof protection IP address
- Deletes existing DNS Spoof protection IP addresses (IPv4, IPv6 or both) from the Protected Server List (PSL)
- Re-lists the DNS spoofing protection IP address

Syntax:

`dnsprotect <add/delete/> <ipv4/ipv6> <IP address>`

While using the <resetlist> parameter, use the following syntax: **`dnsprotect <resetlist> <ipv4/ipv6/all>`**

Parameter	Description
add	Adds a new DNS spoofing protection IP address
delete	Deletes an existing DNS spoofing protection IP address
resetlist	Resets the list the DNS spoofing protection IP address
ipv4	Indicates that the IP address is for IPv4 packet
ipv6	Indicates that the IP address is for IPv6 packet
all	Indicates that the reset list of the existing DNS spoofing protection IP address is for both IPv4 and IPv6.

Example:

The following example shows the **`dnsprotect`** command used for adding the DNS Spoof protection IP address for IPv4.

`dnsprotect add ipv4 157.125.202.255.`

The following example shows the **`dnsprotect`** command used for reset listing of DNS Spoof protection IP address for all the IP addresses (IPv4 and IPv6).

`dnsprotect resetlist all`

NOTE

This command does not perform on IPv6 packets that have a routing header.

Firewall policies

You can use Firewall policies to prevent DoS attacks.

A Firewall policy consists of ordered rules for permitting and denying traffic from reaching a Sensor's inspection engine and continuing on through the network. Firewall policies complement IPS policies and ignore rules to help tune a deployment. You can use Firewall policies with a Sensor in inline mode to drop or deny traffic from or to specific hosts or within a range of hosts, or traffic that meets particular requirements such as protocol type, port, application, and Windows Active Directory credentials.

Firewall policies can be created for a combination of any source IP addresses, destination IP addresses, specified CIDR blocks, destination protocol/port, by TCP/UDP port, by ICMP type, and by IP protocol for the Sensor as a whole and per individual port pair.

Firewall policies can be used to mitigate DoS attacks by creating policies specific to the nature of traffic in a network. For instance, if you are aware of what protocols are normally seen in your network, you can configure Firewall policies to drop the type of traffic that is not normally expected in your network.

Deny, **Drop**, **Ignore**, **Require Authentication**, **Scan**, **Scan with Priority**, **Stateless Scan** or **Stateless Ignore** response action can be set while enabling intrusion prevention matching a configured rule. When used within an enterprise, **Scan** can be configured from all known CIDRs.

Connection limiting with Trellix GTI integration enabled

You can define a threshold value to limit the number of connections per second or the number of active connections to prevent connection based DoS attacks.

The Sensor provides the ability to define threshold values to limit number of connections (three-way TCP handshakes) a host can establish. The number of connections or connection rate that is less than or equal to the defined threshold value is allowed. When this number is exceeded, the subsequent connections are dropped. This helps in minimizing the connection-based DoS attacks on server.

The threshold value is defined as the number of connections/second or active connections. For example, if you define 1 connection per second as the threshold value then, there are 10 connections in the first second, all the other connections from the second to the tenth second will be dropped. On the other hand, if you have 1 connection for each second, all the 10 connections until the tenth second will be allowed. This is also known as traffic sampling.

You can define the Connection Limiting rules of the following types:

- **Protocol** — use this to limit TCP/UDP/ICMP active connections or connection rate from a host.
- **GTI** — In this case, the Sensor integrates with Trellix GTI IP Reputation to obtain the reputation score and geo-location of the external host. Therefore, use this to define Connection Limiting rules for traffic to and from external hosts based on reputation and geo-location of the external hosts.

Custom Reconnaissance Attack Definition

You can create custom signature-based attack definitions to prevent exploit based DoS attacks. Using the Custom Attack Editor, you can define correlated attacks using these individual attack definitions. For example, Custom Attacks that check for URI can be further correlated to test for multiple occurrences in a defined time interval to raise a correlated attack. The correlation methods supported are the following:

- Brute force
- Host sweep
- Port scan
- Service sweep
- Fingerprinting

When traffic passing through the Sensor exceeds the threshold count set for the Custom Reconnaissance Attack within a configured Interval, the Sensor raises an alert to the Manager. You can then opt to take the response actions, such as blocking or quarantining the host.

Managing DoS-related actions using command line interface

You can use Trellix IPS command line interface (CLI) commands in conjunction with the options available in the Manager to set DoS prevention severity, block DoS traffic, and to protect against DNS spoof attacks.

The following CLI commands can be used to view information on profiles and severity:

- **`show dospreventionprofile`**: Displays the specified denial of service profile information for the Sensor. This is defined in two arguments: a DoS measure name and traffic direction.
- **`show dospreventionseverity`**: Displays the severity for a specified DoS profile

Set Denial-of-Service prevention severity

The **`set dospreventionseverity`** command, when executed, sets severity for the specified DoS measure. Increasing the DoS prevention severity increases the number of DoS packets dropped. The default value is 30. The largest value is 200, and the smallest is 0.

Syntax

```
set dospreventionseverity <dos-measure-name> <inbound | outbound> <0-200>
```

Takes two arguments:

- A DoS measure name: one of 'tcp-syn', 'tcp-syn-ack', 'tcp-fin', 'tcp-rst', 'udp', 'icmp-echo', 'icmp-echo-reply', 'icmp-non-echo-reply', 'ip-fragment', and 'non-tcp-udp-icmp'
- A direction (one of 'inbound' or 'outbound')

For example, **`set dospreventionseverity tcp-syn-ack outbound 100`**

Block DoS attack traffic from a specific host

This section provides the high-level steps, with examples, on how to block a host that is launching a DoS attack.

1. Keep the inline Sensor in learning mode for 48 hours so that normal traffic pattern is learnt.
2. Send some particular type of traffic from selected IP addresses through the Sensor during the learning mode, that is, for the first 48 hours.

   For example, send 5 Mbps of UDP packet type to the Sensor from selected IP address, such as **`10.10.0.1, 198.19.0.2, 120.100.10.1, 100.10.10.11 and 99.40.10.30.`**

   > **NOTE**
   >
   > The Sensor automatically switches to detection mode after the first 48 hours.

3. Enable blocking for the corresponding attack in the DoS policy.

   For example, enable blocking for **Inbound UDP Packet Volume Too High** attack definition in the DoS policy.

4. Set the maximum value on the Sensor using the CLI command: **`set dospreventionseverity <packet type> <direction> <value>`**
5. Send significantly more similar traffic from the selected IP address through the Sensor than what was sent during the learning mode.

   For example, send more than 50 Mbps traffic from the IP address 10.10.0.1. Now, the traffic from the IP address 10.10.0.1 is blocked.

Viewing a DoS profile

The **`show dospreventionprofile`** command, when executed, displays the specified DoS prevention profile information for the Sensor that is defined in two arguments: a DoS measure name and a traffic direction.

Syntax:

`show dospreventionprofile <dos-measure-name> <inbound | outbound>`

Parameter	Description
<dos-measure-name>	Indicates the DoS measure name — one of **`tcp-syn`**, **`tcp-syn-ack`**, **`tcp-fin`**, **`tcp-rst`**, **`udp`**, **`icmp-echo`**, **`icmp-echo-reply`**, **`icmp-non-echo-reply`**, **`ip-fragment`**, or **`non-tcp-udp-icmp`**.
<direction>	Indicates the direction. It can be **`inbound`** or **`outbound`**.

Example - Command execution:

`show dospreventionprofile udp inbound`

Information displayed by the **`show dospreventionprofile`** command includes the Sensor's DoS profile and the traffic direction protected by the profile.

Example - Result:

```
 show dospreventionprofile udp inbound

packet type: UDP IN (12), profile stage: normal operation (65)

long-term average rate=0.000(pkts/s), last_rate=0.000(pkts/s)

no attack in progress

each line: bin_index, IP_prefix/prefix_len, AS, LT, ST, ltR(ate), stR(ate)

AS(%) -- percentage of the IP address space this bin occupies

LT(%) -- percentage of long-term traffic that falls into this bin

ST(%) -- percentage of short-term traffic that falls into this bin

ltRate -- long-term average traffic rate (in pkts/s) for this bin

stRate -- short-term traffic rate (in pkts/s) for this bin

0: 0.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000
```

```
1: 128.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000

2: 64.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000

3: 192.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000
```

The following is an example of a "bad" bin marked with a "*". The Sensor blocks packets with source IPs in the particular bin.

```
0: 0.0.0.0/6 AS=1.563% LT=49.969% ST=100.00% stR=1.000

1: 128.0.0.0/2 AS=25.000% LT=0.021% ST=0.00% stR=0.000

*2: 64.0.0.0/2 AS=25.000% LT=1.615% ST=100.00% ltR=2357.098 stR=148966.400

3: 192.0.0.0/2 AS=25.000% LT=0.021% ST=0.00% stR=0.000

4: 32.0.0.0/3 AS=12.500% LT=0.000% ST=0.00% stR=0.000

5: 16.0.0.0/4 AS=6.250% LT=0.000% ST=0.00% stR=0.000

6: 8.0.0.0/5 AS=3.125% LT=0.000% ST=0.00% stR=0.000

7: 4.0.0.0/6 AS=0.000% LT=11.752% ST=0.00% ltR=16885.654 stR=0.000
```

Viewing DoS prevention severity

The **show dosPreventionseverity** command, when executed, displays the severity for a specified denial of service profile.

Syntax

show dosPreventionseverity <dos-measure-name> <inbound | outbound>

Parameter	Description
<dos-measure-name>	Indicates the DoS measure name — one of **tcp-syn**, **tcp-syn-ack**, **tcp-fin**, **tcp-rst**, **udp**, **icmp-echo**, **icmp-echo-reply**, **icmp-non-echo-reply**, **ip-fragment**, or **non-tcp-udp-icmp**.
<direction>	Indicates the direction. It can be **inbound** or **outbound**.

Example - Command execution

show dospreventionseverity tcp-syn-ack outbound

Example - Result

```
DOS Prevention Severity for tcp-syn-ack outbound is 30
```

Connection Limiting policies

Connection Limiting policies consist of a set of rules that enable the Sensors to limit the number of connections a host can establish or a connection rate.

The Sensor provides the ability to define threshold values to limit number of connections (three-way handshakes for TCP) a host can establish. The number of connections or the connection rate that is less than or equal to the defined threshold value

is allowed, whereas the same exceeding the value is dropped. This helps in minimizing connection-based DoS attacks on your network.

The integration of this technology with Trellix GTI IP Reputation helps to define the connection limiting rules for traffic to and from external hosts based on reputation and geographical-location of the external hosts. These defined Connection Limiting policies can also be assigned at the interface and subinterface levels.

Examples:

- When 100 active HTTP connections are limited from a single source, subsequent connections are dropped.
- When 500 active overall connections (all TCP and UDP) are limited from a single source, subsequent connections are dropped.
- When 200 DNS requests per second are limited from a single source, subsequent connections within this time interval are dropped.

NS-series Sensors provide capability to limit the number of connections a host can establish or a connection rate.

The policy specifies connection rules of following two types:

- Trellix GTI based to limit connection rate based on reputation and/or geo location of external hosts.
- Protocol based to limit TCP/UDP/ICMP connections or connection rate from a host.

Both the above-mentioned rules are specified on a per direction basis. The connection policy is assigned to interface or subinterface level. Trellix GTI-based rules are only applicable when IP Reputation is enabled on the interface or subinterface level. They query the IP Reputation server to get reputation and geographical location of the external host.

NOTE

In case of Trellix GTI-based rules, connection limiting is applicable only to IPv4 traffic. Protocol-based rules are applicable for both IPv4 and IPv6 traffics.

How Connection Limiting policies work

You can create the Connection Limiting policy at the admin domain level. You can configure the Connection Limiting policy with the monitoring ports in SPAN, tap, or inline modes.

NOTE

The response actions differ for SPAN and tap modes. In these modes, the Sensor cannot block the connections or quarantine the hosts.

The connections are limited based on the predefined threshold value. The threshold value is defined as connections per second or active connections. For example, if you define 1 connection per second as the threshold value, then, 10 connections are allowed per 10 seconds. So, if there are 10 connections in the first second, all the other connections from the second to the tenth second are dropped. On the other hand, if you have 1 connection for each second, all the 10 connections until the tenth second are allowed. This is also known as *traffic sampling.*

NOTE

The minimum and maximum threshold values are 1 connection per second and 65535 connections per second respectively.

After you create a Connection Limiting policy, you can assign it to a Sensor's interfaces and subinterfaces.

NOTE

These Sensor resources must be of type VLAN or CIDR. You can assign the policy to these levels depending upon the configuration of the monitoring ports.

After you assign the Connection Limiting policy, the Sensor limits the connections based on the configured threshold values. An alert is sent each time the connection exceeds the defined threshold value. You can have any of the following response actions for that connection:

- Alert only
- Alert and drop excess connections
- Alert and deny excess connections
- Alert and quarantine

Considerations for Connection Limiting policies

Consider the following when you use Connection Limiting policies:

- Threshold values defined in any rule are based on the source IP address.
- A maximum of 1024 rules can be defined for each Sensor.
- Traffic sample time for the connection rate monitoring is 10 seconds. This means if you define 5 connections per second, then, 50 connections are limited in 10 seconds. So, an alert will only be raised if you send more than 50 connections in 10 seconds.
- In a fail-over setup, each Sensor monitors the traffic based on its own system time. As the system time for each Sensor differs, the time each Sensor samples a traffic might not be exactly same. This can result in a mismatch of the connection limiting response actions for each Sensor.
- Each Sensor model has a limitation of a maximum number of new hosts that it can handle per second. When the new host rate exceeds this value, the connections are not limited by the Sensor.
- Protocol based connection limiting rule type applies to both IPv4 and IPv6 traffic. Trellix GTI does not support IPv6 traffic, so GTI-based connection limiting rule type applies to IPv4 traffic only.
- Connection Limiting rules can be applied to SPAN ports. If CIDRs are not defined for the SPAN port, inbound connection limiting rules are applied to all traffic on SPAN port. If CIDR is defined for the SPAN port, the traffic to the CIDR is treated as inbound traffic and traffic from the CIDR is treated as outbound traffic.
- Trellix GTI IP Reputation has to be enabled for Trellix GTI rule type.
- Connection Limiting is applicable for stateless inspection.

The following table shows the maximum host entries supported for different Sensor models.

Sensor	Maximum host entries supported
NS9500 stack - 100 Gbps throughput	256,000
NS9500 stack - 60 Gbps throughput	256,000
NS9500 stack - 40 Gbps throughput	256,000
NS9500 standalone - 30 Gbps throughput	256,000
NS9500 standalone - 20 Gbps throughput	256,000
NS9500 standalone - 10 Gbps throughput	256,000
NS9300, NS9200, NS9100	256,000
NS7600 - 15 Gbps	256,000
NS7600 - 10 Gbps	256,000
NS7600 - 5 Gbps	256,000
NS7500 - 7.5 Gbps	256,000
NS7500 - 5 Gbps	256,000
NS7500 - 3Gbps	256,000
NS7350, NS7250, NS7150	256,000
NS7300, NS7200, NS7100	256,000
NS5200, NS5100	128,000
NS3600 - 5 Gbps	256,000
NS3600 - 3 Gbps	256,000
NS3600 - 1 Gbps	256,000
NS3500	128,000
NS3200, NS3100	128,000
IPS-VM600	128,000
IPS-VM5000	128,000

Components of Connection Limiting rules

You define Connection Limiting rules in a Connection Limiting policy. To effectively use Connection Limiting policies, familiarize yourself with the components that make up a Connection Limiting rule.

Figure 473. Connection Limiting rules options

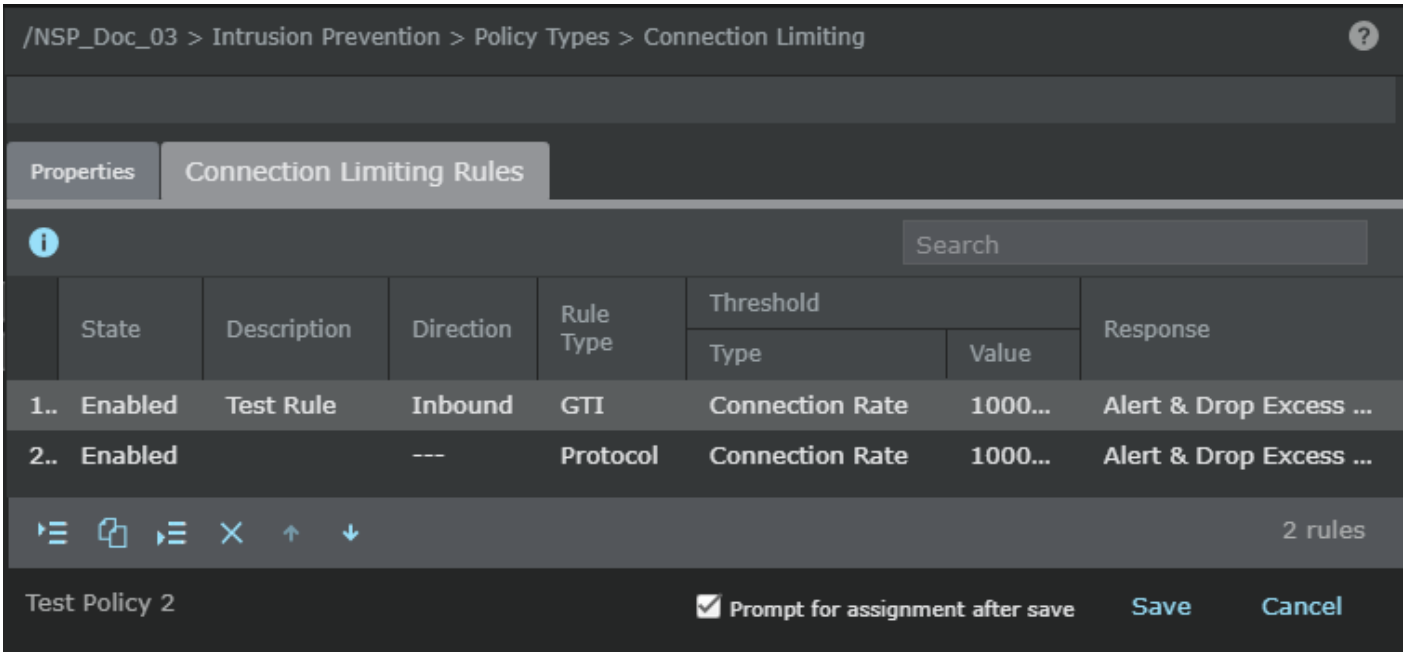
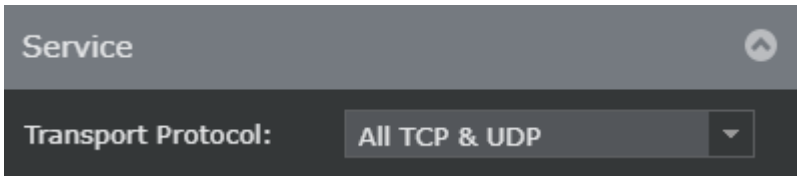


Table 57. Connection Limiting rules option definitions

Option	Definition
#	Displays the serial number of the rule. This is referenced in the alerts.
State	Displays whether a rule is enabled or disabled. Sensor does not apply disabled rules. This option might help you during troubleshooting.
Description	Optionally enter additional information about the rule. You can enter a description up to 64 characters long and click **OK**.
Direction	• **Inbound** — To apply this rule only to traffic seen at the outside port. • **Outbound** — To apply this rule only to traffic seen at the inside port. • **Any** — To apply this rule at both the ports.
Rule Type	• **Protocol** — To limit TCP/UDP/ICMP active connections or connection rate from a host. • **GTI** — To limit connection rate based on reputation and/or geo-location of external hosts. **NOTE** Trellix GTI-based rules are only applicable when Trellix GTI IP Reputation is enabled. **NOTE** Both the rule types are specified on a per-direction (inbound/outbound) basis.

Option	Definition
Threshold	**Type** : • **Connection Rate** — The rate of the connection defined per second. • **Active Connections** — The number of active connections. **NOTE** Only **Connection Rate** is available for Trellix GTI rules.
	Value: Define the connections per second or the number of active connections based on the threshold type you selected.
External	**Reputation** : Select one of the external Trellix GTI reputations (risk levels): • **High Risk** • **Medium Risk or High Risk** • **Unverified, Medium or High Risk** • **Any** **NOTE** This option is applicable only for Trellix GTI rule type.
	Location : Select the external geo-location (Trellix GTI countries). **NOTE** This option is applicable only for Trellix GTI rule type.

Option	Definition
Service	Select one of the following transport protocols from the **Transport Protocol** drop-down list: • **TCP** (You can specify the port number for TCP protocol.) • **UDP** (You can specify the port number for UDP protocol.) • **Ping (ICMP echo Request)** • **All TCP & UDP** **Figure 474. Service option**  **NOTE** Service component is only applicable for protocol rule type.
Response	Select the response action that the Sensor must perform when the traffic matches the options you specified in the Connection Limiting rule. The following are the response options: • **Alert Only** • **Alert & Drop Excess Connection** • **Alert & Deny Excess Connection** • **Alert & Quarantine**
Prompt for assignment after save	When selected, the **Assignments** window opens when you save a policy and you can assign the policy to the required Sensor resources. When deselected, the rule is saved in the Manager database and the policy appears in the **Connection Limiting** list.
Save	Saves the Connection Limiting rules in the Manager database. The Connection Limiting policy is listed in the **Connection Limiting** list.

Comparison between Protocol and Trellix GTI rule type

The following table shows the comparison between the two rule types.

Table 58. Protocol and Trellix GTI rule types - comparison

Rule components	Protocol rule type	Trellix GTI rule type
Description	Applicable	Applicable
Direction	Applicable	Applicable

Rule components	Protocol rule type	Trellix GTI rule type
Threshold Type	Both the threshold types are applicable	Only **Connection Rate** threshold type is applicable
Threshold	Applicable	Applicable
External Reputation	Not applicable	Applicable
External Location	Not applicable	Applicable
Service	Applicable	Not applicable
Response	Applicable	Applicable

Considerations for rule types

Follow these considerations for the rule types.

- **For Protocol rule type**:
  - In one policy, for one direction, only one *All TCP/UDP* connection rate rule can be defined.
  - In one policy, for one direction, only one *All TCP/UDP* active connection rule can be defined.
- **For Trellix GTI rule type**:
  - For Trellix GTI connection rate rule, geo-location and risk level should not be "any" at the same time.
  - For Trellix GTI connection rate rule, defined risk level means the selected risk level and above. For example, medium risk rules can be applied to high risk traffic if no high risk rule is defined.
  - For one specific geolocation, user can only create two Trellix GTI rules:
    - One Trellix GTI rule with a specific reputation level (high risk, medium risk, unverified, minimal risk) defined: this rule will apply to the traffic for this geo-location has the reputation same or worse than the defined level. The level defined in this rule can be taken as the malicious cut off level for this geo-location.
    - One Trellix GTI rule with ANY reputation: this rule will apply to ANY traffic for this geo-location (including all reputation levels and even for the traffic that has no reputation information available). This rule is only based on geo-location and can work even without Trellix GTI enabled (as long as the geo-location database is pushed to the Sensor).
  - For Trellix GTI connection rate rule, for outbound direction, "Quarantine" response action is not applicable.
  - When different rule types affect same traffic, the action is taken for the threshold hitting first.

    The rule applying order is as follows:

    Proto-conn-rate-rule->proto-active-conn rule -> all TCP/UDP conn-rate-rule->all TCP/UDP active-conn-rule->geoLocation specific reputation GTI-conn-rate-rule->geoLocation specific Any reputation GTI-conn-rate-rule->Any geoLocation reputation specific GTI_conn_rate_rule
  - No Trellix GTI rules apply to allowed hosts.
  - When Trellix GTI is enabled and Connection Limiting rules are configured, you can block the malicious traffic received on the inbound connections. For example, you can deploy a Sensor in front of a web server, and enable Trellix GTI along with Connection Limiting rules to limit access to the server and prevent DoS attacks.

Effects of X-Forwarded-For (XFF) on connection limiting

Review this section to know how the Sensor implements Connection Limiting policies if you have enabled XFF.

Effect on HTTP traffic when XFF is enabled

When XFF is enabled, it is assumed that all HTTP traffics on that VIDS level are XFF traffic. No connection limiting is done if the traffic is non-XFF when XFF is enabled.

Sensor checks the XFF traffic against protocol-based rules. When the connections exceed the threshold value, a response action is triggered. An alert can be raised or the connection can be blocked based on the configuration.

NOTE

This works irrespective of syn cookie setting. Quarantine response is not supported for XFF traffic.

Effect on HTTPS traffic when XFF is enabled

When SSL is disabled, the Sensor handles the connection limiting for HTTPS traffic based on the source IP address. It is not dependent on whether XFF is enabled or not.

When SSL is enabled, and if the Sensor cannot decrypt the traffic (no server certificate on Sensor), no connection limiting takes place for XFF and non-XFF HTTPS traffic.

When SSL is enabled, and if the Sensor can decrypt the traffic (Sensor has server certificate), no connection limiting takes place for non-XFF https traffic.

NOTE

The behavior of connection limiting is same for XFF HTTPS and HTTP traffics.

Effect of non-standard port on HTTP/HTTPS traffic

By default, XFF connection limiting is only performed for HTTP/HTTPS traffic on standard port. If the HTTP/HTTPS traffic runs on non-standard port, you must define the non-standard port on Manager.

Effect of XFF IP address on an alert

An XFF IP address can be IPv4 or IPv6 irrespective of the proxy IP address (it can also be IPv4 or IPv6). Connection limiting is only based on XFF IP address and not the proxy IP address.

NOTE

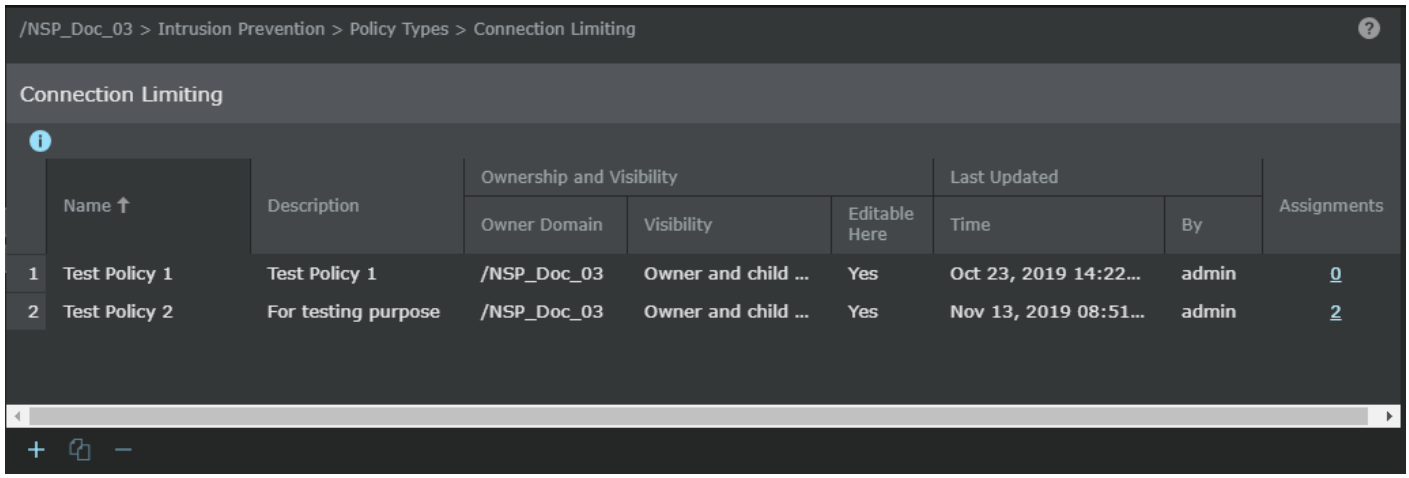
Trellix GTI does not support XFF IP address, so no Trellix GTI rule types are applied to XFF traffic.

If both XFF and connection limiting are enabled, **no** connection limiting processing will be done for normal non-XFF https traffic.

Create, clone, and modify Connection Limiting policies

You can create and manage Connection Limiting policies at an admin-domain level. After you create the Connection Limiting policies for an admin domain, you can assign it to the corresponding Sensor interfaces and sub-interfaces.

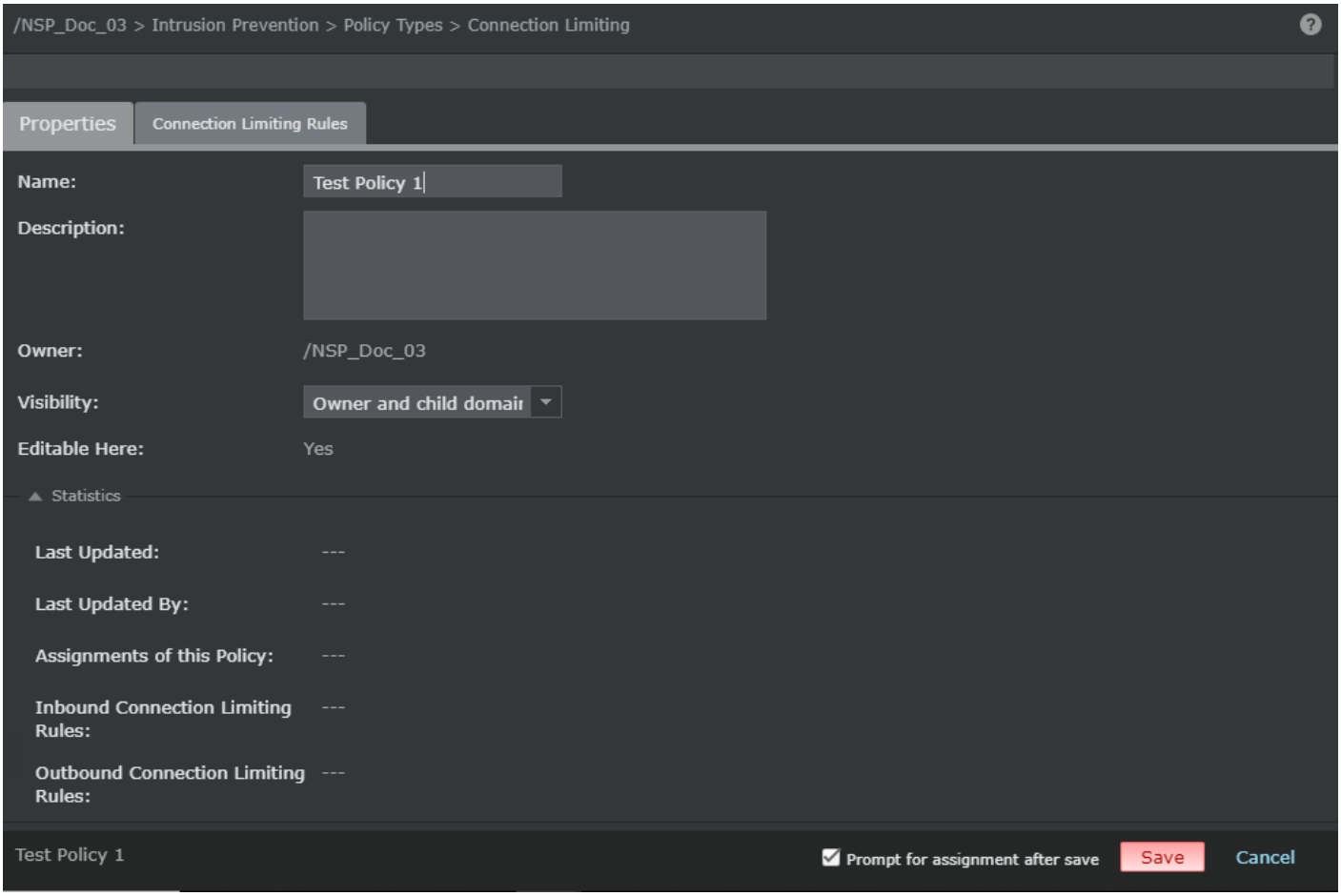
1. Select Intrusion Prevention → Policy Types → **Connection Limiting**.



2. Click + to create a new policy.

   The **Properties** tab opens.

3. Specify the details on the **Properties** tab.



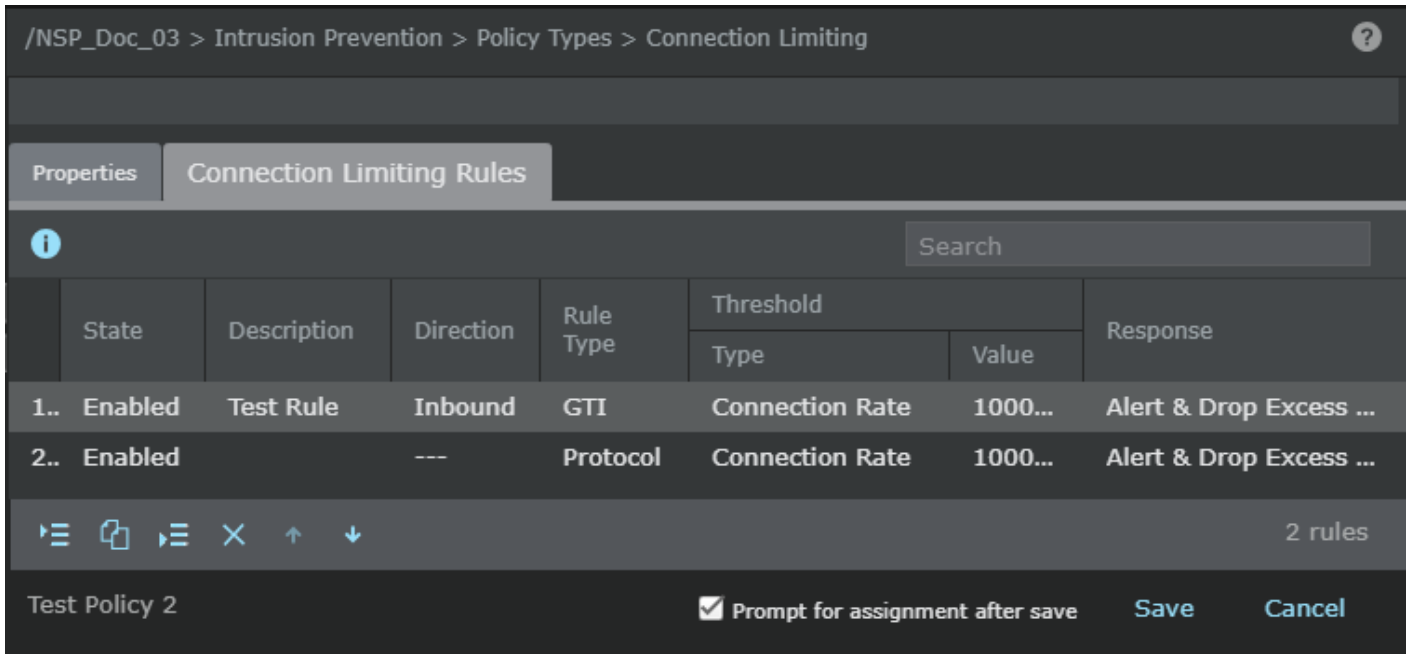
Option	Definition
Name	Enter a unique name to easily identify the policy.
Description	Optionally describe the policy for other users to identify its purpose.
Owner	Displays the admin domain to which the policy belongs
Visibility	Select **Owner domain only** to make the policy available only to the owner domain or select **Owner and child domains** to makes the policy available to the corresponding child admin domains. **NOTE** However, the policy cannot be edited or deleted from the child admin domains.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Statistics	**Lasted Updated** — Displays the time stamp when the policy was last modified
	Last Updated By — Displays the user who last modified the policy
	Assignments of this policy — Indicates the number of interfaces and sub-interfaces to which the policy is assigned

Option	Definition
	Inbound Connection Limiting Rules: Displays the number of Connection Limiting rules currently defined for inbound traffic
	Outbound Connection Limiting Rules: Displays the number of Connection Limiting rules currently defined for outbound traffic
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Saves the changes made on the **Properties** tab. This is visible only when you open an existing policy.
Next	Saves the changes made on the **Properties** tab and to access the **Connection Limiting Rules** tabbed region. This button is available only when you create a policy.
Cancel	Reverts to the last saved configuration

4. In the **Connection Limiting Rules**, click the appropriate button to insert a new rule.

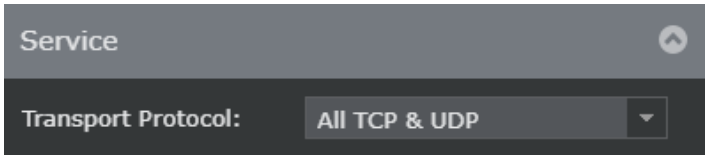
Button	Definition
	Inserts a new rule above the currently selected rule
	Inserts a new rule below the currently selected rule
	Clones the currently selected rule
	Deletes the currently selected rule
	Moves the currently selected rule one row up
	Moves the currently selected rule one row down

5. Double-click each column of a Connection Limiting rule and specify your choices.



Option	Definition
#	Displays the serial number of the rule. This is referenced in the alerts.
State	Displays whether a rule is enabled or disabled. Sensor does not apply disabled rules. This option might help you during troubleshooting.
Description	Optionally enter additional information about the rule. You can enter a description up to 64 characters long and click **OK**.
Direction	• **Any** — To apply this rule at both the ports • **Inbound** — To apply this rule only to traffic seen at the outside port • **Outbound** — To apply this rule only to traffic seen at the inside port
Rule Type	• **Protocol** — To limit TCP/UDP/ICMP active connections or connection rate from a host • **Trellix GTI** — To limit connection rate based on reputation and/or geo-location of external hosts **NOTE** Trellix GTI-based rules are only applicable when Trellix GTI IP Reputation is enabled. **NOTE** Both the rule types are specified on a per-direction (inbound/outbound) basis.

Option	Definition
Thresh-old	**Type**: • **Connection Rate** — The rate of the connection defined per second. • **Active Connections** — The number of active connections. **NOTE** Only **Connection Rate** is available for Trellix GTI rules.
	Value — Define the connections per second or the number of active connections based on the **Thresh-old Type** you selected.
External	**Reputation** — Select one of the external Trellix GTI reputations (risk levels): • **High Risk** • **Medium Risk or High Risk** • **Unverified, Medium or High Risk** • **Any** **NOTE** This option is applicable only for Trellix GTI rule type.
	Location — Select the external geo-location (Trellix GTI countries). **NOTE** This option is applicable only for Trellix GTI rule type.

Option	Definition
Service	Select a protocol from the Transport Protocol drop-down list: • **TCP** (You can specify the port number for TCP protocol.) • **UDP** (You can specify the port number for UDP protocol.) • **Ping (ICMP echo Request)** • **All TCP & UDP** **Figure 475. Service option**  **NOTE** Service component is only applicable for protocol rule type.
Response	Select the response action that the Sensor must perform when the traffic matches the options you specified in the Connection Limiting rule. The following are the response options: • **Alert Only** • **Alert & Drop Excess Connection** • **Alert & Deny Excess Connection** • **Alert & Quarantine**
Prompt for assignment after save	When selected, the **Assignments** window opens when you save a policy and you can assign the policy to the required Sensor resources. When deselected, the rule is saved in the Manager database and the policy appears in the **Connection Limiting** list.
Save	Saves the Connection Limiting rules in the Manager database. The Connection Limiting policy is listed in the **Connection Limiting** list.

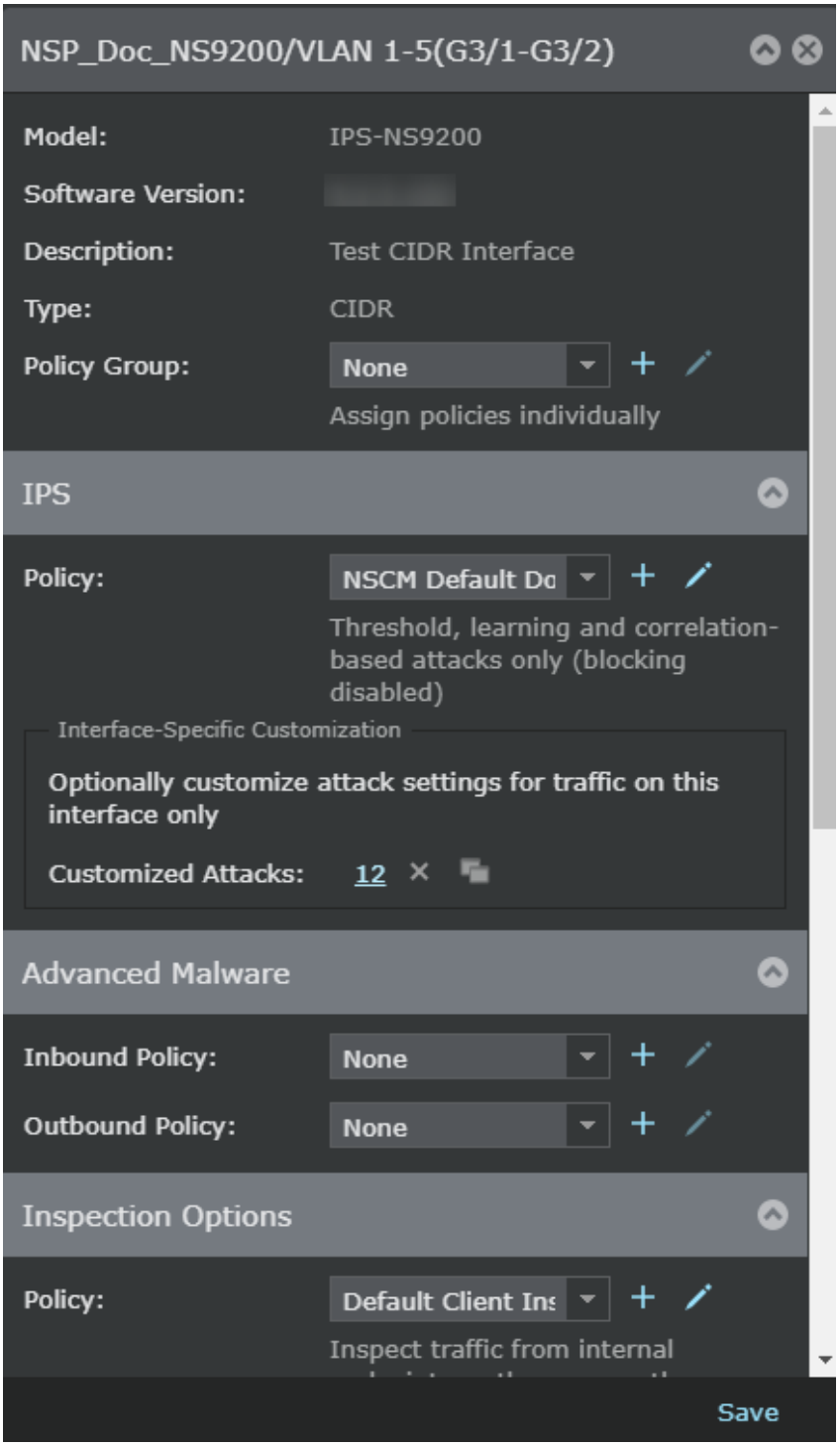
Assign a Connection Limiting policy to an interface or subinterface

After you define a Connection Limiting policy at the admin domain, you can assign it to an interface or subinterface.

Steps:

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Select Intrusion Prevention → **Policy Manager**.
4. Double-click on the interface to which you want to assign a connection limiting policy.

The **<Device Name/Interface>** panel opens on the right side.



5. Under the **Connection Limiting** section, select the policy from the **Policy** drop down list.
6. Click **Save**.
7. Deploy the configuration changes to the Sensor.

Alert for Connection Limiting policies

You can define the threshold values while creating rules in a Connection Limiting policy. When the Sensor monitors a traffic and the connection exceeds the configured threshold value, the connection is limited and an alert is raised. You can set any of the following response actions:

- Alert only
- Alert and drop excess connection
- Alert and deny excess connection
- Alert and quarantine

There is only one reconnaissance alert defined for the Connection Limiting feature: **Too Many TCP/UDP/ICMP Sessions**. You can view the alert in **Attack Log** under the **Analysis** tab. Double-click the alert to view the alert details.

Scenario

Same host triggering the same rule:

In this scenario, no alert will be sent to the Attack Log during the alert timeout interval. So, when a traffic is sent to the Sensor, you can see the alert only after 5 minutes the first alert is triggered. This condition is not true for the Connection Limiting alerts for different hosts or different rules.

> **NOTE**
>
> By default the alert timeout interval is 5 minutes. You can edit the alert timeout from the reconnaissance policy editor.

Exceed connection count

Exceed Connection Count is displayed by the Connection Limiting alert when the response action is **Alert Only**.

Sensor sends out Connection Limiting alert as soon as the pre-defined threshold value is reached. So, the first alert always shows **Exceed Connection Count** as 1. If the traffic continues and triggers another alert after the alert timeout interval (with same connection limiting policy), then the **Exceed Connection Count** displayed in the next alert equals to the exceed connection count that the Sensor monitors between these two alert time intervals.

If the traffic does not continue long enough to reach the next alert time interval, another Connection Limiting alert will not be triggered. In this case, even if the connection exceeds the configured threshold value, the connection will not be limited.

Connection Limiting Host Entries Exhausted alert

The connection is limited based on the threshold defined but no alerts are sent.

CLI commands

The following CLI commands are used for the debugging purpose for Connection Limiting policy.

- **`show connlimitstat`**: Shows connection limiting statistics

- **`show connlimithost`**: Shows connection limiting host table stats
- **`clrconnlimithost`**: Clears connection limiting host table

Refer to the [CLI commands] section for more details.

Working with Inspection options policies

You can create inspection options policies for configuring traffic inspection, advanced callback detection, endpoint reputation analysis, heuristic analysis of web server and prevention of denial of service on web server. After creating an inspection option policy, you can assign the policy to interfaces and subinterfaces.

Inbound traffic is that traffic received on the port designated as **Outside** (that is, originating from outside the network) in Inline or Tap mode. Typically, inbound traffic is destined to the protected network, such as an enterprise intranet. Outbound refers to any traffic that originated from your internal network. Outbound traffic is that traffic sent by a system in your intranet, and is on the port designated as **Inside** (that is, originating from inside the network) in Inline or Tap mode.

When GTI participation is enabled, the IP address reputation is applicable only for inbound connections. When GTI is enabled and Connection Limiting rules are configured, you can block the malicious traffic received on the inbound connections. For example, you can deploy a Sensor in front of a web server, and enable GTI with Connection Limiting rules to limit access to the server and prevent DoS attacks.

With the advanced traffic inspection options, the HTTP and SMTP traffic can be inspected and the traffic segments can be encoded or reassembled for detection of any threats and anomalies. For more information, refer Advanced Traffic Inspection (page 1507).

Advanced callback detection provides detailed information retrieved from different attack phases at the end of a successful correlation. For more information, refer Advanced Botnet Detection (page 987).

Endpoint reputation analysis configuration can be set for inbound and outbound traffic and to influence it for SmartBlocking. Endpoint reputation is determined using a combination of IP address and port. For more information, refer IP address Reputation (page 1525).

You can enable behavior-based detection of attacks against your Web servers, and optionally add blocked text. For more information, refer Implementing the Heuristic Web Application Server Inspection option (page 1134).

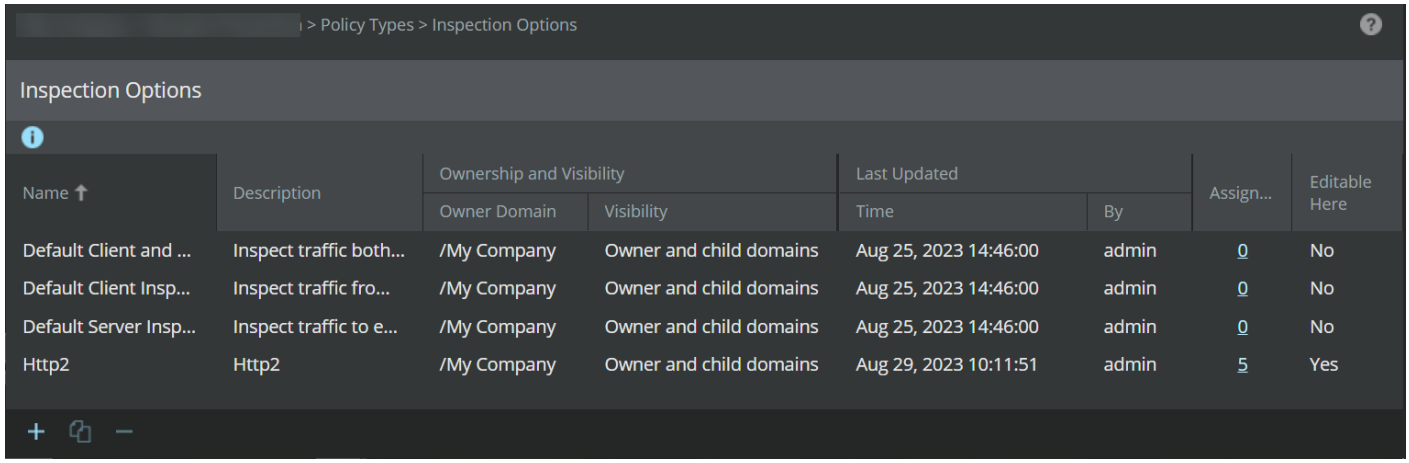
You can configure the Layer 7 DoS inspection options to prevent denial-of-service attacks against your Web servers. For more information, refer Layer 7 DoS protection for web servers (page 1064).

You create Inspection Options policies at the domain level. Then, you can apply the Inspection Options policy to the required Sensor interfaces and subinterfaces owned by that domain.

1. In the Manager, click **Policy** and then select the required **Domain**.
2. Go to Intrusion Prevention → Policy Types → **Inspection Options.**

   The **Inspection Options** page is displayed.

Figure 476. Inspection options policies page



The options in this page are as follows:

Option	Definition
Name	The name assigned to the inspection options policy.
Description	The description of the inspection options policy.
Owner	**Owner Domain Only**: Indicates the admin domain to which an inspection options policy belongs. **Owner and Child Domains**: Indicates that the policy is available to the corresponding child admin domains also.
Visibility	Indicates the visibility settings of settings to the domains, whether it is visible only to the owner domain or to both owner and child domains.
Editable here	Indicates whether you can edit or delete an inspection options policy from the current admin domain. You can edit but not delete the predefined IPS Policies. You can edit or delete a user-defined inspection options policy only from the admin domain from where it was created. **Yes** indicates that the IPS policy belongs to the current admin domain. If it is **No**, you cannot edit the IPS policy because it is defined at a parent admin domain.
Statistics	**Last Updated**: Displays the time when the inspection options policy was last updated.
	Last Updated By: Displays the user who changed the inspection options policy.
	Assignments: The number of interfaces and subinterfaces to which a policy is assigned. This information is according to the current information in the Manager database. Click the link in the **Assignments** column to assign the corresponding policy to the required interfaces and subinterfaces.
	Click to create an inspection options policy. The **Properties** and **Inspection Options** tabs are explained in the sections that follow.
	Select an inspection options policy and click to copy it. This is helpful especially if you want to use a non-editable policy with slight changes.
	Select any of the listed policies and click to edit or view the details.

Option	Definition
−	Select an eligible policy and click − to delete. Make sure that this policy is not assigned to any Sensor resources. To delete in bulk, select more than one policy and click −.

Add an inspection options policy

This page can be used to customize the policies as well as to configure the inspection options at the interface level. Inbound refers to any traffic destined for the internal network from an external source. Outbound refers to any traffic that originated from your internal network.

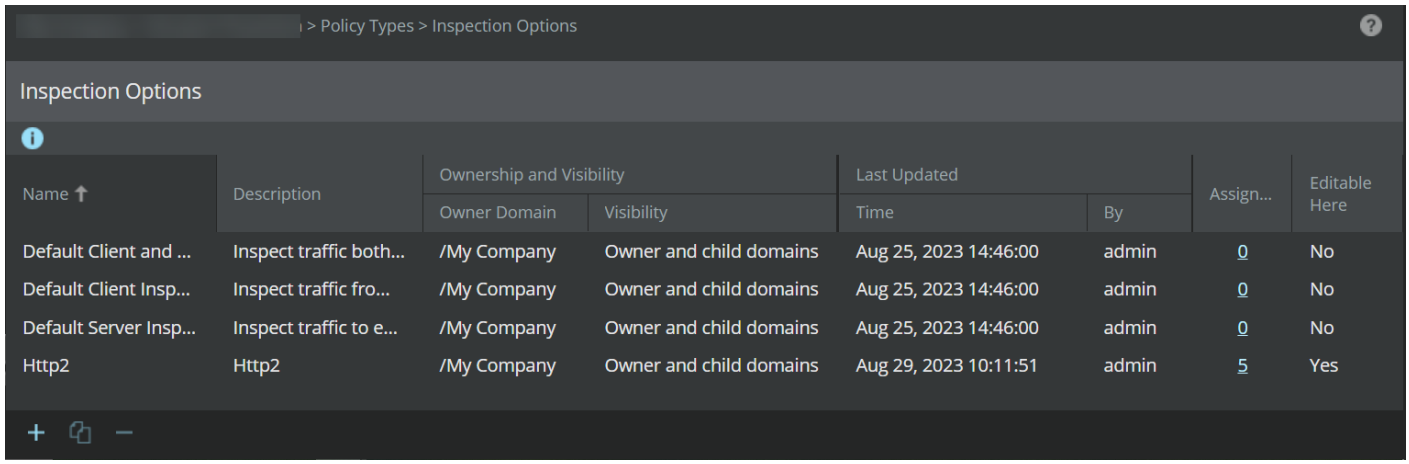
NOTE

Each window has either a **Save** or a **Cancel** button. Clicking **Save** saves the information to the database and closes all policy configuration actions. Clicking **Cancel** ends any operation and closes the window. If you want to continue creating or modifying a policy, do not click **Save** until you have completed every tab, step, or action available in the window.

1. In the Manager, click **Policy** and select the required **Domain.**
2. Select Intrusion Prevention → Policy Types → **Inspection Options.**

   The **Inspection Options** page is displayed.

Figure 477. Inspection Options Policies page



The following are the available default inspection options policies:

- **Default Client Inspection** — To inspect traffic from internal endpoints as they access the Internet
- **Default Server Inspection** — To inspect traffic to exposed Web and mail servers
- **Default Client and Server Inspection** — To inspect traffic both from internal endpoints and to exposed Web and mail servers

3. Click +.

   The **New Policy** window opens with the **Properties** tab selected.

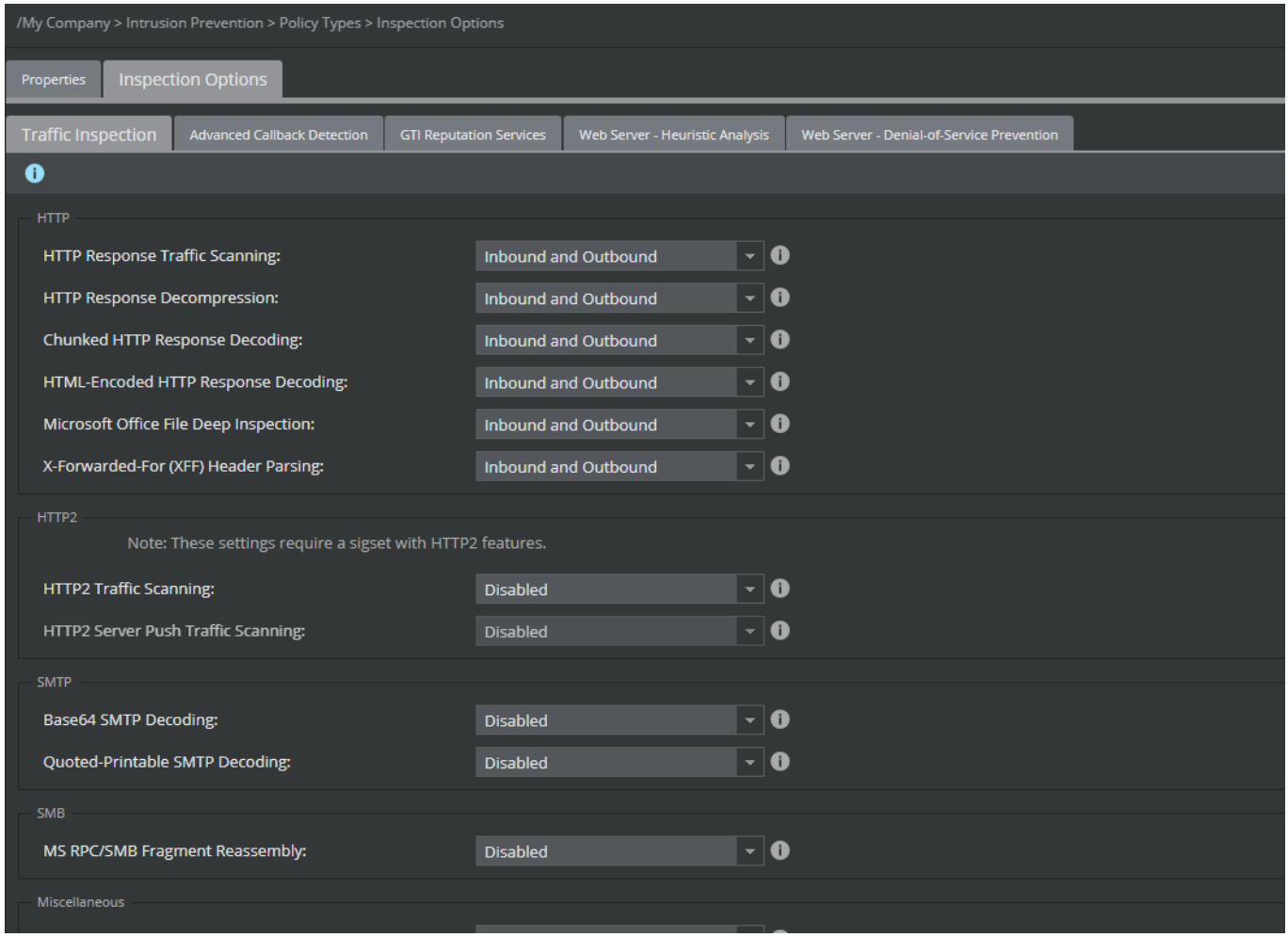
4. Update the following fields:

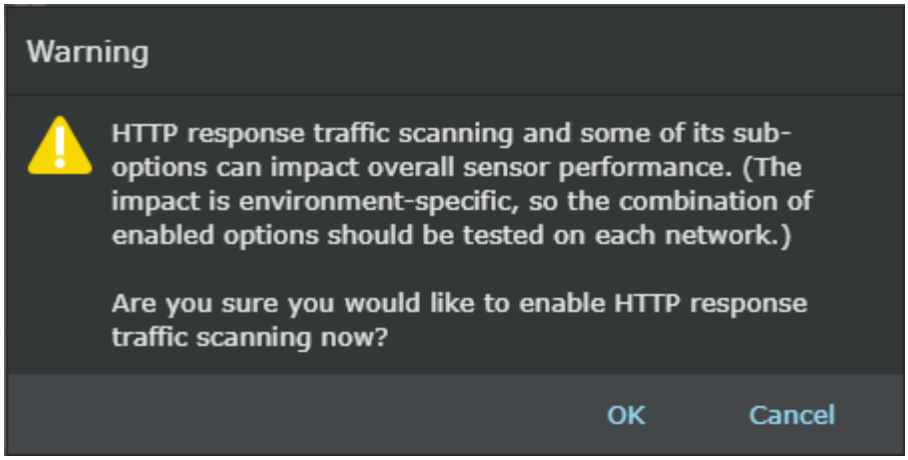
Option	Definition
Name	Enter a unique name to easily identify the policy.
Description	Describe the policy for other users to identify its purpose.
Owner	Displays the admin domain to which the policy belongs
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are **Owner and child domains** and **Owner domain only**.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain. This field is uneditable.
Statistics	
Lasted Updated	Displays the time stamp when the policy was last modified. This field is uneditable.
Last Updated By	Displays the user who last modified the policy. This field is uneditable.
Assignments	Indicates the number of inline ports to which the policy is assigned
Prompt for assignment after save	If you deselect this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the **Assignments** window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Cancel	Reverts to the last saved configuration

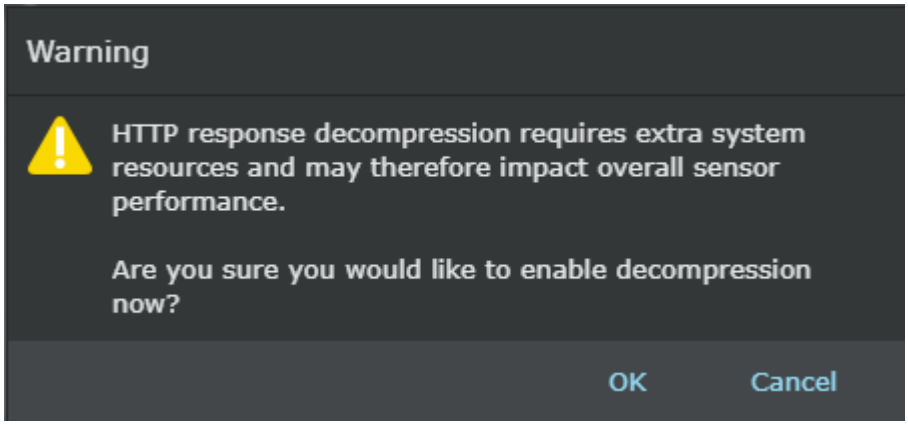
5. Click **Next**.

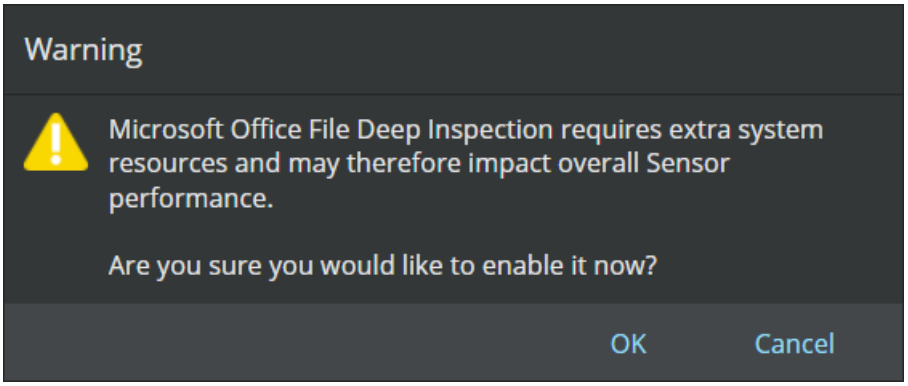
   The **Inspection Options** tab is displayed. By default, the **Traffic Inspection** tab within the **Inspection Options** tab is displayed.

Figure 478. Traffic Inspection



Option	Definition
HTTP Response Traffic Scanning	Enabling this option instructs the Sensor to inspect HTTP response headers and payload for attacks. The **HTTP Response Traffic Scanning** option is disabled by default because scanning response traffic requires extra system resources. To minimize the impact on performance, we recommend enabling this option only where necessary. When you enable the HTTP Response Traffic Scanning option a warning message is displayed. 

Option	Definition
HTTP Response Decompression	HTTP response traffic is commonly compressed in gzip format to improve performance. This format reduces transfer time and bandwidth consumption. However, attackers use it to evade detection of malicious payload. Enabling this option instructs the Sensor to decompress compressed HTTP response traffic for inspection. **NOTE** The **HTTP Response Decompression** option is disabled if the **HTTP Response Traffic Scanning** option is selected as disabled. When you enable the HTTP Response Decompression option a warning message is displayed. Review the warning message and click **OK** to proceed.  Note the following if you use this option: • HTTP response decompression is supported for gzip compressed files only. • Advanced malware inspection of decompressed files is not supported.
Chunked HTTP Response Decoding	Chunked transfer encoding is a data transfer mechanism of HTTP. The web server breaks the HTTP response content into chunks. Chunked transfer encoding uses the HTTP response header in place of the content-length header, which the protocol would otherwise require. Enabling this option instructs the IPS Sensor to decode chunked HTTP response traffic for inspection. **NOTE** **Chunked HTTP Response Decoding** field is disabled if the **HTTP Response Traffic Scanning** field option is selected as disabled.

Option	Definition
HTML-Encoded HTTP Response Decoding	HTTP response traffic can be sent using HTML encoding, and attackers can use this encoding mechanism to evade detection of malicious payload. Enable this for the Sensor to decode such traffic for inspection. Some of the encoding techniques used are: • Deflate — This compression technique is used mainly to compress data in PDF file formats. PDF documents support using “deflate” encoding in parts of the document. • HTML encoding — The HTML response data is encoded using the "&#" encoding technique. The encoding can be in decimal or hexadecimal format. • Base64 — Base64 encoding is used to encode binary data that is to be stored and transferred over media that are designed to deal with textual data. This encoding technique ensures that the data remains intact without modification during transport. Enabling this option instructs the IPS Sensor to decode HTML-encoded HTTP response traffic for inspection. **NOTE** **HTML-Encoded HTTP Response Decoding** is disabled when Response Scanning is disabled.
Microsoft Office File Deep Inspection	Microsoft Office version 2007 and later uses Office Open XML format, a zipped XML based file format. The zipped file contains multiple files upon extraction. Enabling this option instructs the Sensor to decompress compressed Office files for inspection. **NOTE** **Microsoft Office File Deep Inspection** field is disabled if the **HTTP Response Traffic Scanning** field option is selected as disabled. When you enable this option, a warning message is displayed. Review the warning message and click **OK** to proceed.  For more information, see Microsoft Office File Deep Inspection (page 1139).

Option	Definition
X-Forwarded-For (XFF) Header Parsing	Enabling this option allows the Manager to indicate when a connection has been proxied and report both the proxy server IP address and the true endpoint IP address.
HTTP2 Traffic Scanning	Enabling this option instructs the Sensor to inspect HTTP2 request and response traffic. **NOTE** • By default, HTTP2 traffic inspection is disabled. • **HTTP2 Traffic Scanning** can be enabled only when **HTTP Response Traffic Scanning** is enabled. For more information, see [Enable HTTP2 traffic inspection from the Manager] in the section HTTP2 traffic inspection (page 1635).
HTTP2 Server Push Traffic Scanning	Enabling this option instructs the Sensor to inspect HTTP2 push response from server. **NOTE** **HTTP2 Server Push Traffic Scanning** can be enabled only when **HTTP2 Traffic Scanning** is enabled.
Base64 SMTP Decoding	Enabling this option instructs the IPS Sensor to decode Base64-encoded SMTP for inspection.
Quoted-Printable SMTP Decoding	The SMTP protocol specification uses MIME content transfer encoding to transport binary data. Since SMTP protocol can handle only 7-bit ASCII data, each 3-byte group of binary data is converted to 6-bit number and replaced with an ASCII character. Quoted-printable and Base64 are the two basic MIME content transfer encodings. Quoted-printable encoding uses printable ASCII characters, such as alphanumeric and the equals sign (=), to transmit 8-bit data over a 7-bit data path. Enabling this option instructs the IPS Sensor to decode quoted-printable encoded SMTP for inspection.
MS RPC/SMB Fragment Reassembly	SMB is a network file sharing protocol. MS-RPC provides a framework for interprocess communication mechanism to exchange data between two processes residing on the same system or on two remote systems accessible over a network. MS-RPC's transport layer could be TCP, UDP, HTTP, or SMB. SMB protocol supports segmentation of its data. Also, MS-RPC protocol supports fragmentation of its payload. Since MS-RPC can be carried within SMB protocol data, either fragmentation or segmentation or a combination of both can be used to evade any network packet inspection device. Enabling this option instructs the IPS Sensor to reassemble MS RPC/SMB fragments for inspection.

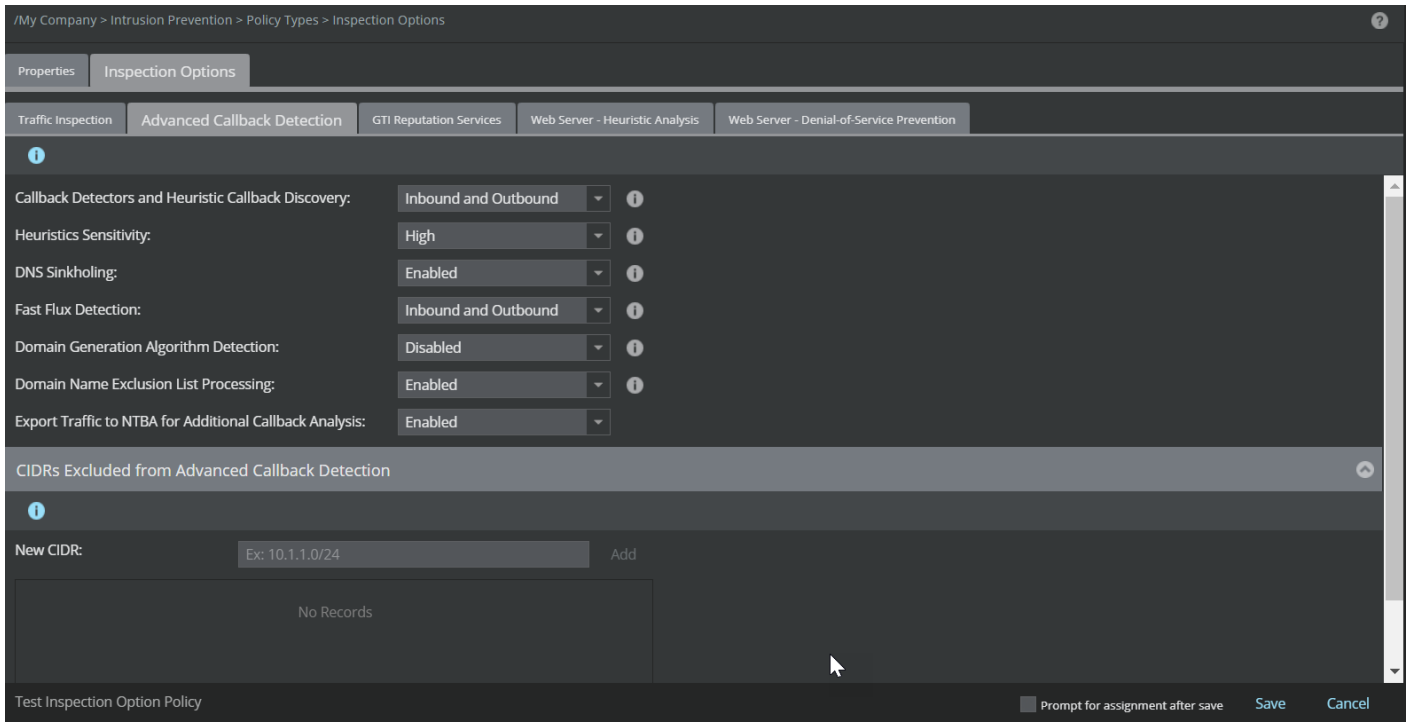
Option	Definition
Layer 7 Data Collection	Enabling this option instructs the Sensor to include Layer 7 information, such as HTTP URLs, SMTP email addresses, and FTP logon names, in alerts and to export them to NTBA appliances for analysis. The following options are available in this field: • **Disabled** • **Inbound Only** • **Outbound Only** • **Inbound and Outbound Only** By default, the option **Disabled** is selected.
Passive Device Profiling	Enabling this option instructs the Sensor to parse DHCP, TCP, and HTTP packets to identify the device type and operating system, and to make that information available for display for attack relevance analysis.
Simulated Blocking	Enabling this option instructs the Sensor to merely simulate blocking, sending a TCP reset, and ICMP host unreachable message. Simulation applies to signature-based attack definitions only. The following options are available in this field: • **Enabled** • **Disabled**
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Click **Save** to save the changes
Cancel	Reverts to the last saved configuration

All fields except **Simulated Blocking** have the following 4 options:

- **Disabled**
- **Inbound only**
- **Outbound only**
- **Inbound and Outbound**

6. Click the **Advanced Callback Detection** tab.

Figure 479. Advanced Callback Detection



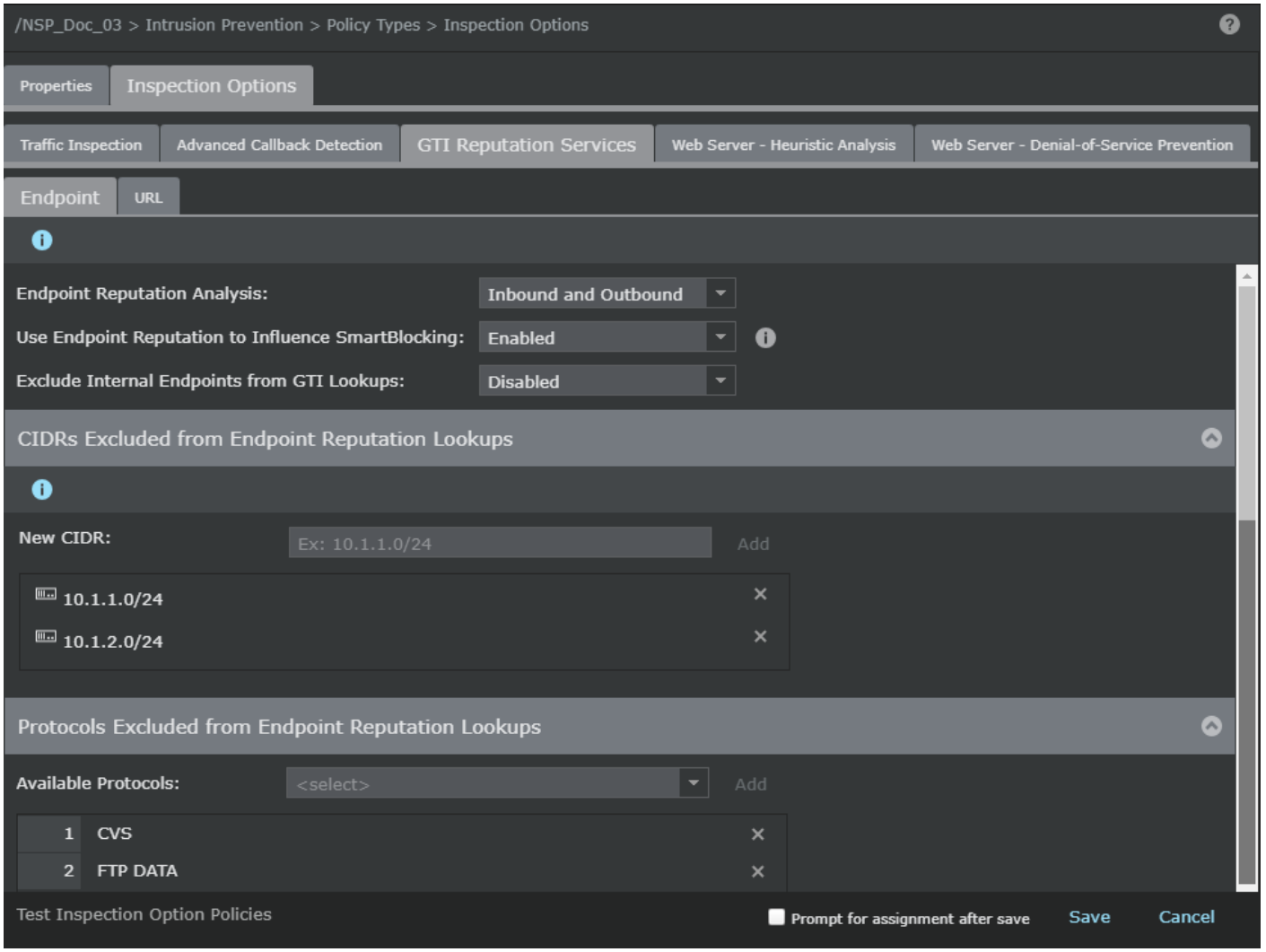
The **Advanced Callback Detection** tab displays the following fields:

Option	Definition
Callback Detectors and Heuristic Callback Discovery	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound** **NOTE** If you wish to disable **Layer 7 Data Collection** option in **Traffic Inspection** ensure that **Callback Detectors and Heuristic Callback Discovery** option is also disabled.
Heuristic Sensitivity	The sensitivity level determines the level of confidence the heuristic engine must have for the analysis. For example, when a low sensitivity level (default) is selected, the engine must have high confidence that it has detected a Bot before raising an alert. Select the following sensitivity level options: • **High** • **Medium** • **Low**

Option	Definition
DNS Sinkholing	Select any of the following options: • **Enabled** • **Disabled**
Fast Flux Detection	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**
Domain Generation Algorithm Detection	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**
Domain Name Exclusion List Processing	Select any of the following options: • **Enabled** • **Disabled**
Export Traffic to NTBA for Additional Callback Analysis	Enable this option to send the Botnet events to NTBA for further analysis.
CIDRs Excluded from Advanced Callback Detection	
New CIDR	Enter the new CIDR and click **Add** to add to the CIDR list to be excluded. Click ✕ to remove the CIDR from the list.
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Click **Save** to save the changes.
Cancel	Reverts to the last saved configuration

7. Click the **GTI Reputation Services** tab.

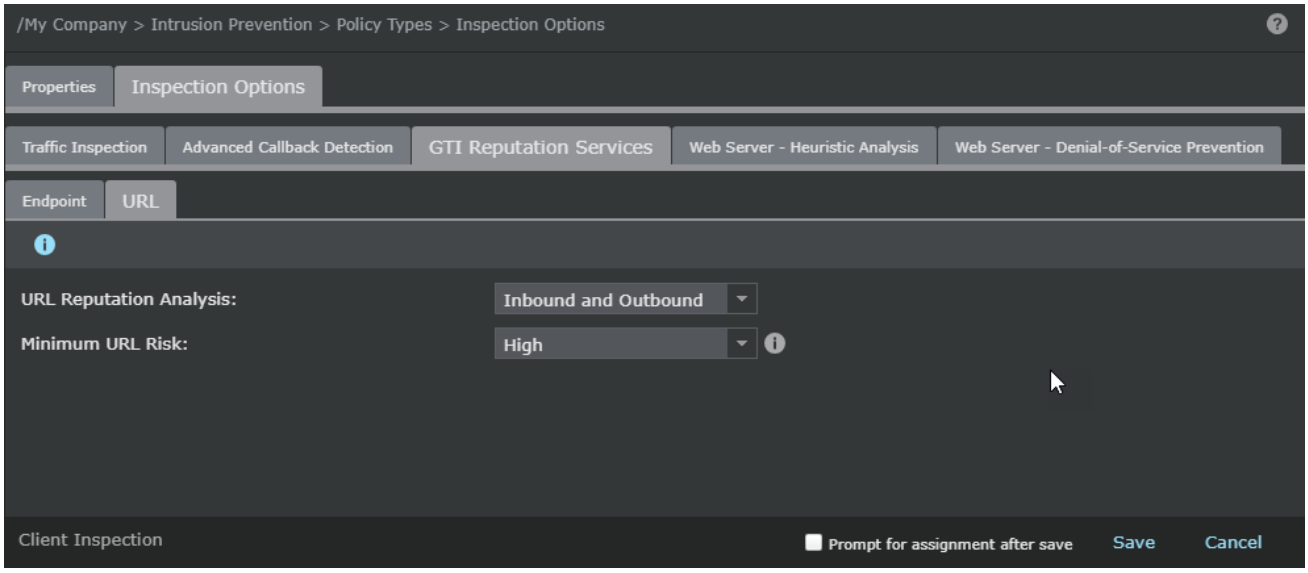
a. **Figure 480. Endpoint Reputation Analysis**



The **Endpoint** sub-tab in the **GTI Reputation Services** tab displays the following fields:

Option	Definition
Endpoint Reputation Analysis	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound** **NOTE** Make sure **Layer 7 Data Collection** is enabled in **Traffic Inspection** tab to detect the GTI risky URL attacks.
Use Endpoint Reputation to Influence SmartBlocking	Select **Enabled** to enable endpoint reputation to Influence SmartBlocking. Select **Disabled** to disable the option.
Exclude Internal Endpoints from GTI Lookups	Select **Enabled** to exclude internal endpoints from Trellix GTI Lookups. Select **Disabled** to disable the option.
CIDRs Excluded from Endpoint Reputation Lookups	
New CIDR	Enter the new CIDR and click **Add** to add to the CIDR list to be excluded. Click ✕ to remove the CIDR from the list. **NOTE** The CIDR exclusion list is shared by **Advanced Callback Detection** and **Endpoint Reputation Analysis**
Protocols Excluded from Endpoint Reputation Lookups	In the drop-down list, select the protocol to be excluded from Trellix GTI Lookups and click **Add**. The selected protocol is displayed in the field below. Click ✕ to remove the protocol from the list.
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Click **Save** to save the changes.
Cancel	Reverts to the last saved configuration

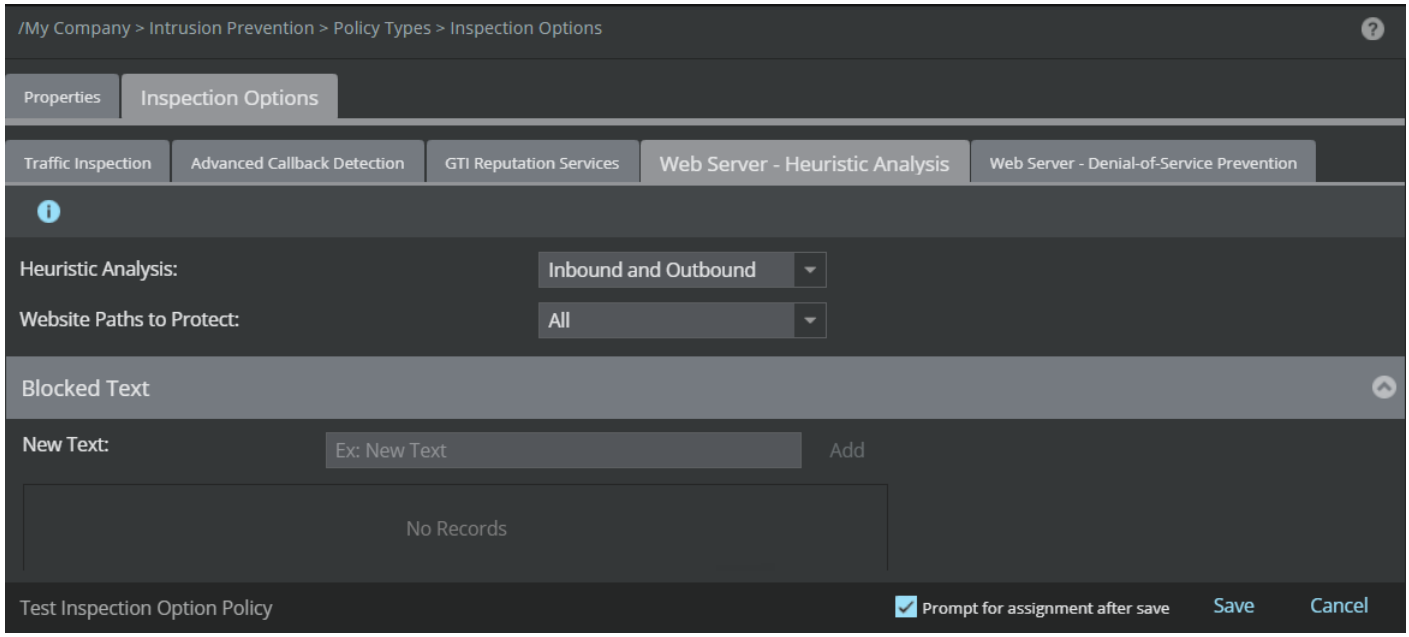
b. The **URL** sub-tab in the **GTI Reputation Services** tab displays the following fields:



Option	Definition
URL Reputation Analysis	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**
Minimal Risk URL	Select any of the following options: • **Medium** • **High**
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Click **Save** to save the changes.
Cancel	Reverts to the last saved configuration

8. Click the **Web Server- Heuristic Analysis** tab. In the **Web Server- Heuristic Analysis,** you can enable behavior-based detection of attacks against your web servers. You can also optionally add blocked text, such as the name of a stored procedure that is treated as an attack.

Figure 481. Web Server- Heuristic Analysis



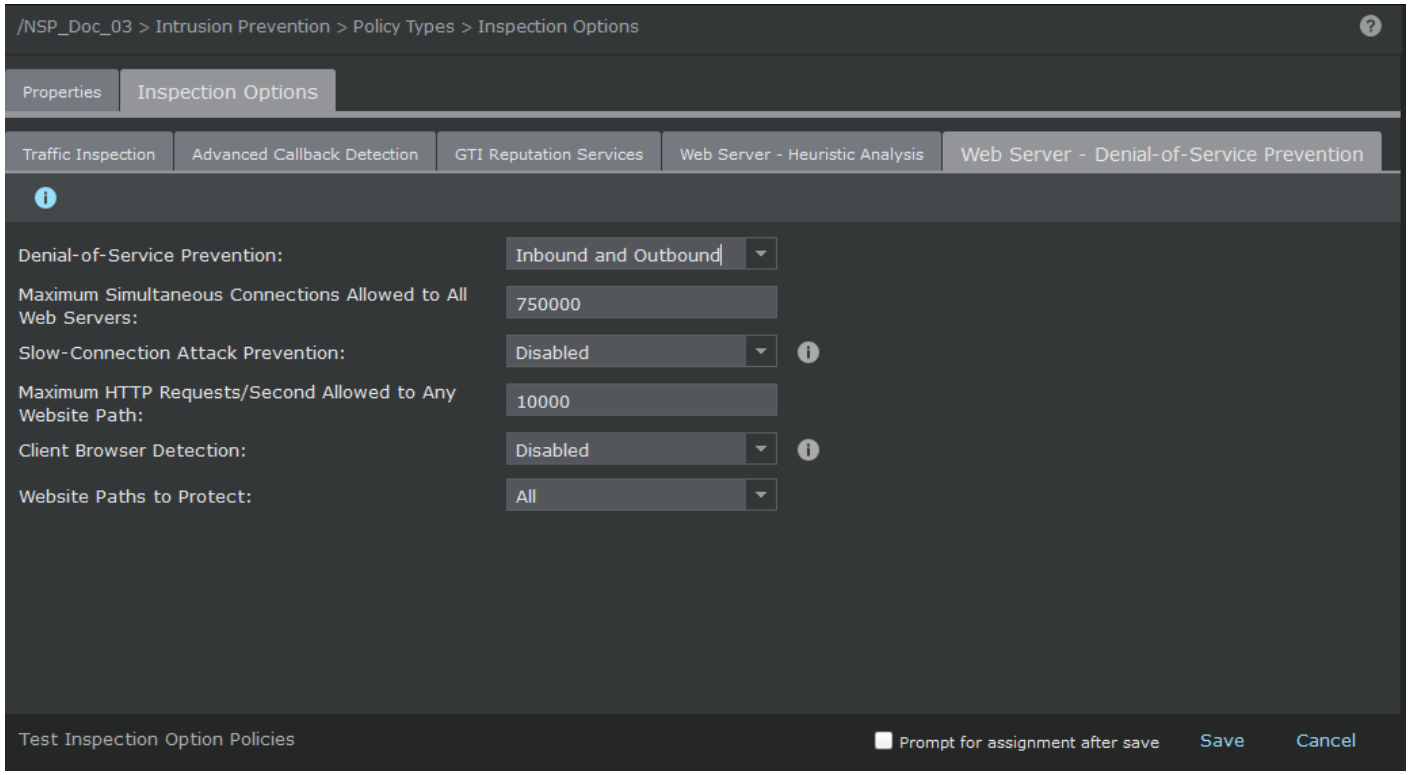
The **Web Server- Heuristic Analysis** tab displays the following fields:

Option	Definition
Heuristic Analysis	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**
Website Paths to Protect	Select **All** to protect all website paths or select **Specific** to protect specific website paths.
Website Paths to Protect	
New Website Path	Enter the website paths that you want to protect and click **Add**. The website path is displayed in the field below. Click ✕ to remove the website path from the list. **NOTE** This field is displayed only when you select the option **Specific** in field **Website Paths to Protect**
Blocked Text	

Option	Definition
New Text	Enter the blocked text which is treated as an attack and click **Add**.The blocked text is displayed in the field below. Click ✕ to remove the blocked text from the list.
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Click **Save** to save the changes.
Cancel	Reverts to the last saved configuration

9. Click the **Web Server - Denial-of-Service** tab. In **Web Server - Denial-of-Service,** you can configure to prevent denial-of-service attacks.

Figure 482. Web Server - Denial-of-Service Prevention



The **Web Server - Denial-of-Service Prevention** tab displays the following fields:

Option	Definition
Denial-of-Service Prevention	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**

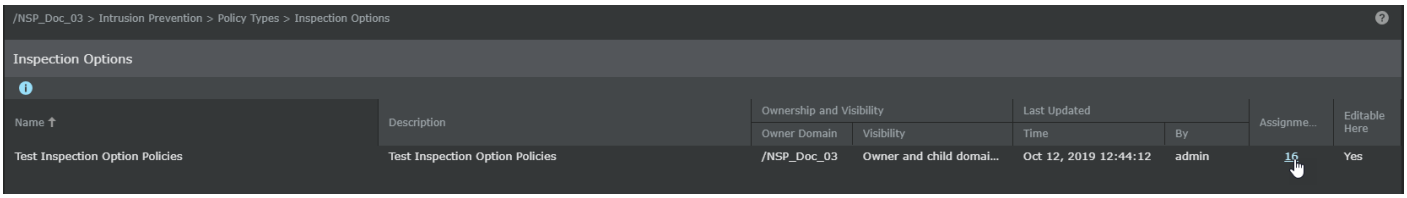
Option	Definition
Maximum Simultaneous Connections Allowed to All Web Servers	Specify the threshold for maximum connections allowed to all web servers.
Slow-Connection Attack Prevention	Select the option **Enabled** to close 10 percent of the oldest slow open connections. This option is **Disabled** by default.
Maximum HTTP Requests/Second Allowed to Any Website Path	Specify the maximum HTTP requests/second that should be allowed to any website path.
Client Browser detection	Select the option **Enabled** or **Disabled**.
Browser Detection Method	The detection methods use the challenge/response mechanism to detect a valid client browser. The options are **HTML Challenge** and **JavaScript Challenge** **NOTE** This field is displayed only when you select the option **Enabled** in field **Client Browser detection**
Website Paths to Protect	Select **All** to protect all website paths or select **Specific** to protect specific website paths.
Website Paths to Protect	
New Website Path	In the first text field, enter the website paths that you want to protect and in the second text field, enter the maximum number of requests per second to any website. click **Add**. The website path and the maximum requests per second is displayed in the field below. Click to remove the website path and requests per second from the list. **NOTE** This field is displayed only when you select the option **Specific** in the field **Website Paths to Protect**
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Click **Save** to save the changes.
Cancel	Reverts to the last saved configuration

Assign inspection options policies

You can assign inspection option policies to interfaces and subinterfaces. This is especially useful when you want to define inspection option policies and also quickly assign it to Sensor interfaces.

1. On the **Policy** tab, select the required domain from the **Domain** drop-down list.
2. Select Intrusion Prevention → Policy Types → **Inspection Options**.
3. Click the **Assignments** value of the inspection options policy that you want to assign.

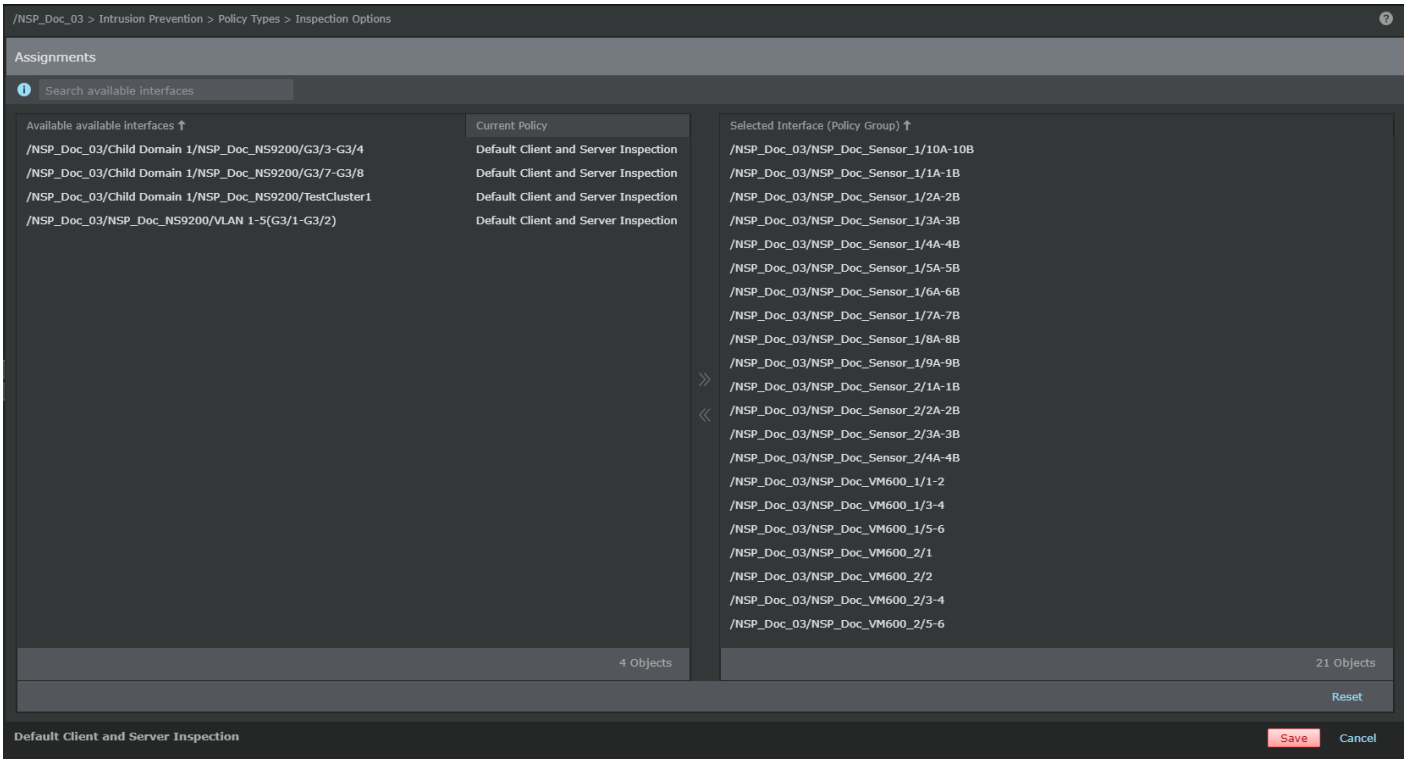
Figure 483. Assignments



The **Assignments** page is displayed.

4. Assign the inspection options policy to the required interfaces and subinterfaces.

Figure 484. Assignments page



Option	Definition
Search Interfaces	To filter the list of available interfaces, enter a string that is part of the **Available Interfaces**.
Available Interfaces	Lists the interfaces and subinterfaces of the Sensors in the admin domain. The Sensor interfaces to which you have already assigned inspection options policy are displayed under **Selected Interface**. Select an interface and click » to move it to **Selected Interface**.

Option	Definition
Current Policy	The inspection options policy that is assigned to an interface. To replace that policy with the policy that you are currently assigning, move the resource to **Selected Interface**.
Selected Interface (Policy Group)	Lists the Sensor interfaces to which you have assigned the selected inspection options policy
Reset	Reverts to last saved configuration
Save	Saves the changes to the Manager database
Cancel	Closes the **Assignments** window without saving the changes

Protecting web applications servers and inspecting HTTP traffic

You can configure specific features in Trellix IPS to inspect HTTP traffic and to protect web application servers.

Protecting your web application servers

One of the biggest challenges for network security professionals is securing their web servers. Because of their location in the network and the nature of applications hosted by them, enterprise web servers are generally the most vulnerable and the most targeted. The motivation to attack a web server could be financial gain, confidential data, an entry into your organization's network, or just to cause an embarrassment or inconvenience.

A critical component of a web application is its database. Web applications use SQL to interact with their databases to retrieve and store data. During these interactions, a web application server sends SQL queries combined with user-provided data to its database. This makes web applications and databases vulnerable for SQL injection attacks, where attackers attempt arbitrary SQL commands and queries on a web application's database. These attacks might succeed when validation of user-provided data is inadequate or due to vulnerabilities in the server application.

An SQL injection is kind of a code injection. It is a malicious SQL query injected along with a legitimate SQL query to a database. A successful SQL injection can read or write to the database, execute operations on the database server, or run commands on the operating system.

Example:

Consider the URI, `http://www.example.com/news.php?ID=378144` that triggers the following legitimate SQL query: `"SELECT * FROM news WHERE ID = " . $ID;`

An attacker can inject a malicious SQL query within the legitimate query as shown here:

`http://www.example.com/news.php?ID=378144 UNION SELECT 1,2,3,password FROM admin`. This SQL injection can fetch the admin password and display it on the resulting web page.

Options to prevent SQL injection attacks

The following are the options to prevent SQL injection attacks:

- Address the vulnerabilities on the web server, but this option might not prevent all attacks. This option can also be complicated and expensive.
- Use the SQL-injection prevention mechanism in Trellix IPS. This feature is referred to as Heuristic Web Application Server Protection. Review these details to know how to implement the Heuristic Web Application Server Protection feature.

Advantages of Heuristic Web Application Server Protection

Traditionally, IPS products use string-matching to find malicious strings in HTTP traffic. However, this method might not be effective in case of SQL injections, because SQL queries are plain text that use common words. For example, the string SELECT is used in legitimate queries as well as in malicious ones.

The Heuristic Web Application Server Protection feature of Trellix IPS uses heuristic analysis. The heuristic engine identifies SQL injections by the following method:

1. It checks the head token of malicious SQL queries, and recognizes any malicious keywords such as **`UNION`**. Such keywords can potentially alter the structure of an SQL query.
2. It analyzes valid and legitimate SQL statements such as `SELECT password FROM admin WHERE LastName = 'Doe'`
3. It does correlated analysis of points 1 and 2 and triggers an alert.

Implementing the Heuristic Web Application Server Inspection option

Heuristic Web Application Server Protection is the outcome of an extensive and ongoing research by Trellix. You can enable this feature at the interface and subinterface levels. When you enable this feature, the Sensor inspects HTTP and HTTPS traffic on the corresponding interfaces and subinterfaces for SQL injections. For HTTPS traffic, you must have enabled decryption and shared the server keys with the Sensor.

The following options are available when you enable Heuristic Web Application Server Protection:

- You can enable heuristic analysis for all HTTP traffic seen at a specific interface/ subinterface or you can enable it only for specific website paths. So, for heuristic analysis, the Sensor considers only those HTTP requests that contain these paths. In the Manager, these paths are referred to as **Website Paths to Protect.** Specifying paths optimizes the performance of the feature.
- You can enable the default heuristic detection mechanism for the protected website Paths. The Sensor considers each reserved SQL keyword in the normalized HTTP requests to the protected website paths. It considers factors such as the number of keywords in the query and the syntax of the query to determine if it is an attack. Because the research for heuristic analysis is ongoing, Trellix might tune the heuristic rules and algorithm from time to time. The changes are available to you when you update the signature set.

  When the Sensor detects an attack through the default heuristic detection mechanism, it raises an alert for *HTTP: SQL Injection Attack Detected* (Trellix IPS attack ID: 0x4029d300).
- You can augment the default heuristic detection mechanism with specific strings. The Sensor treats these strings as blocked tokens. When it detects any of these strings in the HTTP requests to the protected website paths, it considers it as an attack. For example, you can specify the names of stored procedures because these are not expected in an HTTP request. In the Manager, these blocked tokens are referred to as **Blocked Text.**

  When the Sensor detects a blocked text, it raises an alert for *HTTP: Stored Procedure Name Detected by SQL Injection Heuristic Engine* (Trellix IPS attack ID: 0x00011200).

High-level steps for implementing the Heuristic Web Application Server Protection

1. Make sure the web application servers that you want to protect are connected to the appropriate Sensor monitoring ports.
2. For the Sensor to inspect HTTPS traffic, make sure that you have enabled SSL decryption and that you have imported the required SSL keys into the Sensor.

3. If required, create the subinterfaces for your web application servers.
4. Make sure that you have applied the required IPS policies to the interfaces or subinterfaces to which the web application servers are connected. Also, make sure that the following attacks are present and enabled in those IPS policies:
   a. HTTP: SQL Injection Attack Detected (Trellix IPS attack ID: 0x4029d300)
   b. HTTP: Stored Procedure Name Detected by SQL Injection Heuristic Engine (Trellix IPS attack ID: 0x00011200)

   Configure the required response actions for the above-listed attacks.
5. Configure the Heuristic Web Application Server Inspection options at the admin domain.
6. Configure and enable Heuristic Web Application Server Protection for the required interfaces and subinterfaces.
7. Monitor Attack Log for alerts related to SQL injections.

Configure Heuristic Web Application Server Protection at the interface level

By default, the Heuristic Web Application Server Protection feature is disabled. For it to work, you must specify your options, which are **Website Paths to Protect** and **Blocked Text.** Then, you must enable the feature for an interface or subinterface. You can specify your options at the admin-domain level and inherit it at the interface and subinterface levels. If required, you can specify different options for an interface or subinterface.

Notes:

- At a child admin domain, interface, and subinterface levels, you cannot modify the configuration that you inherited from an admin domain. So, you must modify the configuration at the parent admin domain. However, modifying the parent domain affects all the child admin domains, interfaces, and subinterfaces that inherit these settings.
- When you create an interface, Heuristic Web Application Server Protection feature is disabled by default. It is also disabled when you create a subinterface regardless of whether it is enabled at the corresponding interface.
- In case of subinterfaces, you can only inherit from the admin domain to which they belong.

1. In the Manager, click the **Policy** and select the required domain.
2. Select Intrusion Prevention → **Policy Manager**.
3. On the **Interfaces** tab, double-click the interface to which you would like to configure the heuristic web application.

   The **<Device Name/Interface>** panel opens.
4. In the **Inspection Options** section, click the + icon to create a new policy, or double click the policy to edit the assigned policy.

   Proceed to step 5 if a new policy has to be created, or if you wish you edit an existing policy proceed to step 7.
5. The **Properties** page opens. Following are the options on the **Properties** tab:

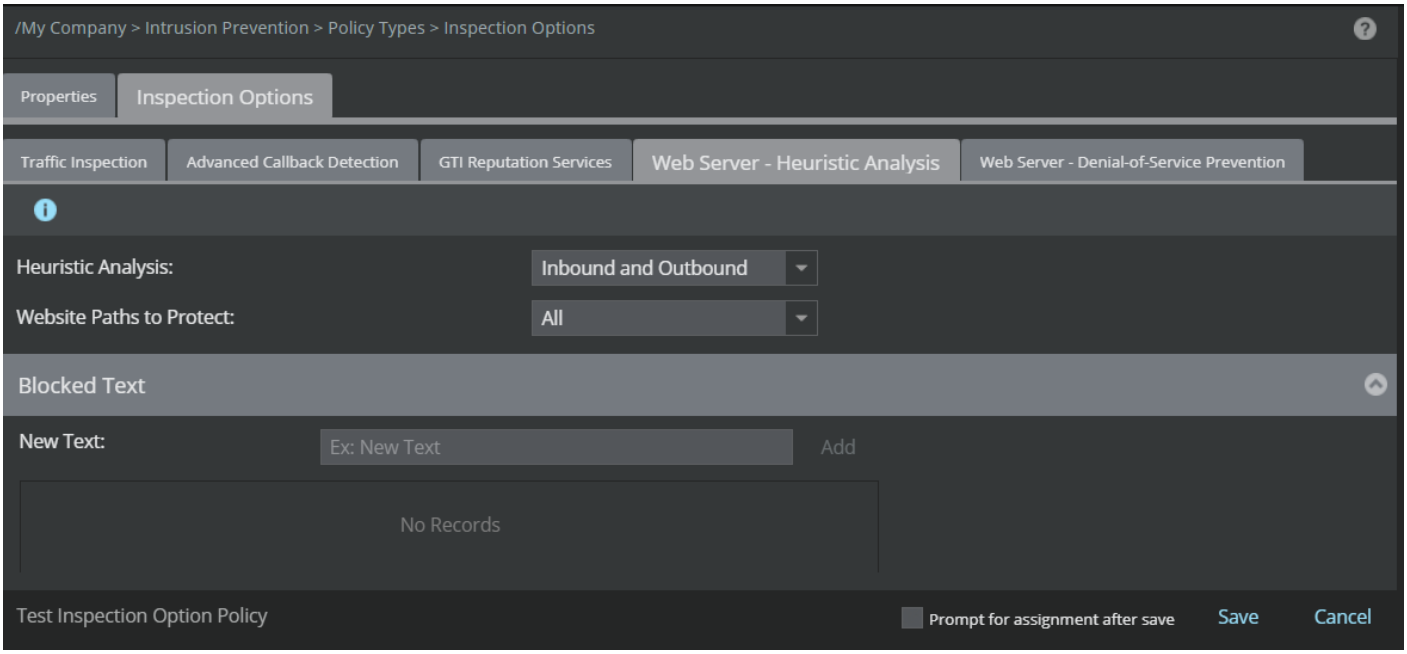
Option	Definition
Name	Name of the policy **NOTE** The name field should not be left blank and no special character should be entered while typing the name.
Description	Description for the policy for other users to identify its purpose
Owner	Displays the admin domain to which the policy belongs
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are **Owner and Child Domains** and **Owner Domain Only**.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Statistics	
Last Updated	Displays the time stamp when the policy was last modified
Last Updated By	Displays the user who last modified the policy
Assignments	Indicates the number of ports to which the policy is assigned

6. Click **Next**.

   The **Inspection Options** page opens.

7. Select the **Web Server - Heuristic Analysis** tab.

8. Specify the required settings in the corresponding fields.



Option	Definition

Heuristic Analysis	Select the direction to which you would like to assign the policy from the drop-down list. Rest of the configuration depends on this selection.
	• If you have selected **Inbound**/**Outbound**/**Inbound and Outbound**, specify the options for **Website Paths to Protect** as described below.
	  • **All**: Select to inherit only the blocked text. The Sensor applies the built-in heuristic rules and the inherited blocked tokens on all the HTTP requests seen at this interface or subinterface.
	  • **Specific**: Select to inherit the website paths and the blocked text.
	NOTE
	You cannot inherit just the website paths from the admin domain.
	  • For the Sensor to consider any HTTP request for Heuristic Web Application Protection, select **All** for **Website Paths to Protect**.
	  • To specify website paths, select **Specific** for **Website Paths to Protect** and then enter the path in **New Website Path** and click **Add.** For example, if you specify /private-banking/ as a path, then the Sensor considers only those requests that contain /private-banking/ for Heuristic Web Application Protection. You can specify up to 512 such paths per Sensor. If you do not specify a path, the Sensor checks all the HTTP requests.
	NOTE
	To delete an existing path, hover over it and click the "x" icon.
	  • To specify blocked text, enter the text in **New Text** and click **Add**. The added text are listed in the box below. Their type is always custom. Note the following:
	  • These texts must be between 3 and 255 characters in length.
	  • You can specify up to 256 texts per Sensor.
	  • If the Sensor detects any of these texts in a query to the protected website paths, it treats it as an attack. If you define these texts, the Sensor checks the queries for both these texts as well as the built-in, default heuristic rules. If not, it checks only for the default heuristic rules.
	  • For the Sensor to raise an alert, a blocked text should appear after the path in a request URI. For example, if *private-banking* is a path and *get_balance* is a blocked text, then in the request URI, *get_balance* should occur after *private-banking* for the Sensor to detect the blocked text.
	  • To delete an existing blocked texts, hover over it and click the "x" icon.

Save	Click to save the configuration.

9. Click **Save** in the **<Device Name/Interface>** panel to save the changes.
10. Complete a configuration update to the Sensor for the configuration to take effect.

The Sensor protects your web application servers according to your configuration.

When the Sensor detects an attack through the default heuristic detection mechanism, it raises an alert for *HTTP: SQL Injection Attack Detected* (Trellix IPS attack ID: 0x4029d300). This is treated as an exploit attack. The **Alert Details** panel of Attack Log displays any reserved SQL keywords that the Sensor detected in the query. These are displayed in the **SQL Injection Details** section of the **Alert Details** panel.

When the Sensor detects a custom blocked text, it raises an alert for *HTTP: Stored Procedure Name Detected by SQL Injection Heuristic Engine* (Trellix IPS attack ID: 0x00011200). This is treated as a policy violation. The **SQL Injection Details** section displays the custom blocked text that the Sensor found in the corresponding HTTP requests.

HTTP response scanning

HTTP response scanning provides additional protection for the malicious or compromised web servers. When response scanning is enabled, HTTP response headers and the downloaded payload are inspected for attacks.

HTTP Response Decompression

HTTP response is commonly compressed in gzip or deflate format to improve performance. In gzip compression format, the web servers replace the common text in the HTTP response traffic by an arbitrary placeholder to reduce the file size. Whereas in deflate compression format, the web servers encode the HTTP response traffic content using LZ77 and Huffman encoding algorithms. The web servers then replace common text in the encoded HTTP response traffic by an arbitrary placeholder to attain better compression. Therefore, these formats reduce transfer time and bandwidth consumption. However, attackers use it to evade detection of malicious payload. Enabling this option instructs the Sensor to decompress compressed HTTP response traffic for inspection.

When HTTP response decompression is enabled, the Sensor inspects the HTTP response traffic for compressed data. The compressed data identified are categorized as gzip or deflate based on their compression mechanism. After categorization, the HTTP response traffic is decompressed using the decompression engine. The decompressed HTTP response traffic is further inspected for anomalies using the signature set. Post inspection, the response actions configured in the inspection options are triggered.

Points for consideration:

- HTTP Response Decompression is disabled by default.
- To enable HTTP Response Decompression, HTTP response traffic scanning should be enabled.
- HTTP Response Decompression is supported for gzip and deflate compressed files only.
- Advanced malware inspection of decompressed files is not supported.
- This feature is supported on NS-series and Virtual IPS Sensors.

Chunked HTTP Response Decoding

Chunked transfer encoding is a data transfer mechanism of HTTP (HyperText Transfer Protocol) version 1.1. Here, the web servers break the HTTP response content into series of non-overlapping chunks. These chunks contain http response payload. It uses transfer encoding header in place of the content-length header, which the protocol would otherwise require. Chunked transfer encoding supports sending dynamically generated content to clients without having to buffer it. Such payload chunks could be used to evade network inspection devices.

When Chunked HTTP Response Decoding is enabled, the Sensor inspects chunks in the http response traffic. The chunks identified are dechunked, and the dechunked payload is inspected further after separating the metadata. Post inspection, the response actions configured in inspection options are triggered.

Points for consideration:

- Chunked HTTP Response Decoding is disabled by default.
- To enable Chunked HTTP Response Decoding, HTTP Response Traffic Scanning should be enabled.
- Chunked HTTP Response Decoding is supported in inline and span modes for both Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).
- Chunked HTTP Response Decoding feature relatively lowers overall performance of the Sensors depending on chunked content in the network traffic.
- Advance Malware inspection of dechunked payload is not supported.

Microsoft Office File Deep Inspection

With Microsoft Office File Deep Inspection, compressed Microsoft Office files in HTTP traffic are inspected. Further, the traffic segments are decompressed for detection of any threats and anomalies.

With Microsoft Office File Deep Inspection, compressed Microsoft Office files in HTTP traffic are inspected.

Microsoft Office version 2007 and later uses Office Open XML format, a zipped XML based file format. The zipped file contains multiple files upon extraction. This format is compact and reduces bandwidth consumption and transfer time. However, attackers use this to avoid detection of malicious payload.

When Microsoft Office File Deep Inspection feature is enabled, it instructs the Sensor to inspect traffic segments for the Microsoft Office files (i.e. docx, .pptx, or.xlsx). Initially, the docx, .pptx, or.xlsx files identified are scanned using the Microsoft Office File Deep Inspection signatures. These signatures identify the files that are to be decompressed. The decompressed files are inspected further for attack identification. Post inspection, when an attack is detected, the malicious files are blocked, and alerts are generated in the Manager. The process of Microsoft Office File Deep Inspection in the Sensors is achieved using advanced signature sets with multi-level threat detection mechanism. These signature sets are customized and cannot be created using UDS framework.

Points for consideration:

- Microsoft Office File Deep Inspection feature is supported only for .docx, .pptx, and .xlsx file extensions in HTTP traffic on NS-series Sensor version 10.1 and later.
- Microsoft Office File Deep Inspection is disabled by default.
- To enable Microsoft Office File Deep Inspection, HTTP Response Traffic Scanning should be enabled.
- Microsoft Office File Deep Inspection feature detects malicious hostnames present in URLs mentioned in any .docx, .pptx, or .xlsx files submitted for inspection. The files downloaded through a URL in the Microsoft Office files are inspected as new files.
- Microsoft Office File Deep Inspection is supported in inline and span modes for both Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).
- Microsoft Office File Deep Inspection feature impacts the Sensor performance depending on the number of Microsoft Office files (i.e. docx, .pptx, or.xlsx) in the traffic.

- The Microsoft Office files (i.e. docx, .pptx, or.xlsx) can have any number of files embedded within them using Office Open XML format. While inspecting such Microsoft Office files, the Sensor scans all embedded files, but only a few files are selectively decompressed using Microsoft Office File Deep Inspection signatures and inspected further for attack detection.
- Nested decompression is not supported in the following situations:
    1. When a Microsoft Office XML file is zipped inside another .zip file.
    2. When the traffic flowing through the network is zipped. That is, when traffic to be inspected is completely zipped and contains the Microsoft Office files (i.e.docx, .pptx, or.xlsx) files in the zipped content.
- User defined signatures, Trellix IPS Snort, and Suricata Snort cannot be used to create Microsoft Office File Deep Inspection signatures.
- To disable any Microsoft Office attack, you should disable the correlation attack for the respective attack in IPS policies.
- Microsoft Office File Deep Inspection and Malware analysis features are mutually exclusive. If Malware Analysis is enabled, the malware analysis engine takes precedence over Microsoft Office File Deep Inspection. Microsoft Office File Deep Inspection feature considers files in the traffic as zipped archives unlike Advance Malware Inspection feature where the files are inspected as single executables.

Inspecting X-Forwarder-For header information

A client connection to a web server might be established through an HTTP proxy or load balancer. When an explicit (non-transparent) proxy server (or load-balancer farm) is used, it closes the original client connection and creates a secondary connection between itself and the intended destination IP address. If the Sensor monitoring ports sit on the proxied side of the connection, all alerts will show the external IP address of the proxy server as either the source or destination IP address (depending on the direction of the attack) instead of the original source IP address. Therefore, the actual IP address is not available in alerts.

If you enable X-Forwarded-For (XFF) header parsing in the Sensor, the Sensor can parse the XFF field in the HTTP header to identify the original source IP address. In addition, the Sensor can parse True-Client-IP in the HTTP header (for example, Akamai) to obtain the original source IP address.

If your proxy server or the load balancer supports XFF header, the Sensor can parse the XFF header for HTTP connections, by which it recognizes the proxy servers or load balancers the data packet has traversed through. The alerts generated while the Sensor is positioned on the proxied side of the connection, include both the external proxy IP address and the original endpoint IP address.

When attacks are detected, the Sensor forwards both proxy IP address and original source IP address to the alerting mechanism and indicates them in the alert messages sent to the Manager.

The XFF feature supports enabling/disabling per interface or subinterface. It supports both IPv4 and IPv6 addresses.

Enabling XFF header parsing for a Sensor gives you the ability to use original source IP addresses in your firewall policies and quarantine.

- In case of firewall policies, when executing ACL **Drop**, **Deny**, **Scan**, or **Ignore**, the Sensor uses the original source IP address.

> **NOTE**
>
> Depending on the traffic order, some firewall policies will not work as expected for the original source IP address as the Sensor detects the traffic before parsing the XFF header.

NOTE

If you have configured any ACL rules such as **Drop** or **Deny** for the source or destination IP address, which is the proxy IP address, these rules will be run first. This is because the Sensor acts on these rules before parsing the XFF header or HTTP header.

- In case of quarantine, any quarantine resulting from an attack will quarantine the original source IP address and not the proxy IP address.

NOTE

The Ignore rules feature is unsupported with X-Forwarded-For (XFF) header parsing feature for HTTP or HTTPS traffic.

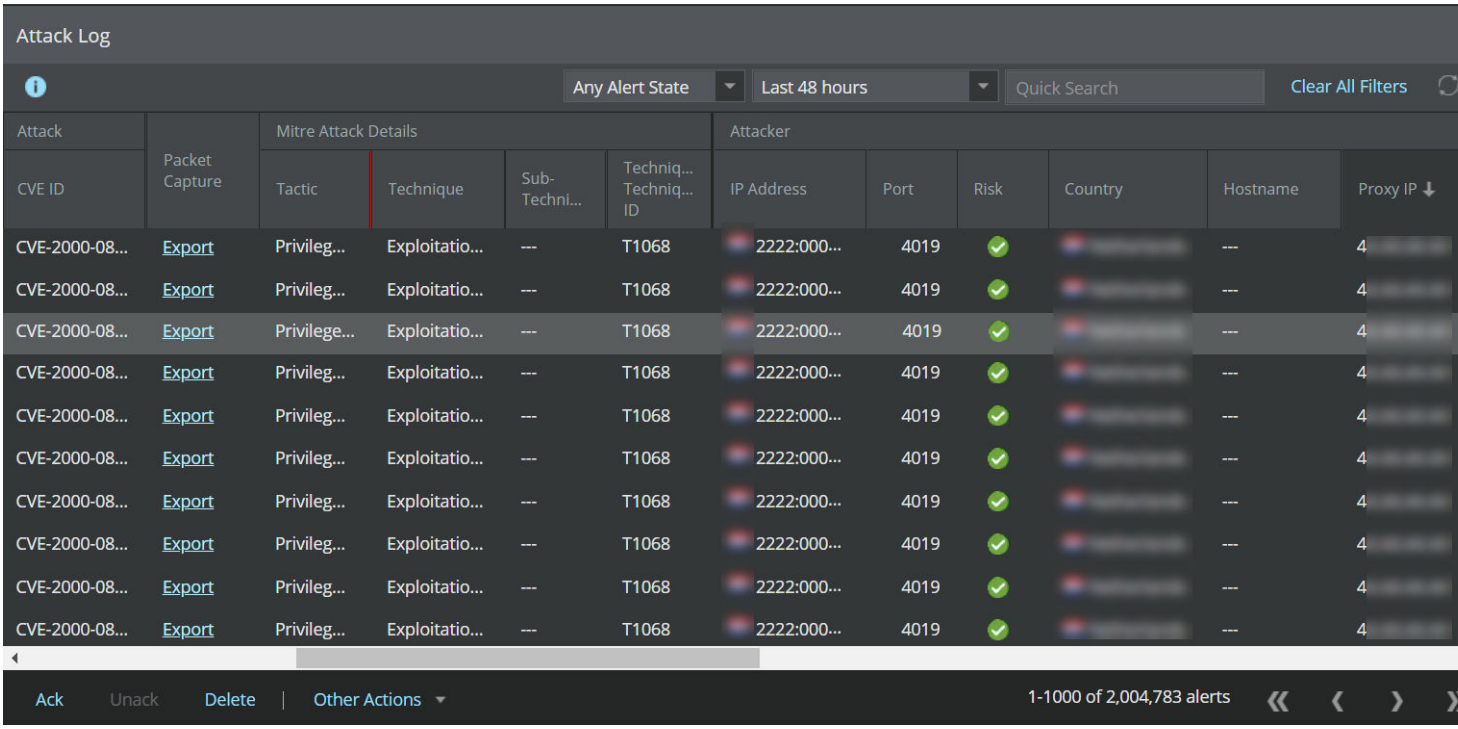
View original source IP address in the Attack Log

You must have enabled **XFF Header Parsing** in one of the ports in the Sensor.

To view the original attacker IP address, you will need to go to the Attack Log in the Manager. To view details of the proxy server, you will need view alert details for that alert.

1. Select Analysis → <Admin Domain Name> → **Attack Log**.
2. From the list of alerts, locate and click one that displays the original attacker IP address.

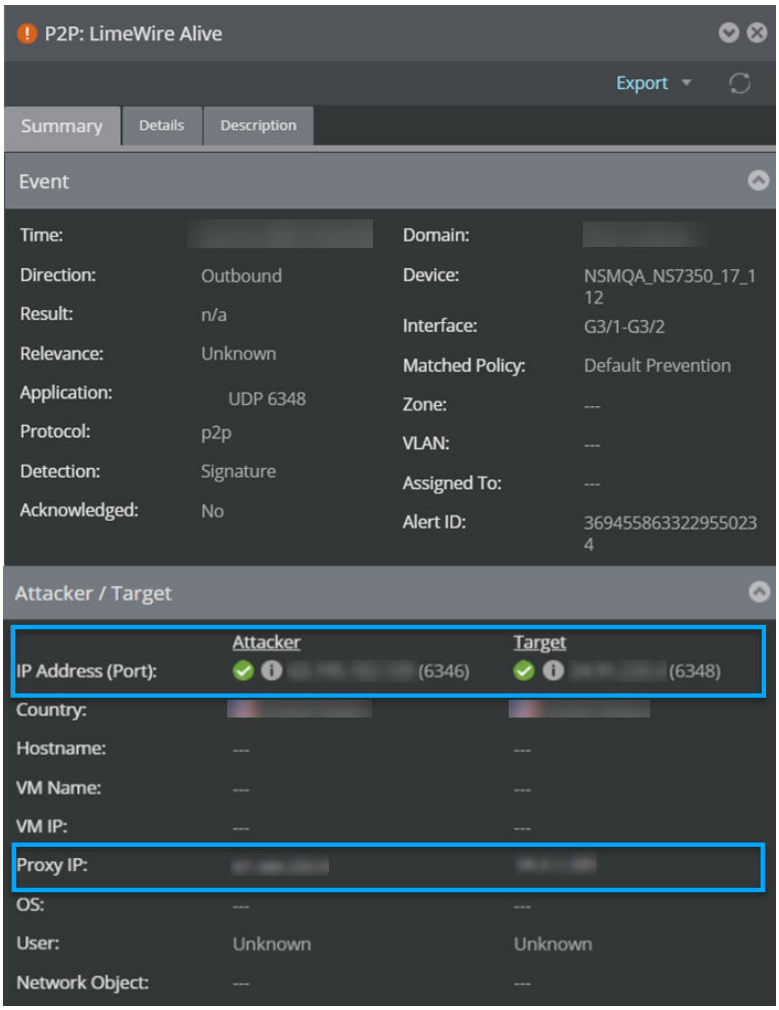
Figure 485. Attack Log page shows the original attacker IP address



3. Double-click the alert.

   The alert details panel opens.

Figure 486. Proxy server in the alert details panel



4. In the **Attack Log** page, you will find the IP address listed in the **Proxy IP** column under the **Attacker** and **Target** columns.
5. The **Proxy IP** displays the proxy server IP address.

Inspection of SSL traffic

Several web and cloud servers use Secure Socket Layer (SSL) to encrypt traffic these days. Using SSL creates a secure environment for clients to access web content and cloud content. This gives the cyber criminals a window to get into a secure company network.

As web content increasingly becomes encrypted with SSL, so does the need to inspect and analyze encrypted traffic. Trellix IPS's IPS Sensors are equipped to decrypt SSL packets for inspection and respond in cases of an attack. The Sensor also has the ability to decrypt traffic in both directions.

For outbound SSL and inbound SSL, while establishing an SSL connection, the client and the server establish a handshake to determine the SSL version, compression method, and cipher suite. Once these details are ascertained, the server sends the

public key and its certificate to the client to validate. The client browser checks for the following details while validating the certificate:

- Expiry date of the certificate — While issuing the certificate, the Certificate Authority (CA) such as Verizon or Comodo adds a date in the certificate after which it becomes invalid.
- Format of the certificate — Different file formats are used for certificates based on how they are encoded. The most common format is Public-Key Cryptography Standards (PKCS) which is published by RSA Laboratories. For Inbound and outbound SSL Decryption, Trellix IPS supports the PKCS12 format. The private key must be a part of the PKCS12 file.
- Authenticity of the certificate — The client browser uses the public key of the certificate to decrypt and authenticate the certificate.

Each web browser has a list of trusted certificates. When a client receives the certificate from the server, the browser compares the certificate with the trusted list. If the certificate is trusted, the connection is established between the client and the server. If a match is not found, the browser displays a error message. For example, in Mozilla Firefox, you get an error message that says Your connection is not secure.

For increased security, you can restrict access to the Manager by using secure ciphers like TLS 1.2. By default, Manager allows connections from all ciphers. You can remove the less secure ciphers from the Manager configuration thereby restricting access to the Manager. For example, you can remove Manager access using TLS1.0 and provide access only through TLS 1.2. This restricts access to the Manager. To edit the cipher list in the Manager configuration, go to **`C:\Program Files\Trellix\IPS Manager\App\apache-tomcat\conf`**.

SSL decryption support for NS-series and Virtual IPS Sensors

The table below shows the types of inbound and outbound SSL decryption support on different NS-series Sensor models:

Sensor Model	Inbound SSL decryption			Outbound SSL decryption
	Known-key SSL decryption	Agent based SSL decryption	Proxy SSL decryption	Proxy SSL decryption
NS3100	NA	NA	NA	NA
NS3200	NA	NA	NA	NA
NS3500	NA	NA	NA	NA
NS3600	Yes	Yes	NA	NA
NS5100	Yes	Yes	NA	NA
NS5200	Yes	Yes	NA	NA
NS7100	Yes	Yes	NA	NA
NS7200	Yes	Yes	NA	Yes
NS7300	Yes	Yes	NA	Yes
NS7150	Yes	Yes	NA	NA
NS7250	Yes	Yes	NA	NA
NS7350	Yes	Yes	NA	NA

Sensor Model	Inbound SSL decryption			Outbound SSL decryption
	Known-key SSL decryption	Agent based SSL decryption	Proxy SSL decryption	Proxy SSL decryption
NS7500	Yes	Yes	Yes	Yes
NS7600	Yes	Yes	NA	NA
NS9100	Yes	Yes	NA	Yes
NS9200	Yes	Yes	NA	Yes
NS9300	Yes	Yes	NA	NA
NS9500 Standalone	Yes	Yes	Yes	Yes
NS9500 Stack	Yes	Yes	NA	NA

The table below distinguishes between the inbound and outbound SSL decryption support on Virtual IPS Sensors by platform:

Sensor Model	Inbound SSL decryption			Outbound SSL decryption
	Known-key SSL decryption	Agent based SSL decryption	Proxy SSL decryption	Proxy SSL decryption
IPS-VM600 (ESX and KVM)	Yes	Yes	NA	NA
IPS-VM5000 (ESX and KVM)	Yes	Yes	NA	NA
IPS-VM600-VSS (AWS, Azure, and OCI)	Yes	NA	NA	NA

Managing licenses for proxy based SSL decryption

The proxy based SSL decryption feature requires the proxy based SSL licenses to be assigned to specific Sensors. Configuration updates like signature set and policy updates are enabled only when a valid license is assigned to the Sensors. The license is provided as a .zip or .jar file which is supported by the Manager. The license procured contains the number of Sensors on which the inbound or outbound SSL decryption can be enabled.

NOTE

To obtain a demo license for proxy based SSL decryption, contact MB Licensing. An email containing the license will be sent from MB Licensing.

To procure a valid license for outbound proxy based SSL decryption and upload it in the Manager, refer to the following SKUs:

Sensor Model	SKUs
NS9500 (Standalone) with 30 Gbps	SSL9530ECE-AT
NS9500 (Standalone) with 20 Gbps	SSL9520ECE-AT
NS9500 (Standalone) with 10 Gbps	SSL9510ECE-AT
NS9200	OSLNS92ECE-AT
NS9100	OSLNS91ECE-AT
NS7500 with 7.5 Gbps	SSL75075ECE-AT
NS7500 with 5 Gbps	SSL7505ECE-AT
NS7500 with 3 Gbps	SSL7503ECE-AT
NS7300	OSLNS73ECE-AT
NS7200	OSLNS72ECE-AT

To procure a valid license for inbound proxy based SSL decryption and upload it in the Manager, refer to the following SKUs:

Sensor Model	SKUs
NS9500 (Standalone) with 30 Gbps	SSL9530ECE-AT
NS9500 (Standalone) with 20 Gbps	SSL9520ECE-AT
NS9500 (Standalone) with 10 Gbps	SSL9510ECE-AT
NS7500 with 7.5 Gbps	SSL75075ECE-AT
NS7500 with 5 Gbps	SSL7505ECE-AT
NS7500 with 3 Gbps	SSL7503ECE-AT

NOTE

For NS9500 Sensors, the same proxy based SSL license can be used for both Inbound and Outbound proxy based SSL decryption.

Add license to the Manager

A license is required to enable proxy based inbound or outbound SSL decryption. This license has to be added in the Manager.

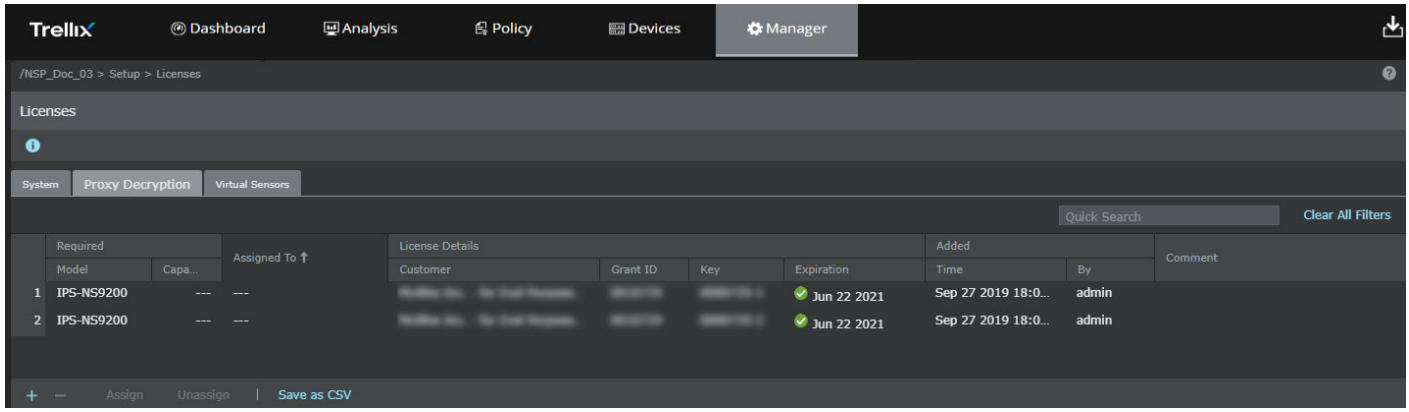
To add a license to the Manager, perform the following steps:

1. Go to Manager → <Admin Domain Name> → Setup → **Licenses**.
2. Click the **Proxy Decryption** tab.

   The following details are displayed on the **Proxy Decryption** tab:

Table 59. Option definitions

Option	Definition
Required	**Model** — Displays the Sensor model **Capacity** — Displays the throughput of the Sensor
Assigned To	Displays the Sensor to which the license is assigned
License Details	**Customer** — Displays the name of the customer who purchased the license **Grant ID** — Displays the grant ID of the customer **Key** — Displays the license key number **Expiration** — Displays the expiration date and time of the license
Added	**Time** — Displays the time at which the license was added to the Manager **By** — Displays the user who added the license to the Manager
Comment	Displays any comments for the license if any



3. Click +

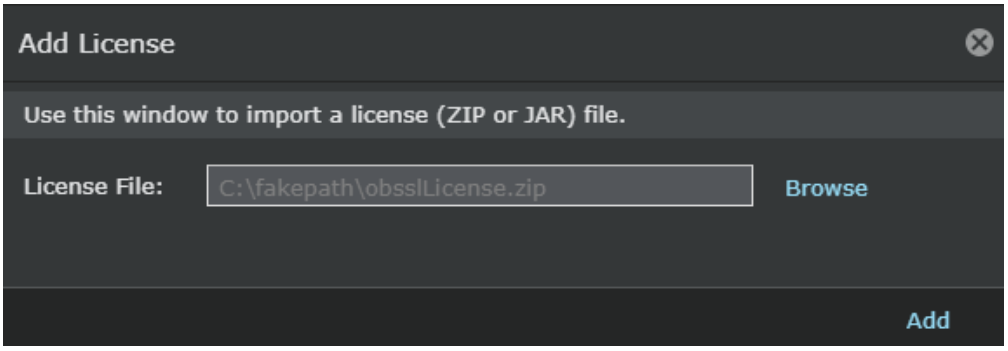
   The **Add License** pop-up opens.

4. Click **Browse**.

   Navigate to the location where the license is saved. Select the license and click **Open**.

> **NOTE**
>
> The supported license formats are .zip and .jar.

Figure 487. Upload license to the Manager



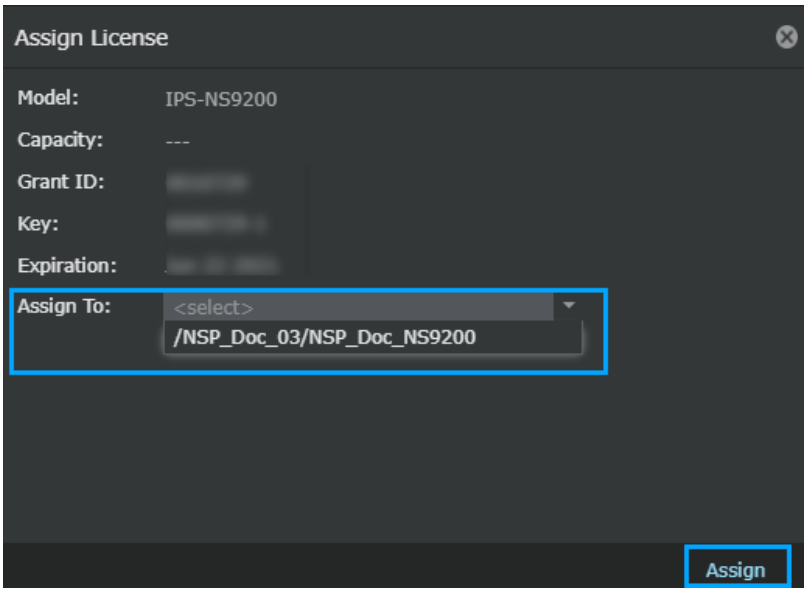
5. Click **Add**.

   The license is added to the Manager.

6. To assign the license to a Sensor, click **Assign**.

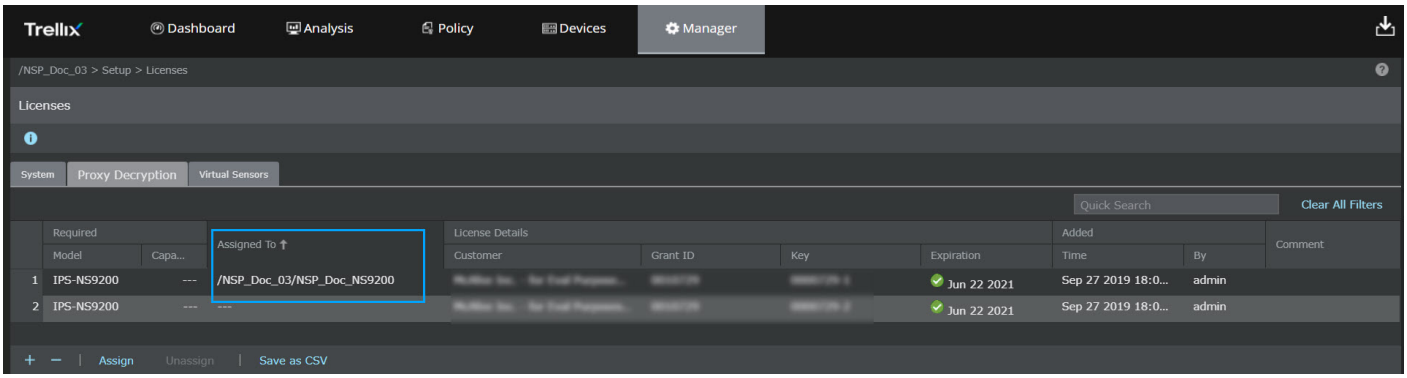
   The **Assign License** pop-up opens.

7. Select a Sensor model from the **Assign To** drop-down list to which the license has to be assigned.



8. Click **Assign**.

   A pop-up message The license has been successfully assigned appears. Click **OK**.



NOTE

If a valid license is not assigned to the Sensor, signature set and policy updates are disabled for the Sensor.

9. To delete a license, select the license to be deleted and click −

   A warning message appears to confirm the deletion. Click **OK**.

10. To export the list of licenses, click **Save as CSV**.

Supported cipher suites for proxy SSL inspection

The following is the complete list of SSL cipher suites (as named in their respective RFCs) that are supported for Proxy SSL inspection:

- SSLv3 cipher suites:
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_SEED_CBC_SHA
  - TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_NULL_SHA
  - TLS_RSA_WITH_NULL_MD5
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
  - TLS_DH_anon_WITH_AES_256_CBC_SHA
  - TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA

    - TLS_DHE_RSA_WITH_SEED_CBC_SHA
    - TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
    - TLS_DH_anon_WITH_AES_128_CBC_SHA
    - TLS_DH_anon_WITH_SEED_CBC_SHA
    - TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
    - TLS_DH_anon_WITH_RC4_128_MD5
    - SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
- TLSv1 cipher suites:
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDH_anon_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDH_anon_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
    - TLS_ECDHE_RSA_WITH_RC4_128_SHA
    - TLS_ECDH_anon_WITH_RC4_128_SHA
    - TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
    - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_NULL_SHA
    - TLS_ECDHE_RSA_WITH_NULL_SHA
    - TLS_ECDH_anon_WITH_NULL_SHA
- TLSv1.2 cipher suites:
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
    - TLS_ECDHE_ECDSA_WITH_AES_256_CCM
    - TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
    - TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
    - TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CCM_8
- TLS_RSA_WITH_AES_256_CCM
- TLS_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM
- TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CCM_8
- TLS_RSA_WITH_AES_128_CCM
- TLS_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_NULL_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_256_CCM_8
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_DH_anon_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DH_anon_WITH_AES_256_CBC_SHA256
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM_8

- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_DH_anon_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_anon_WITH_AES_128_CBC_SHA256
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256

- TLSv1.3 cipher suites:
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256

Decrypting outbound SSL traffic

For outbound SSL traffic, when you access a secure server using SSL, the Sensor acts as a proxy between the client and the server. The Sensor intercepts the client request and forwards the request to the server as the client. The server receives the request and sends its certificate to the Sensor. The Sensor validates the server certificate using its list of trusted CA certificates. The Sensor uses the imported certificate to implement the re-signing functionality within the proxy. The re-signing certificate is used by the Sensor to re-sign the server certificate for validation by the client.

You can also create decryption exceptions to exclude certain outbound SSL traffic from decryption based on source or destination IP addresses, destination domain name, and URL category.

NOTE

You can configure Outbound SSL in inline mode only on standalone NS9500, NS9200, NS9100, NS7300, NS7200, and NS7500 Sensors.

NOTE

Decryption of VLAN tagged packets on Outbound SSL traffic in proxy based method is supported in NS9500 Standalone Sensor version 10.1.5.41 or later, and in NS7500 Sensor version 10.1.5.64 or later.

NOTE

Decryption of double VLAN tagged packets on Outbound SSL traffic in proxy based method is not supported.

NOTE

You cannot configure Outbound SSL in SPAN or tap mode.

NOTE

Proxy based SSL decryption is not supported on G0/1-G0/2 ports.

NOTE

Jumbo frame traffic with SSL encryption will not be decrypted even if SSL decryption is enabled.

NOTE

You cannot configure proxy based outbound SSL decryption on a stack of NS9500 Sensors.

Figure 488. Steps to decrypt outbound SSL traffic

1. The client sends a secure request to the web server.
2. The Sensor intercepts the request and forwards it to the web server.
3. The web server responds to the request by sending its certificate to the Sensor.
4. Sensor validates (if configured) the certificate and drops the session if invalid.

   Sensor uses its default resign certificate or custom resign certificate to establish the session with the client.

   Sensor is able to decrypt and re-encrypt traffic in both direction using its private key.
5. The Sensor sends the response from the server to the client.
6. Sensor inspects the decrypted packets. If any malicious activity is found, the Sensor raises an alert in the Attack Log.
7. While decrypting Outbound SSL traffic, the Sensor may not be able to decrypt certain SSL flows due to certificate failures. The Sensor takes the configured action when such a failure occurs.

Port clustering for proxy-based SSL decryption in NS9500 standalone Sensor

Multiple monitoring port pairs in inline mode can be grouped together to create a port cluster. The same IPS policy will apply for traffic arriving on any of the inline pairs in the port cluster.

The following are the considerations for using port clusters with proxy based SSL decryption:

1. Port Cluster for proxy based SSL decryption is supported only for inline port pairs.
2. All paths in the network formed by the inline port pairs must be active paths (should not be blocked by any link layer protocols) on which packets can be forwarded.
3. Packets on the egress path (from the Sensor towards the client or server) may not follow the same path on which they arrived. For example, consider ports G1/1-G1/2, G1/3-G1/4 are grouped in a port cluster. A packet arriving on port G1/1 may exit from port G1/4.
4. SSL sessions will always be reported against the least index port of the port cluster even when the traffic is received on the other ports in the port cluster.

   For example, if G1/1, G1/2, G2/1, and G2/2 are in a port cluster with proxy based SSL enabled, even if the client and server packets are received over the physical G2/1 and G2/2 links, the **`show ssl stats outbound proxy sessions`** command displays that sessions are formed on G1/1 and G1/2. This behavior holds good even if ports G1/1 and G1/2 are not operational.

Steps involved in configuring Outbound SSL Decryption

At a high-level, the steps to configure a Sensor to decrypt and inspect outbound SSL traffic are as follows:

1. Procure the license to enable the outbound SSL decryption feature and add it to the Manager.
2. Enable Outbound SSL Decryption at the domain level or on the required Sensors.

   > **NOTE**
   >
   > The Sensor decrypts outbound SSL traffic only on destination TCP port 443. Outbound SSL Decryption is not supported on non-standard ports.

3. Configure the Sensor SSL parameters for failure handling.
4. You have an option to either import your own re-signing certificate or to use the default re-signing certificate bundled with the Manager.

   Once a client sends the request to access a secure server using SSL, the Sensor acts as a proxy between the client and the server and receives the public key and the certificate from the server. After receiving the server certificate, the Sensor uses the re-signing certificate to authenticate the session to the client and encrypt the traffic between the Sensor and the client. The expiry dates for the certificate is passed to the client. In case of expired certificates, the client generates a warning.

   You can configure your own customized certificate issued by the Certificate Authority (CA) on the **Re-Signing Certificate** tab.

   > **NOTE**
   >
   > It is essential to export the re-signing certificate from the Manager, and import them to the client web browser's **Trusted Root CA** list. This helps to validate the external servers and the Sensor certificate.

   The **Trusted CA Certificates** tab displays the list of digital certificates issued by CAs which the Sensor uses to validate the certificates from the server. The difference between **Re-Signing Certificate** and **Trusted CA Certificates** is as follows:

- The **Re-Signing Certificate** is used by the Sensor to substitute the server's certificate when establishing a session with the client. The Sensor uses this certificate on behalf of the server. In the process, the Sensor decrypts the session between the Sensor and client.
- When the Sensor acts as a proxy for the client to the external servers, it uses the **Trusted CA Certificates** to validate the external servers' trustworthiness.

> **NOTE**
>
> **Re-Signing Certificate** and **Trusted CA Certificates** can be managed only at the root admin domain.

5. The Sensor has a default set of trusted CA certificates. You could also import additional trusted CA certificates if any.
6. Reboot of the Sensor is required when you enable or disable outbound SSL decryption. A full reboot of the Sensor is required.

   Any changes to the settings for outbound SSL decryption requires a configuration deployment to the Sensor. For example, any change to the re-signing certificate or failure handling, the configuration update has to be deployed to the Sensor. You can deploy the configuration update for a Sensor from Devices → <Admin Domain Name> → Devices → <Device Name> → **Deploy Pending Changes**.

   Various fault messages related to SSL decryption may also be raised on the **Faults** tab under **Logs** page in the Manager. For example, an imported re-signing certificate might have become invalid. This causes client browser to raise a certificate error.

   For more information on fault messages, see [Trellix Intrusion Prevention System Product Guide.]

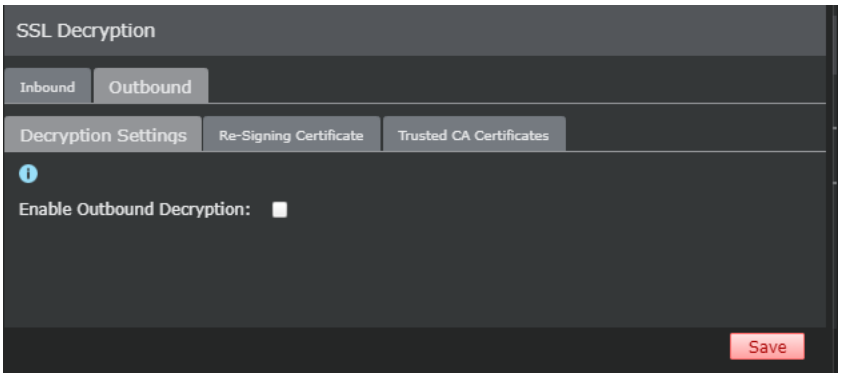
Configuring proxy based outbound SSL decryption at the domain level

Prerequisite: To enable proxy based outbound SSL decryption, you must purchase the license and add it in the Manager. The license required for proxy based SSL decryption is the same for both inbound and outbound.

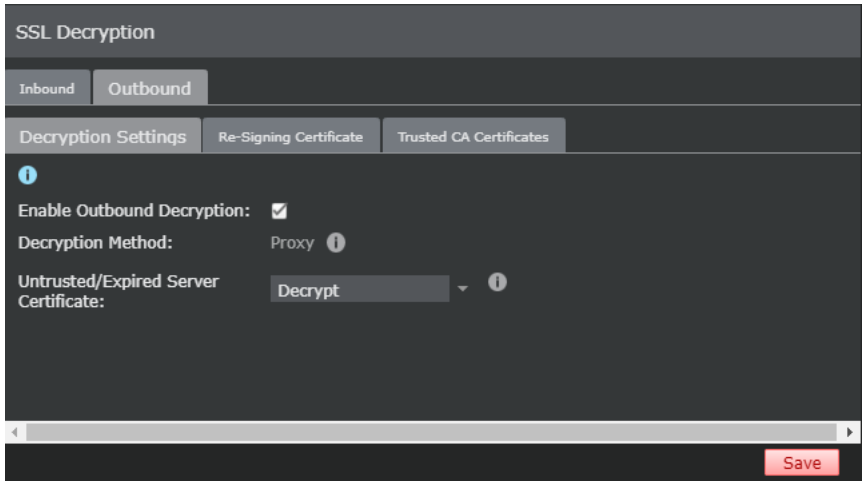
To enable proxy based outbound SSL decryption, perform the following steps:

> **NOTE**
>
> Jumbo frame traffic with SSL encryption will not be decrypted even if SSL decryption is enabled.

1. Go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. On the **Outbound** tab, select **Decryption Settings** tab.



3. Select the **Enable Outbound Decryption** checkbox.



4. Select the required action from the **Untrusted/Expired Server Certificate** drop-down.

   The reasons for failure can be due to the Sensor not being able to validate the web server's certificate. This happens when the certificate signed by a CA is not on the Sensor's trusted CA list.

   The descriptions for the possible Sensor actions in case of a failure are as follows:

Action	Description
Decrypt	The Sensor decrypts the flows from the web server.
Block Flow	The Sensor blocks the flows from the web server.

5. Click **Save**.

> **NOTE**
>
> If a valid license is not assigned to a Sensor, a warning **The device requires a valid proxy decryption license** is displayed in the **Deploy Pending Changes** page for that particular Sensor. To assign a valid license, see section *Add license to the Manager* (page 1145).

6. If you change the mode of operation for SSL decryption, or disable SSL decryption, a reboot of the Sensor is required.

> **NOTE**
>
> Reboot of the Sensor is required after you enable outbound SSL decryption for the feature to function. If you have already configured proxy based inbound SSL decryption, reboot is not required.

   a. Go to, Manager → <Admin Domain Name> → Troubleshooting → Logs → **Faults**.

   b. View the critical messages for the corresponding Sensor to see if a Sensor reboot is required.

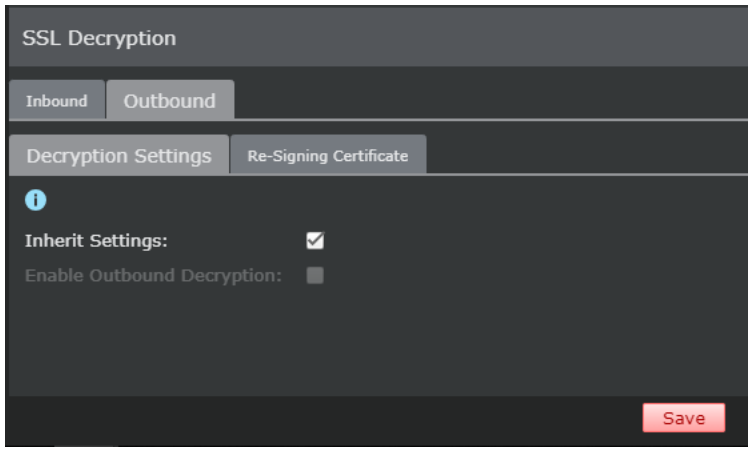
   c. If yes, perform a full reboot of the Sensor.

Configuring proxy based outbound SSL decryption at the device level

Prerequisite: To enable proxy based outbound SSL decryption, you must purchase the license and add it in the Manager. The license required for proxy based SSL decryption is the same for both inbound and outbound.

To enable proxy based outbound SSL decryption, perform the following steps:

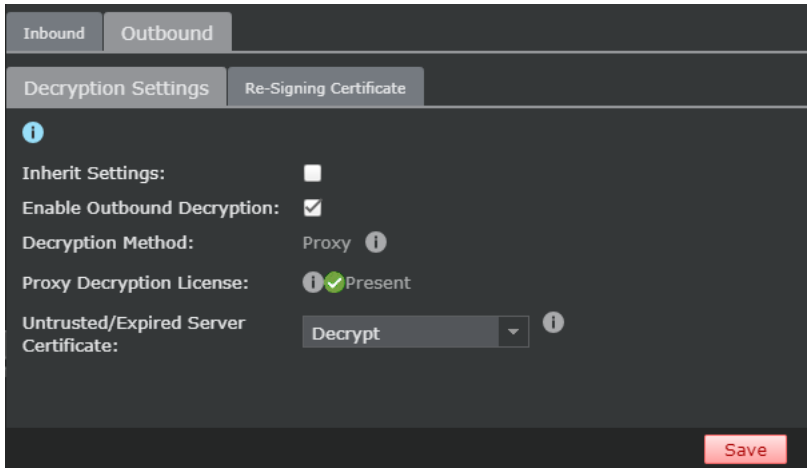
1. Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **SSL Decryption**.
2. On the **Outbound** tab, select **Decryption Settings** tab.



3. Deselect **Inherit Settings** to override the settings of the parent domain.
4. Select the **Enable Outbound Decryption** checkbox.

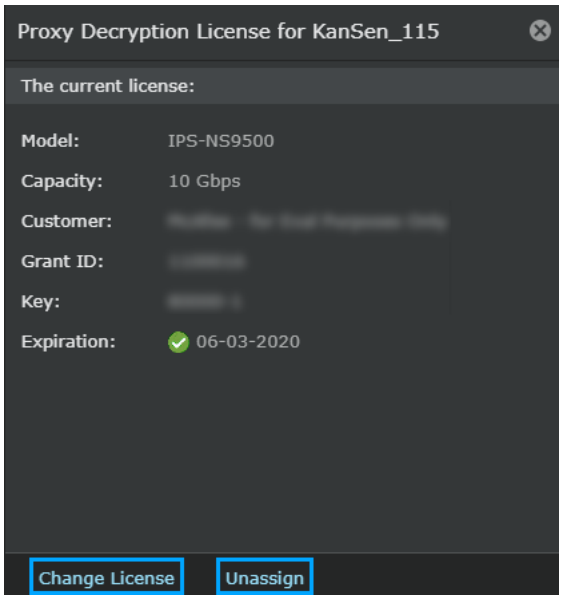
   The **Proxy Decryption License** displays as **Present**.

> **NOTE**
>
> The **Proxy Decryption License** displays as **Required** if a license is not assigned.



   a. Click the tooltip of **Proxy Decryption License** to view the status.

      The **Proxy Decryption License for <Sensor Name>** window opens.



b. [Optional] Click **Change License** or **Unassign**.

If you click **Change License**, it redirects you to **Proxy Decryption** tab, in the **Licenses** page in the **Manager** tab.

If you click **Unassign**, a warning message pops up, click **OK**. The current license will be unassigned and the Sensor will operate without a license.

5. Select the required action from the **Untrusted/Expired Server Certificate** drop-down.

The reasons for failure can be due the Sensor not being able to validate the web server's certificate. This happens when the certificate signed by a CA is not on the Sensor's trusted CA list.

The descriptions for the possible Sensor actions in case of a failure are as follows:

Action	Description
Decrypt	The Sensor decrypts the flows from the web server.
Block Flow	The Sensor blocks the flows from the web server.

6. Click **Save**.

NOTE

If a valid license is not assigned to a Sensor, a warning **The device requires a valid proxy decryption license** is displayed in the **Deploy Pending Changes** page for that particular Sensor. To assign a valid license, see section *Add license to the Manager* (page 1145).

7. If you change the mode of operation for SSL decryption, or disable SSL decryption, a reboot of the Sensor is required.

NOTE

Reboot of the Sensor is required after you enable outbound SSL decryption for the feature to function. If you have already configured proxy based inbound SSL decryption, the reboot is not required.

a. Go to, Manager → <Admin Domain Name> → Troubleshooting → Logs → **Faults**.

b. View the critical messages for the corresponding Sensor to see if a Sensor reboot is required.

c. If yes, perform a full reboot of the Sensor.

Re-signing Certificate

The **Re-Signing Certificate** is used by the Sensor to substitute the server's certificate when establishing a session with the client. The Sensor uses this certificate when responding to the client's request. After the client sends a request, the Sensor receives the public key and the certificate from the web server. The Sensor then validates the certificate by comparing it with the list of trusted certificates available in the trusted CA list. After the Sensor validates the server certificate, it re-signs the certificate using its own certificate before sending it back to the client. This allows the Sensor to decrypt the traffic between the client and server. You can configure your own certificate on the **Re-Signing Certificate** tab. It can be a customized certificate issued by the CA.

NOTE

Re-Signing Certificate can be managed only at the domain level. Certificates more than 2048-bit certificates are not supported.

NOTE

You must re-import the **Re-Signing Certificate** after adding a new Sensor.

NOTE

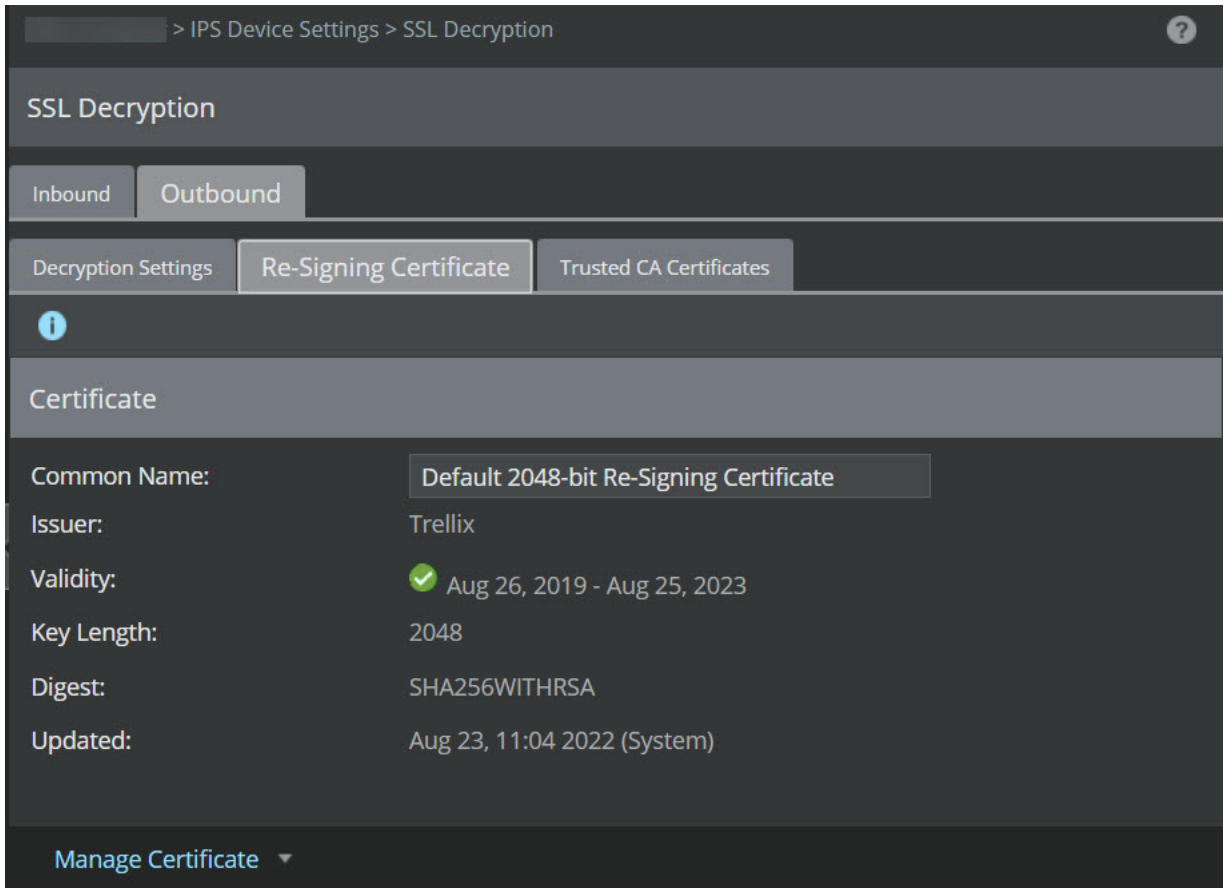
For a stack of NS9500 Sensors, you must re-import the **Re-Signing Certificate** after a capacity upgrade from 40 Gbps or 60 Gbps to 100 Gbps.

When you enable outbound SSL decryption for the first time, the default re-signing certificate provided with the Manager is displayed. You cannot enable the outbound SSL decryption feature with a customized re-signing certificate when you enable the feature for the first time. You can import the customized certificate later.

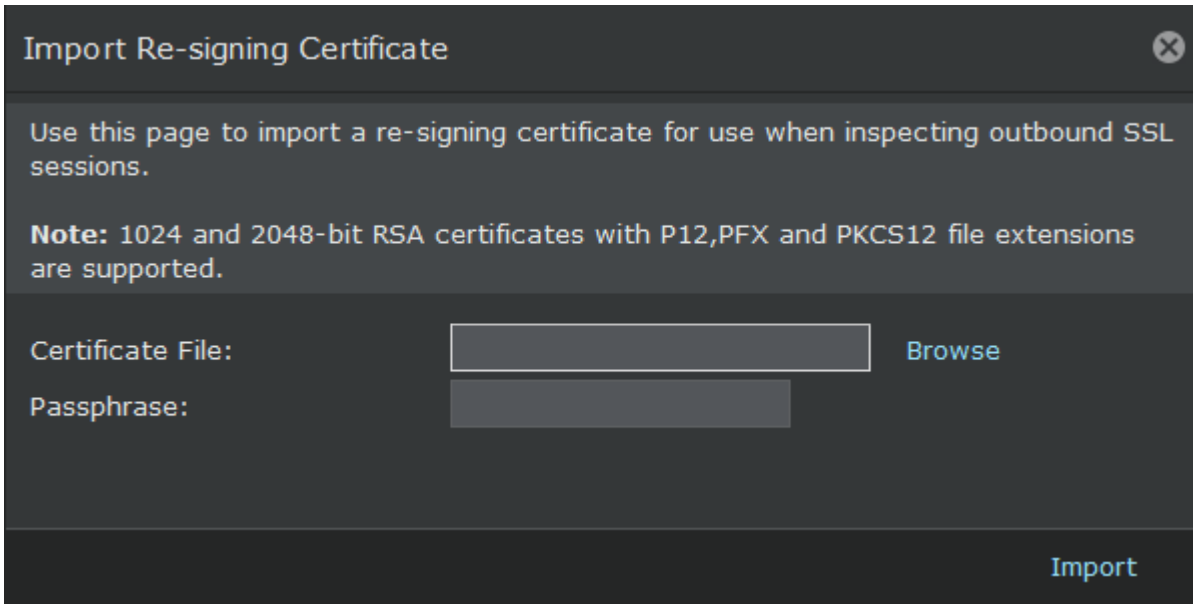
Actions for re-signing certificate

Once the Sensor validates the web server certificate, the Sensor uses the trusted certificates to encrypt the SSL session with the client.

1. Go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. On the **Outbound** tab, select **Re-Signing Certificate** tab.



3. To import a trusted certificate:
   a. Click **Manage Certificate**.
   b. Click **Import**. The **Import Re-Signing Certificate** dialog box opens.



   c. Click **Browse**.

d. Select the .p12 file stored in the local system.

e. Enter the **Passphrase** for the certificate file.

This is the phrase (export password) you used for encrypting your PKCS12 file.

f. Click **Import**.

> **NOTE**
>
> If you import a custom certificate, the default certificate is removed from the Sensor. If you want to use the default certificate, click the **Use Default** option to use the default certificate.

4. To export the public key of the certificate, click **Export Public Key**.

   You need to export the public key of the Sensor and import it to the browsers in the client systems.

5. (Optional) Click **Use Default**.

6. (Optional) Click **Regenerate Default** to regenerate the default certificate.

   You can use this option if the certificate you are using has expired.

   To ensure that the Sensors are using the correct certificates, deploy the configuration changes to the Sensor.

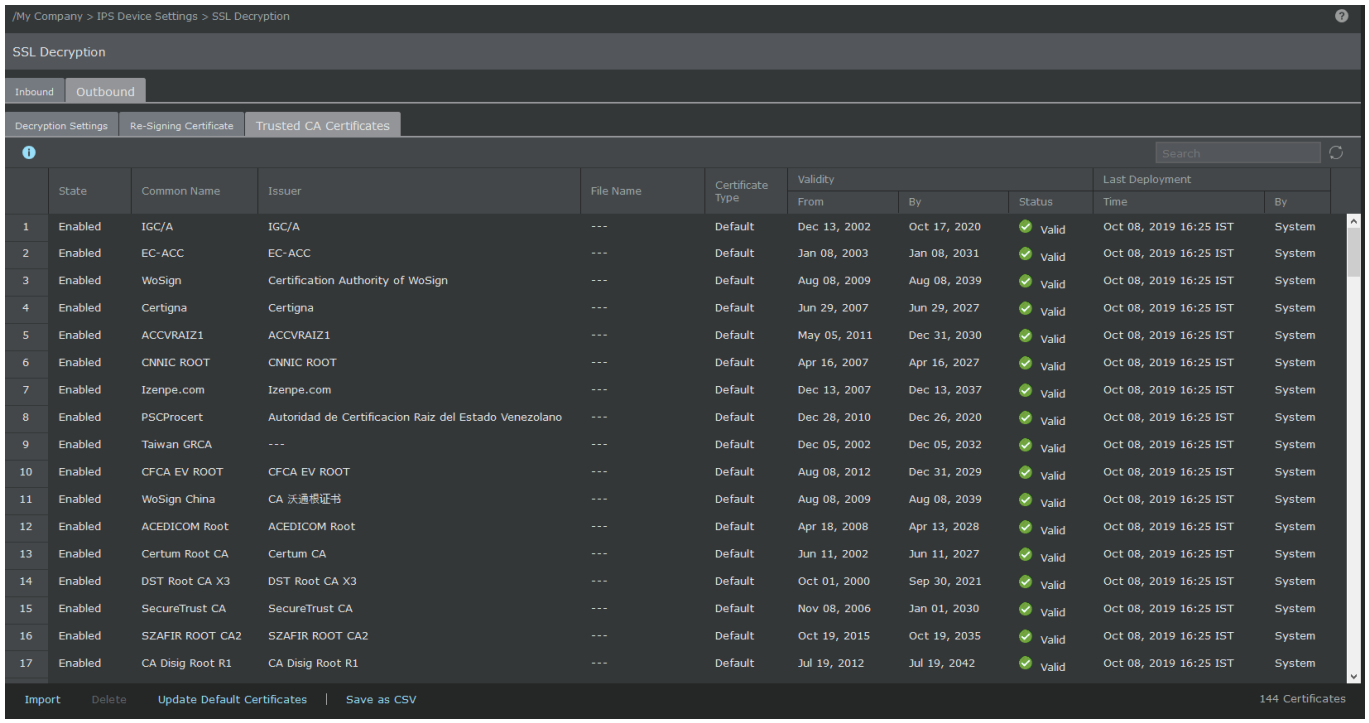
Trusted CA Certificates

The **Trusted CA Certificates** tab displays the list of certificates from the CA that the Sensor uses to validate the certificate from the web server.

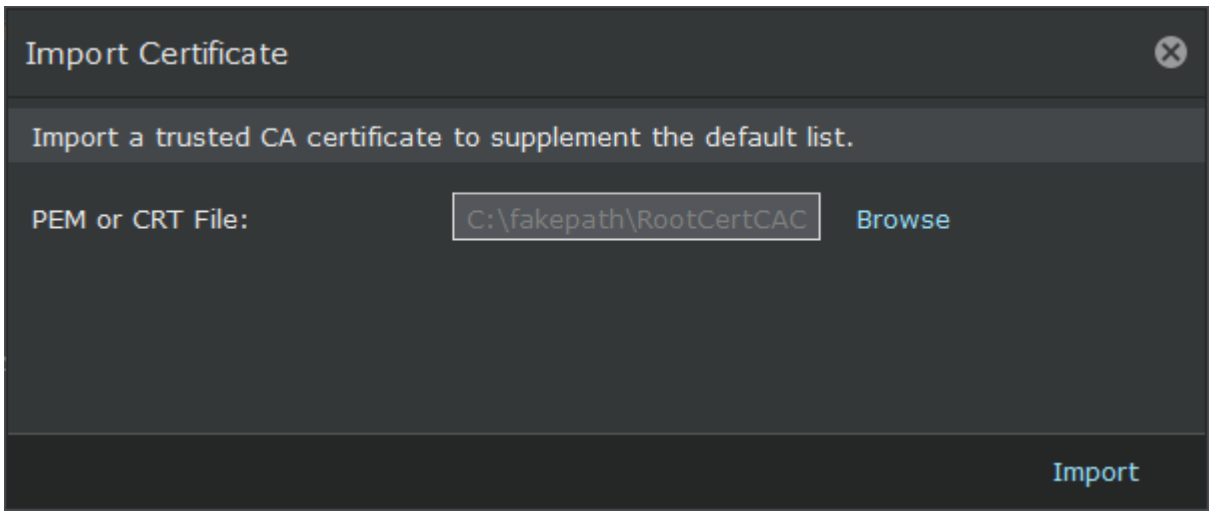
Actions for Trusted CA Certificates

To configure **Trusted CA Certificates** follow the steps below:

1. Go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. On the **Outbound** tab, select **Trusted CA Certificates** tab.



3. To import a trusted CA certificate:
   a. Click **Import**. The **Import Certificate** dialog box opens.



   b. Click **Browse**.
   c. Select the .pem file stored in the local system.
   d. Click **Import**.
4. (Optional) Click **Delete** to remove a custom CA certificate.

> **NOTE**
>
> You cannot delete a default CA certificate that is bundled with the Manager.

5. (Optional) Click **Update Default Certificates** to update all default CA certificates.

> **NOTE**
>
> You cannot update a custom CA certificate using **Update Default Certificates**. You have to manually re-import the updated custom CA certificate.

6. (Optional) Click **Save as CSV** to export the list of certificates.

Manage exclusions to outbound SSL flows

You can exclude flows from decryption by adding it to the Outbound SSL decryption exclusion list. This helps to avoid decrypting personal and sensitive information. It also helps in Sensor performance optimization by reducing the load on the Sensor. This is achieved by avoiding decryption of trusted sessions. You can exclude certain outbound SSL traffic from decryption based on source or destination IP address, destination domain name, and URL category.

> **NOTE**
>
> SSL decryption exclusions are applicable to outbound SSL decryption only.

To manage outbound SSL decryption exclusions, select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Outbound SSL Decryption Exclusions**. The **Outbound SSL Decryption Exclusions** page is displayed.

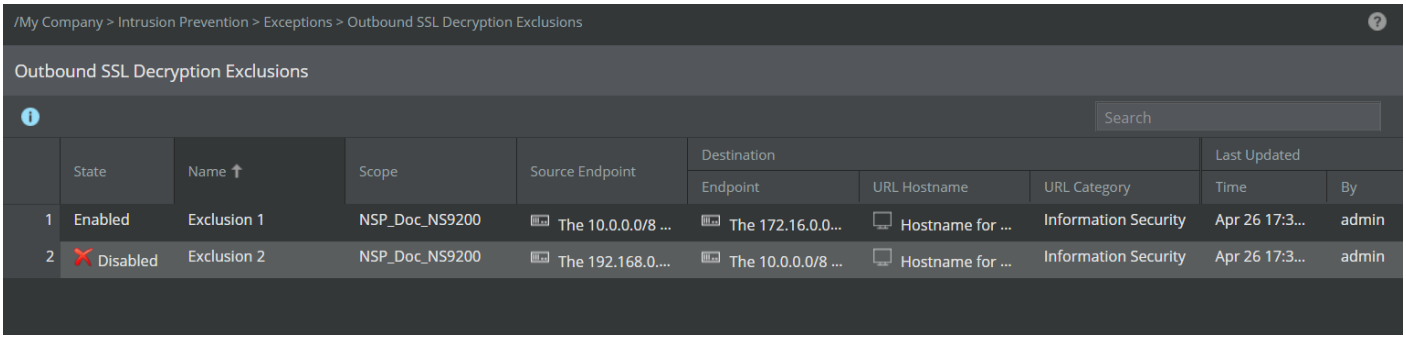
The list on the **Outbound SSL Decryption Exclusions** page displays the following information:

Field	Description
State	Specifies whether the state of the exclusion is **Enabled** or **Disabled**.
Name	Name of the SSL decryption exclusion.
Scope	Device to which the outbound SSL decryption exclusion is applied.
Source End-point	Specifies the source IP address.
Destination	**Endpoint** — Specifies the IP address or domain name of the destination endpoint. **URL Hostname** — Specifies the destination hostname of the URL. **URL Category** — Specifies the URL category of the destination endpoint. The Manager retrieves the list of URL categories from the GTI server.
Last Updated	**Time** — Specifies the time when the exclusion was last modified. **By** — Displays the user who modified the exclusion.
Comment	Additional comment specified for the exclusion.
Search	Type your search criteria in the field to find the exclusion.

You can perform the following actions from this page:

Option	Definition
+	Add outbound SSL decryption exclusion.
	Copy outbound SSL decryption exclusion.
−	Delete outbound SSL decryption exclusion.
View or Edit	To view or edit an outbound SSL decryption exclusion object, double-click the row of the exclusion.
Save as CSV	Export the outbound SSL decryption exclusion in CSV format.

Figure 489. Outbound SSL decryption exclusions



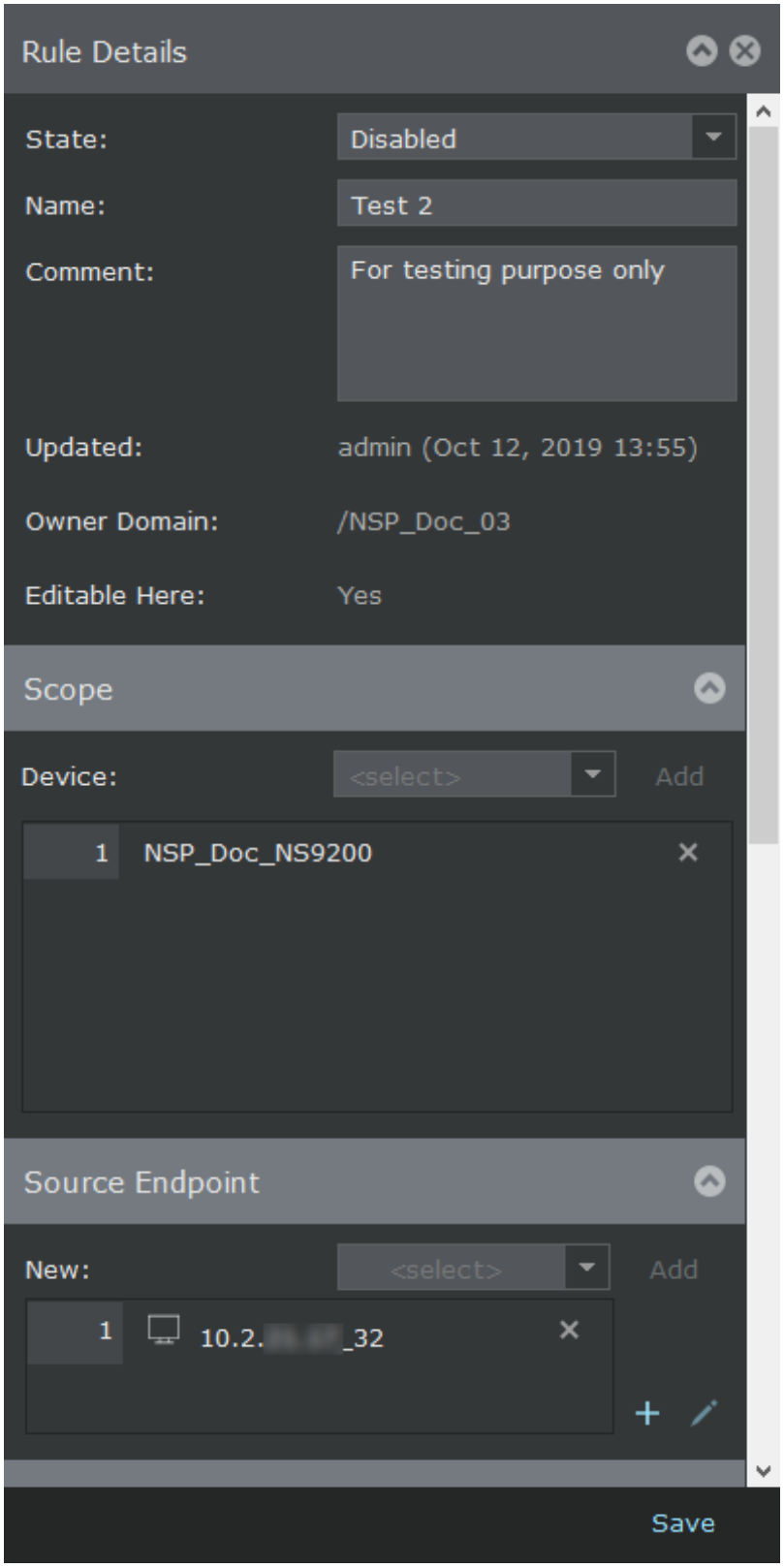
Actions for Outbound SSL Decryption Exclusions

To add outbound SSL decryption exclusions in the Manager, complete these tasks:

1. Go to Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Outbound SSL Decryption Exclusions**.
2. Add an outbound SSL decryption exclusion.
   a. In the **Outbound SSL Decryption Exclusions** page, click +.

      The **Rule Details** panel appears.

Figure 490. Rule Details panel for Outbound SSL Decryption Exclusion



Option	Definition
State	State of the exclusion. The state can either be **Enabled** or **Disabled**.
Name	Name for the exclusion.
Comment	Additional comments for the exclusion.
Updated	Displays the user who last modified the exclusion.
Owner Domain	Displays the name of the admin domain under which the outbound SSL decryption exclusion is added.
Editable here	Displays **Yes** if the exclusion is owned by the current admin domain. Displays **No** if the exclusion is not owned by the current admin domain.
Scope	
Device	Device or interface to which you want to assign the exclusion. The actions supported are add and delete. **NOTE** If the **Scope** is not specified for the exclusion, the exclusion will be applied to all the Sensors connected to the Manager that has Outbound SSL Decryption enabled.
Source Endpoint	
New	Source endpoint IP address or CIDR to which you want to assign the exclusion. The actions supported are add, create, edit, and delete. Click **Add** to add a rule object. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in Outbound SSL Decryption Exclusions is 10. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.
Destination Endpoint	

Option	Definition
New	Destination endpoint IP address or CIDR to which you want to assign the exclusion. The actions supported are add, create, edit, and delete. Click **Add** to add a rule object. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in Outbound SSL Decryption Exclusions is 10. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.
Destination URL Hostname	URL hostname of the destination to which the outbound SSL decryption exclusion is assigned to. The actions supported are add, create, edit, and delete. Click **Add** to add a rule object. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in Outbound SSL Decryption Exclusions is 10. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list. **NOTE** The Sensor uses SSL extension "Server Name Indication" (SNI) in the "CLIENT HELLO" message to get the host name and category. If SNI is absent, the Sensor cannot match against these exclusions.

Option	Definition
Destination URL Category	URL category for which you want to assign the exclusion. The Manager retrieves the list of URL categories from the GTI server. It can retrieve the list from the Public GTI cloud or the Private GTI cloud based on the configuration. **NOTE** If **Alert Data Details** is not enabled in the Manager → <Admin Domain Name> → Integration → **GTI** page, URL category is disabled. Also, DNS resolution must be enabled in the Sensor for functioning of GTI. The actions supported are add and delete.

b. Click **Save**.

The outbound SSL decryption exclusion is displayed in the **Outbound SSL Decryption Exclusions** pane.

3. Select the exclusion and click  to clone an outbound SSL decryption exclusion.

NOTE

You can use the Search function to find the outbound SSL decryption exclusion.

4. Double-click the row of the exclusion to modify. The **Rule Details** panel is displayed. You can edit the values for the fields.
5. Select the exclusion, click  to delete the exclusion.
6. Click **Save as CSV** to export the outbound SSL decryption exclusions list as a .csv file.

Clone Outbound SSL Decryption Exclusions object

To clone an outbound SSL decryption exclusion:

1. Go to Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Outbound SSL Decryption Exclusions**.
2. Select the exclusion and click  .

NOTE

You can use the Search function to find the outbound SSL decryption exclusion.

3. Make the required changes and click **Save**.

Import Outbound SSL Decryption Exclusions

Between the same versions of the Manager, you can export and import outbound SSL decryption exclusions list. When you export the outbound SSL decryption exclusions, a .xml file is created with the list of exclusions. On importing this .xml file into the Manager, the outbound SSL decryption exclusions list is created with the exclusions contained in the .xml file.

1. Select Intrusion Prevention → Advanced → Policy Import → **Outbound SSL Decryption Exclusions.**

2. Specify the required options to import the outbound SSL decryption exclusions.

Option	Definition
Append the existing set of rules	When selected, the Manager appends the outbound SSL decryption exclusions to the existing set of rules.
Import File	Click **Browse** to locate the file to import.
Import	Begins the import process.

Export Outbound SSL Decryption Exclusions

You can export the outbound SSL decryption exclusions in XML format.

1. Select Intrusion Prevention → Advanced → Policy Export → **Outbound SSL Decryption Exclusions**.

   The **Outbound SSL Decryption Exclusions** page is displayed.

2. Click **Export** to export the outbound SSL decryption exclusions list into an XML file.

Outbound SSL mixed traffic - throughput for proxy based SSL: NS-series Sensors

The following section contains outbound SSL best practices for mixed traffic:

NS9500 standalone - 30 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	4,500
SSL Throughput	5.0 Gbps
HTTP 1.1 Throughput	21.5 Gbps
Total Throughput	26.5 Gbps

NS9500 standalone - 20 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	3,600
SSL Throughput	4.0 Gbps
HTTP 1.1 Throughput	15.5 Gbps
Total Throughput	19.5 Gbps

NS9500 standalone - 10 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	2,250
SSL Throughput	2.5 Gbps
HTTP 1.1 Throughput	7.5 Gbps
Total Throughput	10.0 Gbps

NS9200

Parameter	Throughput
Max. SSL Connections / Sec.	5,000
SSL Throughput	3.6 Gbps
HTTP 1.1 Throughput	14.7 Gbps
Total Throughput	18.3 Gbps

NS9100

Parameter	Throughput
Max. SSL Connections / Sec.	3,000
SSL Throughput	2.5 Gbps
HTTP 1.1 Throughput	10 Gbps
Total Throughput	12.5 Gbps

NS7500 - 7.5 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	2,250
SSL Throughput	2.5 Gbps
HTTP 1.1 Throughput	3 Gbps
Total Throughput	5.5 Gbps

NS7500 - 5 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	1,125
SSL Throughput	1.25 Gbps
HTTP 1.1 Throughput	2.75 Gbps
Total Throughput	4 Gbps

NS7500 - 3 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	675
SSL Throughput	750 Mbps
HTTP 1.1 Throughput	1.65 Gbps
Total Throughput	2.4 Gbps

NS7300

Parameter	Throughput
Max. SSL Connections / Sec.	2,500
SSL Throughput	2 Gbps
HTTP 1.1 Throughput	6 Gbps
Total Throughput	8 Gbps

NS7200

Parameter	Throughput
Max. SSL Connections / Sec.	800
SSL Throughput	900 Mbps
HTTP 1.1 Throughput	5 Gbps
Total Throughput	5.9 Gbps

Limitations

Following are few limitations when using the outbound SSL decryption feature:

- Decryption of VLAN tagged packets is not supported in NS9300, NS9200, NS9100, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, NS3500, NS3200, and NS3100 Sensor models.
- Decryption of double VLAN tagged packets is not supported in NS-series Sensor models.
- Only SSL HTTP traffic on port 443 is decrypted.
- If the Sensor performing decryption fails, all the sessions timeout and you have to recreate the session manually.
- Failover is not supported for outbound SSL decryption as the session keys are always available in the active Sensor only. The session keys are not synchronized to the passive Sensor.
- Traffic statistics and performance charts are not supported for outbound SSL decryption.

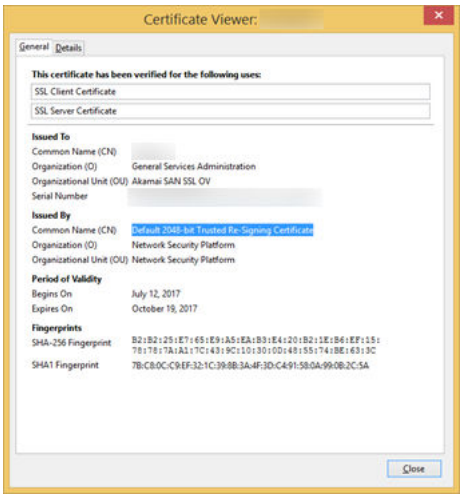
Use case scenarios for outbound SSL decryption

Below are few use case scenarios for outbound SSL decryption:

With re-signing certificate imported to the browser

When the client initiates a request to the web server, the Sensor intercepts the traffic and initiates connection to the web server. For example, when you initiate a request from a secure Amazon website to the Amazon web server, the Sensor intercepts the connection from the website and initiates a connection with the web server. The connection from the web server is checked against the trusted CA list by the Sensor. The re-signing certificate must be exported from the Manager and installed in the browsers' certificate store to initiate a secure connection. This is the re-signing certificate that the Sensor uses on the server's behalf when establishing connection with the client. In the process, the Sensor decrypts the traffic before sending it to the client. You can view the re-signing certificate from the Sensor by viewing the issuer name in the servers' certificate list of the browser. Once the connection is established, the Sensor inspects the traffic between the client and web server.

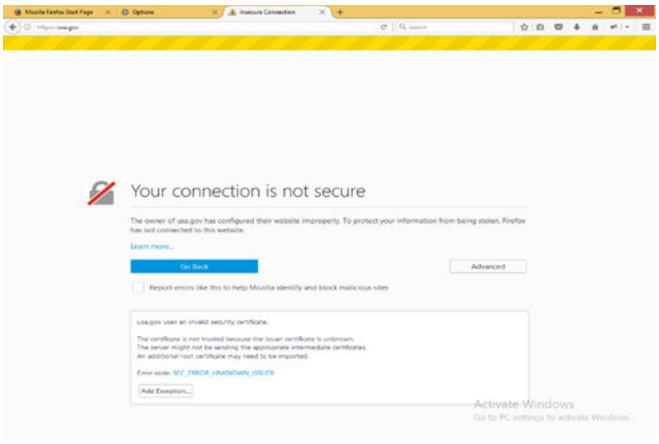
Figure 491. View the re-signing certificate in the browser



Without certificate in the trusted list of the Sensor

When a request from the client is sent to the web server, the Sensor intercepts the traffic and initiates a connection to the web server. If you have the failure handling configured to decrypt the flow when the certificate is untrusted/absent, a warning pops up in the browser stating that the connection is not secure. You can either proceed to the website or add the website as an exception. This happens when the certificate is not present in the trusted CA list. For the connection to establish, the certificate of the server must be present in the trusted CA list. When you add a website as an exception, the certificate will not be uploaded in the browser. The Sensor decrypts the traffic, but will not be inspected for malicious activity.

Figure 492. Warning in the browser for untrusted certificate



Decrypting inbound SSL traffic

Web servers are prone to attacks as there are multiple requests coming to the server from various clients. It becomes difficult to track the requests especially when it is over a secure channel like SSL. Most web servers now use the secure channel for its connections. They use a secure form of HTTP called HTTPS. With HTTPS, security devices have a tough time inspecting the packets. It is even more a reason to decrypt the traffic as attackers can use this channel for initiating attacks. Web servers must be protected from untrusted client connections coming from internet or intranet.

The Sensors intercepts the traffic from the client to the server. All connections to the Sensor are considered inbound as the Sensors are deployed to protect the server. The Sensor decrypts the traffic and inspects it establishing a secure connection between the client and server.

In case of inbound SSL traffic, the Trellix IPS SSL functionality decrypts the traffic in three ways depending on the cipher suite used:

1. RSA ciphers (Known key method)
2. DHE, ECDHE, and RSA ciphers (Shared key method/Agent based method)
3. Proxy method

SSL decryption for DHE/ECDHE ciphers

Users are now moving to a more secure cipher suite like the DHE (Diffie-Hellman), ECDHE (Elliptic Curve Diffie-Hellman) ciphers. The RSA cipher suites have vulnerabilities and hence, there is a requirement to use stronger ciphers for secure connections. The stronger ciphers use the Perfect Forward Secrecy (PFS) method where the keys are generated dynamically for each session. The main advantage of this method is that if an attacker obtains a session key, the previous encrypted sessions cannot be decrypted.

In case of inbound SSL decryption for DHE/ECDHE cipher suites, an agent is installed in the web servers to be protected. The Agent passes the keys to the Sensor every time a connection is established with the web server. The session key must be passed to the Sensor as the keys are generated dynamically for every session. The key transfer is through TLS encrypted channel.

In the Agent based approach for inbound SSL decryption, the Trellix IPS's IPS Sensor is placed between the client and server. When the client sends a request to the web server, the Sensor intercepts the connection. The Sensor then initiates a connection with the server. This way the Sensor retrieves information about the keys used at both ends.

The Agent and the Sensor communicates over the management port for session key exchange. You can specify the number of concurrent connections between the Sensor and Agent in the Manager. This avoids unnecessary consumption of the management port bandwidth. The IP address of the web server should be added in the Manager which allows the server to communicate with the Sensor for inbound decryption.

You can download the Trellix SSL Agent from the Trellix Download Server. The link is available in the **SSL Decryption** page in the Manager. You can log into the Download Server using your Grant Number. The SSL Agent download file is available under **Utilities & Connectors** in the Download Server. The web server to be protected should have the Agent installed on it. In case of DHE/ECDHE ciphers suites since the public keys are dynamically generated, the Agent passes the keys to the Sensor every time a new connection is established. When the traffic flows through the Sensor, the keys are already available in the Sensor which helps in inspecting the traffic. When an attack is detected, the Sensor generates an alert in the Manager.

NOTE

The Trellix SSL Agent can be installed on Linux based web servers only across multiple distributions like RHEL, Ubentu, Fedora, etc.

Once the inbound SSL decryption feature is disabled, the Agent is disconnected from the Sensor. The keys shared with the Sensor is purged once the Agent is disconnected. You can view the number of active Agent connections using the CLI command **`show sslagentaccesscontrol status`**.

Inbound SSL decryption is supported in Inline, TAP, and SPAN modes.

NOTE

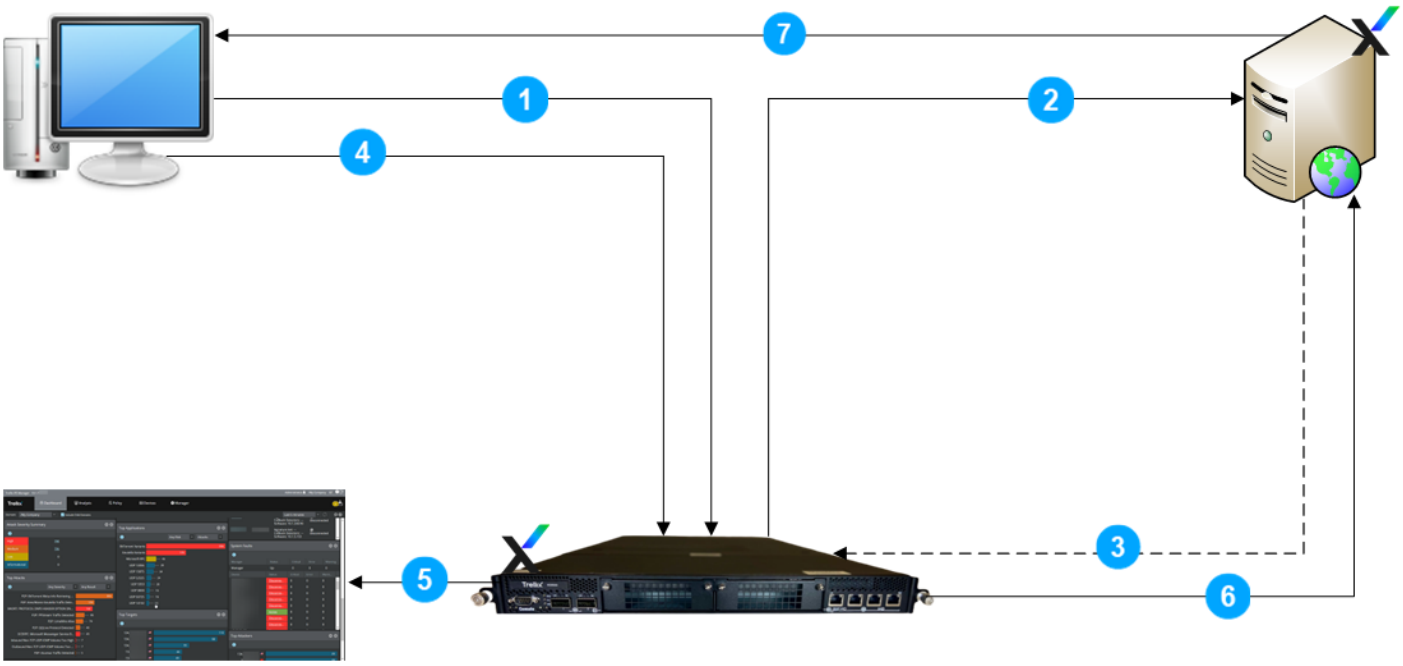
The Agent based method is supported only on NS9500 standalone and stack, NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, and NS3600 series Sensors.

NOTE

Agent based method is not supported for AWS, Azure, and OCI cloud platforms.

Below is the working of the Agent based inbound decryption method:

Figure 493. Steps to decrypt inbound SSL traffic using DHE/ECDHE ciphers



Steps:

1. The Sensor intercepts the initial request from the client. (Steps 1, 2, and 3 constitute the handshake process)
2. The Sensor forwards the request to the web server.
3. The Agent in the web server sends the SSL keys to the Sensor through an encrypted channel.
4. Using the SSL keys received from the Agent, the Sensor decrypts and inspects the subsequent requests from the client.
5. If an attack is detected, the Sensor generates an alert in the Manager.
6. If there are no attacks, the Sensor forwards the request to the web server.
7. The web server responds to the client's request.

Factors to be considered:

- Port 8501 should be opened for communication between the Agent and the Sensor.

- A restart of the web server is required once you install the Agent.
- One Agent must be installed per web server to be protected. Any number of Agents can be installed across different web servers.
- When you disable an enabled inbound SSL decryption feature, you must uninstall the Agent manually from the web servers.
- In case of failure in the Sensor, the Agent is configured to have a fail-open policy where the traffic is allowed to flow. In such cases the traffic will not be inspected.
- In case of a HA pair, IP addresses of both the primary and secondary Sensors must be available in the Agent.

SSL decryption for RSA ciphers

Trellix IPS SSL functionality allows a Sensor to maintain a copy of a server's private key, thereby allowing the Sensor to properly determine the session key for SSL sessions terminating on that server. The Manager provides a passthru interface for importing a set of public/private keys of the servers to the Sensor. You import the SSL keys separately for each Sensor.

After you import the required SSL keys into the Manager, you must deploy changes to the corresponding Sensors. Then the Manager pushes the encrypted SSL keys to the corresponding Sensors. The Sensors keep the SSL keys in their volatile memory when they receive the SSL keys from the Manager. If a Sensor reboots, the SSL keys are lost. When the Sensor starts, it requests all of the SSL keys that the Manager has for that Sensor.

In case of inbound SSL traffic, the Manager stores an escrow of the imported keys it its database for Sensor recovery purpose. However, the Manager does **not** interpret the escrowed keys, nor does it attempt to recover the keys themselves in case a Sensor has lost its encryption key. In order to protect the imported keys both in transit and in escrow, the Manager uses the public key of the corresponding public/private key pair of the Sensor. Only the corresponding Sensor can decrypt the SSL keys.

NOTE

The Known key method is supported only on NS9500 standalone and stack, NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, IPS-VM600, and IPS-VM5000 Sensors.

Trellix IPS supports the PKCS12 format — file suffixes like ".pkcs12", ".p12", or ".pfx" — with an RSA private key no longer than 2048 bits. The keys work across all of a Sensor's Virtual IPS (VIPS) instances. The private key must be a part of the PKCS12 file.

NOTE

The Sensor decrypts inbound SSL traffic only on TCP port 443. To decrypt SSL on a non-standard port, make sure you have defined the non-standard port for HTTP with SSL enabled. To do this, select the device and go to Setup → Advanced → **Non-Standard Ports.**

NOTE

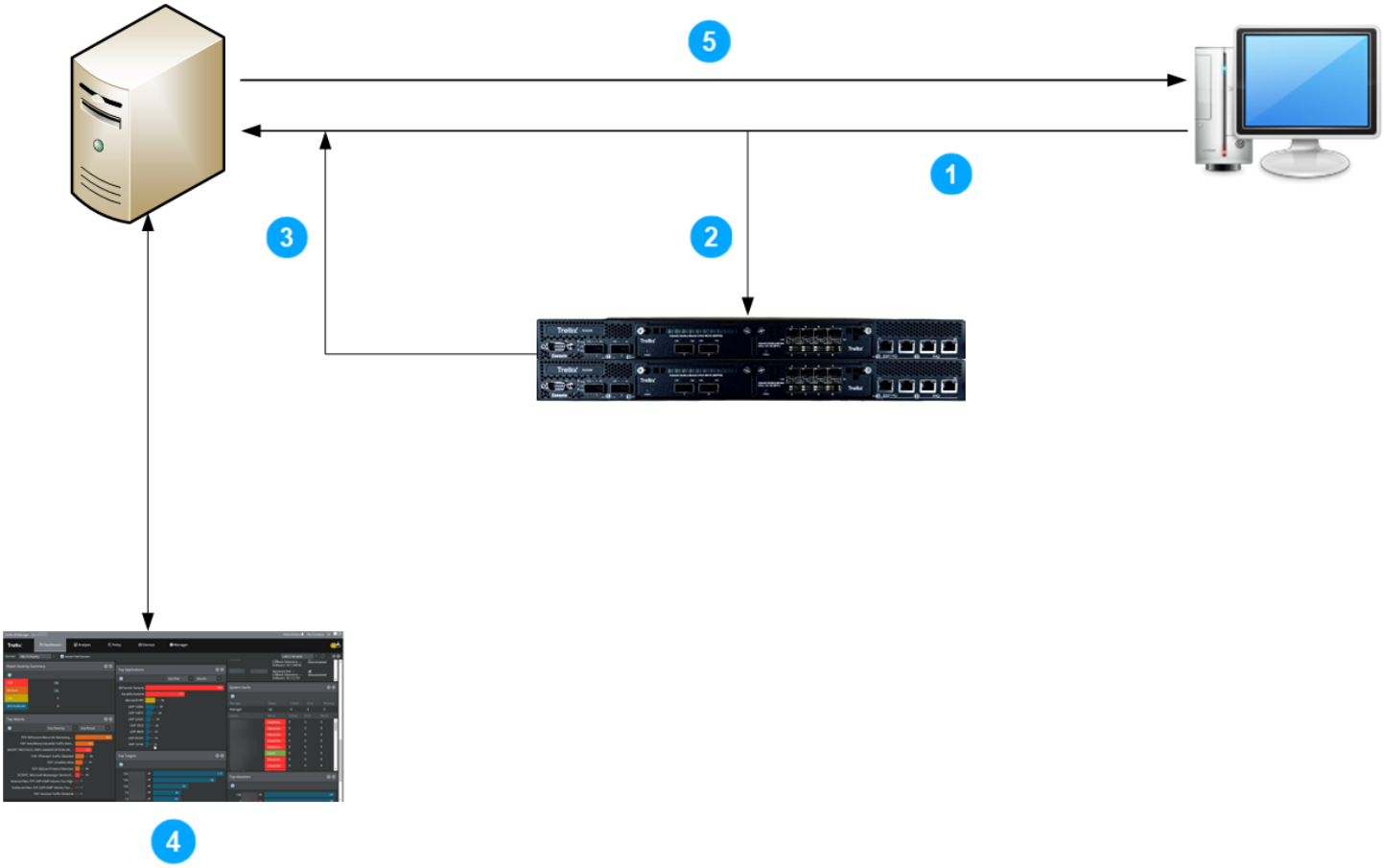
Jumbo frame traffic with SSL encryption is not supported in Sensor.

NOTE

For Virtual IPS Sensors, OpenSSL version 1.1.1 and above SSL decryption is not supported.

The steps to decrypt inbound SSL traffic by the Sensor are given below:

Figure 494. Steps to decrypt inbound SSL traffic using RSA ciphers



1. The client sends the secure request to the web server.
2. The Sensor intercepts the request, validates the certificates, and scans the packets.
3. If any malicious activity is found, the Sensor blocks the packets. If no malicious activity is found, the Sensor lets the request reach the server.
4. The Sensor raises an alert on the Attack Log.
5. The web server sends encrypted packets to the client.

Factors to be considered:

- There is a performance impact when using the SSL decryption feature. See the section [SSL best practices] at the end of this chapter for Sensor throughput information when you enable SSL decryption.

> **NOTE**
>
> There is a performance impact when using the SSL decryption feature. If there is a lot of outbound SSL traffic from the client to the internet as well, it consumes SSL flows. Therefore, to enable the Sensor to effectively utilize the SSL decryption feature, it is recommended to bypass these outbound SSL traffic using ACL Ignore rules.

- Inbound SSL Decryption is not supported by NS3500, NS3200, and NS3100 Sensors.
- NS-series Sensors can support up to 1024 SSL certificates.
- Sensors which are capable of SSL traffic inspection support both SSL session IDs and TLS session tickets to resume SSL session.
  - **SSL session ID** — The web server attaches the session ID when the web server sends the handshake to the client. The client can use the session ID to resume the SSL session with the web server.
  - **TLS session ticket** — The web server sends its secret state to the client, encrypted with a key only known to it as a session ticket. The client will store its secret information for a TLS session along with the ticket received from the web server. The client sends the session ticket along with its information to the Web server to resume the SSL session.

Supported web servers and cipher suites for inbound SSL inspection

SSL decryption is supported for the following web servers:

- Apache
- Tomcat
- Nginx

In addition to the above web servers, the following web servers are also supported for the RSA ciphers:

- Microsoft Internet Information Server (IIS)
- IBM WebSphere

While Trellix IPS offers three decryption methods for inbound SSL inspection — Known-key, Agent based and Proxy — each of them supports a list of cipher suites for traffic decryption.

List of SSL cipher suites (as named in their respective RFCs) supported for Known-key method:

- SSLv3/TLSv1.0 cipher suites:
  - TLS_NULL_WITH_NULL_NULL
  - TLS_RSA_WITH_NULL_MD5
  - TLS_RSA_WITH_NULL_SHA
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_IDEA_CBC_SHA
  - TLS_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLSv1.1 cipher suites:
  - TLS_NULL_WITH_NULL_NULL
  - TLS_RSA_WITH_NULL_MD5
  - TLS_RSA_WITH_NULL_SHA
  - TLS_RSA_WITH_RC4_128_MD5

    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_IDEA_CBC_SHA
    - TLS_RSA_WITH_DES_CBC_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
- TLSv1.2 cipher suites:
    - TLS_NULL_WITH_NULL_NULL
    - TLS_RSA_WITH_NULL_MD5
    - TLS_RSA_WITH_NULL_SHA
    - TLS_RSA_WITH_NULL_SHA256
    - TLS_RSA_WITH_RC4_128_MD5
    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA256
    - TLS_RSA_WITH_AES_256_CBC_SHA256
    - TLS_RSA_WITH_AES_128_GCM_SHA256
    - TLS_RSA_WITH_AES_256_GCM_SHA384

List of SSL cipher suites (as named in their respective RFCs) supported for Agent based method:

- SSLv3/TLSv1.0 cipher suites:
    - TLS_NULL_WITH_NULL_NULL
    - SSL/TLS_RSA_WITH_NULL_MD5
    - SSL/TLS_RSA_WITH_NULL_SHA
    - SSL/TLS_RSA_WITH_RC4_128_MD5
    - SSL/TLS_RSA_WITH_RC4_128_SHA
    - SSL/TLS_RSA_WITH_IDEA_CBC_SHA
    - SSL/TLS_RSA_WITH_DES_CBC_SHA
    - SSL/TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - SSL/TLS_DH_DSS_WITH_DES_CBC_SHA
    - SSL/TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
    - SSL/TLS_DH_RSA_WITH_DES_CBC_SHA
    - SSL/TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
    - SSL/TLS_DHE_DSS_WITH_DES_CBC_SHA

    - SSL/TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
    - SSL/TLS_DHE_RSA_WITH_DES_CBC_SHA
    - SSL/TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLSv1.1 cipher suites:
    - TLS_NULL_WITH_NULL_NULL
    - TLS_RSA_WITH_NULL_MD5
    - TLS_RSA_WITH_NULL_SHA
    - TLS_RSA_WITH_RC4_128_MD5
    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_IDEA_CBC_SHA
    - TLS_RSA_WITH_DES_CBC_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_DH_DSS_WITH_DES_CBC_SHA
    - TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
    - TLS_DH_RSA_WITH_DES_CBC_SHA
    - TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_DHE_DSS_WITH_DES_CBC_SHA
    - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
    - TLS_DHE_RSA_WITH_DES_CBC_SHA
    - TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLSv1.2 cipher suites:
    - TLS_NULL_WITH_NULL_NULL
    - TLS_RSA_WITH_NULL_MD5
    - TLS_RSA_WITH_NULL_SHA
    - TLS_RSA_WITH_NULL_SHA256
    - TLS_RSA_WITH_RC4_128_MD5
    - TLS_RSA_WITH_RC4_128_SHA
    - TLS_RSA_WITH_3DES_EDE_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA
    - TLS_RSA_WITH_AES_128_CBC_SHA256
    - TLS_RSA_WITH_AES_256_CBC_SHA256
    - TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
    - TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DH_DSS_WITH_AES_128_CBC_SHA
- TLS_DH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DH_DSS_WITH_AES_256_CBC_SHA
- TLS_DH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DH_DSS_WITH_AES_128_CBC_SHA256
- TLS_DH_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DH_DSS_WITH_AES_256_CBC_SHA256
- TLS_DH_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DH_RSA_WITH_AES_128_GCM_SHA256
- TLS_DH_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- ECDH/E Cipher suites:
  - TLS_ECDHE_RSA_WITH_NULL_SHA
  - TLS_ECDHE_RSA_WITH_RC4_128_SHA
  - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

List of SSL cipher suites (as named in their respective RFCs) supported for Proxy method:

- SSLv3 cipher suites:
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_SEED_CBC_SHA
  - TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_NULL_SHA
  - TLS_RSA_WITH_NULL_MD5
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
  - TLS_DH_anon_WITH_AES_256_CBC_SHA
  - TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_SEED_CBC_SHA
  - TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
  - TLS_DH_anon_WITH_AES_128_CBC_SHA
  - TLS_DH_anon_WITH_SEED_CBC_SHA
  - TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA
  - TLS_DH_anon_WITH_RC4_128_MD5
  - SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
- TLSv1 cipher suites:
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_ECDH_anon_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDH_anon_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
  - TLS_ECDHE_RSA_WITH_RC4_128_SHA
  - TLS_ECDH_anon_WITH_RC4_128_SHA
  - TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
  - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDH_anon_WITH_NULL_SHA

- TLSv1.2 cipher suites:
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8
  - TLS_ECDHE_ECDSA_WITH_AES_256_CCM
  - TLS_ECDHE_ECDSA_WITH_ARIA_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
  - TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384
  - TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
  - TLS_RSA_WITH_AES_256_GCM_SHA384
  - TLS_RSA_WITH_AES_256_CCM_8
  - TLS_RSA_WITH_AES_256_CCM
  - TLS_RSA_WITH_ARIA_256_GCM_SHA384
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8
  - TLS_ECDHE_ECDSA_WITH_AES_128_CCM
  - TLS_ECDHE_ECDSA_WITH_ARIA_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_128_CCM_8
  - TLS_RSA_WITH_AES_128_CCM

- TLS_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_NULL_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_DHE_RSA_WITH_AES_256_CCM_8
- TLS_DHE_RSA_WITH_AES_256_CCM
- TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384
- TLS_DH_anon_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DH_anon_WITH_AES_256_CBC_SHA256
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CCM_8
- TLS_DHE_RSA_WITH_AES_128_CCM
- TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256
- TLS_DH_anon_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_anon_WITH_AES_128_CBC_SHA256
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256

- TLSv1.3 cipher suites:
  - TLS_AES_128_CCM_SHA256
  - TLS_AES_128_CCM_8_SHA256
  - TLS_AES_128_GCM_SHA256
  - TLS_AES_256_GCM_SHA384
  - TLS_CHACHA20_POLY1305_SHA256

Steps involved in configuring SSL decryption

At a high-level the following are the steps to configure a Sensor to decrypt and inspect SSL traffic:

1. Enable SSL decryption on the required Sensors and configure Sensor SSL parameters.
2. SSL decryption is by two methods:
   a. **For Agent based method** — Select the **Enable Diffie-Helman Support** checkbox to enable decryption. In the Agent based method, install the Agent on the web servers to be protected.

NOTE

Agent based method is not supported for AWS, Azure, and OCI cloud platforms.

b. **For the Known key method** — Import the private SSL certificates of the corresponding web servers into the Manager. The Sensors subsequently download these certificates from the Manager.

NOTE

- Various fault messages are raised in the Manager related to SSL decryption. For example, an imported SSL certificate might have become invalid or you might have modified SSL configuration settings that requires a Sensor reboot. All these fault messages are explained in detail in the System fault messages (page 2408).
- After you install the Agent on a virtual machine, the VM will auto reboot.

Installation of the Agent for DH ciphers

Before you enable the inbound SSL decryption for DH ciphers, install the Agent on the web servers to be protected. You can download the **Trellix SSL Agent** from the Download Server using your Grant Number. The SSL Agent download file is available under **Utilities & Connectors** in the Download Server. The **Trellix SSL Agent** is a tgz file that is downloaded as a **trellixsslagent.tgz** file to be installed on the web servers. The web server to be protected should have the Agent installed on it.

NOTE

Agent based method is not supported for AWS, Azure, and OCI cloud platforms.

NOTE

The Trellix SSL Agent can be installed on Linux based web servers only across multiple distributions like RHEL, Ubuntu, Fedora, etc.

To install the Agent on the web server, perform the following steps:

1. Untar the agent tarball trellixsslagent.tgz.

   ```
   #tar -zxvf trellixsslagent.tgz
   ```

2. Untar produces a directory that has similar content as the following:

   ```
   [root@Server_FC12_174_136 ~]# ls -al /root/trellixsslagent
   total 132
   drwxr-xr-x 2 root root 4096 Oct 11 16:02 .
   drwxr-xr-x 3 root root 4096 Oct 11 16:02 ..
   -rw-r--r-- 1 1001 1001 87 Oct 11 09:59 install.sh
   -rw-r--r-- 1 1001 1001 27436 Oct 11 09:59 trellixsslagent-1.0.1-0.i686.deb
   -rw-r--r-- 1 1001 1001 29218 Oct 11 09:59 trellixsslagent-1.0.1-0.i686.rpm
   -rw-r--r-- 1 1001 1001 27778 Oct 11 09:59 trellixsslagent-1.0.1-0.x86_64.deb
   ```

```
-rw-r--r-- 1 1001 1001 29556 Oct 11 09:59 trellixsslagent-1.0.1-0.x86_64.rpm
[root@Server_FC12_174_136 ~]#
```

3. Install the agent by executing the following shell script:

   ```
   chmod +x install.sh
   /install.sh
   ```

   Verify the installation by looking for the below files:

   ```
   ls -al /etc/trellixsslagent/agent.conf
   ls -al /usr/lib/libtrellixsslagent.so
   ```

4. Edit the Trellix SSL Agent configuration file **/etc/trellixsslagent/agent.conf** to set the correct parameters primarily the Sensor IP address and SSL library name (parameters are described in the configuration file).

   ```
   # IP address of the sensor(v4/v6) in case of
   # a standalone deployment
   # In case of HA/Stack setup(Active/standby or
   # Active/Active), comma-separated IP address's
   # of primary and secondary/stack nodes
   # for e.g: 10.1.1.190,10.1.1.191
   #
   SENSORIP=x.x.x.x
   #
   # libopenssl library name used by the
   # Apache or nginx
   # on some platforms, there are multiple
   # versions of openssl installed
   # and this ensures that correct openssl
   # library is intercepted
   #
   # default: libssl.so
   #
   LIBSSLNAME=libssl.so.10
   ```

5. For Apache/HTTPD, edit the script is located at /usr/lib/systemd/system/httpd.service to add a new **Environment** variable under the section **"[Service]"** as shown below:

   ```
   Environment="LD_PRELOAD=/usr/lib64/libtrellixsslagent.so"
   ```

6. For Apache Webserver:

   Edit the Apache Startup script to load the Trellix SSL Agent as shown as follows:

   /usr/sbin/apachectl (On some installations the path may be different. In such cases, you have do a find)

   Original script

   ```
   --------------
   ```

```
case $ARGV in
start|stop|restart|graceful|graceful-stop)
$HTTPD -k $ARGV
ERROR=$?
;;
Modified script
---------------
case $ARGV in
start)
LD_PRELOAD=/usr/lib/libtrellixsslagent.so $HTTPD -k $ARGV
#$HTTPD -k $ARGV
ERROR=$?
;;
stop|restart|graceful|graceful-stop)
$HTTPD -k $ARGV
ERROR=$?
;;
```

Restart the Apache

```
#apachectl stop; apachectl start
```

7. For Nginx Webserver:

   Nginx is usually started by the command line **/usr/bin/nginx** or **/usr/sbin/nginx**.

   Edit the startup command line and use

   ```
   <bash>#LD_PRELOAD=/usr/lib/libtrellixsslagent.so /usr/bin/nginx
   ```

   or

   ```
   <bash>#LD_PRELOAD=/usr/lib/libtrellixsslagent.so /usr/sbin/nginx
   ```

   Optional steps:

   On most of the servers, syslog is configured to log till "INFO" level only. If LOG_DEBUG messages are to be logged, which is what the Agent uses to dump more information, syslog configuration needs modification.

   Edit the file **/etc/rsyslog.conf** and search for the line similar to the line below:

   ```
   *.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages
   ```

   change it to

   ```
   *.debug;mail.none;news.none;authpriv.none;cron.none /var/log/messages
   ```

8. For CentOS server:

   a. Install **semanage** utility using the below command:

      ```
      yum install /usr/sbin/semanage
      ```

   b. Check the ports assigned to Apache/HTTPD process:

semanage port -l | grep -w http_port_t

Example:

```
[root@localhost Apurva]#  semanage port -l | grep -w http_port_t
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000
```

c. Add port **8501** to the list.

> **NOTE**
>
> **8501** is the listening port in the Sensor. The apache process in the CentOS server needs to initiate a connection to port **8501** of the Sensor.

semanage port -a -t http_port_t -p tcp 8501

d. Verify that port **8501** has been added to the list.

Example:

```
[root@localhost Apurva]#  semanage port -l | grep -w http_port_t
http_port_t tcp 8501, 80, 81, 443, 488, 8008, 8009, 8443, 9000
```

e. Reload the system daemon and restart the Apache/HTTPD service.

Reload the system daemon using the command **root#systemctl daemon-reload**.

Restart the Apache/HTTPD service using the command **root#service httpd restart OR apachectl restart**.

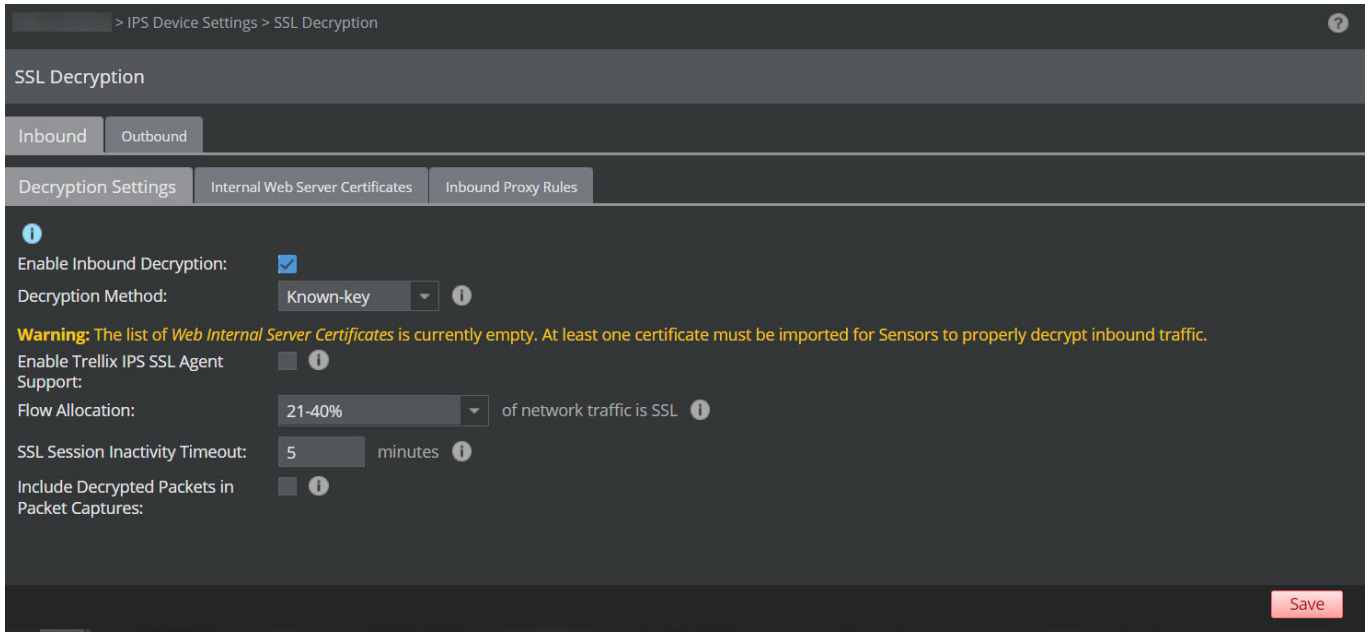
Configuring Inbound SSL decryption at domain level

Configuring Inbound SSL Decryption includes enabling SSL decryption with the required decryption method, enabling packet logging for SSL encrypted attacks, setting the number of SSL flows to monitor simultaneously, and setting the session cache time.

> **IMPORTANT**
>
> - If you enable or disable SSL decryption on a Sensor or modify the count of SSL flows, you must reboot the Sensor for the changes to take effect. You can opt for a hitless or full reboot.
>
>   For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.
> - In case of a virtual Sensor, if you enable or disable SSL decryption or modify the count of SSL flows, the Sensor will auto reboot.
> - In public cloud, if a virtual Sensor is added to a Cluster which has inbound SSL enabled, the SSL decryption configuration and the SSL key is automatically pushed to the new Sensor. The Sensor will auto reboot after the configuration push is complete.

To enable SSL decryption, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.



2. On the **Inbound** tab, select **Decryption Settings** tab.
3. Select the **Enable Inbound Decryption** checkbox.
4. From the **Decryption Method** drop down, select **Known-key**.
5. To enable decryption using the shared key method for Diffie-Helman, click the **Enable Trellix SSL Agent Support** checkbox.
6. For Agent based method, enter the **Maximum Concurrent Agent Connections** to limit the number of connections to avoid overloading the Sensor.

   The maximum number of concurrent connections supported are 1024 and minimum is 1.
7. Select the percentage for SSL flows from the **Flow Allocation** drop down.

   This value represents the percentage of SSL flows that you expect to see on your network so that the Sensor can pre-allocate a corresponding number of SSL flows. This configuration helps the Sensor to balance its resources between the total number of concurrent flows and number of SSL flows it is capable of handling. 21-40 % is allocated as the default value.

   The options for **Flow Allocation** are:

   - 1-20%
   - 21-40%
   - 41-60%
   - 61-80%
   - 81-100%

   For more information on total SSL flows supported for different Sensor models, go to Sensor limits for SSL flows (page 1211).
8. Enter the time duration in minutes for **SSL Session Inactivity Timeout**. The default value is 5 minutes. The maximum value you can configure is 120 minutes.

This time relates to session resumption in SSL. The value represents the duration for which a session is kept alive after the last connection closes. This value must be equal to or slightly longer than the session cache time on the corresponding server.

> **NOTE**
>
> A Sensor could be processing traffic destined to many servers. Due to this, the number of sessions the Sensor can maintain may be considerably lower than the number the servers that can be maintained. When the Sensor runs out of SSL sessions, SSL flows will not be processed and an alert is raised in Attack Log.

9. Optionally, select **Include Decrypted Packets in Packet Capture**.

   If this setting is configured, the Sensor captures encrypted and decrypted packets if an attack is detected. Otherwise only encrypted packets are captured.

10. For the Agent based method, add the web server IP addresses with the agent installed in the **Permitted Web Servers** section. Only the web servers added can connect to the Sensor.

    To add an IP address of the web server, enter the IP address in New IPv4/IPv6 CIDR block and then click Add.

    The maximum number of permitted web servers for IPv4 and IPv6 are 64 together.

> **TIP**
>
> The IPv6 IP address is different from IPv6 CIDR address. For example, in the CIDR address 209.173.53.167/20 the /20 indicates that the first 20 bits are used for network ID and the remaining 12 (there are 32 bits in the IP address) are used for host ID. You can also use tools to calculate and verify the IPv6 CIDR address range.

11. Click **Save**.
12. Any change to the direction of SSL Decryption will require you to reboot the Sensor.
    a. Select Manager → <Admin Domain Name> → Troubleshooting → **Logs**.
    b. View the critical messages on the **Faults** tab for the corresponding Sensor to see if a Sensor reboot is required.
    c. If yes, then do a hitless or full reboot of the Sensor.

> **NOTE**
>
> For NS-series Sensors, hitless reboot is not supported when SSL decryption is enabled.

Configuring Inbound SSL Decryption at device level

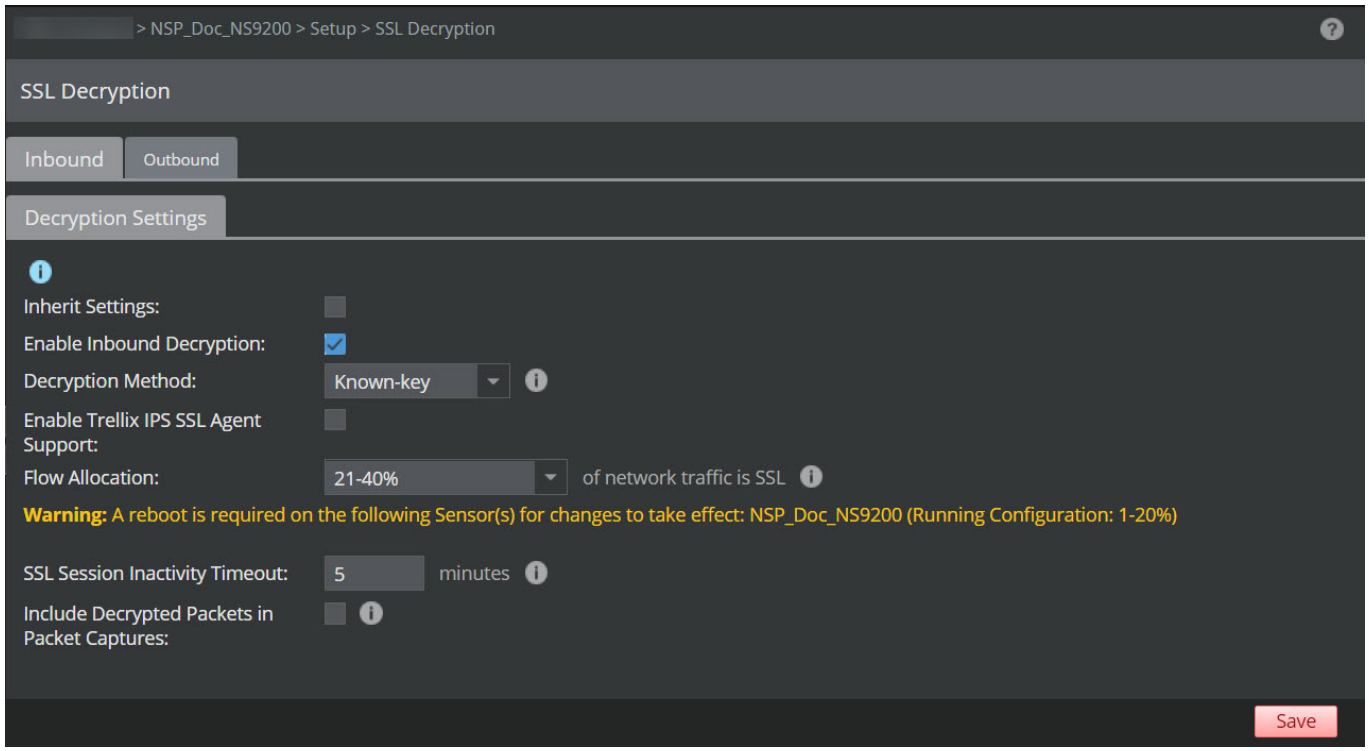
SSL configuration includes enabling SSL decryption, enabling packet logging for SSL encrypted attacks, setting the number of SSL flows to monitor simultaneously, and setting the session cache time.

IMPORTANT

- If you enable or disable SSL decryption on a Sensor or modify the count of SSL flows, you must reboot the Sensor for the changes to take effect. You can opt for a hitless or full reboot.

  For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.
- In case of a virtual Sensor, if you enable or disable SSL decryption or modify the count of SSL flows, the Sensor will auto reboot.
- In public cloud, if a virtual Sensor is added to a Cluster which has inbound SSL enabled, the SSL decryption configuration and the SSL key is automatically pushed to the new Sensor. The Sensor will auto reboot after the configuration push is complete.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **SSL Decryption**.



2. On the **Inbound** tab, select **Decryption Settings** tab.
3. Deselect **Inherit Settings** to override the settings of the parent domain.
4. Select the **Enable Inbound Decryption** checkbox.
5. From the **Decryption Method** drop down, select **Known-key**.
6. To enable decryption using the shared key method for Diffie-Helman, click the **Enable Trellix SSL Agent Support** checkbox.
7. For Agent based method, enter the **Maximum Concurrent Agent Connections** to limit the number of connections to avoid overloading the Sensor.

   The maximum number of concurrent connections supported are 1024 and minimum is 1.
8. Select the percentage for SSL flows from the **Flow Allocation** drop down.

This value represents the percentage of SSL flows that you expect to see on your network so that the Sensor can pre-allocate a corresponding number of SSL flows. This configuration helps the Sensor to balance its resources between the total number of concurrent flows and number of SSL flows it is capable of handling. 21-40 % is allocated as the default value.

The options for **Flow Allocation** are:

- 1-20%
- 21-40%
- 41-60%
- 61-80%
- 81-100%

For more information on total SSL flows supported for different Sensor models, go to Sensor limits for SSL flows (page 1211).

9. Enter the time duration in minutes for **SSL Session Inactivity Timeout**. The default value is 5 minutes. The maximum value you can configure is 120 minutes.

   This time relates to session resumption in SSL. The value represents the duration for which a session is kept alive after the last connection closes. This value must be equal to or slightly longer than the session cache time on the corresponding server.

   NOTE

   A Sensor could be processing traffic destined to many servers. Due to this, the number of sessions the Sensor can maintain may be considerably lower than the number the servers that can be maintained. When the Sensor runs out of SSL sessions, SSL flows will not be processed and an alert is raised in Attack Log.

10. Optionally, select **Include Decrypted Packets in Packet Capture**.

    If this setting is configured, the Sensor captures encrypted and decrypted packets if an attack is detected. Otherwise only encrypted packets are captured.

11. For the Agent based method, add the web server IP addresses with the agent installed in the **Permitted Web Servers** section. Only the web servers added can connect to the Sensor.

    To add an IP address of the web server, enter the IP address in New IPv4/IPv6 CIDR block and then click Add.

    The maximum number of permitted web servers for IPv4 and IPv6 are 64 together.

    TIP

    The IPv6 IP address is different from IPv6 CIDR address. For example, in the CIDR address 209.173.53.167/20 the /20 indicates that the first 20 bits are used for network ID and the remaining 12 (there are 32 bits in the IP address) are used for host ID. You can also use tools to calculate and verify the IPv6 CIDR address range.

12. Click **Save**.
13. Any change to the direction of SSL Decryption will require you to reboot the Sensor.
    a. Select Manager → <Admin Domain Name> → Troubleshooting → **Logs**.
    b. View the critical messages on the **Faults** tab for the corresponding Sensor to see if a Sensor reboot is required.

c. If yes, then do a hitless or full reboot of the Sensor.

> **NOTE**
>
> For NS-series Sensors, hitless reboot is not supported when SSL decryption is enabled.

Uninstallation of the Agent for DH ciphers

When you disable the inbound SSL decryption feature using the Agent based method, the Sensor and Agent are disconnected. No keys are passed from the Agent to the Sensor. You must uninstall the Agent manually from the web servers once you disable the inbound SSL decryption.

To uninstall the Agent, run the following command in the web server where the Agent is installed:

```
[root@Server_174_7 trellixsslagent]# ./install.sh -u
```

SSL decryption using proxy method

For inbound SSL traffic, when a client tries to access the secure server using SSL, the Sensor acts as a proxy between the client and the server. The Sensor intercepts the client request and forwards the request to the server as the client. Based on the rule configured the Sensor decrypts and scans the traffic.

> **NOTE**
>
> Proxy based inbound SSL decryption can be configured only on NS7500 and NS9500 standalone Sensors. You cannot configure proxy based inbound SSL decryption on a stack of NS9500 Sensors.

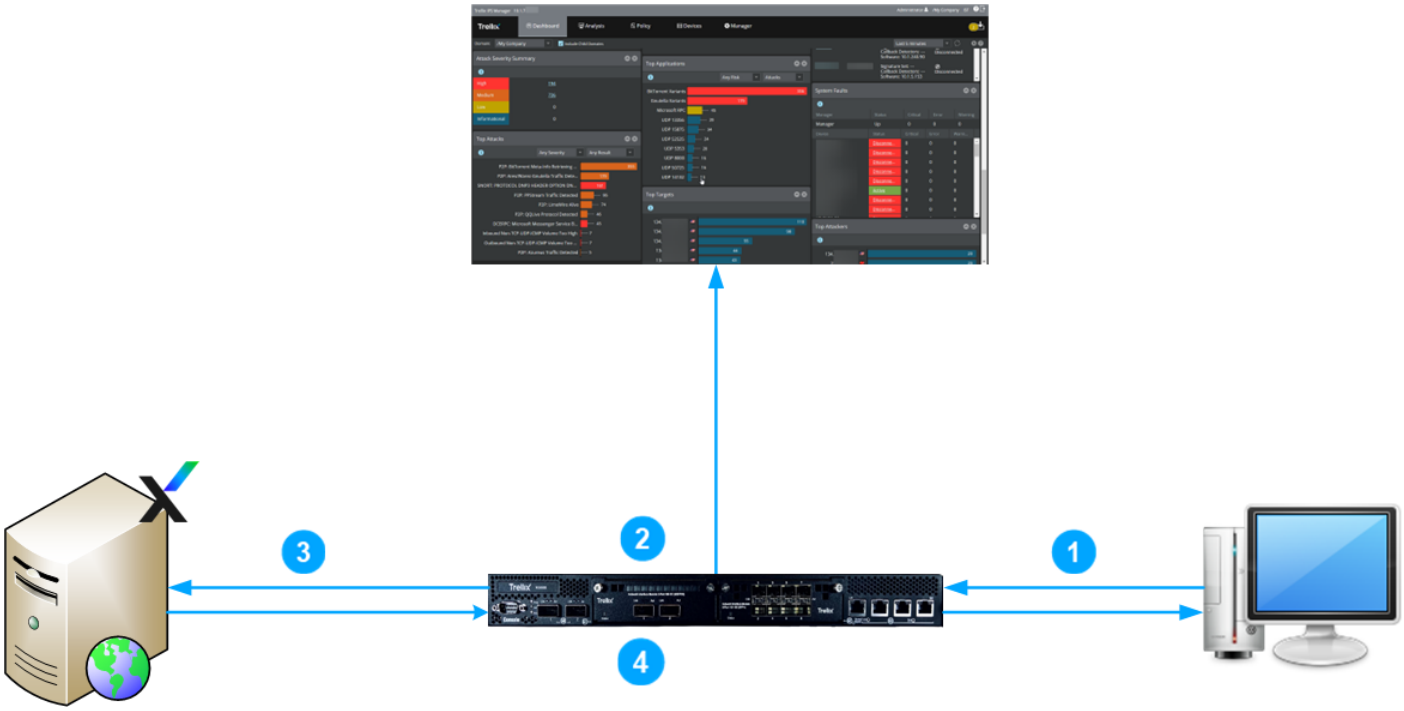
> **NOTE**
>
> Proxy based SSL decryption is not supported on G0/1-G0/2 ports.

> **NOTE**
>
> Decryption of VLAN tagged packets on Inbound SSL traffic in proxy based method is supported in NS9500 Standalone Sensor software version 10.1.5.41 or later and NS7500 Sensor software version 10.1.5.64 or later.

> **NOTE**
>
> Decryption of double VLAN tagged packets on Inbound SSL traffic in proxy based method is not supported.

The steps to decrypt inbound SSL traffic by the Sensor are given below:

Figure 495. Steps to decrypt inbound SSL traffic using proxy



1. The client sends a secure request to the web server.
2. The Sensor intercepts the request and responds with the server certificate configured as part of the proxy rule.
3. Sensor decrypts and inspects the client request. If any malicious activity is found, the Sensor raises an alert in the Attack Log.
4. The Sensor sends the response from the server to the client.

Port clustering for proxy-based SSL decryption in NS9500 standalone Sensor

Multiple monitoring port pairs in inline mode can be grouped together to create a port cluster. The same IPS policy will apply for traffic arriving on any of the inline pairs in the port cluster.

The following are the considerations for using port clusters with proxy based SSL decryption:

1. Port Cluster for proxy based SSL decryption is supported only for inline port pairs.
2. All paths in the network formed by the inline port pairs must be active paths (should not be blocked by any link layer protocols) on which packets can be forwarded.
3. Packets on the egress path (from the Sensor towards the client or server) may not follow the same path on which they arrived. For example, consider ports G1/1-G1/2, G1/3-G1/4 are grouped in a port cluster. A packet arriving on port G1/1 may exit from port G1/4.
4. SSL sessions will always be reported against the least index port of the port cluster even when the traffic is received on the other ports in the port cluster.

   For example, if G1/1, G1/2, G2/1, and G2/2 are in a port cluster with proxy based SSL enabled, even if the client and server packets are received over the physical G2/1 and G2/2 links, the **`show ssl stats outbound proxy sessions`** command displays that sessions are formed on G1/1 and G1/2. This behavior holds good even if ports G1/1 and G1/2 are not operational.

Configuring proxy based inbound SSL decryption at domain level

To enable Inbound SSL decryption using proxy, you must purchase the license and add it in the Manager. The license required for proxy based SSL decryption is the same for both inbound and outbound.

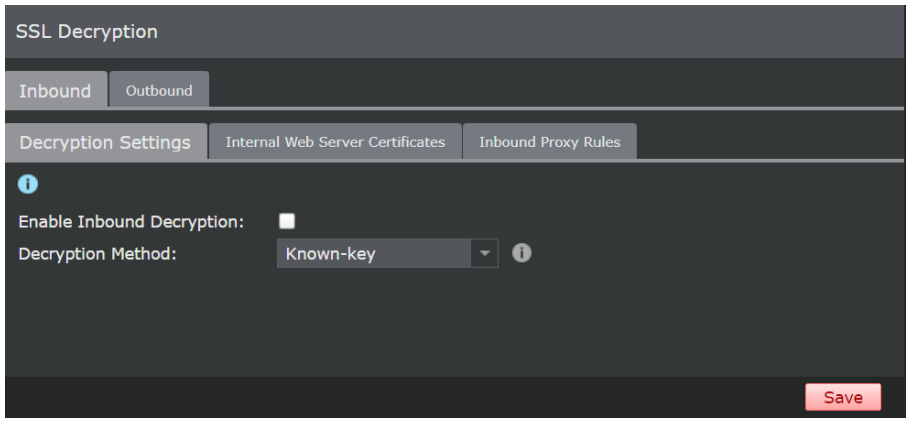
IMPORTANT

If you enable or disable proxy based SSL decryption on a Sensor, you must reboot the Sensor for the changes to take effect. You can opt for a hitless or full reboot.

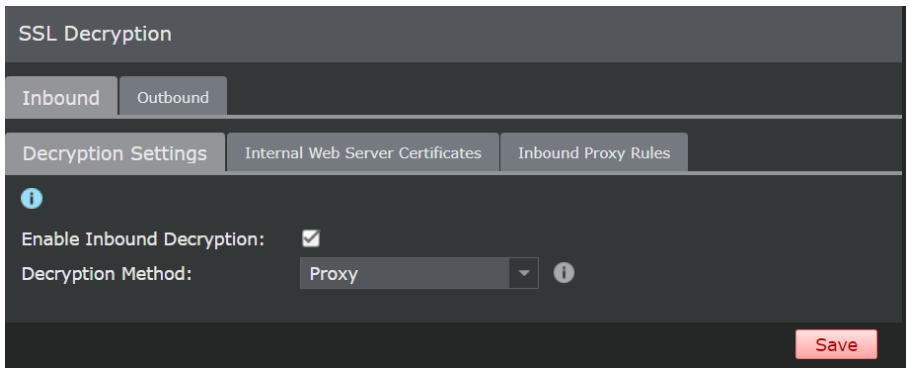
For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.

To enable proxy based inbound SSL decryption, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. On the **Inbound** tab, select **Decryption Settings** tab.



3. Select the **Enable Inbound Decryption** checkbox.
4. From the **Decryption Method** drop-down, select **Proxy**.



5. Click **Save**.

NOTE

If a valid license is not assigned to a Sensor, a warning **The device requires a valid proxy decryption license** is displayed in the **Deploy Pending Changes** page for that particular Sensor. To assign a valid license, see the section *Add license to the Manager* (page 1145).

NOTE

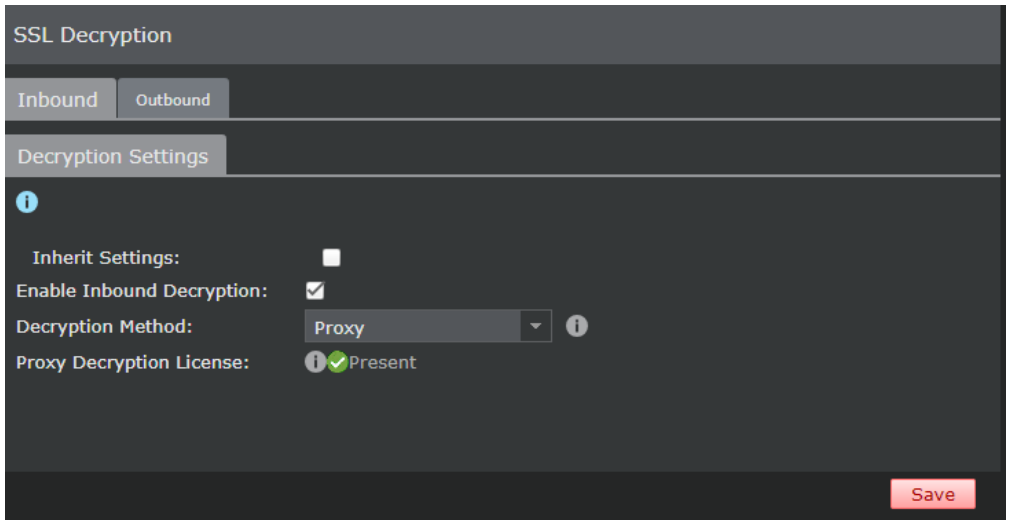
Reboot of the Sensor is required after you enable outbound SSL decryption for the feature to function. If you have already configured proxy based inbound SSL decryption, the reboot is not required.

Configuring proxy based inbound SSL decryption at device level

To enable Inbound SSL decryption using proxy, you must purchase the license and add it in the Manager. The license required for proxy based SSL decryption is the same for both inbound and outbound.

To enable proxy based inbound SSL decryption, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **SSL Decryption**.
2. On the **Inbound** tab, select **Decryption Settings** tab.
3. Deselect **Inherit Settings** to override the settings of the parent domain.
4. Select the **Enable Inbound Decryption** checkbox.



5. To enable SSL decryption using proxy, select **Proxy** from the **Decryption Method** drop-down.

   The **Proxy Decryption License** displays as **Present**.

NOTE

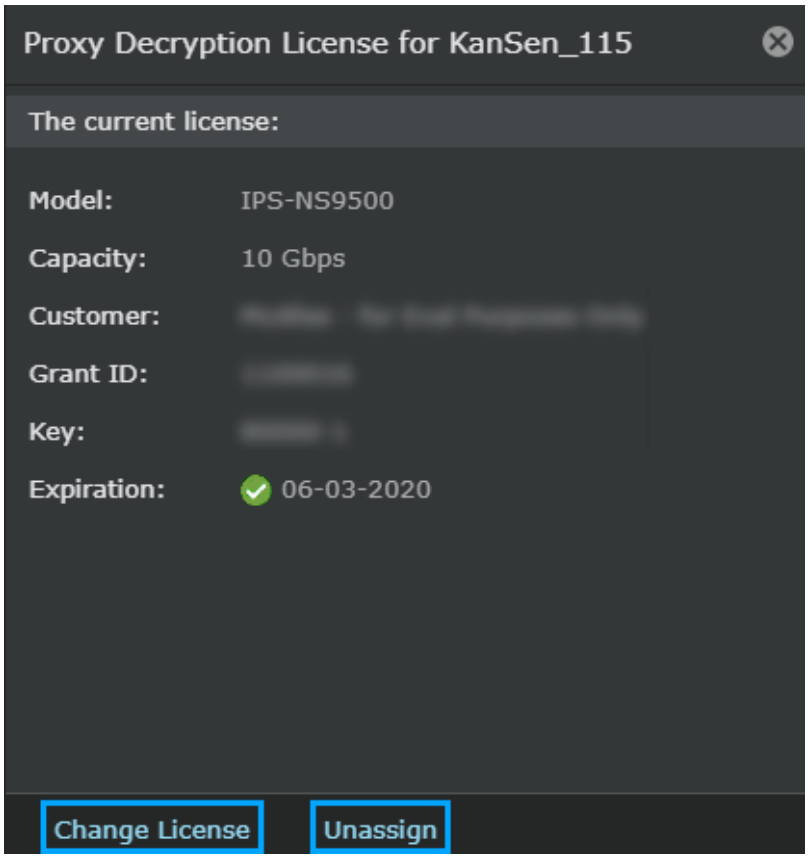
The **Proxy Decryption License** displays as **Required** if a license is not assigned.

NOTE

Ensure that the **Inbound Proxy Rules** has been created for the server you wish to protect.

a. Click the tooltip of **Proxy Decryption License** to view the status.

The **Proxy Decryption License** window opens.



b. [Optional] Click **Change License** or **Unassign**.

If you click **Change License**, it redirects you to **Proxy Decryption** tab, in the **Licenses** page on the **Manager** tab.

If you click **Unassign**, a warning message pops-up, click **OK**. The current license will be unassigned and the Sensor will operate without a license.

6. Click **Save**.

NOTE

If a valid license is not assigned to a Sensor, a warning **The device requires a valid proxy decryption license** is displayed in the **Deploy Pending Changes** page for that particular Sensor. To assign a valid license, see the section *Add license to the Manager* (page 1145).

NOTE

Reboot of the Sensor is required after you enable inbound SSL decryption for the feature to function. If you have already configured proxy based outbound SSL decryption, the reboot is not required.

Manage proxy rules

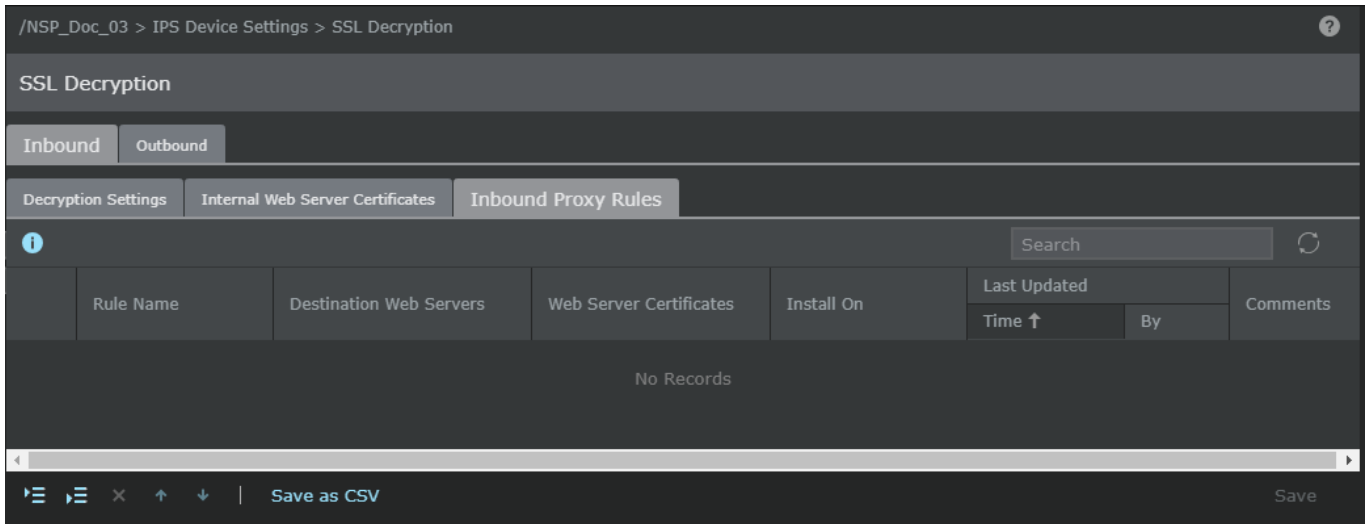
When using proxy mode, you need to configure a proxy rule for the web server you wish to protect and their certificate and key. Trellix IPS Manager supports PKCS12 keys with file suffixes ".pkcs12", ".p12", or ".pfx". This can be configured on the **Internal Web Server Certificates** tab of the **SSL Decryption** page. Proxy rules are used by the Sensor to identify the web servers that are to be protected. The rule contains the IP address and the web certificate of the server. When the sensor detects SSL traffic which contains the IP address of a server that has a proxy rule defined, then the Sensor intercepts and decrypts the traffic.

To manage a proxy rule, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. In the **Inbound** tab, select **Inbound Proxy Rules** tab.

   Inbound Proxy Rules tab contains the following:

Option	Definition
Rule Name	Name of the proxy rule
Destination Web Servers	Specifies the IPv4 CIDR of the destination web server
Web Server Certificates	SSL certificates of the corresponding web servers
Installed On	The Sensor that has the certificate
Last Updated	**Time** - Specifies the time when the exception was last modified **By** - Displays the user who modified the exception
Comments	Additional comment specified for the exception
	Add rule before the selected rule.
	Add rule after the selected rule.
	Delete the selected rule.
	Move the selected rule up.
	Move the selected rule down.
Save as CSV	Export the proxy rules in CSV format.



Add a proxy rule

To add a proxy rule, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. In the **Inbound** tab, select **Inbound Proxy Rules** tab.
3. Click to add a rule above the selected rule.

   Click to add a rule below the selected rule.

   The rule details pane opens.
4. Enter the name of the rule.
5. Enter the IPv4 CIDR of the web server you wish to protect.
6. Enter the comment for the rule.
7. Select the web server certificate from the drop down in the **Web Server Certificates** pane.
8. Click **Add**.
9. (Optional) Click **Set as default** to set the selected web server certificate as default certificate.

   The **Installed On** pane displays the Sensor on which the web server certificate is saved on.

   NOTE

   If you do not specifically set a default, the first certificate in the list is set as the default certificate.

   NOTE

   If the server supports Server Name Indication (SNI), multiple certificates must be available in the Sensor.
10. Click **Save** to save the rule order details.

Move proxy rules

To move one or more proxy rules, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. In the **Inbound** tab, select **Inbound Proxy Rules** tab.
3. Select the rules you want to move.
4. Click to move the rule up.

   Click to move the rule down.
5. Click **Save** to save the rule order change.

Delete proxy rules

To delete one or more proxy rules, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. In the **Inbound** tab, select **Inbound Proxy Rules** tab.
3. Select the rules you want to delete.
4. Click to delete the selected rule.
5. Click **Yes** in the confirmation pop up.

Export proxy rules

To move one or more proxy rules, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. In the **Inbound** tab, select **Inbound Proxy Rules** tab.
3. Click **Save as CSV** button to export the proxy rules.

Management of the imported SSL keys of a device

In the Manager, you can import, re-import, and delete the private SSL certificates and their key of the web servers that you want a specific Sensor to protect. All these actions require a configuration update for the changes to take effect. The Manager stores these keys in an encrypted format and sends them to the corresponding Sensor when you do a configuration update. If a Sensor reboots, it automatically requests the Manager for its SSL keys.

NOTE

For virtual Sensors in public cloud, you need to complete a signature set push to import the SSL keys to the virtual Sensors.

NOTE

You need to manage the SSL keys on a per Sensor basis. For example, if there are two different data paths to a server that are protected by two different Sensors, you must import the SSL key of the server separately for both the Sensors. In case of failover Sensors, the SSL keys on the primary is automatically copied over to the secondary.

NOTE

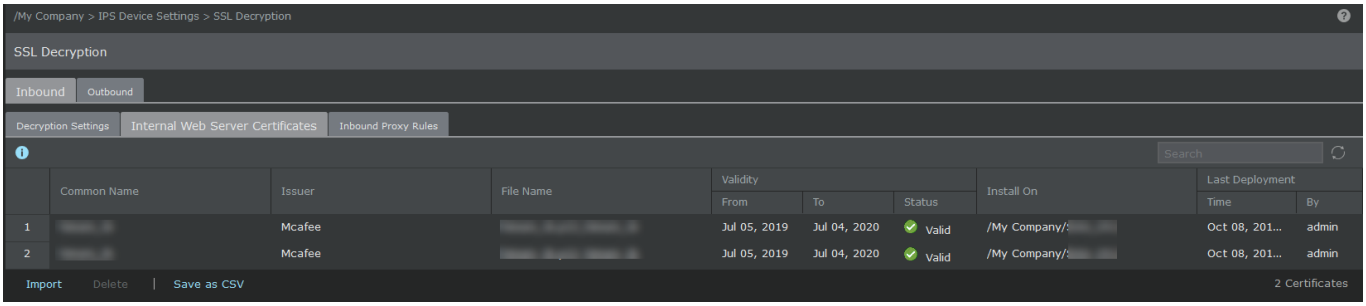
If you upgrade the capacity of a stack of NS9500 Sensors, you need to re-import the SSL keys.

Import SSL keys to the Manager for a Sensor

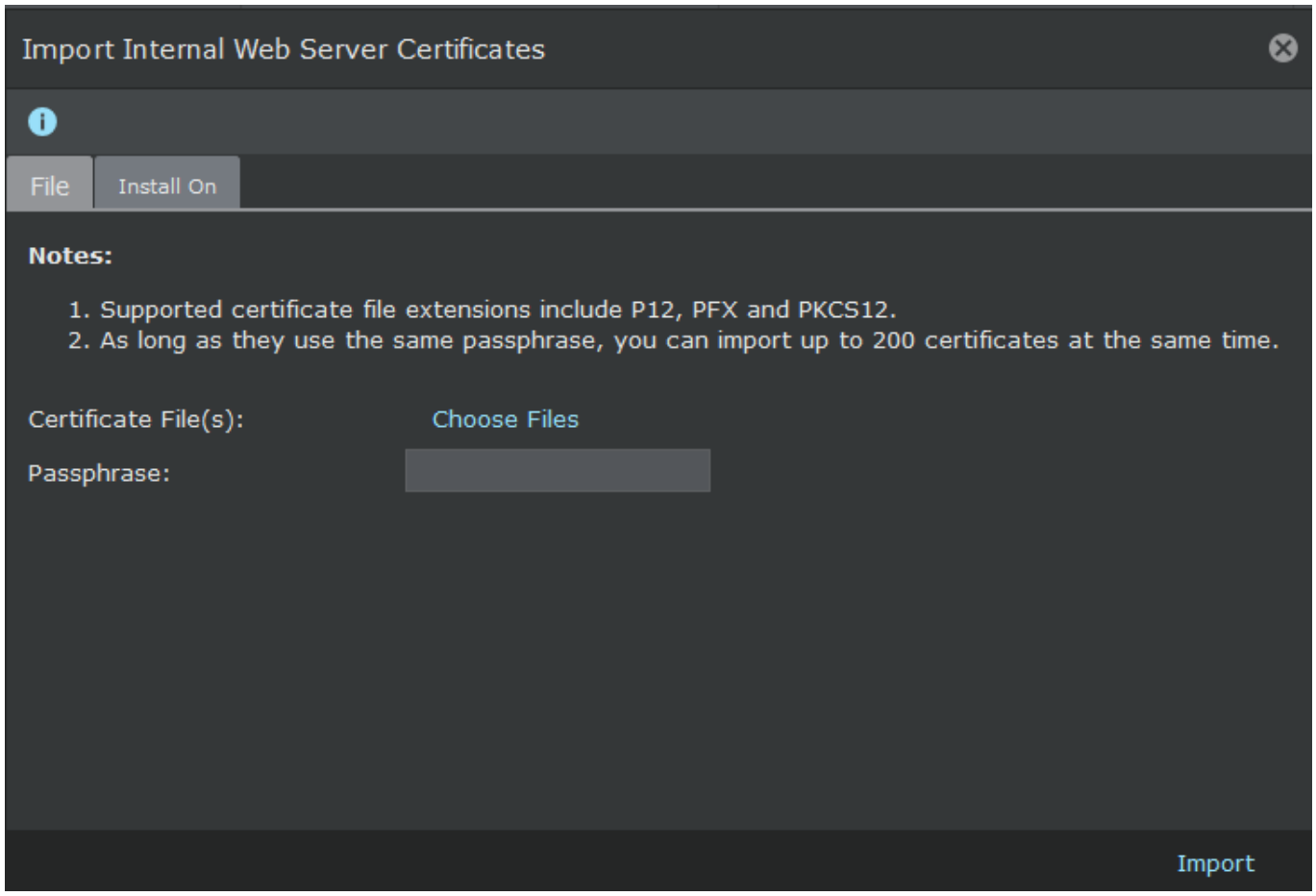
You can download Secure Socket Layer (SSL) keys to Manager for a single Sensor. Once imported to Manager, keys can be pushed to the Sensor via **Configuration Update**. Using provided SSL keys, a Sensor can decrypt SSL traffic for IPS inspection. Manager provides a passthru interface for you to import a set of public/private keys to the Sensor. Manager stores an escrow of the imported keys for Sensor recovery purpose. However, the Manager does not interpret the escrowed keys, nor does it attempt to recover the keys themselves in case a Sensor has lost its key encryption key. In order to protect the imported keys both in transit and in escrow, Manager uses the public key of the Sensor's public/private key pair.

Trellix IPS Manager supports PKCS12 keys with file suffixes ".pkcs12", ".p12", or ".pfx".

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.



2. In the **Inbound** tab, select **Internal Web Server Certificates** tab.
3. Click **Import**. The **Import Internal Web Server Certificates** dialog box opens.

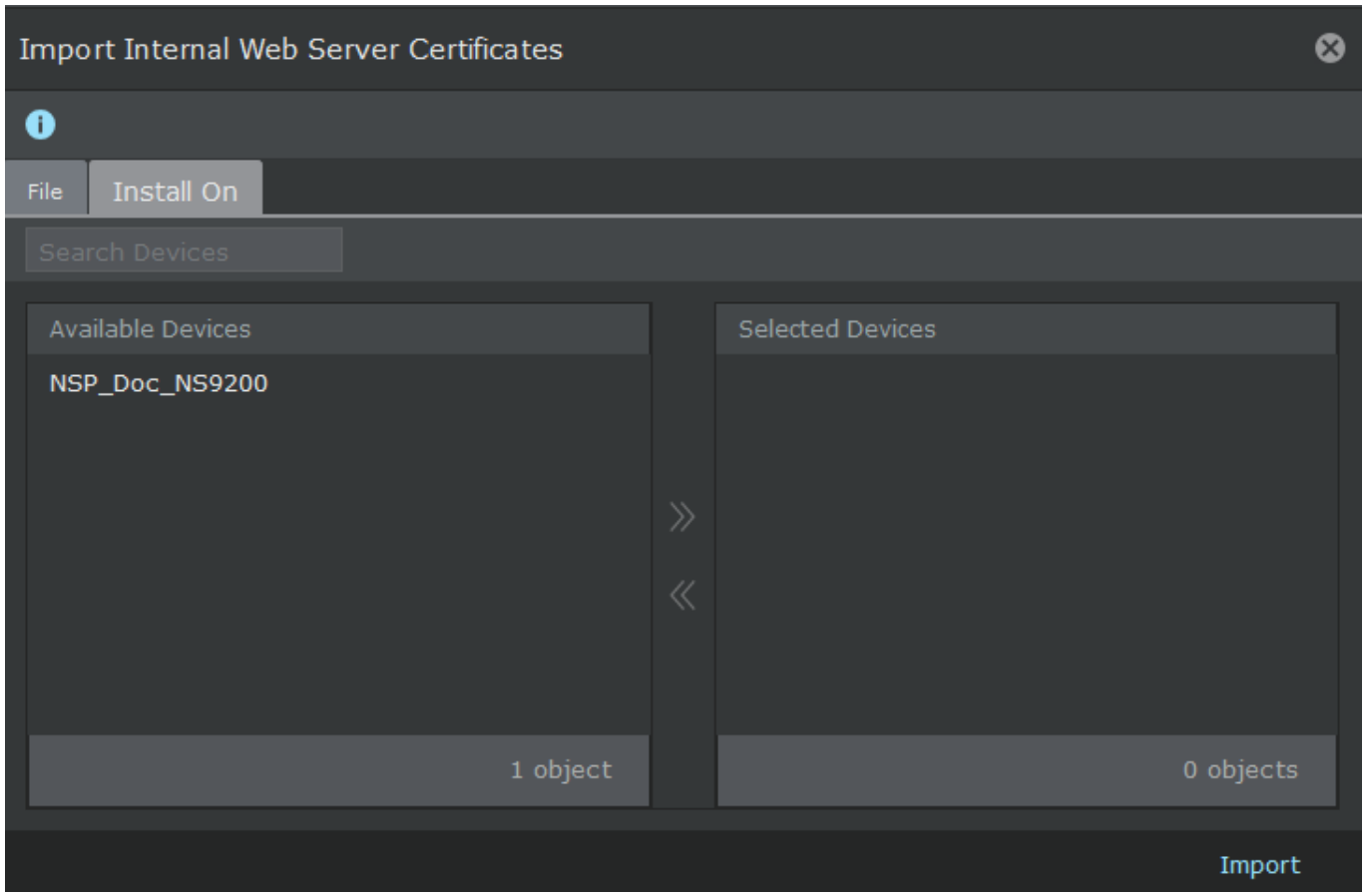


4. Click **Choose Files**.

> **NOTE**
>
> You can import up to 200 certificate files at the same time as long as they use the same passphrase.

5. Select the key **PKCS12 File** on your client system.
6. Type the **Passphrase**.

   This is the phrase (export password) you used for encrypting your PKCS12 file.
7. Click the **Installed On** tab and select the Sensors that you want to push the certificates to.



NOTE

If you do not select any Sensors, the certificates will be pushed to all the devices connected to the Manager.

8. Click **Import**.

   A pop-up window opens detailing import status.

9. You must do a configuration update to the Sensor for the changes to take effect.

Delete SSL certificates

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **SSL Decryption**.
2. In the **Inbound** tab, select **Internal Web Server Certificates** tab.
3. Select the certificate you want to delete.
4. Click **Delete** and confirm the deletion.

NOTE

You cannot delete an SSL certificate if the certificate is used in an inbound proxy rule.

5. You must do a configuration update to the Sensor for the changes to take effect.

Unsupported SSL functionalities

The following SSL functionalities are not supported:

- Compression in the SSL records (a negotiable option in SSLv3 and TLS)

Inbound SSL best practices for RSA ciphers

This section mentions inbound SSL best practices for RSA ciphers.

SSL only traffic - throughput: NS-series Sensors

Testing parameters for NS9500 and other Sensors

- Session resumption for 4 out of 5 TCP connections
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each
- (Applicable to NS9500 Sensors) 5 HTTP 1.1 get page requests per TCP connection with a 21K response each and HTTP response scanning enabled
- Cipher used: AES-128SHA

NS9500 stack - 100 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	132,000	115,200
SSL Throughput	60 Gbps	40 Gbps

NS9500 stack - 60 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	66,000	57,600
SSL Throughput	30 Gbps	20 Gbps

NS9500 stack - 40 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	52,800	43,200
SSL Throughput	22 Gbps	15 Gbps

NS9500 standalone - 30 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	33,000	28,800
SSL Throughput	15 Gbps	10 Gbps

NS9500 standalone - 20 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	26,400	21,600
SSL Throughput	11 Gbps	7.5 Gbps

NS9500 standalone - 10 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	19,800	14,400
SSL Throughput	8 Gbps	5.5 Gbps

NS9300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	44,000	30,800
SSL Throughput	20 Gbps	12 Gbps

NS9200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	22,000	15,400
SSL Throughput	10 Gbps	6 Gbps

NS9100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	17,000	13,600
SSL Throughput	8 Gbps	5.5 Gbps

NS7500 - 7.5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	13,200	13,200
SSL Throughput	6 Gbps	6 Gbps

NS7500 - 5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	8,800	8,800
SSL Throughput	4 Gbps	4 Gbps

NS7500 - 3 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	5,280	5,280
SSL Throughput	2.4 Gbps	2.4 Gbps

NS7350

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	12,000	12,000
SSL Throughput	5 Gbps	5 Gbps

NS7250

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,900	6,900
SSL Throughput	3 Gbps	3 Gbps

NS7150

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,500	3,500
SSL Throughput	1.5 Gbps	1.5 Gbps

NS7300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	12,000	12,000
SSL Throughput	5 Gbps	5 Gbps

NS7200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,900	6,900
SSL Throughput	3 Gbps	3 Gbps

NS7100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,500	3,500
SSL Throughput	1.5 Gbps	1.5 Gbps

NS5200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,000	2,000
SSL Throughput	1 Gbps	1 Gbps

NS5100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,400	1,400
SSL Throughput	600 Mbps	600 Mbps

Testing parameters for NS7600

- 1 HTTP 1.1 get page request per TCP connection with a 5K response each and HTTP response scanning enabled for Connections/Sec test
- 5 HTTP 1.1 get page request per TCP connection with a 21K response each and HTTP response scanning enabled for Throughput Test
- Cipher used for both the tests: AES-128SHA

NS7600 - 15 Gbps throughput

	2048 bit key length
Max. SSL Connections / Sec.	170,000
SSL Throughput	15 Gbps

NS7600 - 10 Gbps throughput

	2048 bit key length
Max. SSL Connections / Sec.	140,000
SSL Throughput	10 Gbps

NS7600 - 5 Gbps throughput

	2048 bit key length
Max. SSL Connections / Sec.	90,000
SSL Throughput	5 Gbps

SSL traffic mixed with HTTP 1.1 traffic: NS-series Sensors

- Session resumption for 4 out of 5 TCP connections
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each
- (Applicable to NS9500 Sensors) 5 HTTP 1.1 get page requests per TCP connection with a 21K response each and HTTP response scanning enabled
- AES-128SHA

NS9500 stack - 100 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	26,400	26,400
SSL Throughput	10 Gbps	10 Gbps
HTTP 1.1 Throughput	90 Gbps	90 Gbps
Total Throughput	100 Gbps	100 Gbps

NS9500 stack - 60 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	13,200	13,200
SSL Throughput	6 Gbps	6 Gbps
HTTP 1.1 Throughput	54 Gbps	54 Gbps
Total Throughput	60 Gbps	60 Gbps

NS9500 stack - 40 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	9,600	9,600
SSL Throughput	4 Gbps	4 Gbps
HTTP 1.1 Throughput	36 Gbps	36 Gbps
Total Throughput	40 Gbps	40 Gbps

NS9500 standalone - 30 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,600	6,600
SSL Throughput	2.6 Gbps	2.6Gbps
HTTP 1.1 Throughput	23.4 Gbps	23.4 Gbps
Total Throughput	26 Gbps	26 Gbps

NS9500 standalone - 20 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,800	4,800
SSL Throughput	1.8 Gbps	1.8 Gbps
HTTP 1.1 Throughput	16.2 Gbps	16.2 Gbps
Total Throughput	18 Gbps	18 Gbps

NS9500 standalone - 10 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	9 Gbps	9 Gbps
Total Throughput	10 Gbps	10 Gbps

NS9300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	9,200	9,200
SSL Throughput	4 Gbps	4 Gbps
HTTP 1.1 Throughput	36 Gbps	36 Gbps
Total Throughput	40 Gbps	40 Gbps

NS9200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,600	4,600
SSL Throughput	2 Gbps	2 Gbps
HTTP 1.1 Throughput	18 Gbps	18 Gbps
Total Throughput	20 Gbps	20 Gbps

NS9100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	9 Gbps	9 Gbps
Total Throughput	10 Gbps	10 Gbps

NS7500 - 7.5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,300	3,300
SSL Throughput	1.5 Gbps	1.5 Gbps
HTTP 1.1 Throughput	5.2 Gbps	5.2 Gbps
Total Throughput	6.7 Gbps	6.7 Gbps

NS7500 - 5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,300	3,300
SSL Throughput	1.5 Gbps	1.5 Gbps
HTTP 1.1 Throughput	3 Gbps	3 Gbps
Total Throughput	4.5 Gbps	4.5 Gbps

NS7500 - 3 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,300	3,300
SSL Throughput	1.5 Gbps	1.5 Gbps
HTTP 1.1 Throughput	1.2 Gbps	1.2 Gbps
Total Throughput	2.7 Gbps	2.7 Gbps

NS7350

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	4 Gbps	4 Gbps
Total Throughput	5 Gbps	5 Gbps

NS7250

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	2 Gbps	2 Gbps
Total Throughput	3 Gbps	3 Gbps

NS7150

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	0.5 Gbps	0.5 Gbps
Total Throughput	1.5 Gbps	1.5 Gbps

NS7300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	4 Gbps	4 Gbps
Total Throughput	5 Gbps	5 Gbps

NS7200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	2 Gbps	2 Gbps
Total Throughput	3 Gbps	3 Gbps

NS7100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	0.5 Gbps	0.5 Gbps
Total Throughput	1.5 Gbps	1.5 Gbps

NS5200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,600	1,600
SSL Throughput	800 Mbps	800 Mbps
HTTP 1.1 Throughput	200 Mbps	200 Mbps
Total Throughput	1 Gbps	1 Gbps

NS5100

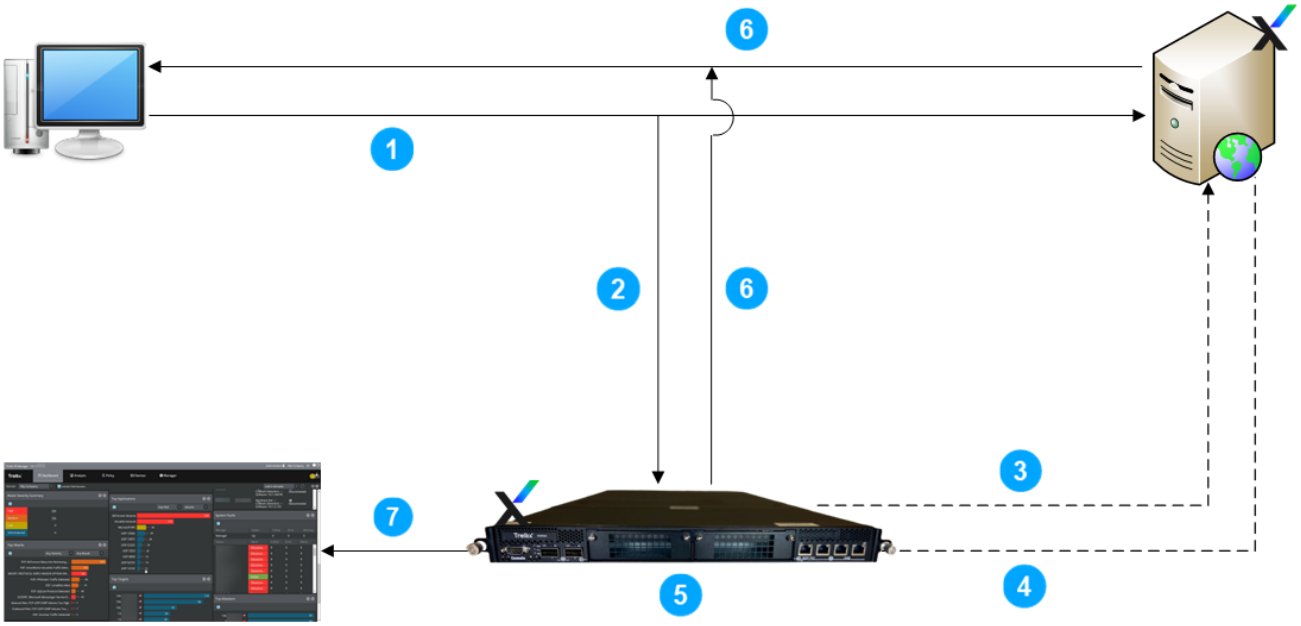
	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,300	1,300
SSL Throughput	500 Mbps	500 Mbps
HTTP 1.1 Throughput	100 Mbps	100 Mbps
Total Throughput	600 Mbps	600 Mbps

Use cases for inbound SSL using the Agent based method

Below are some use case scenarios for inbound SSL decryption using the Agent method:

Scenario 1: Web server without load balancer

When you enable SSL decryption in the inbound direction, the web servers to which the clients send requests needs protection against malicious requests. This is possible by installing the Agent on the web server to be protected. When a client sends a request to the web server, the Sensor intercepts the traffic. The Agent on the web server exchanges the session key with the Sensor. The Sensor uses these keys to decrypt and inspect the traffic. If the traffic is clean, the web server sends a response to the request. In case of malicious requests an alert is generated in the Manager.



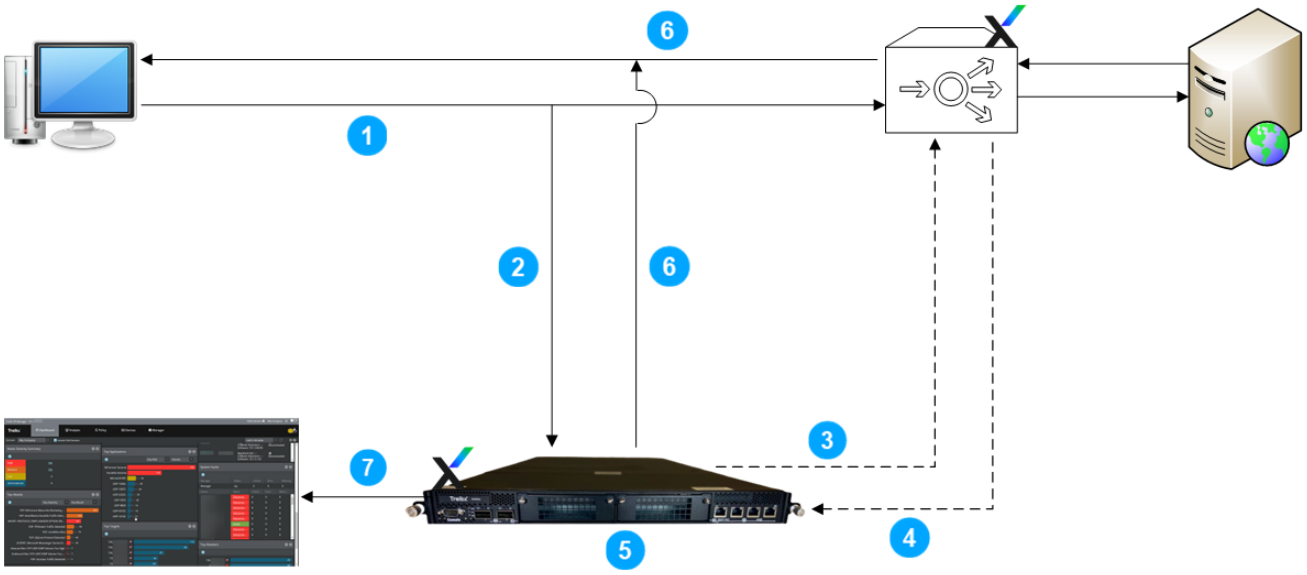
Steps:

1. The client sends a request to the web server.
2. The Sensor intercepts the connection.
3. The Sensor re-establishes the connection with the server through the Agent installed on the server.
4. The Agent sends the SSL keys to the Sensor through an encrypted channel.
5. The Sensor inspects the decrypted traffic.
6. If there are no attacks in the traffic the server responds to the client's request.
7. If an attack is detected, the Sensor generates an alert in the Manager.

Scenario 2: Web server with load balancer

The load balancer usually directs the traffic from the client to the required web server. In such cases, the request from the client is directed to the load balancer first. The load balancer then directs the traffic to the required web server. As the request from the client can be malicious, the load balancer needs to be protected. The Agent shares the session keys with the Sensor for decryption must be installed on the load balancer.

When the client sends a request to the web server, the traffic is first directed to the load balancer. The Sensor intercepts the traffic. The Agent on the load balancer exchanges the session key with the Sensor which the Sensor uses to decrypt and inspect the traffic. If the traffic is clean, the load balancer directs the traffic to the web server which then responds to the client's request. In case of malicious requests an alert is generated in the Manager.



Steps:

1. The client sends a request which is directed to the web server through the load balancer.
2. The Sensor intercepts the connection.
3. The Sensor re-establishes the connection with the load balancer through the Agent installed on it.
4. The Agent sends the SSL keys to the Sensor through an encrypted channel.
5. The Sensor inspects the decrypted traffic.
6. If there are no attacks in the traffic the server responds to the client's request.
7. If an attack is detected, the Sensor generates an alert in the Manager.

Sensor limits for SSL flows

The number of supported SSL flows on a Sensor directly impacts the number of TCP flows that can be processed simultaneously by a 2-to-1 ratio.

The following table describes the total SSL flow supported for different Sensor models:

Sensor	SSL flow count	Total concurrent flow count
NS9500 stack - 100 Gbps throughput	6,400,000	64,000,000
NS9500 stack - 60 Gbps throughput	3,200,000	32,000,000
NS9500 stack - 40 Gbps throughput	2,600,000	26,000,000
NS9500 standalone - 30 Gbps throughput	1,600,000	16,000,000
NS9500 standalone - 20 Gbps throughput	1,300,000	13,000,000
NS9500 standalone - 10 Gbps throughput	1,000,000	10,000,000
NS9300	3,200,000	32,000,000
NS9200	1,600,000	16,000,000

Sensor	SSL flow count	Total concurrent flow count
NS9100	1,200,000	13,000,000
NS7600 - 15 Gbps throughput	1,500,000	15,000,000
NS7600 - 10 Gbps throughput	1,200,000	13,000,000
NS7600 - 5 Gbps throughput	900,000	10,000,000
NS7500 - 7.5 Gbps throughput	1,000,000	10,000,000
NS7500 - 5 Gbps throughput	700,000	7,000,000
NS7500 - 3Gbps throughput	400,000	4,000,000
NS7350	500,000	10,000,000
NS7250	400,000	5,000,000
NS7150	250,000	3,000,000
NS7300	500,000	10,000,000
NS7200	400,000	5,000,000
NS7100	250,000	3,000,000
NS5200	75,000	1,350,000
NS5100	40,000	750,000
NS3600 - 5 Gbps throughput	500,000	5,000,000
NS3600 - 3 Gbps throughput	400,000	4,000,000
NS3600 - 1 Gbps throughput	200,000	2,000,000
NS3500	NA	80,000
NS3200/NS3100	NA	80,000
IPS-VM600	NA	600,000
IPS-VM5000	120,000	2,400,000

How Trellix identifies applications?

NS-series Sensors can identify the applications being used in your network and act on them. So, you can allow or block specific applications on your network. For example, you can block just the connections to Facebook from your network while allowing all other HTTP and HTTPS traffic. Using advanced Quality of Service (QoS) policies, you can also control the bandwidth allocated for applications on your network.

In addition to controlling the applications on your network, you can also view the Internet applications that are accessed from your network. Related details such as the network bandwidth consumed by specific applications is now available. You can also check if these applications generated any attacks.

Application identification is used in the following features: Firewall policies involving applications, QoS policies involving applications, and Top Applications (IPS)/(NTBA) monitor. So, to use these features effectively, you need to understand how application identification works.

With respect to the application identification feature of Trellix IPS, the following are referred to as applications:

- Network connections over a specific protocol, for example, HTTP, DHCP, and FTP.

- A specific computer application accessed over a network, for example, Facebook, Yahoo! Instant Messenger, and Gmail.

Trellix creates signatures for applications based on an ongoing research. This involves creating signatures for applications for which there were no signatures earlier. This also involves removing signatures for invalid and obsolete applications. These application signatures enable the Sensors to accurately detect the applications on your network.

The application signatures are bundled as part of the regular signature set that the Trellix IPS Update Server downloads to the Manager. So, if the Manager is connected to the Trellix IPS Update Server, the application database of your Trellix IPS remains up-to-date.

Applications

With respect to the application identification feature of Trellix IPS, the following are referred to as applications:

- Network connections over a specific protocol, for example, HTTP, DHCP, and FTP.
- A specific computer application accessed over a network, for example, Facebook, Yahoo! Instant Messenger, and Gmail.

Trellix creates signatures for applications based on an ongoing research. This involves creating signatures for applications for which there were no signatures earlier. This also involves removing signatures for invalid and obsolete applications. These application signatures enable the Sensors to accurately detect the applications on your network.

The application signatures are bundled as part of the regular signature set that the Trellix IPS Update Server downloads to the Manager. So, if the Manager is connected to the Trellix IPS Update Server, the application database of your Trellix IPS remains up-to-date.

Applications-related terminologies

Knowing the terminologies can enable you to understand how to use the application identification feature better.

Application category

Trellix categorizes similar applications into categories. Based on its functions and features, an application could belong to multiple categories. For example, Skype could belong to instant messaging, file sharing, and voice over categories.

Typically, a category consists of applications that you would want to handle in a similar manner. Therefore, categories can reduce the number of Firewall access rules that you would require. For example, you can create a rule to block the webmail category instead of creating separate rules for each webmail application.

Application capability

Using Trellix IPS, you cannot only control specific applications but also specific features of applications. For example, you can block the file transfer feature of Yahoo! Messenger while allowing its other features. To provide such granular control, Trellix creates signatures for some of the critical and common features of applications. These features for which signatures exist are referred to as application capabilities.

Functionally, Trellix IPS treats an application capability as an application itself. This is because application capabilities also can belong to an application category. This category could be different from the category to which the parent application belongs. However, a Firewall access rule for an application may affect a rule written for a corresponding application capability. For example, consider that you have a rule to allow Yahoo! Messenger followed by a rule blocking file transfer through Yahoo!

Messenger. Now, a user will be able to use Yahoo! Messenger's file transfer functionality because this traffic matches the first rule that allows Yahoo! Messenger.

Application capabilities are listed along with the applications in the **Rule Objects** page.

Risk

For you to understand the impact of applications and Application Capabilities on your network, Trellix Advanced Research Center rates them as high, medium, or low risk. Risk is calculated based on the following factors:

- Vulnerability of an application or application capability to attacks.
- The probability of an application or application capability to deliver malware.

How application identification works?

Similar to attack detection, application identification is a function of the Sensor. The Sensor can identify applications in SPAN, tap, and inline modes. However, only inline mode is relevant for QoS. By default the application identification feature is enabled for NS-series Sensors. If you use any of the following features, the application identification function is automatically turned on for that Sensor:

- A Firewall access rule or any type of QoS rule based on an Application, Application on Custom Port, or an Application Group.
- Application identification enabled for the Top Applications (IPS)/(NTBA) monitor.

> **IMPORTANT**
>
> Identifying applications is a resource-intensive process. If the Sensor performs application identification on the entire traffic, the Sensor throughput could be reduced by about 10%. The amount of actual throughput drop varies based on the type of traffic.

Identifying applications is a resource-intensive process. If the Sensor performs application identification on the entire traffic, the Sensor throughput could be reduced by about 10%. The amount of actual throughput drop varies based on the type of traffic.

From a Firewall and QoS perspective, you need to understand how rules based on applications can induce a dependency factor between the rules. The dependency factor with respect to Firewall is explained here, but it has a similar effect on QoS policies as well.

Following are the response actions that you can specify in case of Firewall:

- **Deny** — The Sensor blocks the traffic and does a TCP reset. This applies only to inline mode.
- **Drop** — The Sensor drops the traffic. This applies only to inline mode.
- **Ignore** — The Sensor permits the traffic with no further inspection. This applies to SPAN, tap, and inline modes.
- **Require Authentication** — The Sensor permits only those users with valid AD credentials for HTTP traffic only. This applies only to inline mode.
- **Scan** — The Sensor permits the traffic that matches a Firewall access rule, but inspects it for attacks. This applies to SPAN, tap, and inline modes.
- **Scan with Priority** — The Sensor prioritizes critical network traffic. This is available only for advanced firewall policies.
- **Stateless Drop** — The Sensor drops the packets.

- **Stateless Ignore** — This is the same as ignore option. That is, the Sensor permits the packet without inspection for intrusions.

The dependency factor explained below, applies only for those rules for which you set scan or ignore as the Sensor's response action.

Dependency factor — If you create a rule to allow an application, all the dependent applications and services are allowed by default. For example, if you allow Facebook, HTTP is allowed by default. This also allows all unknown HTTP applications, or HTTP applications for which there are no signatures. For example, to allow Facebook but block all other HTTP traffic you need to create access rules for the following conditions and in the same order:

- Scan Facebook
- Deny HTTP

Consider that a user attempts to access Gmail, which is a known application. So, the Sensor identifies the Gmail traffic and blocks it according to the second rule. Now, consider that a user attempts to access an unknown HTTP application. The Sensor cannot identify this application beyond the HTTP level because there is no signature. Because the first rule implicitly allows HTTP, the Sensor allows this traffic to pass through. In short, all unknown HTTP applications are allowed, and all known HTTP applications except Facebook are blocked.

Suppose if you create Access Rules for the following conditions and in the same order then all HTTP applications, including Facebook, are blocked:

- Deny HTTP
- Scan Facebook

Similarly, rules involving application capabilities also can induce the dependency factor. That is, allowing an application capability allows the application itself and other capabilities of the application for which there are no signatures.

When you calculate the dependency factor between access rules, factor in all the components of the rules such as source, destination, effective time, application categories, and so on. Consider the sample set of rules below:

1. Source: x ¦ Destination: y ¦ Application: TwileShare ¦ Response action: Scan (that is, permit with IPS)
2. Source: x ¦ Destination: y ¦ Application: Twitter ¦ Response action: Drop
3. Source: a ¦ Destination: b ¦ Application: Twitter ¦ Response action: Drop

When the Sensor detects Twitter traffic from x to y, it allows this traffic with IPS, though it must drop this traffic according to the second rule. This is because, TwileShare is dependent on Twitter. So, by allowing TwileShare in the first rule from x to y, you are allowing Twitter from x to y as well. However, if the Sensor detects Twitter traffic from a to b, it drops the traffic according to the third rule, because the first rule that implicitly allows Twitter applies only from x to y and not from a to b.

Consider the rules below:

1. Source: x ¦ Destination: y ¦ Application: Twitter ¦ Response action: Drop
2. Source: x ¦ Destination: y ¦ Application: TwileShare ¦ Response action: Scan (that is, permit with IPS)

In this case, Twitter traffic from x to y is dropped according to rule 1; TwileShare traffic from x to y is allowed with inspection according to rule 2.

Firewall policies

Firewall policies are ordered rules for permitting and denying traffic from reaching a Sensor's IPS/IDS engine and continuing on through the network. Firewall policies can maximize a Sensor's detection and prevention capabilities by preventing, that is dropping or rejecting, specified traffic without requiring full inspection.

In Trellix IPS, a Firewall policy consists of an ordered set of rules that govern what traffic is allowed to pass to a Sensor's inspection engine and beyond. These rules also govern which traffic should be denied, that is either dropped from the network or rejected (TCP traffic only). Thus, this feature enables the Sensor to preemptively drop any traffic by denying access to the inspection engine and beyond.

You can enforce policies based on various parameters. You can base it on the application, Windows Active Directory (AD) user names and user groups, the source or destination country of the traffic, the source or destination network, the source or destination host, and so on.

You can control the traffic both at a broader as well as at a granular level. For example, you can deny all TCP traffic that is using a specific port. You can also define a policy to prevent specific users from accessing specific social-networking sites between 9 am and 5 pm on all week days. Thus, Firewall policies provides you with very flexible options to control the traffic that is entering or leaving your network.

NOTE

The Firewall feature of Trellix IPS is independent of Trellix Firewall Enterprise. This section discusses only the Firewall feature of Trellix IPS.

The Sensor can perform both stateful and stateless inspection of traffic based on the response action configured. For stateful inspection, the Sensor checks either the source and destination IP addresses, or source and destination ports, or the application, or user name. In case of stateless inspection, based on either the source and destination IP addresses, or source and destination ports, the Sensor inspects the traffic on per packet basis. The packets are then either dropped or ignored depending on the response action configured.

Advantages of Firewall policies

Some of the advantages of using Firewall policies are as follows:

- It can provide you visibility to a very granular level. For example, you can identify the users who are trying to use a blocked application, such as Facebook.
- You can enforce different policies based on time. For example, you can allow gaming applications on weekends but block them during weekdays.
- You can control traffic based on geographical locations.
- You can control specific phases of an application. For example, you can allow chatting using Yahoo! Messenger but deny file transfers.
- You can enforce different policies for different sub-networks within your enterprise network. For example, you can have very stringent policies for your finance network compared to your engineering network.
- You can choose to enforce IPS on the allowed traffic, thus fully securing your network. Conversely, you can use the Firewall policies to exempt specific traffic from IPS inspection.

Types of Firewall policies

You can use two types of Firewall policies in Trellix IPS — advanced and classic. Functionally, these two types are similar. However, as the names might suggest, advanced Firewall policies provide you more options to filter traffic when compared to classic.

Notes:

- All Sensor models support Classic and Advanced Firewall policies.

Table 60. Differences between advanced and classic Firewall policies

	Advanced	Classic
Options on source or destination of the traffic	Source or destination are based on: • Country • A host's DNS name • A host's IPv4 or IPv6 address • An IPv4 or IPv6 address range to which a host belongs. • IPv4 or IPv6 networks or a group of IPv4 or IPv6 networks. • Windows Active Directory user names and user groups	Source or destination are based on: • A host's IPV4 address • IPv4 Network
Options on the traffic	Traffic is based on: • A specific or a group of Layer 7 applications. For example, you can filter out Yahoo! Games while allowing Yahoo! Mail. These applications can be on the standard or custom communication ports. • IP protocol or the TCP/UDP port numbers.	Traffic is only based on the IP protocol or the TCP/UDP port numbers.
Option to enforce the Firewall policy based on time.	Yes. For example, the Sensor can enforce a policy on all weekends only.	No.
Option to define a rule that mandates AD authentication	Yes.	No.

Components of Firewall policies

To effectively use Firewall policies, familiarize yourself with the components of Firewall policies.

- **Firewall policies** — These are your network security policies based on which the Sensor allows or blocks traffic in and out of your network. There are two types of Firewall policies — advanced and classic.
- **Access rules** — Access rules are the building blocks of a Firewall policy. Access rules are Access Control Lists (ACLs) – an ordered set of rules, which define the traffic to be allowed and the traffic to be blocked.

- **Rule objects** — You use rule objects to define access rules. Rule objects are mappings to one or more components related to your network traffic. Examples of rule objects are the applications, source and destination hosts, source and destination networks. So, for example, you can group a set of IPv4 addresses to create a rule object. Then you can create an access rule in which you specify this rule object as the source or destination of traffic. Every time you want to refer to this set of IP addresses in your access rules, you can just use this rule object.

  NOTE

  For advanced and classic Firewall policies, you can specify multiple rule objects per component of an access rule. For example, you can specify multiple rule objects as the source of the traffic.

  The following are the rule object types that are currently available:

  - **User** — These are the Windows AD users currently logged on to your network. The Manager gathers this list from Trellix Logon Collector and provides it to the Sensor.
  - **User Group** — These are the user groups of the currently logged on users. The Manager gathers this information from Trellix Logon Collector and provides it to the Sensor.

    NOTE

    You cannot create, modify, or delete Users or User Groups in the Manager. You can view these rule objects only on the **Access Rules** tab of the **Firewall** page. Regarding Users, you cannot view the entire list even in the **Firewall** page; you can query for the required users when defining the access rules. You cannot view the User or User Group rule objects in the **Rule Objects** page.

  - **Application** — These are the various software programs that the Sensor can detect. The Manager derives the list of applications from the signature set. You cannot modify the list of available applications. Applications are relevant only to advanced Firewall policies.

    IMPORTANT

    If Trellix Advanced Research Center deprecates an application that you have used in a Firewall policy, then a fault message of severity *warning* is raised. You will then have to delete those rules from the policies or modify them; if not you will not be able to push a signature set to Sensors.

  - **Application on Custom Port** — You can use this rule object to detect applications when they are communicated over non-standard ports. For example, you might want the Sensor to detect FTP, when it is over port 2021. Application on Custom Port is relevant only to advanced Firewall policies.
  - **Application Group** — If the pre-defined Application Groups do not meet your requirements, you can create one. You create an Application Group to combine more than one Application and Application on Custom Port rule objects. Typically, you create an Application Group for those applications that you want the Sensor to handle in a similar way. For example, you can combine all applications related to Internet games to form one Application Group. You can group up to 10 items in an Application Group. Application Group is relevant only for advanced Firewall policies.

NOTE

You can combine Application and Application on Custom Port rule objects to form an Application Group. You cannot include Application Group within another Application Group.

- **Country** — The Country rule object enables you to allow or block traffic based on the source or destination country. The Sensor identifies the traffic originating or destined to these countries based on the CIDRs mapped to the countries. Country is relevant only for advanced Firewall policies.

  The country-to-CIDRs mapping information is sourced from the geolocation database of Digital Envoy. You cannot modify or update this list of countries manually. Trellix updates this list of country-to-CIDRs mapping through signature sets. Use the **`status`** command in a Sensor's CLI to check if the geolocation database is present in the Sensor.

  NOTE

  If the Manager and Sensor are on software versions prior to 10.1 Update 7, it is recommended to upgrade them to later versions to continue receiving the updated geolocation databases. For more information, refer to KB95636. Always ensure to maintain the latest software versions of the Manager, Sensor, and Signature Sets.

- **IPv4 Endpoint** — You can create a list of source and destination IPv4 addresses that you want to use in a Firewall rule. You can specify a maximum of 140000 IPv4 addresses in a rule object based on the Sensor model. If you have enabled XFF header parsing in your Sensor, you will be able to use the original source IP address of the for HTTP traffic.

  NOTE

  If you are using a Manager which is on or before version 10.1.7.55 and a Sensor which is on or before 10.1.5.153, you can add up to 10 IPv4 addresses in a rule object.

- **IPv6 Endpoint** — This is similar to the IPv4 Endpoint rule object but applies only to advanced policies.
- **Host DNS Name** — You can create the list of source and destination host names that you want to use in a Firewall rule. The Sensor contacts the DNS servers that you configure to resolve these names to IP addresses. For example, you can create a Host DNS Name rule object for facebook.com, faceparty.co.uk, ibibo.com. You can add a maximum of 5000 Host DNS Names in a rule object. Host DNS Name applies only to advanced Firewall policies.

  IMPORTANT

  The Sensor uses only UDP and never falls back to TCP for DNS queries even if the DNS server forces for TCP.

  NOTE

  If you are using a Manager which is on or before version 10.1.7.55 and a Sensor which is on or before 10.1.5.153, you can add up to 10 Host DNS Names in a rule object.

- **IPv4 Address Range** — You can create the list of IPv4 address ranges to use in a Firewall rule. In the rule, you can specify an IPv4 address range as the source or destination of traffic. For example, you may want to apply a rule to traffic from IPs ranging from 10.1.1.1 to 10.1.1.25. This rule object applies only to advanced Firewall policies. You can

specify a maximum of 20000 ranges in a rule object. If you have enabled XFF header parsing in your Sensor, you will be able to use original source IP addresses for HTTP traffic.

> **NOTE**
>
> If you are using a Manager which is on or before version 10.1.7.55 and a Sensor which is on or before 10.1.5.153, you can add up to 10 address ranges in a rule object.

- **IPv6 Address Range** — This is similar to the IPv4 Address Range.
- **IPv4 Network** — You can create a list of IPv4 CIDRs to use in a Firewall rule. In the rule, you can specify a CIDR as the source or destination of traffic. For example, you might want to apply a rule on the traffic targeted for 172.16.225.0/24 network. The three reserved IPv4 ranges according to RFC 1918 are provided as default networks. You can specify a maximum of 140000 CIDRs in one rule object.

  > **NOTE**
  >
  > If you are using a Manager which is on or before version 10.1.7.55 and a Sensor which is on or before 10.1.5.153, you can add up to 10 CIDRs in a rule object.

- **IPv6 Network** — Similar to IPv4 Network but applies only to advanced Firewall policies. Also, there are no predefined **IPv6 Network** rule objects in the Manager.
- **Network Group** — You can combine one or more Country, Host IP, Host Name, IP range, or Network to form a **Network Group**. For example, you can combine all the North American countries and multiple IP ranges to form a Network Group rule object. This rule object applies only to advanced Firewall policies. You can specify up to 10 items in one Network Group rule object.

  > **NOTE**
  >
  > You cannot combine IPv4 and IPv6 based rule objects in the same Network Group rule object. Note that Country and Host DNS are IPv4-based.

- **Finite Time Period** — You can configure the Sensor to enforce an access rule continuously just for a specific time period. For example, you might want to enforce a rule from 9 am on June 10 of this year to 10 am on June 11 of this year. For this, you need to create a **Finite Time Period** rule object specifying the start time and date along with the end time and date. The start and end time are both inclusive. Finite Time Period applies only to advanced Firewall policies. You can specify only one Finite Time Period rule object in a Firewall access rule.

  When you use a time-based rule object, make sure you have configured the corresponding Time Zone. Time-based rules are implemented using the local time zone of the corresponding Sensor. The Sensor automatically factors in the daylight savings time, if applicable. GMT is the default Time Zone in the Manager.
- **Recurring Time Period** — You can repeatedly enforce a Firewall rule at certain frequencies of time. For example, you can enforce a rule from 9 am to 5 pm on all weekdays. Use this rule object to repeatedly enforce a rule. To enforce a rule just once, use the Finite Time Period rule object.

  When you use a time-based rule object, make sure you have configured the corresponding Time Zone. Time-based rules are implemented using the local time zone of the corresponding Sensor. Note that the Sensor automatically factors in the daylight savings time, where applicable. Recurring Time Period applies only to advanced Firewall policies.

- **Recurring Time Period Group** — You can group up to 10 Recurring Time Periods to form a Recurring Time Period Group rule object. Recurring Time Period Group applies only to advanced Firewall policies.

  NOTE

  You can use the Finite Time Period rule object along with Recurring Time Period and Recurring Time Period Group rule objects. In such a case, the Finite Time Period takes precedence. Also, for the Sensor to check for that access rule, the Finite Time Period and at least one Recurring Time Period must be active.

- **Service** — To restrict traffic based on the IP protocol, ICMP codes, or the TCP/UDP port numbers, use the Service rule object. You can create Service rule objects or use the default ones. The well-known services on standard TCP and UDP ports, as well as ICMP codes are pre-defined. For example, telnet is predefined as TCP on port 23. Similarly, ICMP codes such as ICMP echo reply and ICMP request are pre-defined. When you create a Service rule object, the options are to specify the protocol number, TCP port, or UDP port. For custom ICMP codes, you need to specify the IP protocol number and the ICMP code in the port field. You can define only one IP protocol specification per rule object.

  NOTE

  For access rules that use Service rule objects, the Sensor factors in any non-standard ports that you have configured for IPS. For example, if you have specified port 2023 as the non-standard port for FTP, and if you have used the FTP Service rule object in a rule, then the Sensor considers FTP on both ports 21 and 2023.

  For certain protocols, you can use more than a type of rule object. For example, for FTP and HTTP, you can use the Application rule object or the Service rule object. If you use the Application rule object, the Sensor does not consider the port number when detecting the traffic, and relies only on the application signatures. This means that the Sensor can a detect a protocol regardless of the port used in case of Application rule objects. If you use the Service rule object, the port number matters when detecting a protocol. The Sensor considers all the standard ports as well as non-standard port numbers that you have defined in the **Non-Standard Ports** page.

  In case of Service rule object, the Sensor drops even the SYN packet. In case of Application rule object, the Sensor drops the traffic only after the three-way handshake; only after the handshake, the Sensor identifies the application.

  NOTE

  A Sensor processes the access rules of a policy in a top-down fashion. So, if you want to drop traffic based on Services, define those access rules high up in the policy.

  Note the following if you use classic Firewall policies:

  - It is not advisable to set permit rules for protocols, such as FTP, TFTP, and RPC services that negotiate ports dynamically. For RPC services, you can configure explicit allow and deny rules for RPC as a whole, but not its constituents, such as statd and mountd.
  - Multimedia protocols such as H.323 and services such as instant messaging and peer-to-peer communication either negotiate the data channel separate from the control channel or negotiate ports that do not follow a standard. However, you can configure access rules to deny these dynamic protocol instances by denying the fixed control port.

- An option for denying protocols that use dynamic negotiation is to configure policies to drop the attacks that are detected in such transmissions. Trellix IPS detects the use of, and attacks in such programs as Yahoo Messenger, KaZaA, and IRC.

- **Service Group** — You can group the services that you want to be handled in a similar manner. This enables you to easily manage your Firewall policies. Service Group is relevant only for advanced Firewall policies. You can group up to 10 services in one Service Group rule object.

> **NOTE**
>
> Service Range is applicable only to QoS policies.

High-level steps for configuring Firewall policies

You create Firewall policies at the admin-domain level. Then, you assign these policies to the required Sensor resources.

You can enforce Firewall policies with the monitoring ports in SPAN, tap, or inline mode. However, factor in the mode when you specify the response action. For example, dropping the traffic is not a relevant response in SPAN or tap mode.

> **NOTE**
>
> You can enforce policies based on the application, Windows Active Directory (AD) user names and user groups, the source or destination country of the traffic, the source or destination network, the source or destination host, and so on. This section discusses how Firewall policies work in general. There are some additional information that you must know if you plan to use access rules based on applications, user names, or user groups. Also, there are additional configurations required for these features. The concepts and requirements for application-based and user-based access rules are discussed in separate sections that follow.

The following are the high-level steps involved in implementing Firewall policies:

1. Make sure you have deployed Trellix IPS as required.
2. Make sure you have connected the monitoring ports to the networks that you want to monitor.
3. In addition to Firewall, if you want the Sensor to inspect the traffic for attacks, make sure you have configured the IPS or the IDS feature, and that the Sensor is detecting and reporting attacks.
4. Create the rule objects that you plan to use in your access rules. For example, identify the IPv4 Endpoint addresses and the IPv4 Address Range and create the corresponding rule objects.
5. If you use the Host DNS Name rule object, make sure you configure the DNS server details in the Manager. Also, make sure these servers are accessible to the Sensor's management port. If the DNS servers are not accessible, a fault message is raised.

   > **NOTE**
   >
   > The DNS server details apply to Firewall policies, QoS policies, integration with Trellix GTI for File Reputation, and NTBA.

6. If you are using any time-based rule objects, make sure you have configured the Time Zone in the Manager. Time-based rules are implemented using the local time zone of the corresponding Sensor. The pre-configured Time Zone is GMT.

7. Create the required Firewall policies at the corresponding admin domain. When you create the Firewall policies, you will be defining the access rules. So, a policy contains an ordered set of access rules that the Sensor processes in a top-down fashion.
8. After you create a Firewall policy, you need to assign it to a Sensor resource. The following are referred to as Sensor Resources
    - **Pre-device** — This resource is the Sensor itself, and the Firewall policy assigned to this resource is applied to all the traffic reaching the Sensor. This policy is referred to as the pre-device policy. A pre-device Firewall policy has the highest priority. That is, the Sensor matches the traffic against the access rules of this policy first. Typically, you will assign policies that will block specific traffic across your network. For example, you might want to block p2p traffic perpetually on your network.
    - **Interface or subinterface** — These resources are Monitoring ports of type VLAN or CIDR. You can assign Firewall policies to interfaces or subinterfaces based on how you have configured the Monitoring ports.

      The Sensor considers the policy at the interface or subinterface after the policy assigned at the pre-device level. The Sensor enforces this policy only on the traffic seen at the corresponding interface or subinterface. So, typically you will assign policies that are very granular in nature in terms of source and destination. For example, these could be policies targeted at specific hosts or networks.
    - **Physical port level** — Assign those policies that you want to enforce at a port level. Typically, these policies will be less granular when compared to the policies assigned at the interface or subinterface level. The Sensor considers the policy at this level after the policy at the interface or subinterface.
    - **Post-device** — This resource is also the Sensor itself, similar to pre-device. However, the post-device policy is applied only after all the policies assigned to the other Sensor resources.

      You can have a unique Firewall policy to each Sensor resource, but only one Firewall policy per resource. It is not mandatory to assign Firewall policies to Sensor Resources in any specific order. For example, you can assign a policy only at the pre-device level or only at the subinterface level.

      Policies assigned at the Sensor level (pre and post-device) as well as the port/port pair are inherited by the corresponding interface and, if applicable, subinterfaces. In the case of Firewall policies, an interface is a subset of the corresponding port or port pair. That is, the policy assigned for a port/port pair at the Sensor level is inherited by the corresponding interface as well as any subinterfaces. However, a policy assigned at the interface level is not inherited by the corresponding subinterfaces due to the rule of separating interface traffic flows from subinterface traffic flows based on the following policy application rule: if you apply a policy to a subinterface that is different than the inherited policy, the policy enforced at the interface level protects all traffic not specific to the subinterface. Thus, for Firewall policies, the rule of inheritance requires you to create global policies at the Sensor (pre and post-device) or physical port/port pair level: interface policies only apply to interfaces, and subinterface rules only apply to subinterfaces.

      After you assign the Firewall policies, the Manager creates a collective list of all the access rules in those policies. This is the list of **Effective Rules** that the Sensor processes in a top-down fashion. That is, the rule at the top of the list is checked first, followed by subsequent rules down to the bottommost rule. Trellix IPS employs a first-match process; the first rule matched in sequence is enforced and the remaining rules are not processed.

      The order of the rules in an **Effective Rules** list is based on the hierarchy of Sensor resources. That is, the rules of the pre-device Firewall policy are listed on top followed by the rules of the interface or subinterface policy, then followed by the port-level policy, and finally the post-device level policy.

> **NOTE**
>
> The Manager computes the **Effective Rules** separately for inbound and outbound.

You can view the **Effective Rules** in the **Policy Manager** page at the interface and sub-interface levels.

9. After you complete assigning the Firewall policies to the required Sensor Resources, do a configuration update.
10. You can configure the Sensor to send the details of the matched traffic to a syslog server for analysis.
    a. Configure a syslog server.
    b. Enable syslog notification in the **IPS event logging** page.
    c. Also enable **Firewall logging**.

Application identification

NS-series Sensors can identify the applications being used in your network and act on them. So, you can allow or block specific applications on your network. For example, you can block just the connections to Facebook from your network while allowing all other HTTP and HTTPS traffic. Using advanced Quality of Service (QoS) policies, you can also control the bandwidth allocated for applications on your network.

In addition to controlling the applications on your network, you can also view the Internet applications that are accessed from your network. Related details such as the network bandwidth consumed by specific applications is now available. You can also check if these applications generated any attacks.

Application identification is used in the following features: Firewall policies involving applications, QoS policies involving applications, and **Top Applications Summary** monitor. So, to use these features effectively, you need to understand how application identification works.

With respect to the application identification feature of Trellix IPS, the following are referred to as applications:

- Network connections over a specific protocol; for example, HTTP, DHCP, and FTP.
- A specific computer application accessed over a network; for example, Facebook, Yahoo! Instant Messenger, and Gmail.

Trellix creates signatures for applications based on an ongoing research. This involves creating signatures for applications for which there were no signatures earlier. This also involves removing signatures for invalid and obsolete applications. These application signatures enable the Sensors to accurately detect the applications on your network.

The application signatures are bundled as part of the regular signature set that the Trellix IPS Update Server downloads to the Manager. So, if the Manager is connected to the Trellix IPS Update Server, the application database of your Trellix IPS remains up-to-date.

Applications-related terminologies

Knowing the terminologies can enable you to understand how to use the application identification feature better.

Application category

Trellix categorizes similar applications into categories. Based on its functions and features, an application could belong to multiple categories. For example, Skype could belong to instant messaging, file sharing, and voice over categories.

Typically, a category consists of applications that you would want to handle in a similar manner. Therefore, categories can reduce the number of Firewall access rules that you would require. For example, you can create a rule to block the webmail category instead of creating separate rules for each webmail application.

Application capability

Using Trellix IPS, you cannot only control specific applications but also specific features of applications. For example, you can block the file transfer feature of Yahoo! Messenger while allowing its other features. To provide such granular control, Trellix creates signatures for some of the critical and common features of applications. These features for which signatures exist are referred to as application capabilities.

Functionally, Trellix IPS treats an application capability as an application itself. This is because application capabilities also can belong to an application category. This category could be different from the category to which the parent application belongs. However, a Firewall access rule for an application may affect a rule written for a corresponding application capability. For example, consider that you have a rule to allow Yahoo! Messenger followed by a rule blocking file transfer through Yahoo! Messenger. Now, a user will be able to use Yahoo! Messenger's file transfer functionality because this traffic matches the first rule that allows Yahoo! Messenger.

Application capabilities are listed along with the applications in the **Rule Objects** page.

Risk

For you to understand the impact of applications and Application Capabilities on your network, Trellix Advanced Research Center rates them as high, medium, or low risk. Risk is calculated based on the following factors:

- Vulnerability of an application or application capability to attacks.
- The probability of an application or application capability to deliver malware.

View application categories

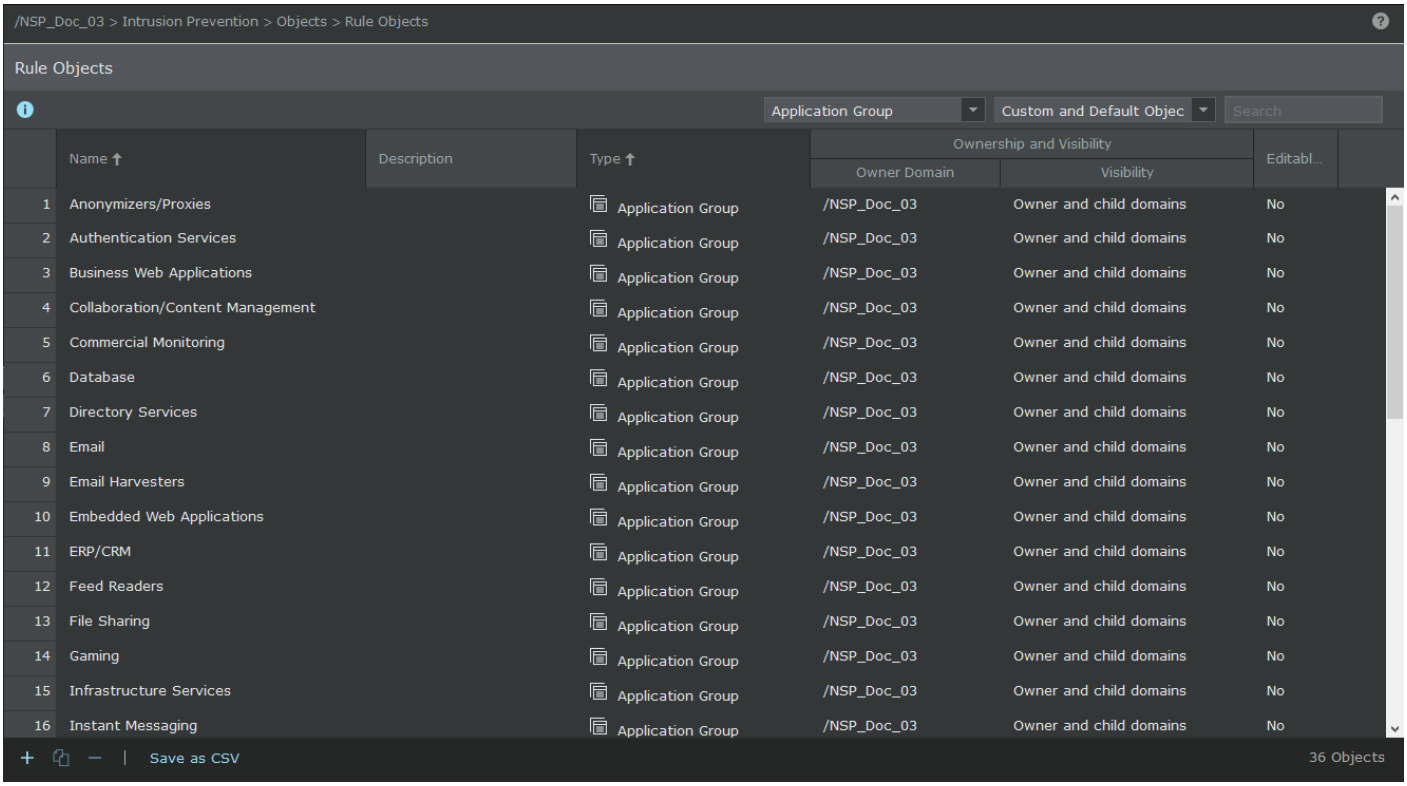
You can view the list of categories in the **Rule Objects** page.

Steps:

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Select Intrusion Prevention → Objects → **Rule Objects**.
4. From the object types drop-down, select **Application Group**.

   The default Application Groups are the application categories.

Figure 496. List of application categories



To view the applications that belong to a category (a default Application Group), double-click a default Application Group. In the **Object Details** panel, select the required application group from the **Available** drop-down list and click + icon.

NOTE

The list of default Application Groups and the constituent Applications may change between versions of the signature set.

How application identification works?

Similar to attack detection, application identification is a function of the Sensor. The Sensor can identify applications in SPAN, tap, and inline modes. However, only inline mode is relevant for QoS. By default the application identification feature is enabled for NS-series Sensors. If you use any of the following features, the application identification function is automatically turned on for that Sensor:

- A Firewall access rule or any type of QoS rule based on an Application, Application on Custom Port, or an Application Group.
- Application identification enabled for the Top Applications (IPS)/(NTBA) monitor.

Identifying applications is a resource-intensive process. If the Sensor performs application identification on the entire traffic, the Sensor throughput could be reduced by about 10%. The amount of actual throughput drop varies based on the type of traffic.

From a Firewall and QoS perspective, you need to understand how rules based on applications can induce a dependency factor between the rules. The dependency factor with respect to Firewall is explained here, but it has a similar effect on QoS policies as well.

Following are the response actions that you can specify in case of Firewall:

- **Deny** — The Sensor blocks the traffic and does a TCP reset. This applies only to inline mode.
- **Drop** — The Sensor drops the traffic. This applies only to inline mode.
- **Ignore** — The Sensor permits the traffic with no further inspection. This applies to SPAN, tap, and inline modes.
- **Require Authentication** — The Sensor permits only those users with valid AD credentials for HTTP traffic only. This applies only to inline mode.
- **Scan** — The Sensor permits the traffic that matches a Firewall access rule, but inspects it for attacks. This applies to SPAN, tap, and inline modes.
- **Scan with Priority** — The Sensor prioritizes critical network traffic. This is available only for advanced firewall policies.
- **Stateless Drop** — The Sensor drops the packets.
- **Stateless Ignore** — This is the same as ignore option. That is, the Sensor permits the packet without inspection for intrusions.

The dependency factor explained below, applies only for those rules for which you set scan or ignore as the Sensor's response action.

Dependency factor — If you create a rule to allow an application, all the dependent applications and services are allowed by default. For example, if you allow Facebook, HTTP is allowed by default. This also allows all unknown HTTP applications, or HTTP applications for which there are no signatures. For example, to allow Facebook but block all other HTTP traffic you need to create access rules for the following conditions and in the same order:

- Scan Facebook
- Deny HTTP

Consider that a user attempts to access Gmail, which is a known application. So, the Sensor identifies the Gmail traffic and blocks it according to the second rule. Now, consider that a user attempts to access an unknown HTTP application. The Sensor cannot identify this application beyond the HTTP level because there is no signature. Because the first rule implicitly allows HTTP, the Sensor allows this traffic to pass through. In short, all unknown HTTP applications are allowed, and all known HTTP applications except Facebook are blocked.

Suppose if you create Access Rules for the following conditions and in the same order then all HTTP applications, including Facebook, are blocked:

- Deny HTTP
- Scan Facebook

Similarly, rules involving application capabilities also can induce the dependency factor. That is, allowing an application capability allows the application itself and other capabilities of the application for which there are no signatures.

When you calculate the dependency factor between access rules, factor in all the components of the rules such as source, destination, effective time, application categories, and so on. Consider the sample set of rules below:

1. Source: x ¦ Destination: y ¦ Application: TwileShare ¦ Response action: Scan (that is, permit with IPS)
2. Source: x ¦ Destination: y ¦ Application: Twitter ¦ Response action: Drop
3. Source: a ¦ Destination: b ¦ Application: Twitter ¦ Response action: Drop

When the Sensor detects Twitter traffic from x to y, it allows this traffic with IPS, though it must drop this traffic according to the second rule. This is because, TwileShare is dependent on Twitter. So, by allowing TwileShare in the first rule from x to y, you are allowing Twitter from x to y as well. However, if the Sensor detects Twitter traffic from a to b, it drops the traffic according to the third rule, because the first rule that implicitly allows Twitter applies only from x to y and not from a to b.

Consider the rules below:

1. Source: x ¦ Destination: y ¦ Application: Twitter ¦ Response action: Drop
2. Source: x ¦ Destination: y ¦ Application: TwileShare ¦ Response action: Scan (that is, permit with IPS)

In this case, Twitter traffic from x to y is dropped according to rule 1; TwileShare traffic from x to y is allowed with inspection according to rule 2.

Enable Application Identification

You can enable Application Identification for the required ports of a Sensor. By default, this feature is disabled.

NOTE

Enabling Application Identification affects only the **Top Application Summary** dashboard and has no impact on the Firewall feature.

Identifying applications is a resource-intensive process. If the Sensor performs application identification on the entire traffic, the Sensor throughput could be reduced by about 10%. The amount of actual throughput drop varies based on the type of traffic.

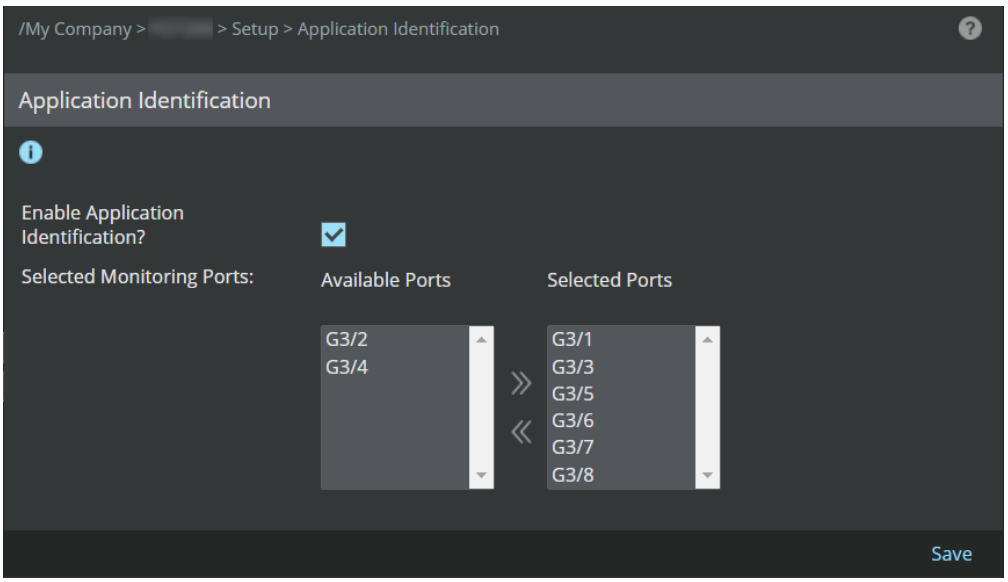
1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Application Identification**.

   The **Application Identification** page is displayed.

2. Select **Enable Application Identification?**

   All the monitoring ports that are currently enabled and up are listed under **Selected Ports**. This means the Application Identification feature is enabled at these ports.

Figure 497. Enabling Application Identification for specific ports



3. Use the arrow marks to move the items between **Available Ports** and **Selected Ports.**

   Make sure only those ports for which you want to enable the Application Identification feature are listed under **Selected Ports.**

4. Click **Save.**
5. Do a configuration update to the Sensor.

User-based access rules

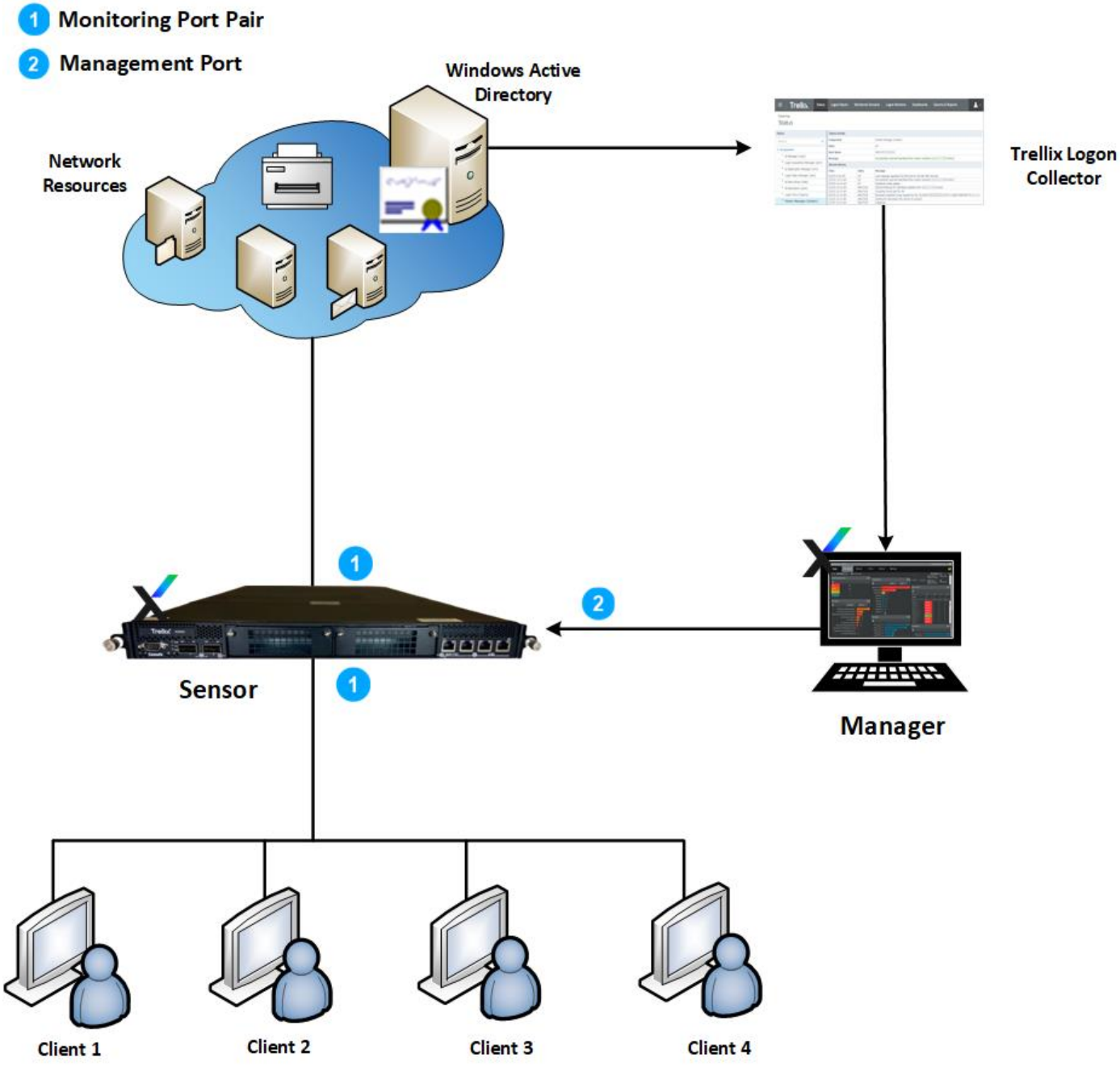
Similar to application identification, the information in this section applies to advanced Firewall policies and advanced QoS policies.

For example, you can create access rules to allow a specific AD group of users to access social-networking applications while blocking the same for some other group during business hours. Such access rules where user data is also a criteria are referred to as user-based access rules. Creating rules that are based on users and user groups is a better option than IP address based rules, especially when the IP address are likely to change dynamically.

NOTE

You cannot specify country and user name or user group in the same rule.

Figure 498. A deployment scenario for user-based access rules



To use user-based rules in your Firewall or QoS policies, you must install Trellix Logon Collector on your network and integrate it with the Manager. Trellix Logon Collector gathers the details of the currently logged on users from the domain controllers. It then regularly updates these details to the Manager. The Manager processes these details and passes them to the relevant Sensors, which use them to evaluate the traffic and take the configured response action.

NOTE

You can configure user-based access rules only in advanced Firewall and QoS policies.

You can create an advanced Firewall access rule with the **Response** set as **Require Authentication.** This option indicates that you want the Sensor to ensure AD authentication of users if the traffic is HTTP. If the Sensor does not have the AD details for a user, it mandates the user to provide the AD logon credentials. The Manager then verifies these credentials with the AD server. So, the Sensor is aware that the user has valid AD credentials and also has the AD user name to apply the correct rule.

Advantages

- User-based rules enable you to effectively identify and regulate traffic originating in your network. So, you can now control what your users can or cannot access regardless of the other criteria. In case of QoS, you can apply traffic management techniques based on user groups.
- Consider organizations where users work in shifts or where users log on from any available host; that is, a host is not dedicated to any particular user. For such cases, user-based access rules can provide the required control.
- Bring Your Own Device (BYOD) environment is another scenario where user-based access rules can be very useful. Using the **Require Authentication** option, you enforce your users to make their host to be part of your corporate domain.

High-level steps for implementing user-based Firewall and QoS rules

The following are the requirements for implementing user-based rules for Firewall and QoS:

- Manager version 10.1.7.65 or above
- NS-series Sensors running on version 10.1 or above
- Trellix Logon Collector version 3.0.11
- Your AD server is configured correctly and that your users are able to logon to the domain.
- You have deployed the required Sensor monitoring ports in SPAN, tap, or inline mode (for QoS, only inline mode applies). Your Trellix IPS deployment is functioning as expected. For example, in the segment where you have deployed the monitoring ports, legitimate traffic is able to reach the destined hosts.
- Optionally, you can log the results of each rule that the Sensor applied. For this you need a syslog server.

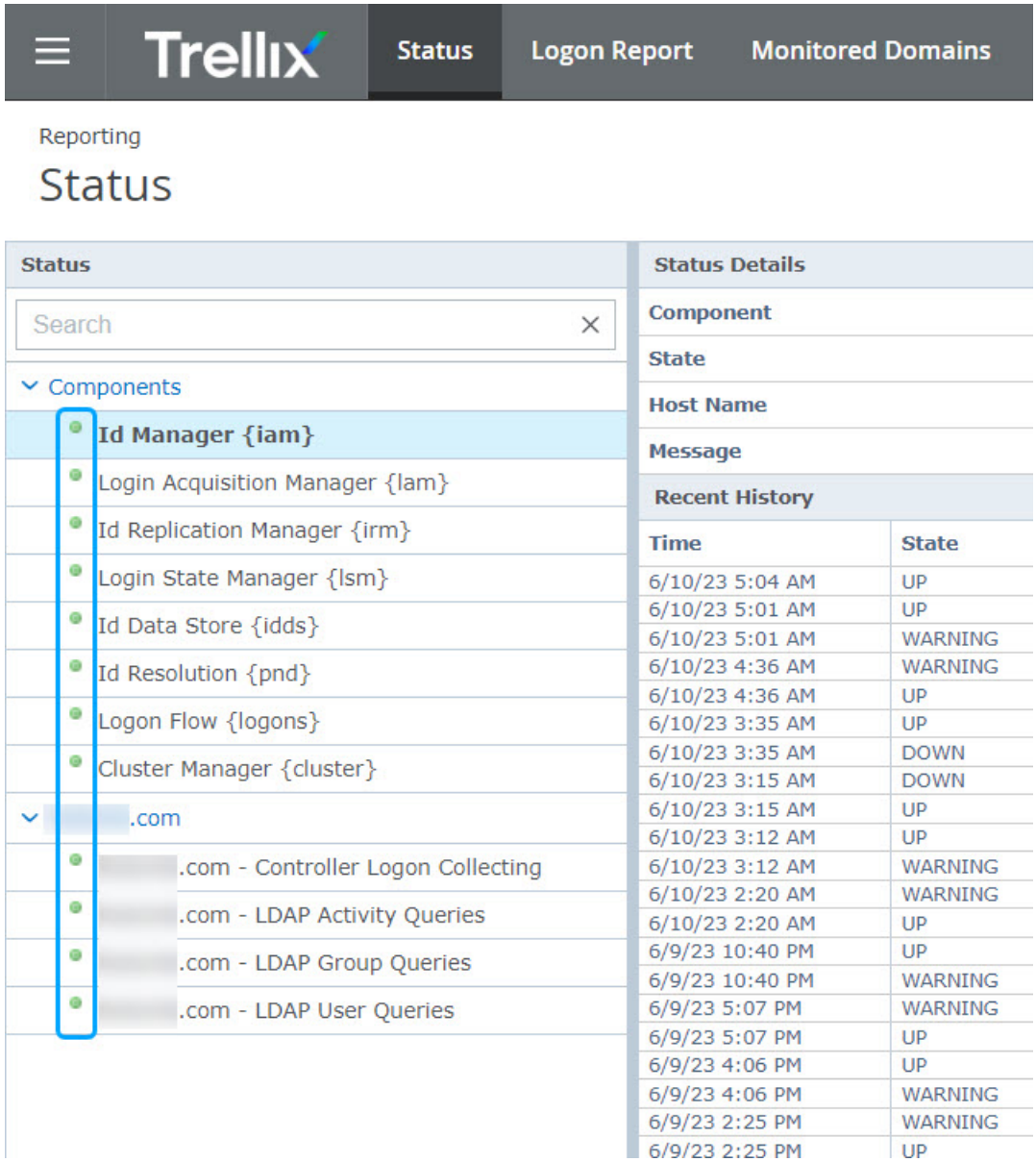
NOTE

To be able to configure and use Firewall policies, you must have administrator permissions for the IPS environment of the Manager. If you are not sure, contact the administrator of the Manager server.

The following are the high-level steps involved in implementing user-based access rules:

1. Install or upgrade Trellix Logon Collector to software version 3.0.11. You can install Trellix Logon Collector on your AD server or on a different one. If you are installing it on a different server, make sure the Trellix Logon Collector and the AD server are reachable to each other over the network. Refer to [Trellix Logon Collector 3.0 Administration Guide] for information on installation and upgrade.
2. Add the relevant domains in Trellix Logon Collector. After you have added the domains, the **Status** in Trellix Logon Collector must be in green. If not, refer to Trellix Logon Collector documentation to troubleshoot and fix the problems.

Figure 499. The status in Trellix Logon Collector



3. Make sure the IP, users, and computer details displayed in the Logon Report of the Trellix Logon Collector are accurate.
4. Integrate Trellix Logon Collector with the Manager. You can integrate only one Trellix Logon Collector with the Manager. See [Trellix Intrusion Prevention System Integration Guide] for more information.

> **NOTE**
>
> If you implement Manager Disaster Recovery (MDR), then you must manually integrate the secondary Manager with Trellix Logon Collector.

5. Optionally, configure the syslog details in the Manager to log the details related to Firewall access rules.

6. As explained in the subsequent sections, the Manager receives the user details from Trellix Logon Collector. Additionally, the Sensor also uses the Kerberos traffic to detect user details. For this method to work, you must configure the details of the AD and Trusted Domain Controllers in the Manager.
7. Configure user-based access rules in the Manager and apply it to the required Sensor resources. In an access rule, you can specify the following as the criteria:
   - Up to 10 AD user names
   - Up to 10 AD user groups
   - A combination of AD user names and user groups not exceeding 10 in a rule in advanced policy.
8. View the access-rule related details in the Manager configuration report and in the syslog server.

How user-based access rules work

The way user-based access rules work can be explained in three parts:

1. How the Manager receives user details.
2. How the Sensor receives user details.
3. How the Sensor evaluates user-based access rules.

How the Manager receives user details

1. When you add the domains in Trellix Logon Collector, it contacts the AD server and collects the details, such as the IP address, user name, host name, and so on of the currently logged on users.
2. When you integrate Trellix Logon Collector and the Manager, Trellix Logon Collector sends all the user details that it currently has to the Manager. The information sent includes the following:
   - IP to user mapping
   - List of users and the user groups to which they belong
   - List of user groups

   NOTE

   Communication between the Manager and Trellix Logon Collector occurs over SSL.
3. Trellix Logon Collector updates the Manager continuously. So, at any point in time, the current user-related data with Trellix Logon Collector is there with the Manager as well.

   Consider situations such as the following:
   - A user logs off from a host and a user logs on from that host again
   - You add a user to more user groups
   - You delete a user group in the AD

   For all such cases, as soon as Trellix Logon Collector has the updated information, it is reflected in the Manager as well.

   TIP

   When you add new users in the AD, modify user groups, or delete user groups you must run the *TLC Refresh Users* server task manually in Trellix Logon Collector. Then the current data from the AD is available in the Manager.

4. If you have configured MDR, then the process explained above happens independently for both the Managers. The Managers themselves do not exchange any user details.

For the following cases, the information might not immediately reflect in the Manager:

1. If a user logs off from a host and no user is currently logged on
2. You remove a user from a user group
3. You delete a user group. In this case, the user attributes are updated but the deleted user group is visible in the Manager

How the Sensor receives user details

1. The Manager sends user-data updates to Sensors when both of these conditions are met:
   - NS-series Sensors of software version 10.1 or above
   - At least one of the Sensor's resources has been assigned a user-based Firewall access rule or QoS rule.
2. The updates to the Sensors includes the following information:
   - IP to user mapping
   - User to user group mapping
   - List of user groups
3. Manager sends the updates using TFTP (standard ports). It sends the updates to both the member Sensors in case of failover.
4. The Manager updates the Sensor in two ways:
   - Full update — that is the Manager sends the entire set of user-data that it currently has to the relevant Sensors. This update entirely refreshes the user-data on a Sensor.
   - Incremental update every one minute — the Manager sends just the changes since the last update.
5. If you have an MDR, only the active Manager sends the updates to the Sensors. If you have a HA pair of Sensors, the active Manager sends the updates to both the Sensors. Whenever the active Manager goes down, the standby Manager sends a full update to the Sensors as soon as it becomes the active Manager.
6. The Manager sends the full update under the following conditions:
   - Sensor reboot
   - If the communication channel between the Manager and Sensor that is used for the updates comes up again
   - Manager restarts
   - By default, at 1200 hours everyday; this is not user-configurable
   - When a standby Manager in an MDR pair becomes the active Manager
   - When connection between the Manager and Trellix Logon Collector is re-established

> **NOTE**
>
> The Manager re-sends an update until it succeeds.

Deriving user details using Kerberos traffic: If the Manager-Trellix Logon Collector communication is disrupted for some reason, the user information with the Sensor might not be current. As a redundant measure, the Sensor is designed to passively *snoop* Kerberos traffic passing through its monitoring ports. This typically happens when users attempt to log on using their

AD credentials. The Sensor sends the user details from the snooped Kerberos traffic to the Manager. Then the Manager communicates with the AD servers to validate the user credentials. This Kerberos-based detection of user details is independent of the updates from Trellix Logon Collector. The updates from Trellix Logon Collector and the user details through Kerberos are used to update the same set of data. When you create user-based rules, only the user names and user groups received through updates from Trellix Logon Collector are displayed. The user names derived through Kerberos snooping are not displayed.

NOTE

In case of Sensor failover, the Sensor that detected the Kerberos traffic sends the details to the Manager. It also sends the details to its peer Sensor. The peer Sensor sends the same details to the Manager. The Manager verifies with the AD servers and responds to both the Sensors separately. In case of MDR pair, the process is same but only the active Manager is involved.

How the Sensor evaluates user-based access rules

1. Consider an access rule that has only AD user names mentioned. To evaluate the traffic against this rule, the Sensor takes the source IP address in the packet and checks it against the IP-to-user mapping list that it has. This way, the Sensor determines the currently logged on user for that IP address. If this matches with any of the user names mentioned in the rule, then it is a match with respect to the source user. If not the Sensor proceeds to check the next rule.
2. Consider that you have mentioned only user groups in the rule. As explained above, the Sensor first determines the currently logged on user. Then it checks this user name against the user-to-user group mapping that it has. If any of the user group of this user matches with any of the user groups in the rule, it is a match with respect to source user. If not the Sensor proceeds to the next rule.
3. In case of both user names and user groups in the rule, the Sensor checks for the user and user group in the same order that you have configured.

Require Authentication access rule and how it works

You can create an advanced Firewall access rule with the **Response** set as **Require Authentication.** When you implement such a rule, the Sensor ensures that the corresponding users have valid AD logon credentials.

NOTE

A **Require Authentication** access rule is effective only when the monitoring ports are inline. These rules are relevant only for HTTP traffic and becomes effective only when configured on top of all the rules in the **Access Rules** tab while creating an internal firewall policy

If you have created a require-authentication access rule, the Sensor ensures AD authentication in the following ways:

1. As discussed in the earlier sections, when users log on to your network, the Sensor receives the user details through the Manager. So, if the Sensor has an IP-to-user mapping, it indicates that the user has been already authenticated by the AD server. So, the Sensor proceeds to evaluate the rest of the rules.
2. If the Sensor does not have a user bound to the IP address in the detected HTTP traffic, it redirects the user to the Guest Portal. This is the Web portal hosted on the Sensor for explicitly determining the identity of users based on their AD credentials.

   The Sensor sends the logon credentials that the user entered in the Guest Portal to the Manager. The Manager checks if it already has the AD details of the user. If yes, it forwards the details to the Sensor. If not, it verifies the user credentials with the configured list of AD servers. The Manager notifies whether the credentials are valid or not to the Sensor. The Manager provides the IP-to-user and user-to-user group mappings to the Sensor.

NOTE

In case of Sensor failover, the Sensor that detected the HTTP traffic redirects the user to its Guest Portal. It sends the AD details to the Manager. The Manager verifies with the AD servers and responds to the Sensor. If the authentication is successful, the Sensor sends the details to its peer Sensor. In case of an MDR pair, the process is same but only the active Manager is involved.

The following are the parameters allowed in a require-authentication access rule:

- You must select the default HTTP *Service* rule object as the Application. You cannot select any other rule object for Application. Even the default HTTP *Application* rule object or a custom HTTP Service rule object are not valid.
- The **Source User** must be set to **Any**.
- Select the **Response** as **Require Authentication**.

For all other parameters, you can specify the values you require. For example, you can specify all your critical Web servers in the **Destination Address** field. So, the Sensor ensures that all users accessing these Web servers have valid AD credentials.

Purpose of require-authentication access rules

Assume that the communication between the Manager and Trellix Logon Collector is down. Now, consider a user who is physically connecting a Windows host that is already unlocked. In this case, the Sensor might not have a IP-to-user mapping because the communication with Trellix Logon Collector is down. Also, the host did not generate any Kerberos traffic since the host is already unlocked. Because the Sensor does not have the IP-to-user mapping, it might not be able to evaluate and apply the correct user-based access rule for this user. If you have a require-authentication rule, then the Sensor will be able to derive the user details even in this case as illustrated by the following example.

Consider the following example rules:

1. Source Address: Other | Source User: Any | Destination Address: Critical Web servers | Application: HTTP | Response: Require Authentication.
2. Source Address: Other | Source User: Jane | Destination Address: Critical Web servers | Application: HTTP | Response: Scan.
3. Source Address: Other | Source User: John | Destination Address: Critical Web servers | Application: HTTP | Response: Deny.

Consider that Jane accesses a critical Web server:

1. If the Sensor has the IP-to-user mapping for this traffic, the Sensor proceeds to the second rule. In this case, only the second rule is considered as a match.
2. If the Sensor does not have the IP-to-user mapping for this traffic, it redirects Jane to its Guest Portal, where the Jane enters her AD credentials. In this case, the first rule is considered as a match. The Manager checks if it has the AD details for Jane. If not, it verifies these credentials with the AD servers and also forwards the details related to Jane to the Sensor. So, the Sensor now has at least the IP-to-user mapping for Jane.
3. Jane retries to access a critical Web server. This time, since the Sensor has the IP-to-user mapping, it proceeds to the second rule. The second rule matches and the Sensor forwards the traffic for IPS inspection.

Requirements for require-authentication access rules

In addition to the requirements in [High-level steps for implementing user-based Firewall and QoS rules,] the following are required for a required-authentication access rule to work:

- You have deployed the required Sensor monitoring ports in inline mode. Required-authentication access rule is not effective in SPAN or tap mode.
- You must specify an IP address to the monitoring port pair to redirect users to the Guest Portal.
- You must specify the AD servers and trusted Domain Controllers that the Manager should check with to verify the AD credentials entered in the Guest Portal.
- Enable the Guest Portal settings through the Manager.

Considerations for access rules

The following are the considerations for access rules:

- You can create user-based access rules only in advanced Firewall policies.
- You integrate the Manager only with one instance of Trellix Logon Collector. Integration with a redundant Trellix Logon Collector setup is not supported.
- You cannot add, modify, or delete a user name or user group in the Manager.
-
- You can specify only user and user group as the criteria. No other AD properties are supported.
- Only IPv4 hosts are supported. A rule will not match if the user logs on from an IPv6 host.
- The following are the limits for user data:
  - Up to 100,000 IP-to-user mappings
  - Up to 75,000 user names
  - Up to 10,000 groups for NS-Series and Virtual IPS Sensors
- Maximum user-based rule objects that you can use in the Firewall policies per Sensor model is as follows:

Sensor	Maximum user-based rule objects
NS9500 stack - 100 Gbps throughput	5,000
NS9500 stack - 60 Gbps throughput	5,000
NS9500 stack - 40 Gbps throughput	5,000
NS9500 standalone - 30 Gbps throughput	5,000
NS9500 standalone - 20 Gbps throughput	5,000
NS9500 standalone - 10 Gbps throughput	2,500
NS9300	5,000
NS9200	5,000
NS9100	2,500
NS7600 - 15 Gbps throughput	1,250
NS7600 - 10 Gbps throughput	1,250
NS7600 - 5 Gbps throughput	1,250

Sensor	Maximum user-based rule objects
NS7500 - 7.5 Gbps throughput	1,250
NS7500 - 5 Gbps throughput	1,250
NS7500 - 3 Gbps throughput	1,250
NS7350	1,250
NS7250	1,000
NS7150	1,000
NS7300	1,250
NS7200	1,000
NS7100	1,000
NS5200	750
NS5100	750
NS3500	500
NS3200/NS3100	500
IPS-VM600	750
IPS-VM5000	750

- In a Firewall access rule or QoS rule, you cannot specify an IPv4-based rule object for one field and IPv6-based rule objects for other applicable fields. For example, if you select an IPv6-based rule object in the **Source Address** field, then you cannot specify IPv4-based rule objects for **Destination Address** or **Source User** fields. For this example, you can specify only an IPv6-based rule object or *other* as the value for **Destination Address** and *any* for **Source User.** Recall that User and User Group rule objects are considered as IPv4-based rule objects because Trellix Logon Collector 3.0.11 does not collect user information from IPv6 hosts. Similarly, Country and Host DNS Name are also IPv4-based rule objects.
- User log off is not monitored.
- User or user group deletion is not monitored.
- When you add new users in the AD, modify user groups, or delete user groups you must run the *TLC Refresh Users* server task manually in Trellix Logon Collector. Then the current data from the AD is available in the Manager.
- Guest Portal user timeout, by default, is 8 hours.

Troubleshooting user-based access rules

The following are some points that you can consider to troubleshoot issues related to user-based access rules:

- Make sure that above your user-based access rules, there are rules that allow DNS, DHCP, and AD traffic to the corresponding servers.
- If a user-based rule is not working as expected, change the **Source User** to **any** and see if the rule is working fine.
- If you are unable to view the users or user groups in the **Firewall** page, check the communication between the Manager and the Trellix Logon Collector.
- CLI commands related to user-based access rules:
  - **`show userInfo stats`**: Displays the number of full (bulk) updates and incremental updates to the Sensor. Also, displays the number of users, user groups, and host IP addresses currently present in the Sensor.

- The Manager raises a fault message for the following conditions :
  - The Manager is unable to contact Trellix Logon Collector.
  - The number of IPs to users mapping has exceeded 100,000.
  - The number of users has exceeded 75,000.
  - The bulk update from the Manager to the Sensor is more than 25 MB in size. In this case, the fault is raised and the Manager aborts the update.
  - When the user groups limit exceed the specified values, the following faults are raised:
    - **AD user groups size exceeded**
    - **TLC IP-User mapping/ User count exceeds limit**
    - **TLC Group Size fault**

    For more information on these faults, refer to Manager faults (page 2409) in the *Troubleshooting* section of this guide.

Configure Firewall policies

To configure the Firewall feature, first create the required rule objects, define the Firewall policy, and then define the access rules for that policy. After you create the Firewall policy, you can assign it to the required Sensor resource. This section provides the step-by-step information on how to configure the Firewall feature.

Manage rule objects

You use rule objects to define Firewall and QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones, and NTBA Communication Rules. To manage the rule objects, go to Policy → <Admin Domain Name> → Intrusion Prevention → Objects → **Rule Objects**.

Option	Definition
Rule Objects	Displays the rule objects according to the filter criteria. Click a column heading to sort the table in ascending or descending order. • **Name** — Indicates the name of the rule objects • **Description** — Indicates the description of the rule object • **Type** — Indicates the rule object type • **Owner Domain** — Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain. • **Visibility** — Indicates the visibility settings of settings to the domains, whether it is visible only to the owner domain or to both owner and child domains • **Editable here** — **Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.

Option	Definition
Object Type	Filters rule objects in the list. • **Default Objects Only** — Trellix pre-defined these rule objects. For example, the Application and Country are default rule objects. You cannot define these rule objects. • **Custom Objects Only** — You need to define these rule objects. For example, you need to define the Host DNS Name rule object. • **Custom and Default Objects** — When selected, it displays both the predefined and user defined rule objects. For example, IPv4 Network Rule Object has the 3 reserved private networks pre-defined, but you can also create your Network rule objects.
Rule Object Type	Select the rule object type that you want to view.
Search	Type your search criteria in the field to find rule objects with matching elements. For example, type **google** to list the rule objects containing *google* as part of their names.
icon	Creates a custom rule object
icon	Clones a rule object. You cannot clone default rule objects other than the IPv4 network rule objects.
icon	Deletes a custom rule object belonging to the current admin domain
Save as CSV	Saves the rule objects for the rule object type selected
To view or edit a rule object	Double-click the rule object belonging to the current admin domain.

In the Manager, each rule object type has an associated icon for easy identification. The following table lists the rule objects and the corresponding icons.

Table 61. Rule object icons

Icon	Rule Object
	Application
	Application Group
	Application on Custom Port
	Country (displays the country's flag. So, the icon varies for each country)
	Finite Time Period
	Host DNS Name, IPv4 Endpoint, and IPv6 Endpoint

Icon	Rule Object
	IPv4 Address Range and IPv6 Address Range
	IPv4 Network and IPv6 Network
	Network Group (Network Group for Exception Object)
	Recurring Time Period
	Recurring Time Period Group
	Service
	Service Group and Service Range (Service Range is applicable only to QoS policies).

NOTE

You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

Notes on IPv4 and IPv6 rule objects

For Firewall and QoS, IPv6 addresses are supported for the following rule objects:

- Host
- Address range
- Network

The default Service rule object for ICMPv6 is also now available.

- You use the above-listed, IPv6-based rule objects to create a Network Group rule object. However, you cannot use a combination of IPv4 and IPv6 based rule objects in one Network Group rule object.
- In a Firewall access rule or QoS rule, you cannot specify an IPv4-based rule object for one field and IPv6-based rule objects for other applicable fields. For example, if you select an IPv6-based rule object in the **Source Address** field, then you cannot specify IPv4-based rule objects for **Destination Address** or **Source User** fields. For this example, you can specify only an IPv6-based rule object or *other* as the value for **Destination Address** and *any* for **Source User**. Recall that User and User Group rule objects are considered as IPv4 based rule objects because Trellix Logon Collector does not collect user information from IPv6 hosts. Similarly, Country and Host DNS Name are also IPv4-based rule objects.

The following table classifies IPv4 and IPv6 rule objects:

Type	Rule objects
IPv4	IPv4 Endpoint, Host DNS Name, IPv4 Address Range, IPv4 Network, User, User Group, Country
IPv6	IPv6 Endpoint, IPv6 Address Range, IPv6 Network

You configure user-based Firewall access rules using the user and user group rule objects. It is important to note the following regarding these rule objects:

- You cannot create, modify, or delete the User or User Group rule objects. The Manager manages these rule objects according to the updates from Trellix Logon Collector.
- You can view these rule objects only n the **Access Rules** tab of the **Firewall** page. You cannot view these rule objects in the **Rule Objects** page.
- The user names verified through Kerberos snooping or the Sensor's Guest Portal are not displayed in the Manager.

View the rule objects

You can view existing rule objects in a selected domain.

For a rule object to be listed, it must meet one of these conditions:

- It is a default rule object.
- It is created at a parent admin domain, but it is set to be visible to the child admin domains.
- The rule object was created at the current admin domain.

Steps:

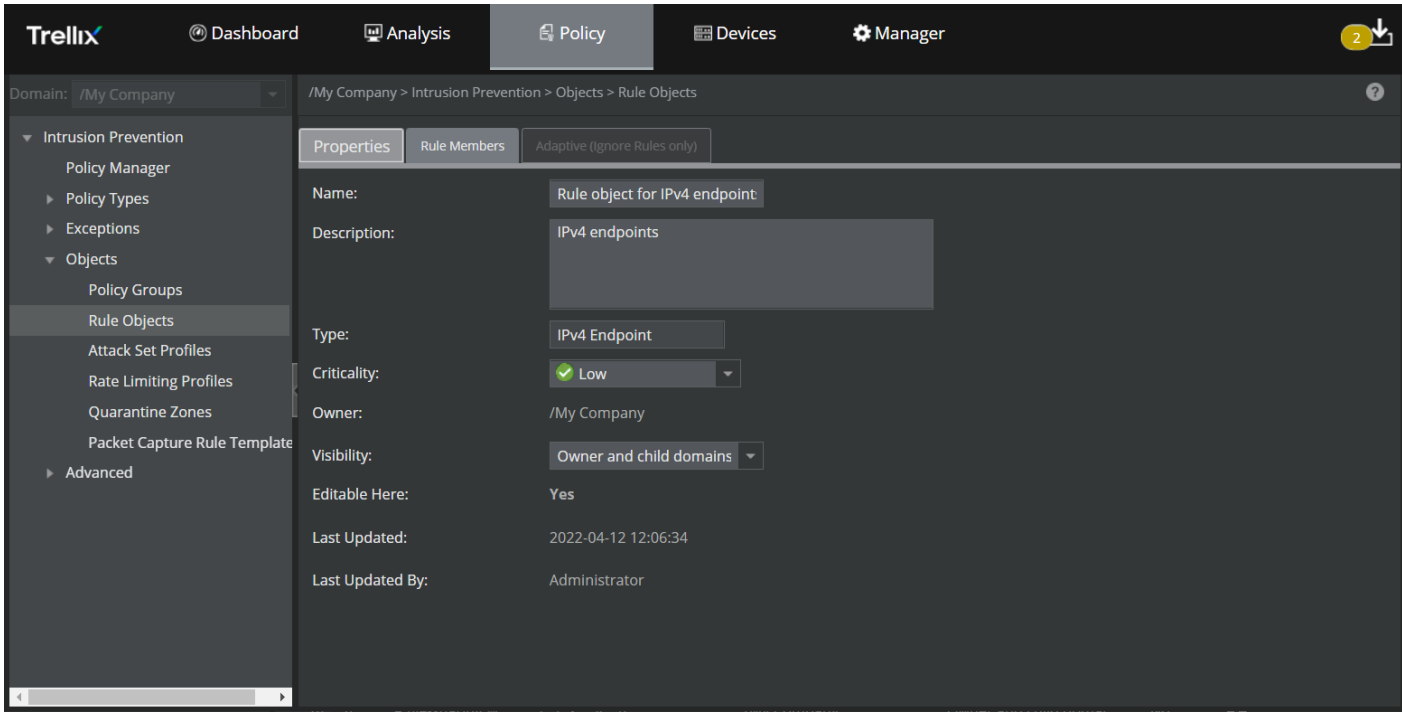
1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.

   - To locate specific rule objects, enter a string in the **Search** text box. For example, type “google” in the **Search** text box to list the rule objects containing “google” as part of their Names.
   - Select the **Custom Objects Only** or **Default Objects Only** or **Custom and Default Objects** from the drop-down list as required.
   - Select the rule object type in the drop-down list.
   - To view limited details of a rule object, point to the object. To view complete details, select and double-click the rule object.
   - The rule object details appear under the **Properties** tab, and the rule members (rule object items) appear under the **Rule Members** tab.

   > **NOTE**
   >
   > An additional tab named **Adaptive (Ignore Rules only)** appears while viewing IPv4 and IPv6 based rule objects.

Figure 500. Viewing Rule Objects



Add a rule object

You can create custom rule objects to use within the Firewall and QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones, and NTBA Communication Rules.

Following table lists the maximum count of rule object items (**Rule Members**) that can be added under each rule object type:

Rule Object type	Rule Members (Maximum count)
Host DNS Name	5000
IPv4 Address Range	20000
IPv4 Endpoint	140000
IPv4 Network	140000
IPv6 Address Range	20000
IPv6 Endpoint	140000
IPv6 Network	140000
Application Group, Application on Custom Port, Finite Time Period, Network Group, Network Group for Ignore Rules, Recurring Time Period, Recurring Time Period Group, Service, Service Group, Service Range	10

NOTE

The rule member count specified in the above table is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object.

NOTE

If you are using a Manager running on or before version 10.1.7.55 and a Sensor running on or before 10.1.5.153, the maximum count of rule members you can add under each rule object type is 10.

NOTE

The above rule object count specified for IPv4/IPv6 based rule objects is also applicable for Central Managers. Central Managers running on or before version 10.1.7.55, however, support only 10 rule members per each rule object.

NOTE

If you are using a Central Manager, do not add more than 10 entries in the Central Manager Rule Objects which are associated with QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones or Quarantine Exceptions in a Manager.

Steps:

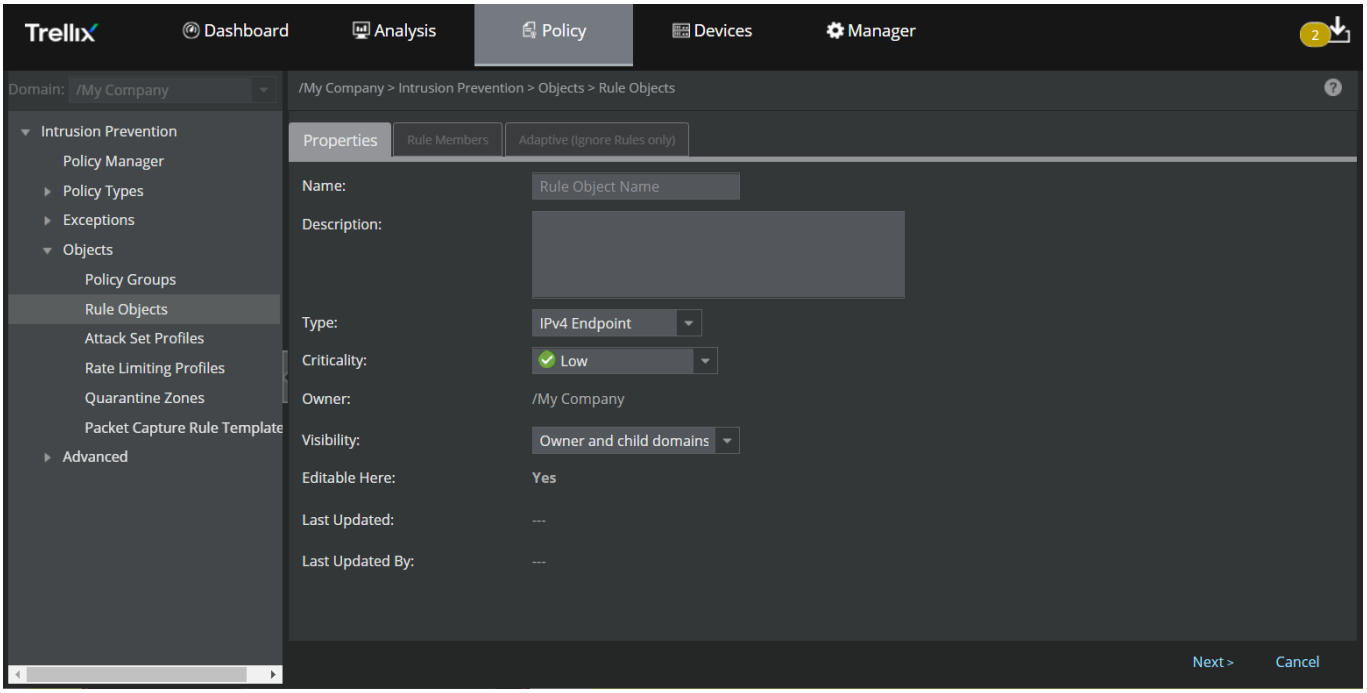
1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.
4. Click +. This displays two tabs, namely the **Properties** tab and the **Rule Members** tab.

   NOTE

   An additional **Adaptive (Ignore Rules only)** tab appears while adding IPv4 and IPv6 based rule objects.

Figure 501. Selecting Criticality for each of your assets

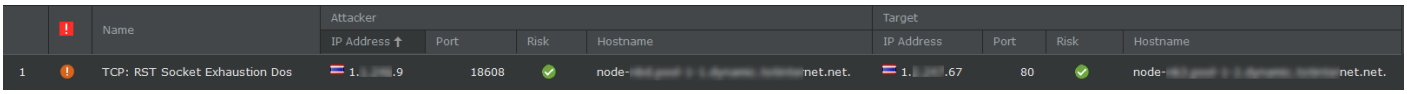


The following table describes the options in the **Properties** tab that are common to all rule objects.

Option	Definition
Name	Enter a unique name to easily identify the rule object.
Description	Enter the description for the rule object.
Type	From the drop-down list, select the type of rule object you want to create. For information on a specific object type, refer to the corresponding sub-section.
Criticality	[Optional] If you have chosen rule object type as IPv4 Endpoint or IPv6 Endpoint, you can specify the **Criticality** of that host by selecting **Low**, **Medium** or **High** from the drop-down list. By default, criticality is **Low**. Determining criticality of a host enables you to categorize all IPv4 Endpoint and IPv6 Endpoint addresses based on their importance to your organization.
Owner	Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain.
Visibility	From the drop-down list, select the option for the visibility level of the rule object. The available options are **Owner and child domains** and **Owner domain only**.
Editable Here	**Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.
Last Updated	Displays the date and time when a rule object was last updated
Last Updated By	Displays the user who modified a rule object

Once you assign criticality to a rule object and an alert involving it is raised, the criticality that you assigned shows up under specific columns in Attack Log. These columns are labeled **Attacker Risk** and **Target Risk**. **Attacker Hostname** and **Target Hostname** displays the names of the rule object.

Figure 502. Display of attacker risk



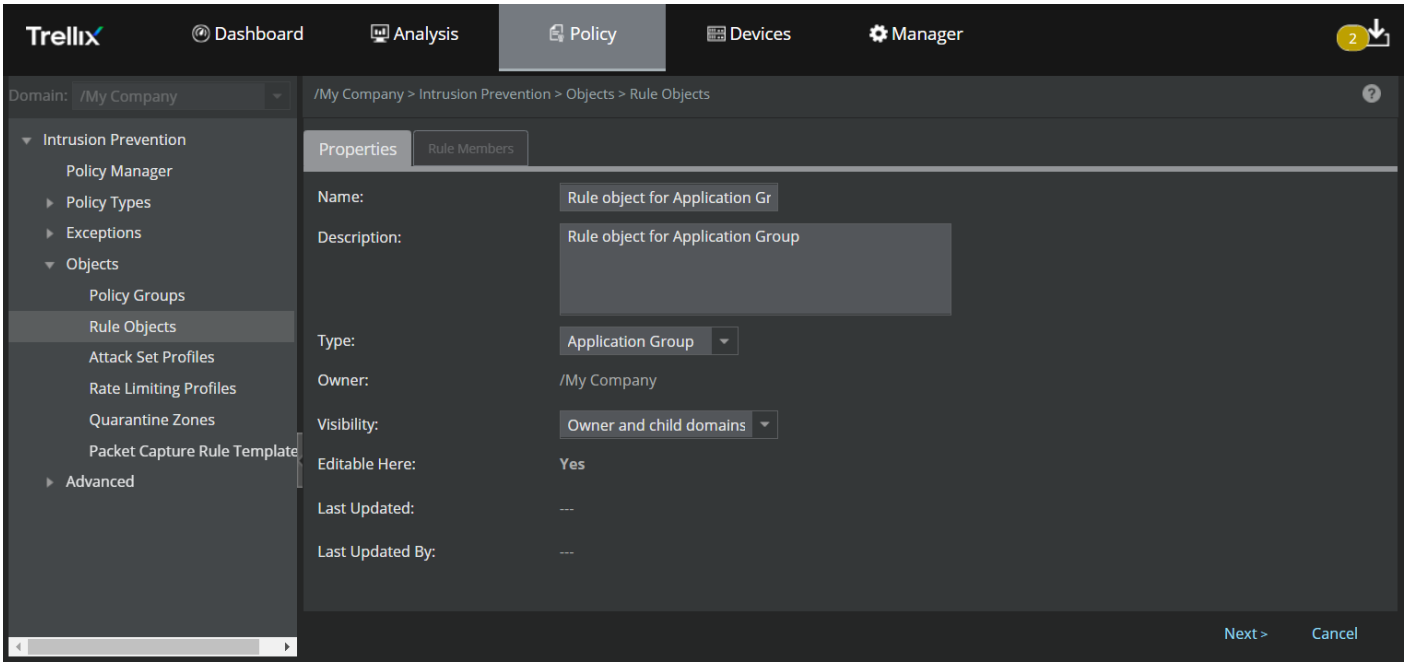
5. Enter the rule object options based on rule object you have selected in the **Type** drop-down list. For information on the subsequent steps to add a rule object, refer to the corresponding sub-sections.

Add an Application Group rule object

Follow these steps to add **Application Group** rule object:

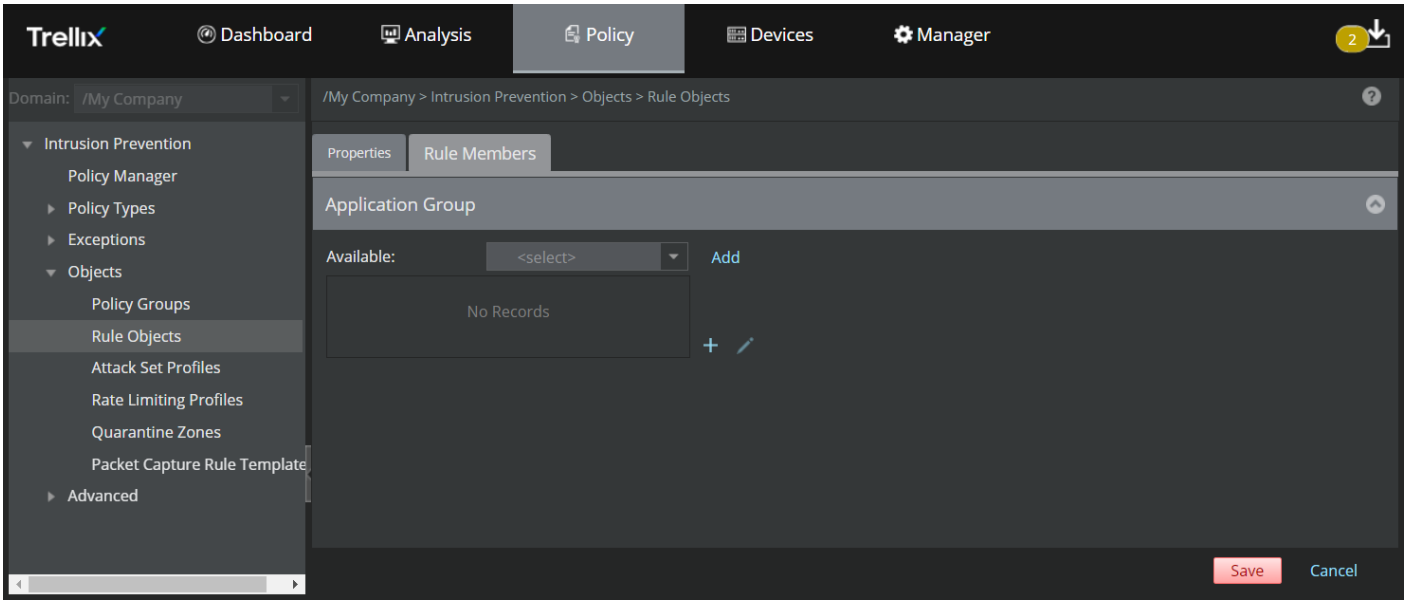
1. Upon specifying the options in the **Properties** tab and selecting **Application Group** from the rule object **Type** drop-down, click **Next**.

Figure 503. Create an Application Group rule object



The **Rule Members** tab is displayed.

Figure 504. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select a pre-defined application or an existing **Application on Custom Port** rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Members** list
	Click this icon to edit a rule member in the list
	Click this icon to add a new **Application on Custom Port** rule object
	Click this icon to remove a rule member from the list

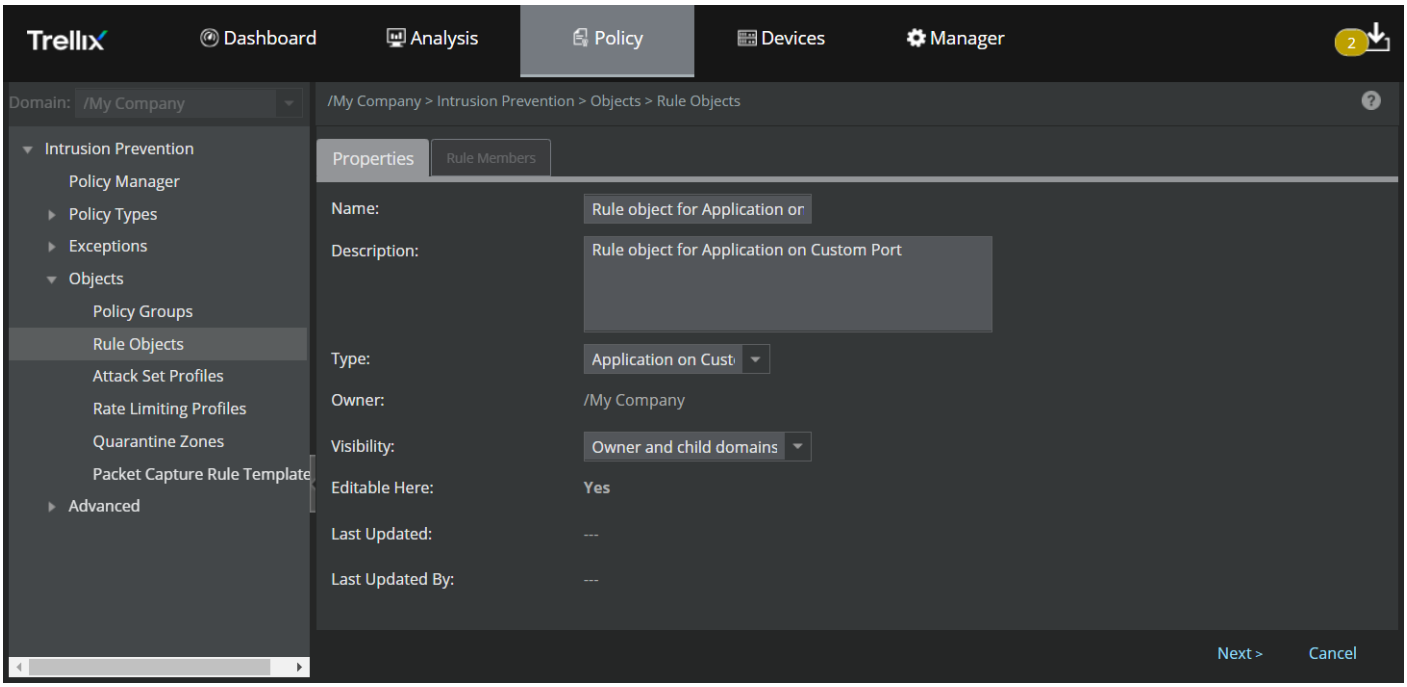
2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Add an Application on Custom Port rule object

Follow these steps to add **Application on Custom Port rule** rule object:

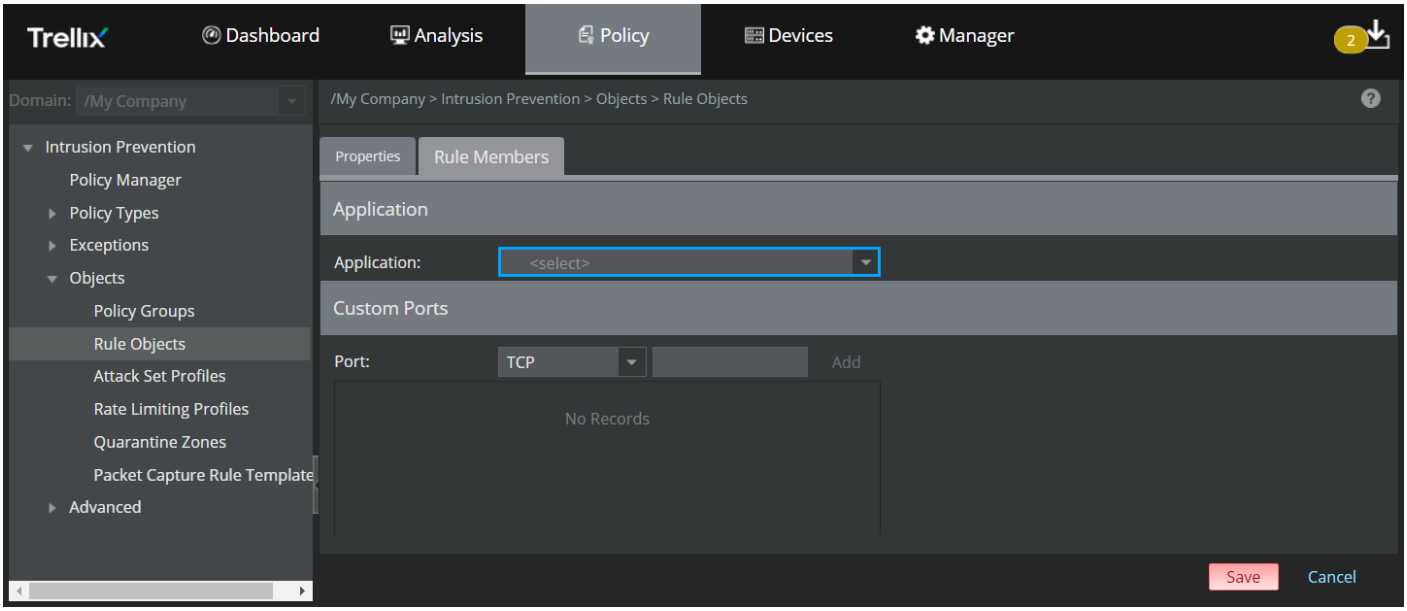
1. Upon specifying the options in the **Properties** tab and selecting **Application on Custom Port rule** from the rule object **Type** drop-down, click **Next**.

Figure 505. Create an Application on Custom Port rule object



The **Rule Members** tab is displayed.

Figure 506. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Application	Lists the pre-defined Application rule objects

Option	Definition
Custom Ports	Select TCP or UDP and type the port number (from 1 to 65534) in the adjacent text box.
Add	Click this button to add the selected IP protocol and the port number to the list. You can define up to 10 port numbers per Application.
	Click this icon to delete the selected IP protocol from the list.

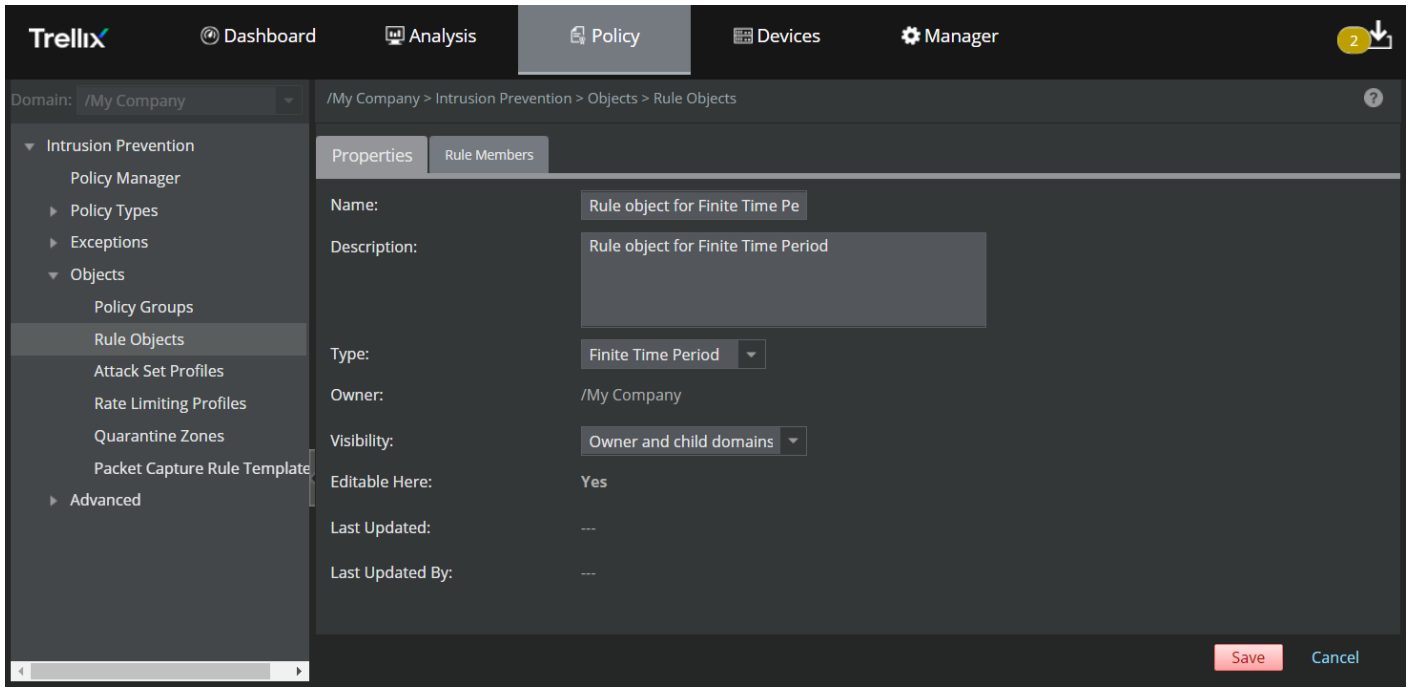
2. Based on the above options, you can select an **Application** from the pre-defined list of applications and assign up to **10** TCP and UDP ports.
3. Click **Save**.

Add a Finite Time Period rule object

Follow these steps to add **Finite Time Period** rule object:

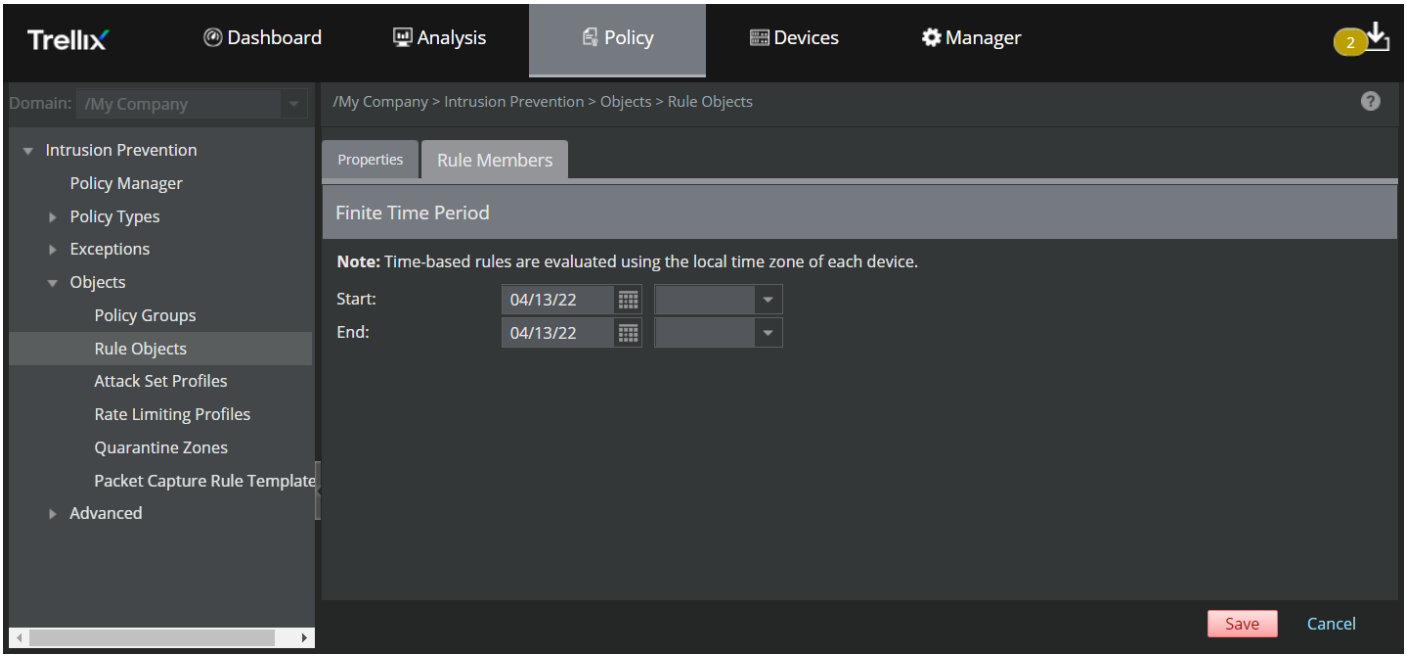
1. Upon specifying the options in the **Properties** tab and selecting **Finite Time Period** from the rule object **Type** drop-down, click **Next**.

Figure 507. Create a Finite Time Period rule object



The **Rule Members** tab is displayed.

Figure 508. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Start and **End**	Select the **Start** date and time and the **End** date and time in the corresponding fields. Time-based rules are implemented using the local time zone of the corresponding Sensor. **NOTE** **Start** date and time must be before **End** date and time.

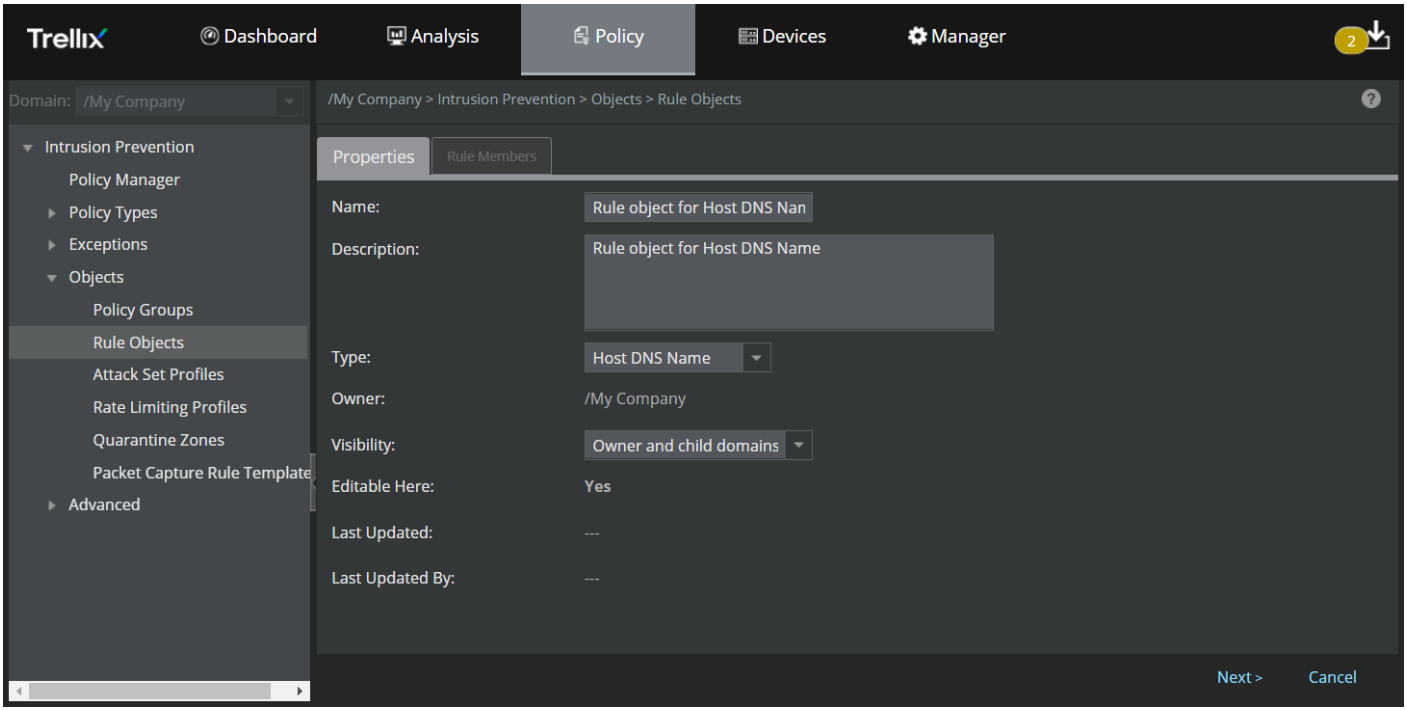
2. Based on the above option, you can select the **Start** date and time and the **End** date and time, and click **Save**.

Add a Host DNS Name rule object

Follow these steps to add **Host DNS Name** rule object:

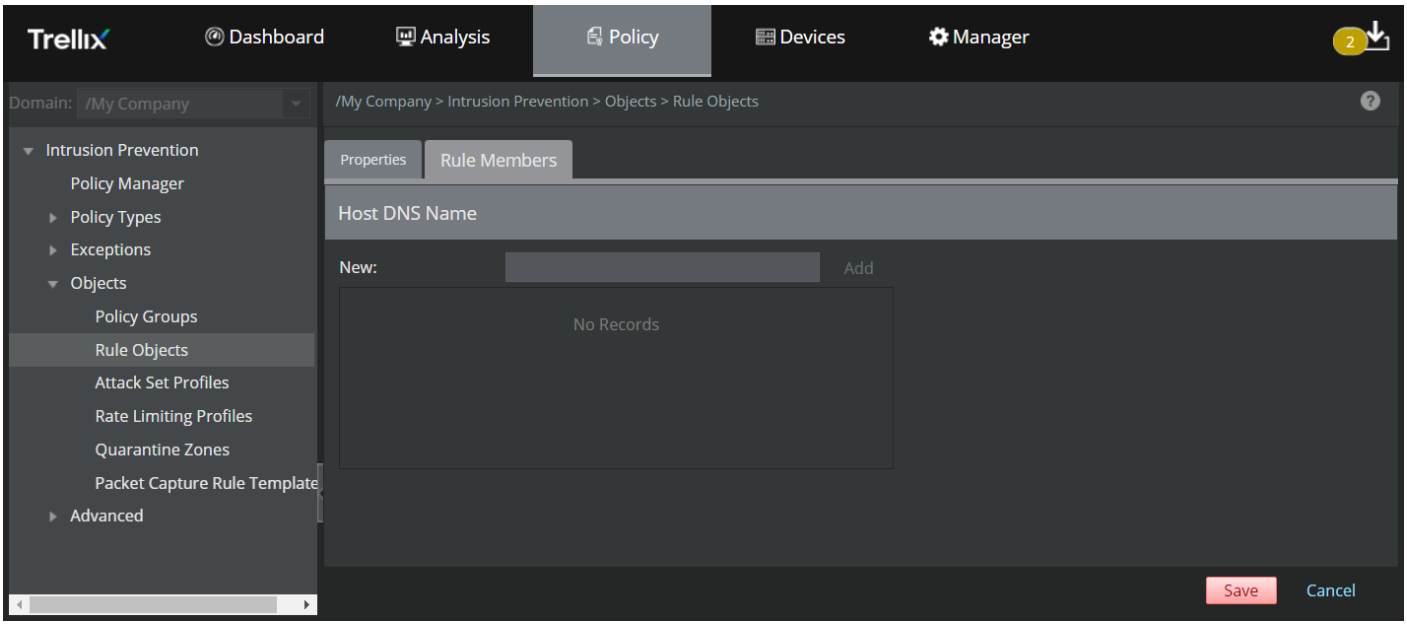
1. Upon specifying the options in the **Properties** tab and selecting **Host DNS Name** from the rule object **Type** drop-down, click **Next**.

Figure 509. Create a Host DNS Name rule object



The **Rule Members** tab is displayed.

Figure 510. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
New	Enter a fully-qualified domain name. If the domain name is not fully-qualified, the Sensor tries to resolve it using the DNS suffixes provided in the **Name Resolution** page. It communicates with the DNS server IPs configured in the **Name Resolution** page.
Add	Click this button to add the host name to the Host DNS Name list. You can add up to 5000 domain names. **NOTE** The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. **NOTE** If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 domain names in any rule object.
	Click this icon to remove the host name from the host names list

2. Based on the above options, you can add the domain names and click **Save**.

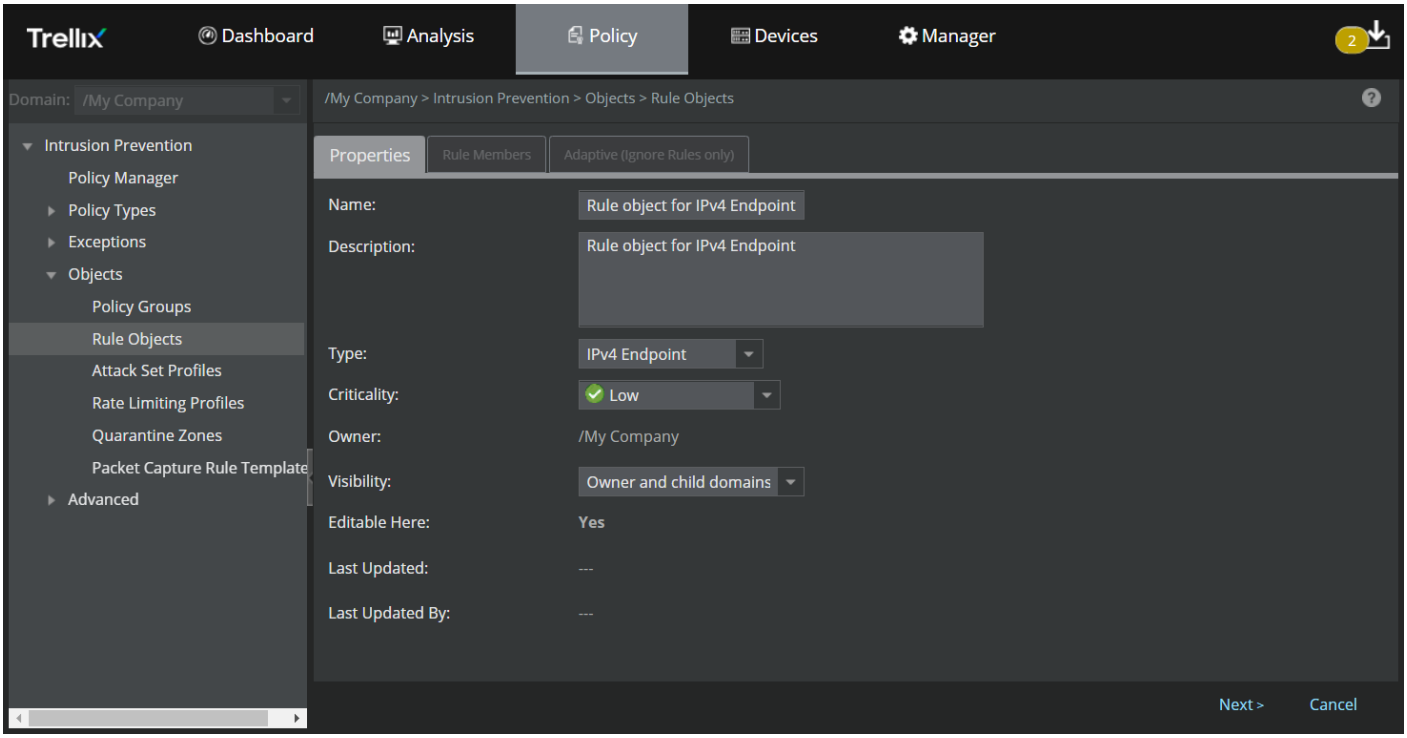
Add IPv4 Endpoint and IPv6 Endpoint rule objects

For quarantine zone access rules, only IPv4 Endpoint rule objects are supported. Also, only one rule member per rule object is applicable for quarantine zone.

The steps to add **IPv4 Endpoint** and **IPv6 Endpoint** rule objects are identical. Follow these steps to add **IPv4 Endpoint** or **IPv6 Endpoint** rule objects:

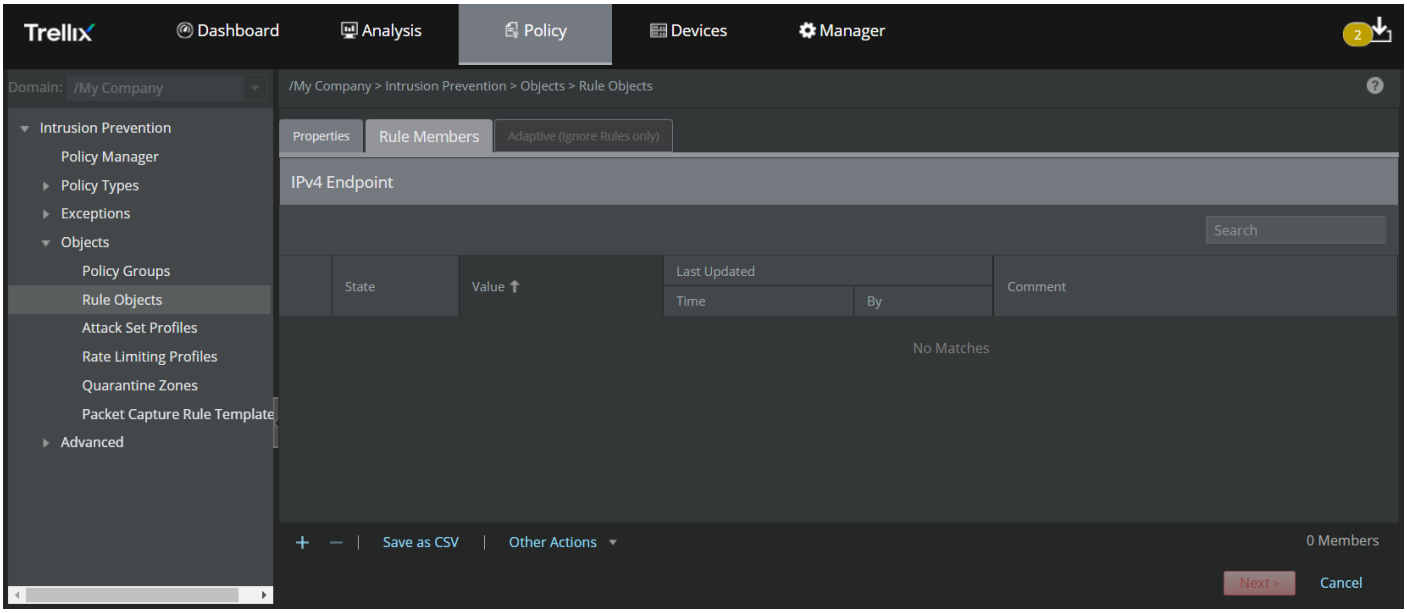
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Endpoint** or **IPv6 Endpoint** from the rule object **Type** drop-down, click **Next**.

Figure 511. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 512. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 62. Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 endpoint based on the rule object type selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 addresses
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address.
−	Click this icon to delete single or multiple IPv4 or IPv6 addresses.
Save as CSV	Click this button to export all the rule members displayed in the grid to a CSV file.
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 addresses • **Export All** — Allows you to export all the IP addresses from the Manager to the local system

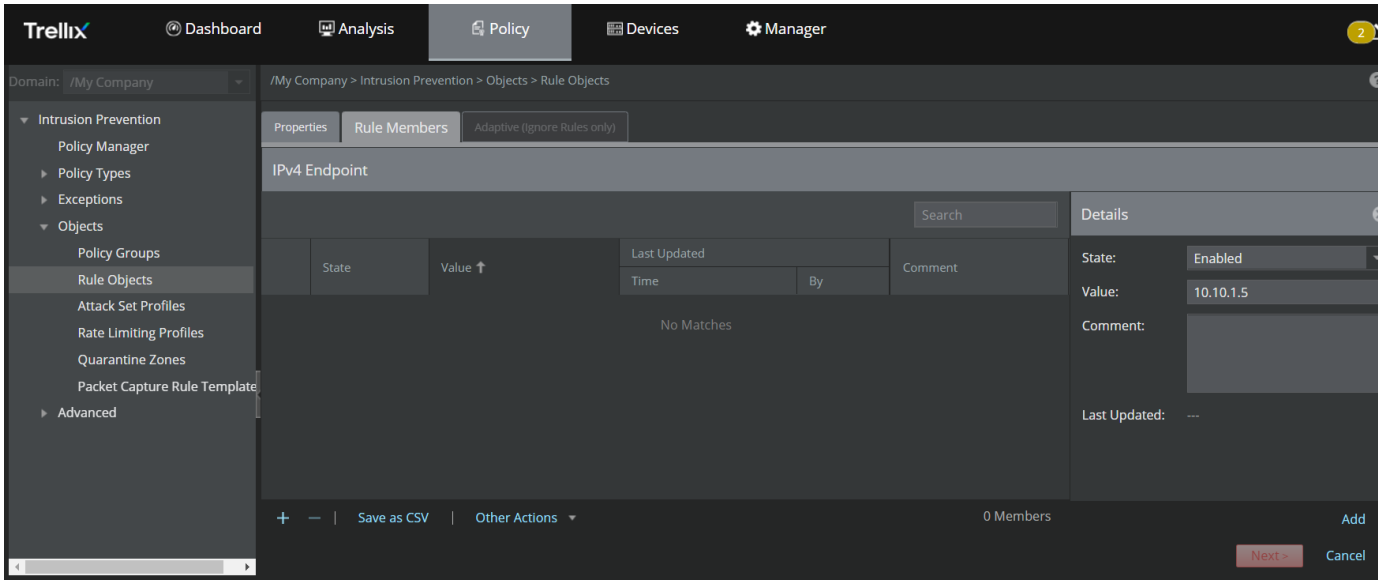
2. There are two ways to add the IP addresses — add individual IP addresses using the + icon or import a list of IP addresses from a CSV file using the Other Actions → **Import** option.
3. To add an individual IPv4 or IPv6 address:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object].

      Select the **State**, enter the IPv4 or IPv6 address in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - Do not specify the CIDR prefix (32) when entering an IPv4 address.
> - You can enter an IPv6 address such as 5507:c0d0:2002:0071:0000:0000:0000:0003. The same address can be represented as 5507:c0d0:2002:0071::0003.
> - You can enter up to 140000 IPv4 or 140000 IPv6 addresses in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 addresses in any rule object.

Figure 513. Add individual IP addresses



c. Upon adding all the required IP addresses, click **Next**.

Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add an IP address to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove an IP address from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of IP addresses from a CSV file using the **Import** option:

a. Click Other Actions → **Import**.

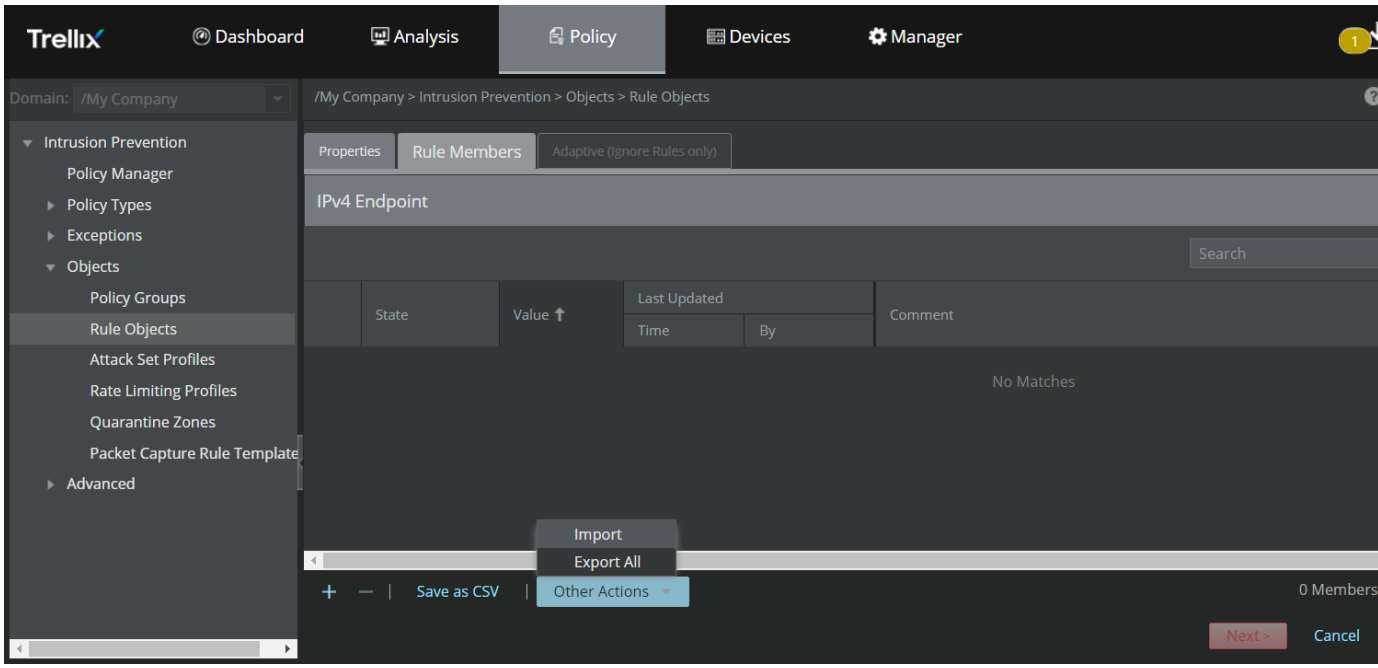
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10 entries.

Figure 514. Import IP addresses from a CSV file



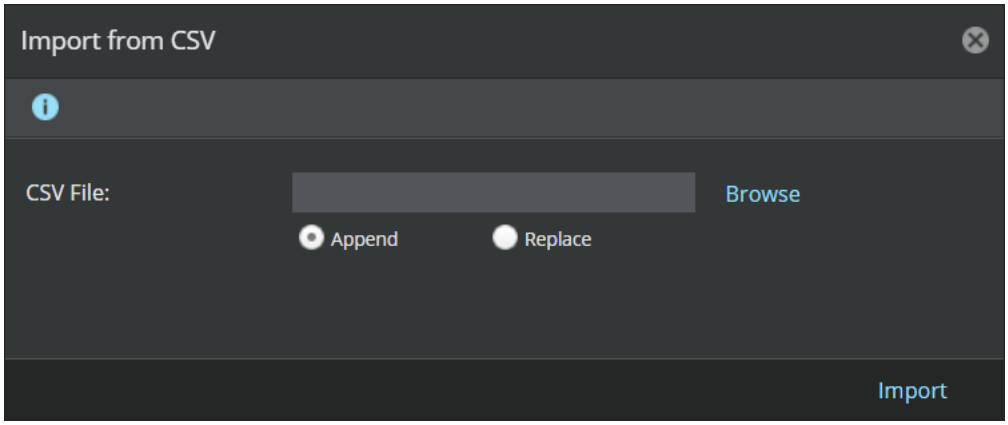
b. **Import from CSV** window appears. Use the **Append** option to add a new list of IP addresses or to append a list of IP addresses to an existing list. Use the **Replace** option to remove the existing list of IP addresses and add a new list from the file being imported.

NOTE

If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IP addresses that you plan to import.

Figure 515. Import IP addresses from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 address>,<Comment>

Example file format: 10.10.1.1,textual description

The following is a sample for a CSV file with multiple IPv4 addresses:

Figure 516. CSV file format for IPv4 or IPv6 Endpoints

```
1  1    ..10,textual description
2  1    ..11,
3  1    ..12,
4  1    ..13,
5  1    ..14,
```

The following table describes the details of the IP addresses to be imported in the CSV file format.

Format	Description
<IPv4 or IPv6 address>	Specifies the IP address to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (**,**) next to the entry and leave it.

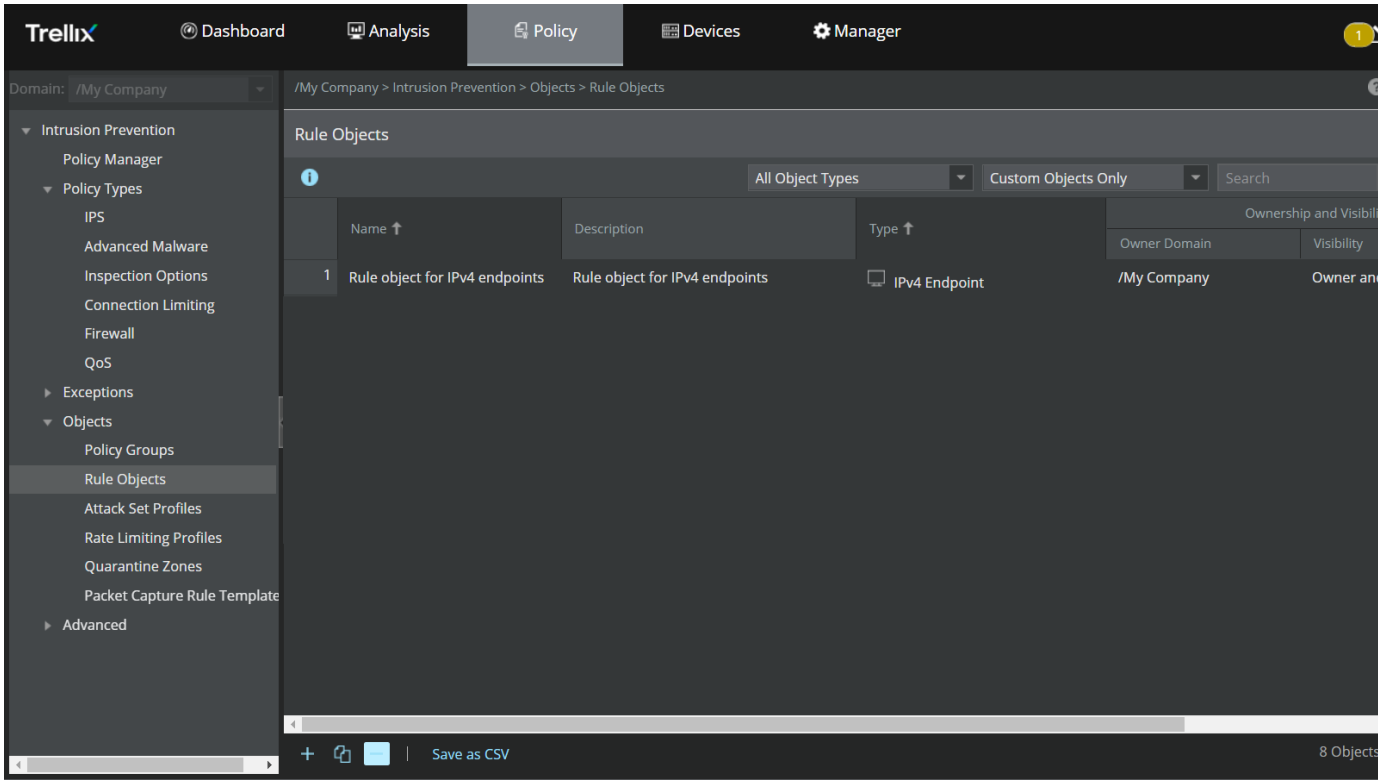
d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

NOTE

The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

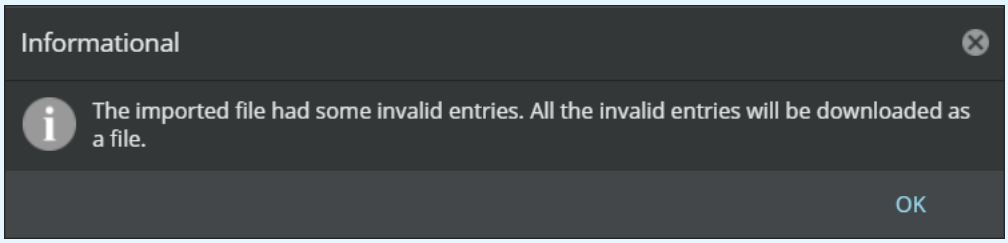
Figure 517. Rule object for IPv4/IPv6 endpoint successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 518. Information dialog-box for invalid entries

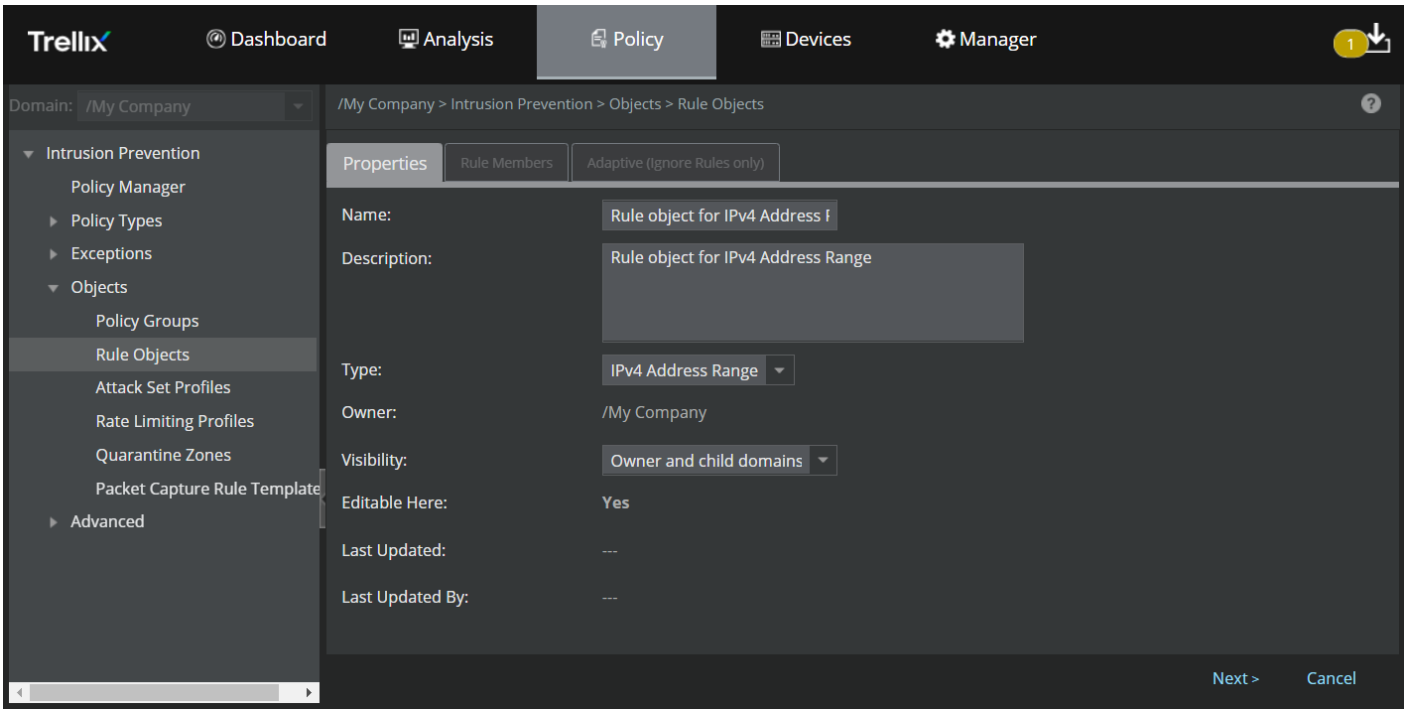


Add an IPv4 or IPv6 Address Range rule object

The steps to add **IPv4 Address Range** and **IPv6 Address Range** rule objects are identical. Follow these steps to add **IPv4 Address Range** or **IPv6 Address Range** rule objects:

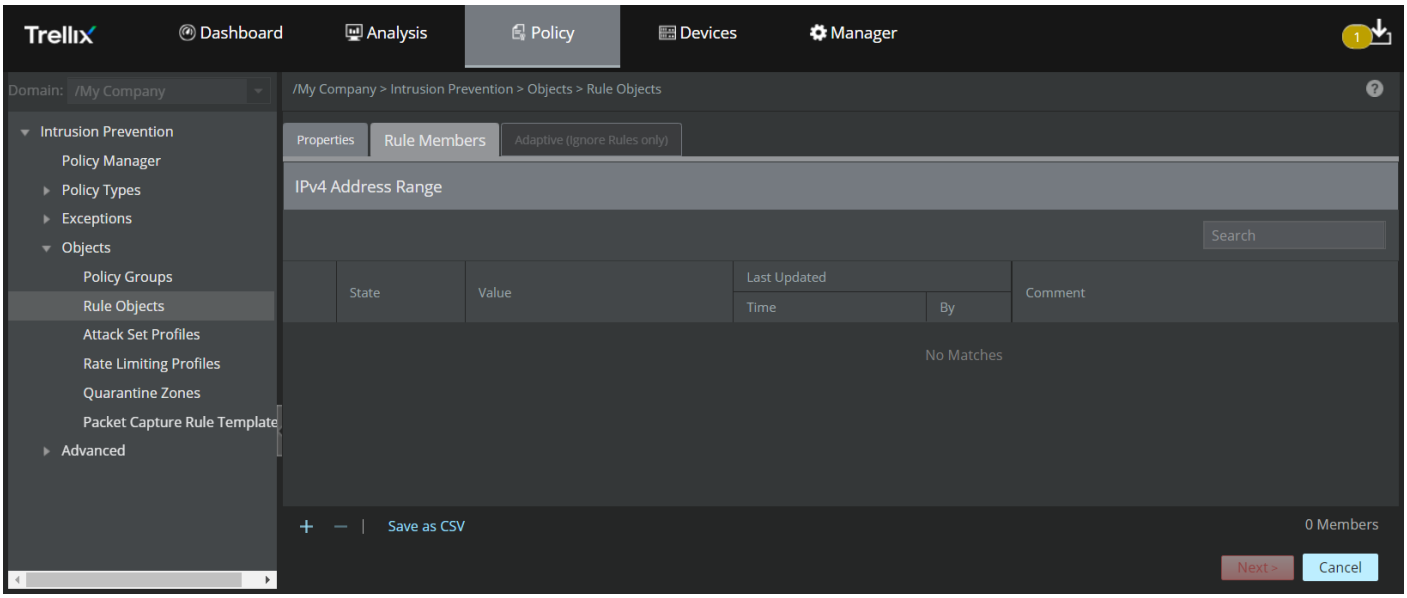
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Address Range** or **IPv6 Address Range** from the rule object **Type** drop-down, click **Next**.

Figure 519. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 520. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 63. Column details in the Rule Members tab - IP Address Range rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 address range based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 address range
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address range.
−	Click this icon to delete single or multiple IPv4 or IPv6 address ranges
Save as CSV	Click this icon to remove a rule object from the list

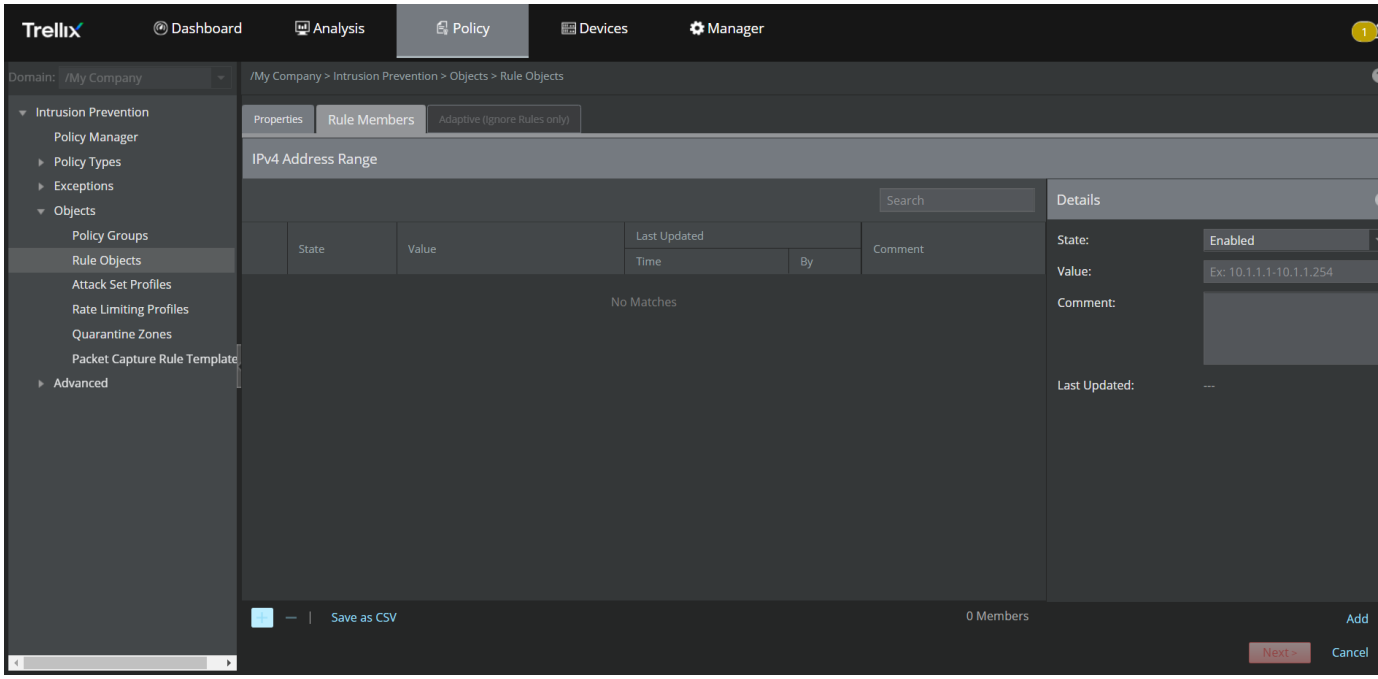
2. To add an IPv4 or IPv6 address range:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Address Range rule object].

      Select the **State**, enter a valid IPv4 or IPv6 starting and ending address range in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - Make sure to enter a hyphen between the starting and ending range (example: 10.1.1.1-10.1.1.25).
> - You can enter up to 20000 IPv4 or 20000 IPv6 address ranges in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 address ranges in any rule object.

Figure 521. Add individual IP addresses



3. Upon adding all the required IP addresses, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Rule Members** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values.
Resource to Customize	Select the resource to customize from the drop-down list. **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**.
Add	Click this button to add the IP address range to the **Customizations** list.
Search	Type the search criteria to search for a resource.
	Click this icon to remove an address range from the list.

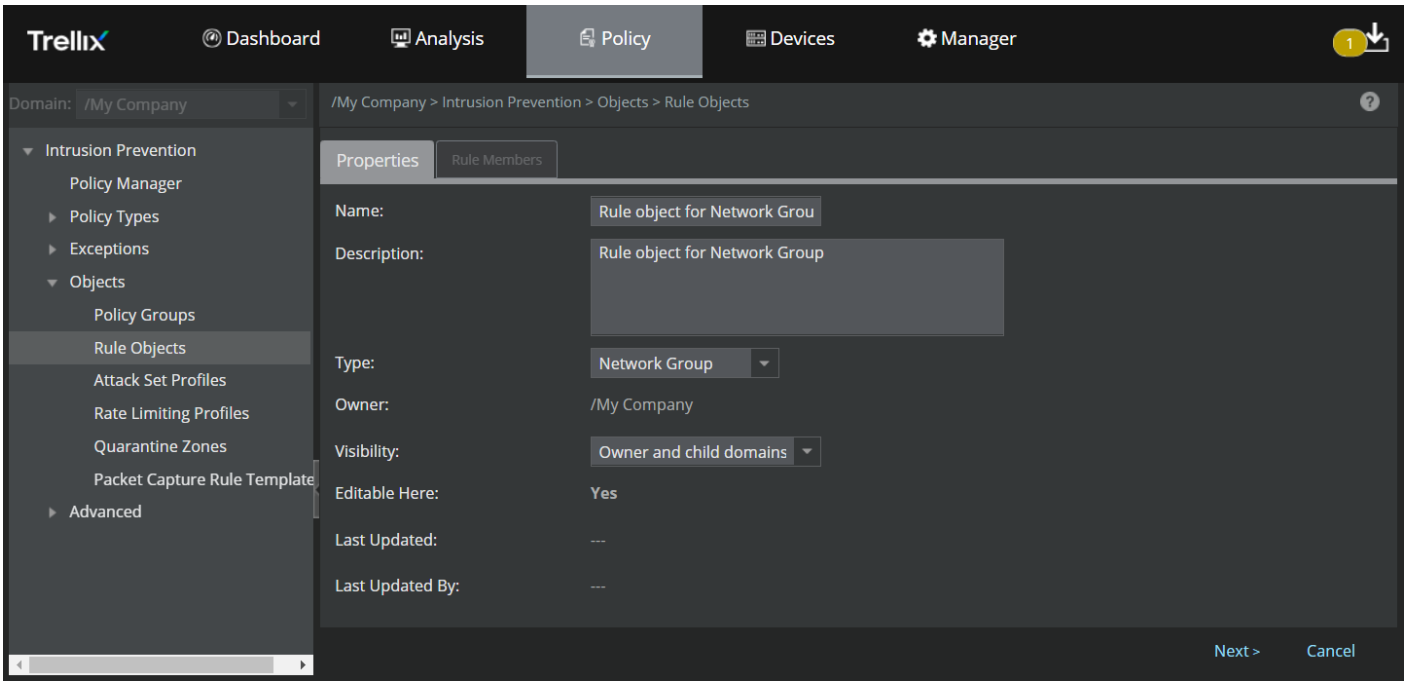
4. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

Add a Network Group rule object

Follow these steps to add a **Network Group** rule object:

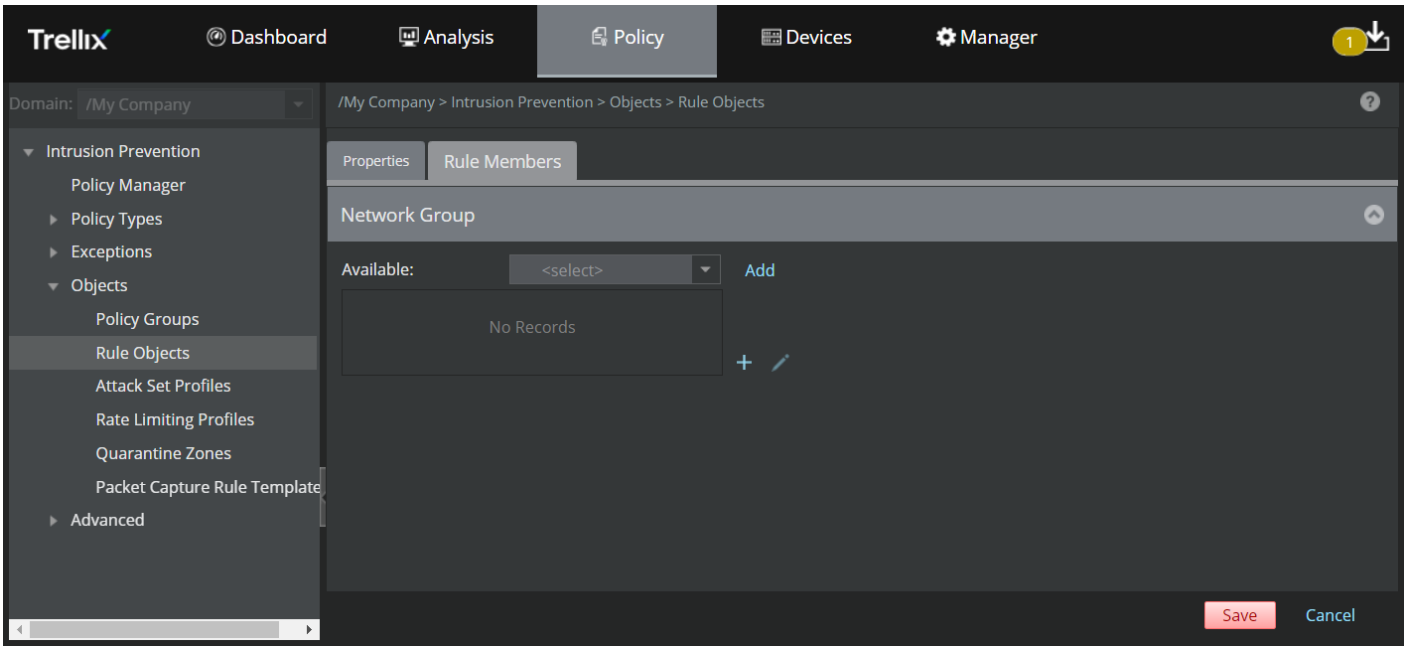
1. Upon specifying the options in the **Properties** tab and selecting **Network Group** from the rule object **Type** drop-down, click **Next**.

Figure 522. Create a Network Group rule object



The **Rule Members** tab is displayed.

Figure 523. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select the rule object from the **Available** drop down list.
Add	Click this button to add the rule object to the list.
	Click this icon to add a new rule object.
	Click this icon to edit the existing rule object.
	Click this icon to remove the rule object from the list.

2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

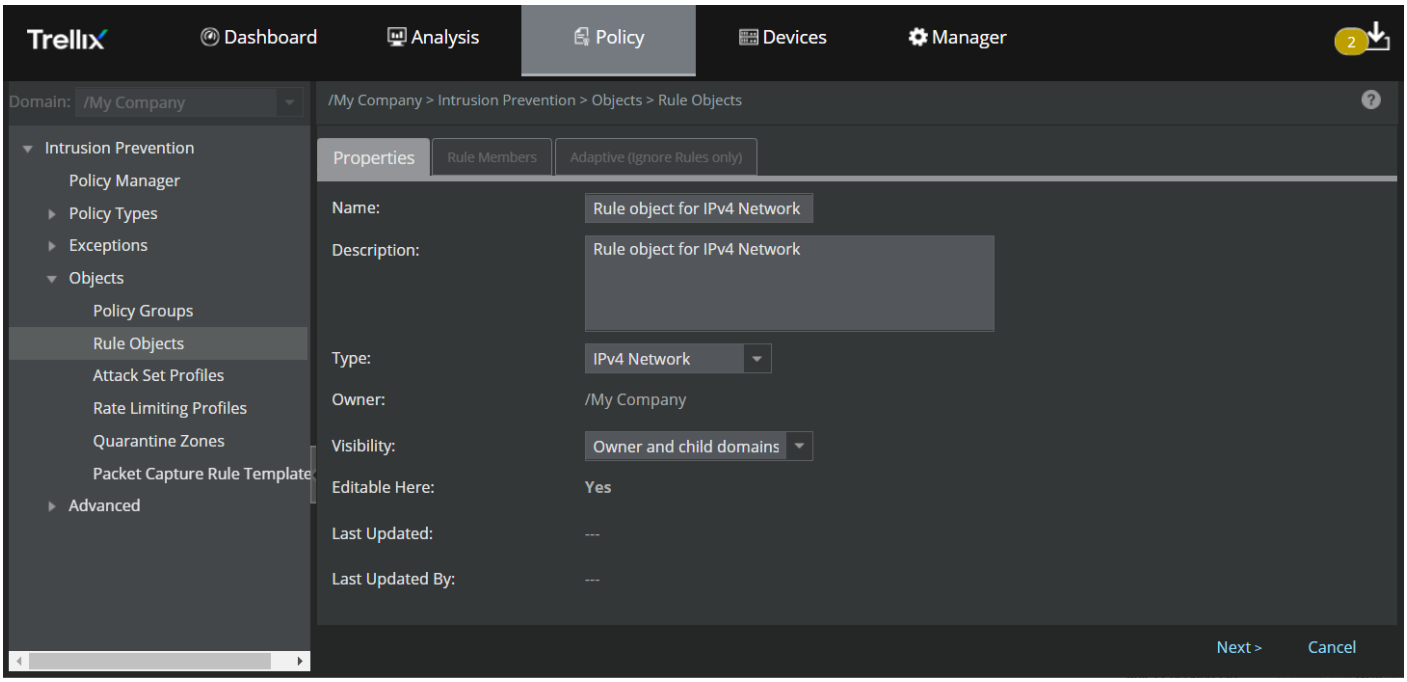
Add IPv4 Network and IPv6 Network rule objects

IPv6 Network is not supported for Quarantine. Also, only one IPv4 Network item per Rule Object is allowed for quarantine zone.

The steps to add **IPv4 Network** and **IPv6 Network** rule objects are identical. Follow these steps to add **IPv4 Network** or **IPv6 Network** rule objects:

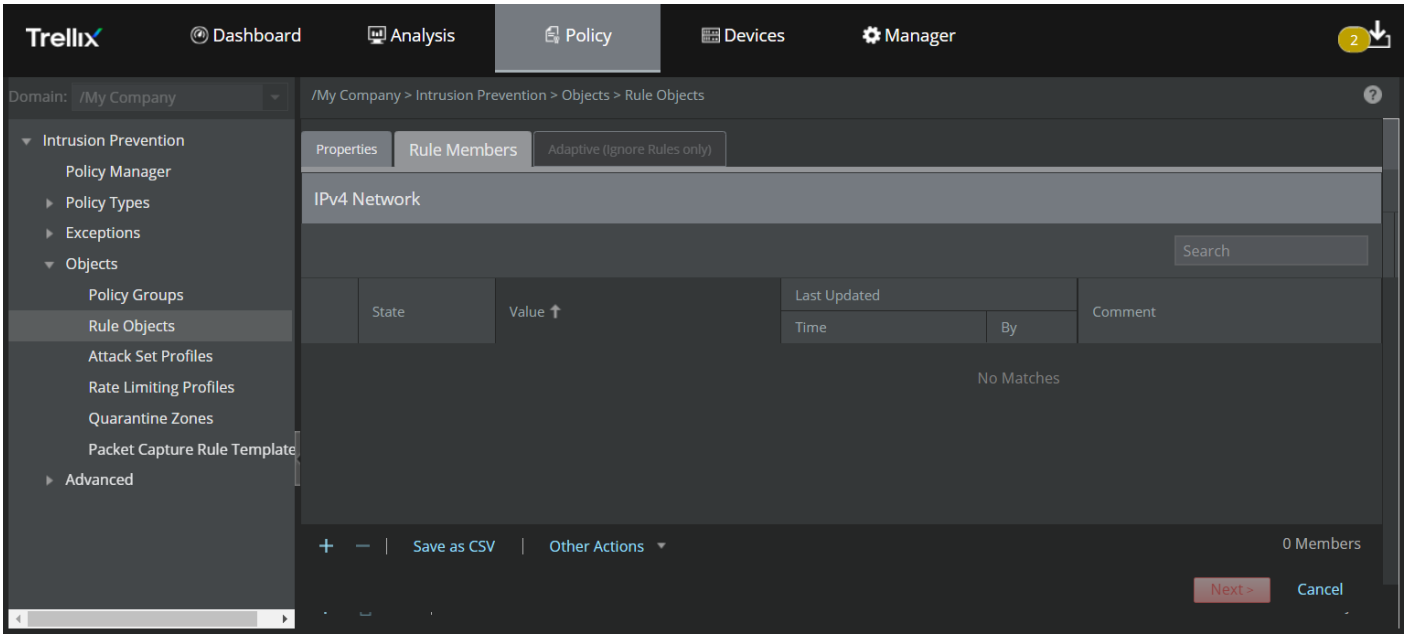
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Network** or **IPv6 Network** from the rule object **Type** drop-down, click **Next**.

Figure 524. Create an IPv4 Network or IPv6 Network rule object



The **Rule Members** tab is displayed.

Figure 525. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 64. Column details in the Rule Members tab - IP Network rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 CIDR block based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 CIDR blocks
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add a valid IPv4 or IPv6 CIDR block. For example, enter 172.16.200.0/24 for IPv4 Network, or 3003:0AB8::/48 for IPv6.
−	Click this icon to delete single or multiple IPv4 or IPv6 CIDR blocks
Save as CSV	Click this icon to remove a rule object from the list
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 CIDRs • **Export All** — Allows you to export all the CIDRs from the Manager to the local system

2. There are two ways to add the IP CIDR blocks — add individual IP CIDR block using the + icon or import a list of IP CIDR blocks from a CSV file using the Other Actions → **Import** option.

3. To add an individual IPv4 or IPv6 CIDR block:

   a. Click the + icon.

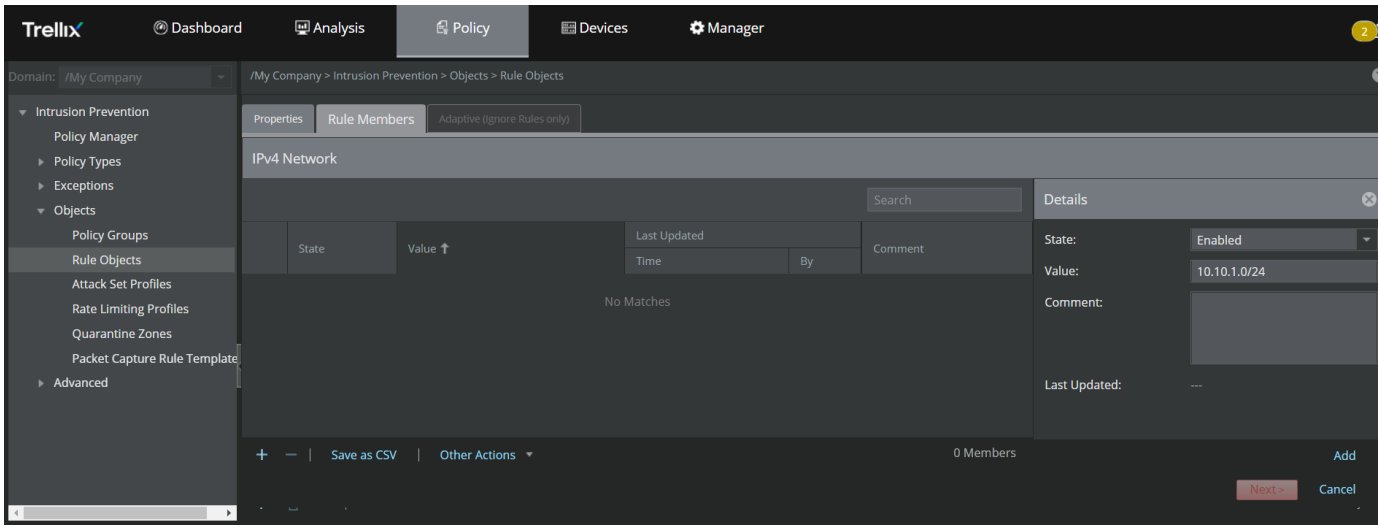
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

   For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Network rule object].

   Select the **State**, enter the IPv4 or IPv6 CIDR block in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - You can enter up to 140000 IPv4 or 140000 IPv6 CIDRs in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 CIDRs in any rule object.

Figure 526. Add individual IP CIDR block



   c. Upon adding all the required IP CIDR blocks, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values

Option	Definition
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add a CIDR block to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove a CIDR block from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of CIDR blocks from a CSV file using the **Import** option:

a. Click Other Actions → **Import**.

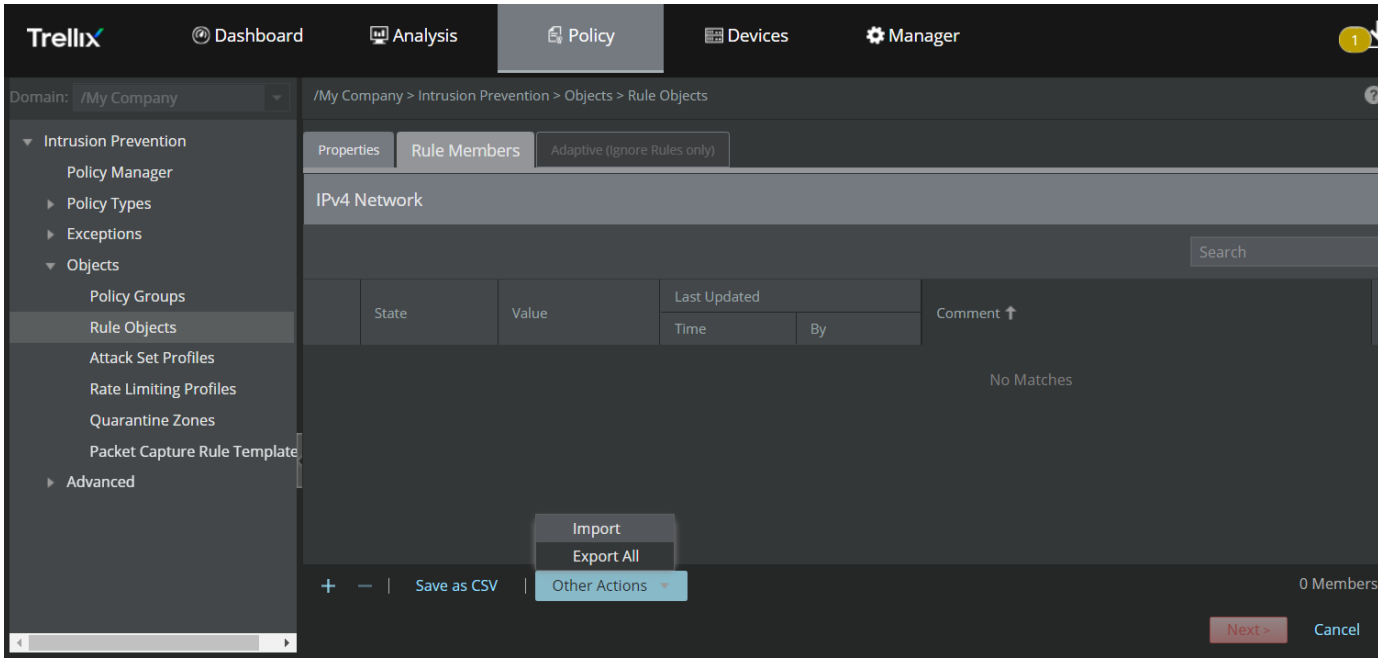
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10.

Figure 527. Import IP CIDRs from a CSV file

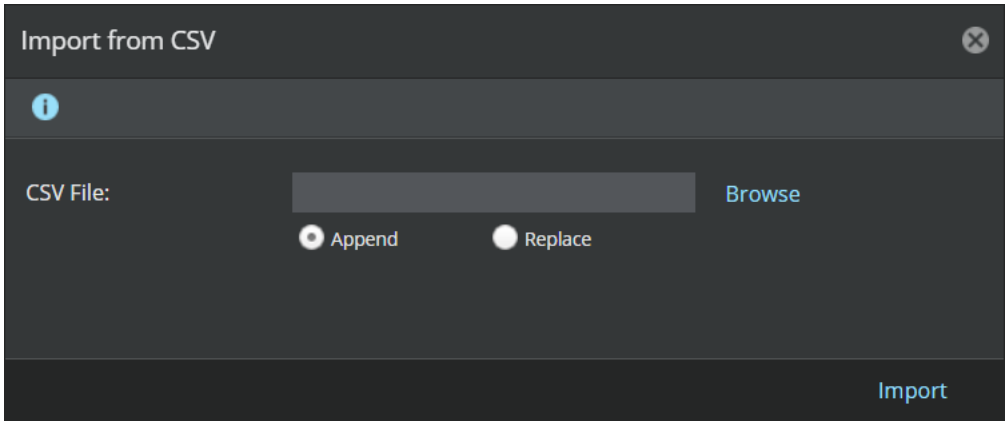


b. **Import from CSV** window appears. Use the **Append** option to add a new list of CIDR blocks or to append a list of CIDR block to an existing list. Use the **Replace** option to replace an existing list of CIDRs with a new list.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IPv4 or IPv6 CIDRs that you plan to import.

Figure 528. Import IP CIDRs from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 CIDR>,<Comment>

Example file format: 10.10.1.0/24,textual description.

The following is a sample for a CSV file with multiple IPv4 CIDRs:

Figure 529. CSV file format for IPv4 or IPv6 Networks

```
134.        .100/7,textual description
134.        .100/8,textual description
134.        .100/9,textual description
134.        .100/10,textual description
134.        .100/11,
134.        .100/12,
```

The following table describes the details of the IP CIDR blocks to be imported in the CSV file format.

Format	Description
<IPv4 or IPv6 CIDR>	Specifies the IPv4 or IPv6 CIDR to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (**,**) next to the entry and leave it.

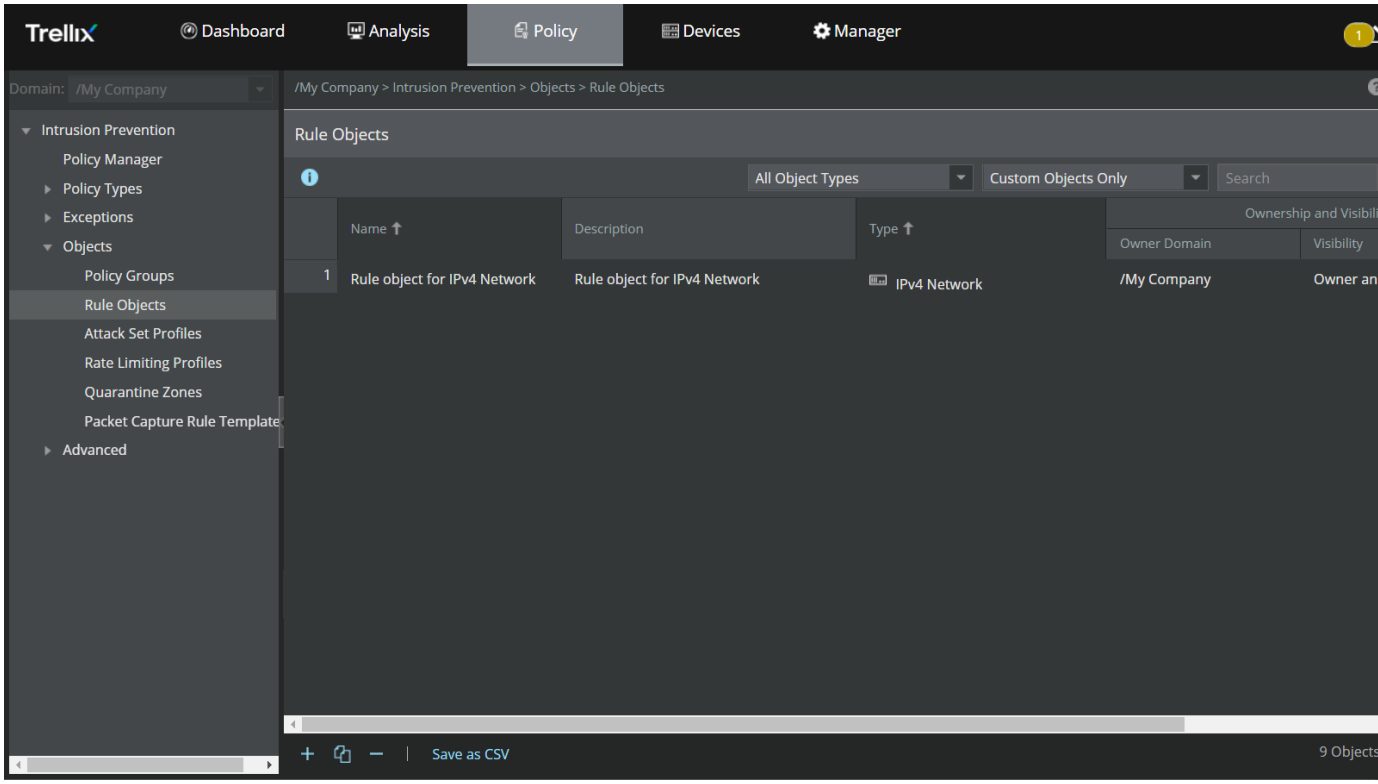
d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

NOTE

The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

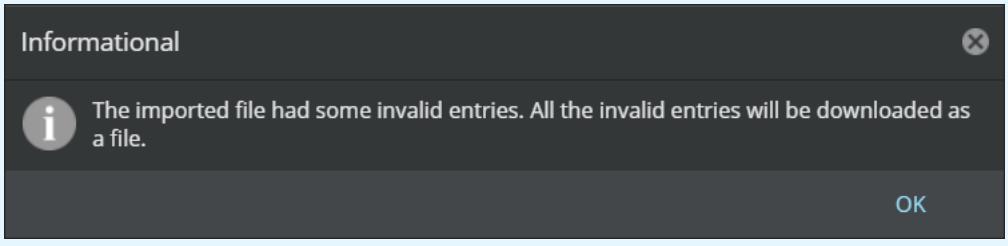
Figure 530. Rule object for IPv4/IPv6 network successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 531. Information dialog-box for invalid entries

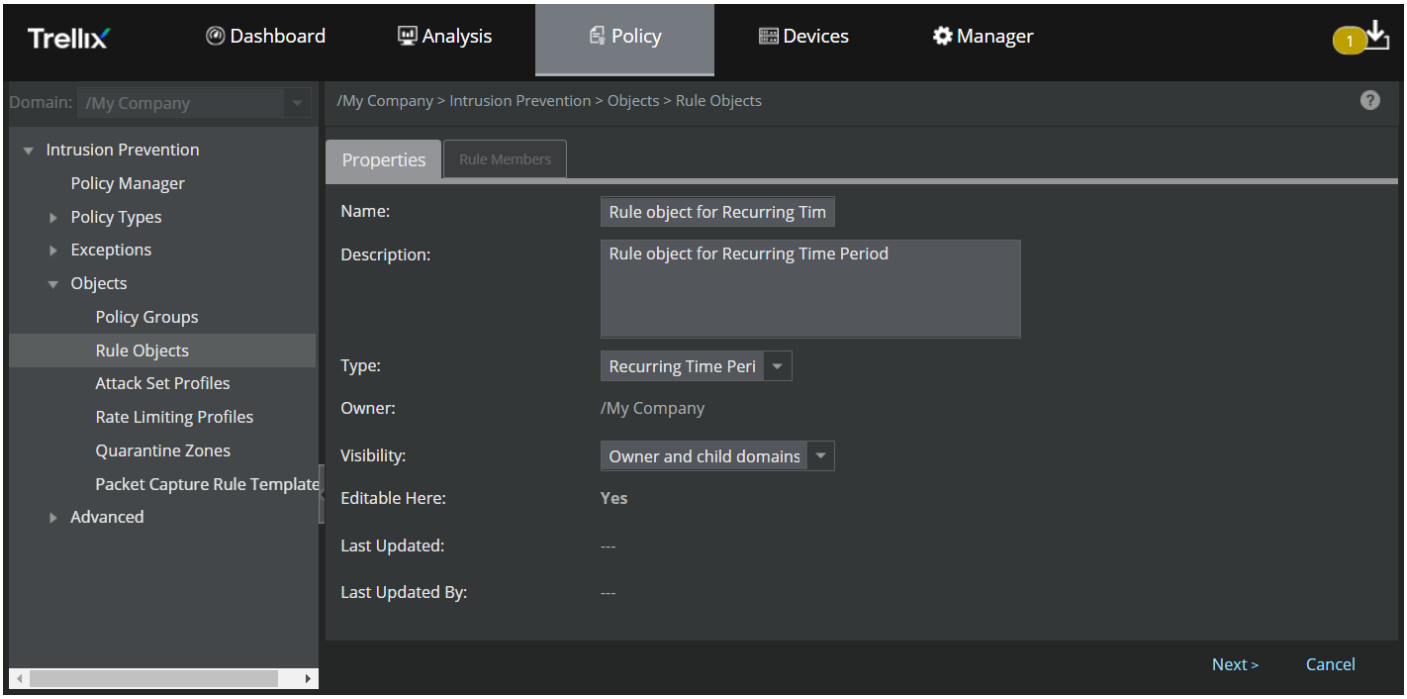


Add a Recurring Time Period rule object

Follow these steps to add **Recurring Time Period** rule object:

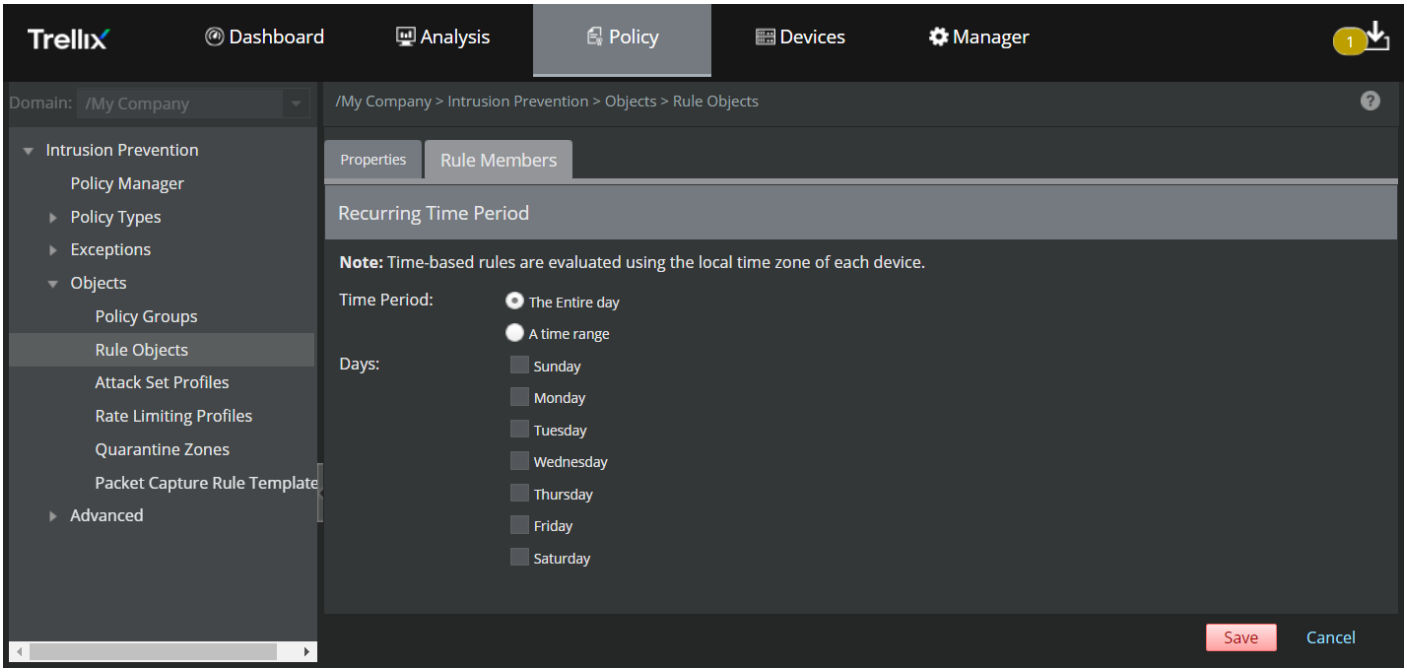
1. Upon specifying the options in the **Properties** tab and selecting **Recurring Time Period** from the rule object **Type** drop-down, click **Next**.

Figure 532. Create a Recurring Time Period rule object



The **Rule Members** tab is displayed.

Figure 533. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Time Period	Select the time when the Sensor must enforce the corresponding rule. Time-based rules are implemented using the local time zone of the corresponding Sensor. You can select the option **The Entire day** or **A time range** for a specific time period.
Time Range	To modify the hour or minute values, place the cursor on the **Time Range** field and type the hour value. Then, click on the drop-down list and select the relevant minute value. Also select the **to** range by selecting the value from the drop-down list.
Days	Select the days when the Sensor must enforce the corresponding rule. You must select at least one of the days.

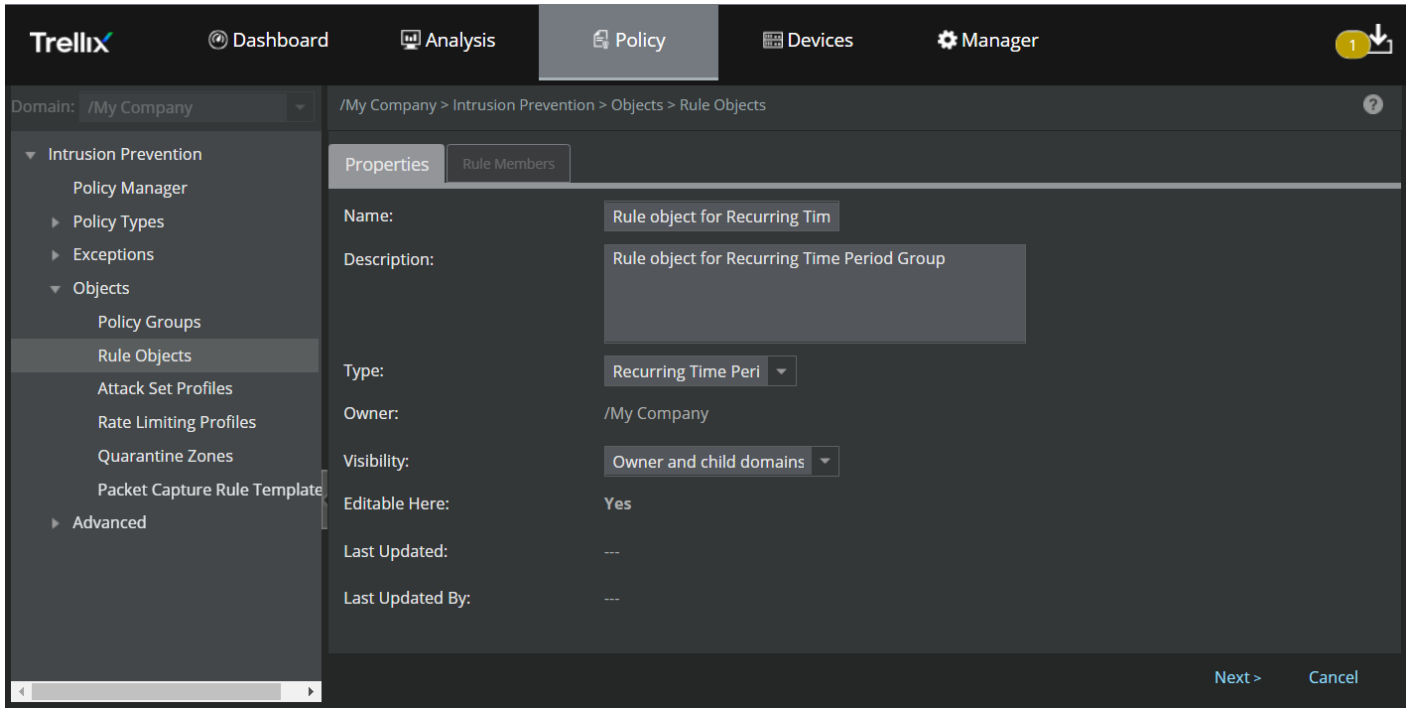
2. Based on the above options, you can select the **Time Period** and the **Days** when the Sensor must enforce the corresponding rule.
3. Click **Save**.

Add a Recurring Time Period Group rule object

Follow these steps to add **Recurring Time Period Group** rule object:

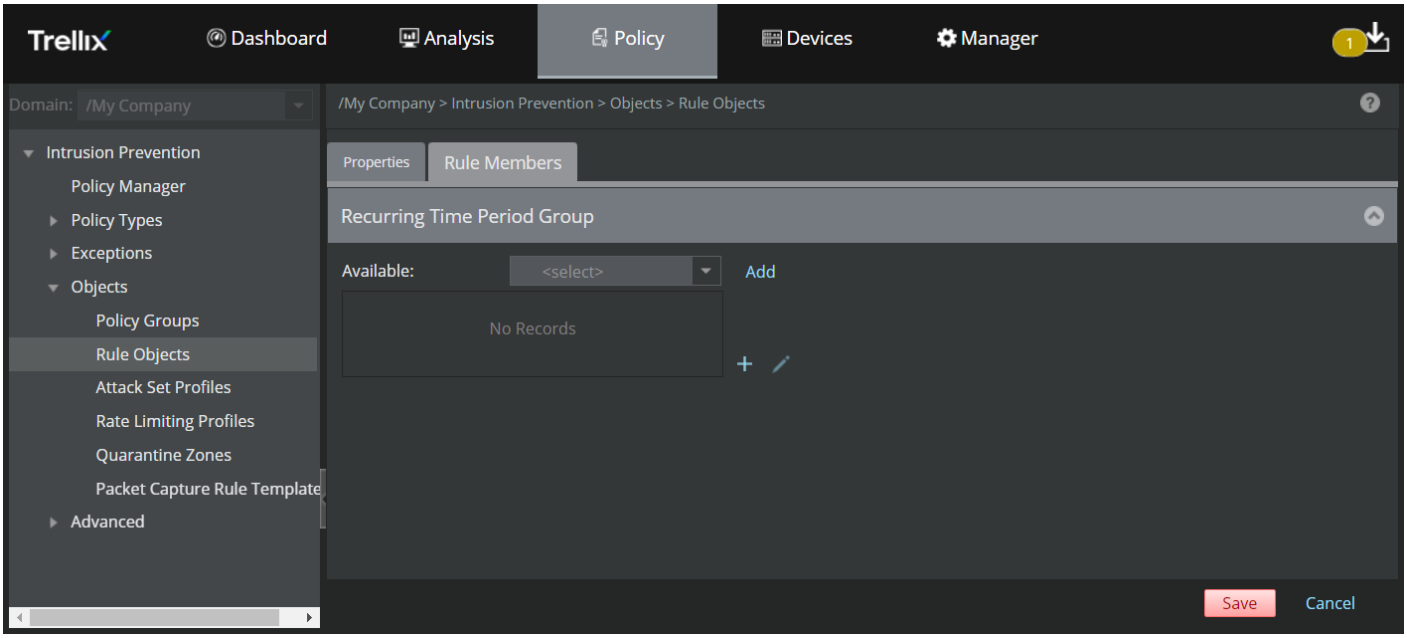
1. Upon specifying the options in the **Properties** tab and selecting **Recurring Time Period Group** from the rule object **Type** drop-down, click **Next**.

Figure 534. Create an Recurring Time Period Group rule object



The **Rule Members** tab is displayed.

Figure 535. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select an existing **Recurring Time Period Group** rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Members** list
	Click this icon to edit a rule member in the list
	Click this icon to add a new **Recurring Time Period Group** rule object
	Click this icon to remove a rule member from the list

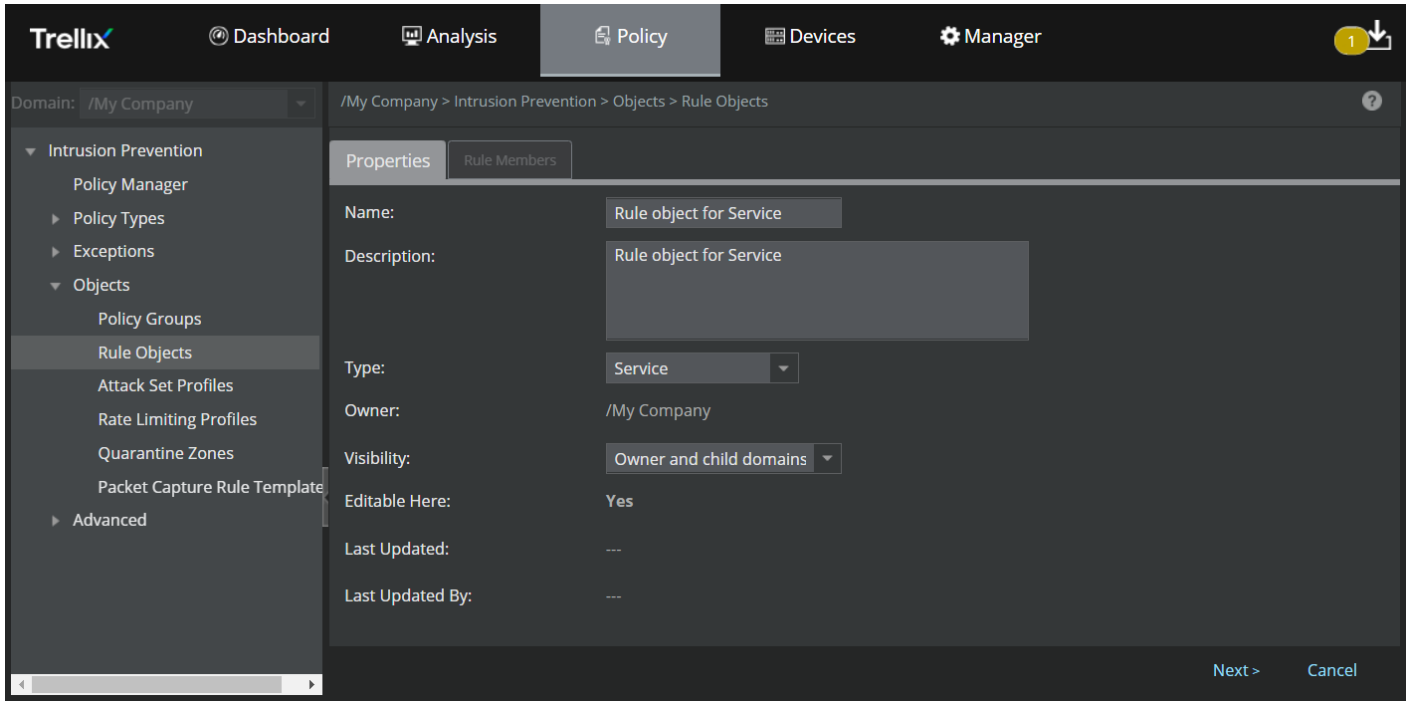
2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Add a Service rule object

Follow these steps to add **Service** rule object:

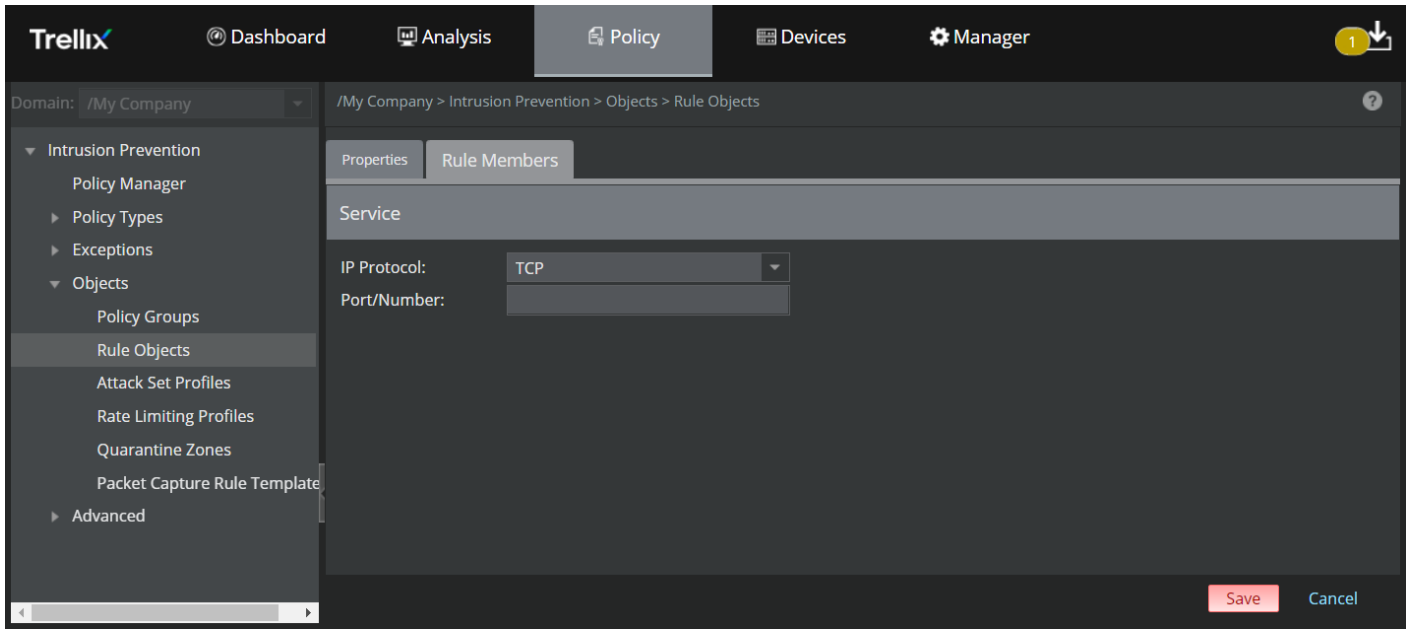
1. Upon specifying the options in the **Properties** tab and selecting **Service** from the rule object **Type** drop-down, click **Next**.

Figure 536. Create a Recurring Time Period rule object



The **Rule Members** tab is displayed.

Figure 537. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
IP Protocol	Select the required protocol from the drop-down list. The options are **TCP**, **UDP** and **Protocol Number**.
Port/Number	If you select **TCP** or **UDP** as the **IP Protocol**, you can optionally enter a port number between from 1 to 65534. Alternatively, you can specify a protocol number between from 0 to 255.

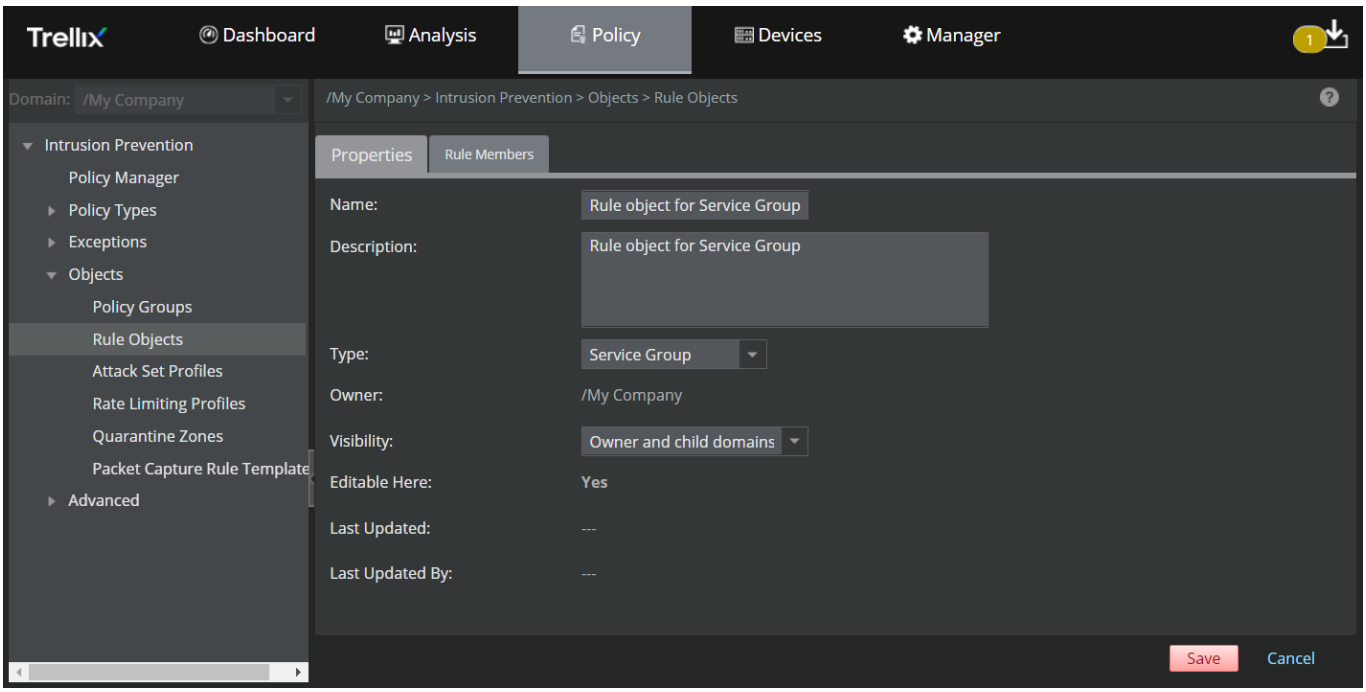
2. Based on the above options, you can select the **IP Protocol** and specify a **Port/Number**.
3. Click **Save**.

Add a Service Group rule object

Follow these steps to add **Service Group** rule object:

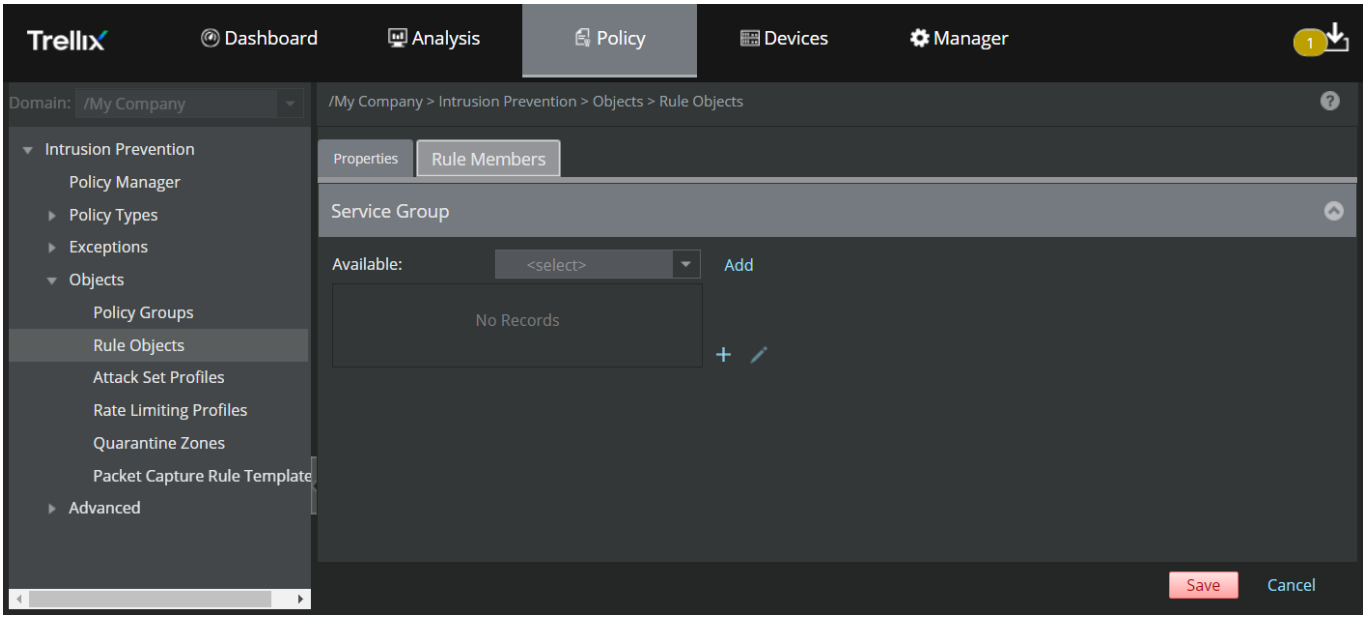
1. Upon specifying the options in the **Properties** tab and selecting **Service Group** from the rule object **Type** drop-down, click **Next**.

Figure 538. Create an Service Group rule object



The **Rule Members** tab is displayed.

Figure 539. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select a pre-defined service or an existing **Service** rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Members** list
	Click this icon to add a new **Service** rule object
	Click this icon to edit a rule member in the list
	Click this icon to remove a rule member from the list

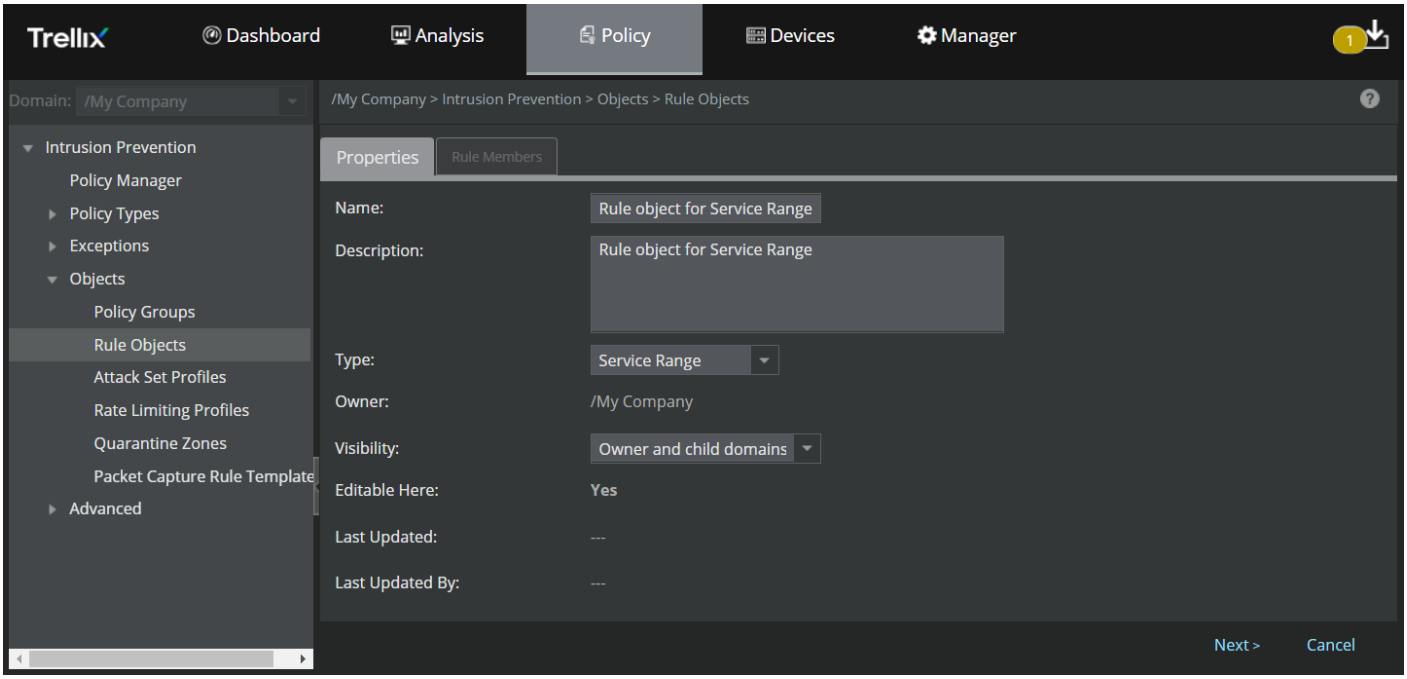
2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Add a Service Range rule object

Follow these steps to add **Service Range** rule object:

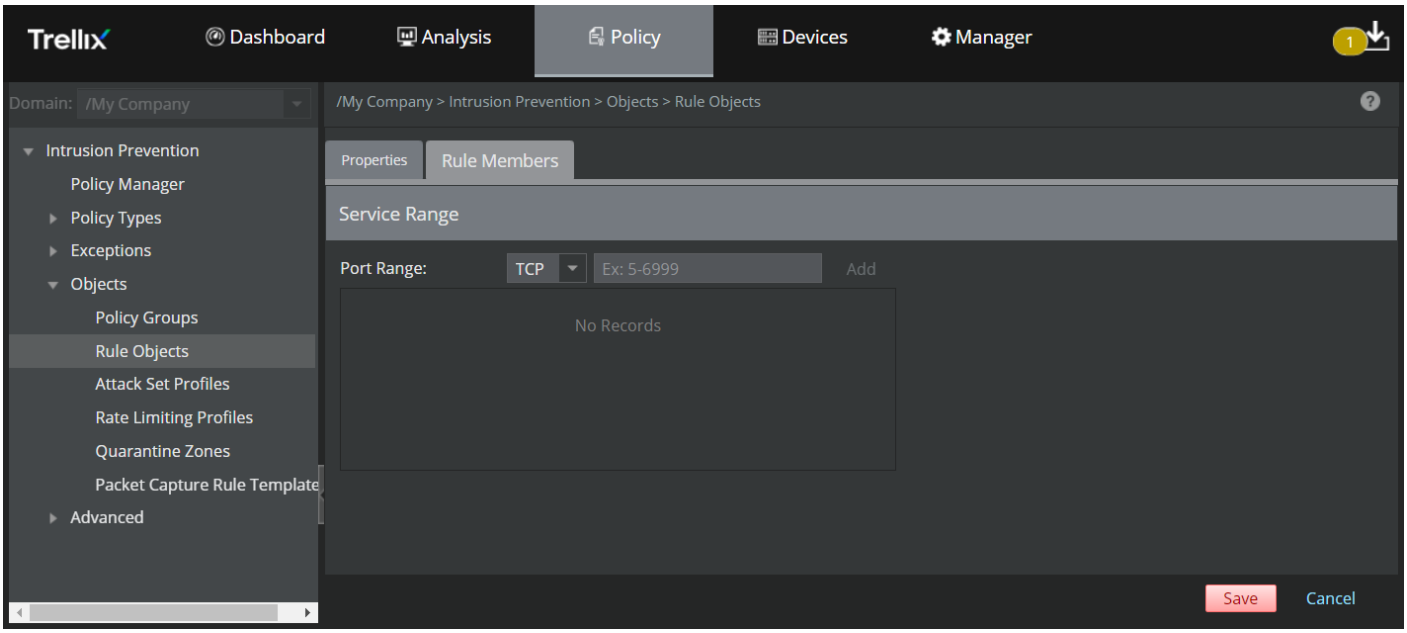
1. Upon specifying the options in the **Properties** tab and selecting **Service Range** from the rule object **Type** drop-down, click **Next**.

Figure 540. Create a Service Range rule object



The **Rule Members** tab is displayed.

Figure 541. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Port Range	Select **TCP** or **UDP** from the drop-down list. Enter the beginning and end port range (Example: 1-65534) in the text box. **NOTE** Ensure to enter a hyphen between the beginning and end port range.
Add	Click this icon to add the Port range to the list.
	Click this icon to remove the Port range from the list.

2. Based on the above options, you can assign up to **10** TCP and UDP port ranges.
3. Click **Save**.

Clone a rule object

You can clone custom rule objects.

- You cannot clone a default rule object except for Network.
- You can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule objects for the selected admin domain are listed.
4. Locate the Rule Object that you want to clone.

   TIP

   You can use the search function to more easily find the rule object.
5. Select the rule object and click  .
6. Make the required changes and click **Save**.

Modify a custom rule object

You can modify custom rule objects.

- You cannot modify or delete a default rule object.
- You can modify or delete a custom rule object only at the admin domain where it was created. If required, you can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.
- You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.
4. Locate the rule object that you want to modify.
   - You can use the search function to easily find the rule object.
   - Make sure the **Editable here** column displays **Yes** for the rule object you want to modify. If the **Editable** column displays **No**, the rule object belongs to a parent admin domain.
5. Double-click the rule object.
6. Make the required changes and click **Save**.

NOTE

If the rule object that you modified is part of a policy that is in use, you must do a configuration update to the Sensor for the changes to take effect.

Delete a custom rule object

Delete a custom rule object that you no longer use. You can delete a custom rule object only at the admin domain where it was created.

- You cannot delete a default rule object.
- You cannot delete a rule object that is used in a Firewall policy, QoS policy or, in a group rule object.
- You can delete a rule object only at the admin domain where it was created.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule objects for the selected admin domain are listed.
4. Locate the Rule Object that you want to modify.
   - You can use the search function to easily find the rule object.
   - Make sure the **Editable here** column displays **Yes** for the rule object you want to delete. If the **Editable here** column displays **No**, the rule object belongs to a parent admin domain.
5. Select the rule object and click −. Then click **Yes** to confirm deletion.

> **NOTE**
>
> To delete rule objects in bulk, press **Shift** key (for continuous selection) or press **Ctrl** key (for discontinuous selection) and then select the rule objects. The selected items are highlighted. Click − and then click **Yes** to confirm deletion.

Automatic deployment of Firewall Rule Objects

This option allows you to automate Firewall Rule Objects deployments to applicable Sensors when there are any changes made in the Firewall Rule Objects. These changes include addition, deletion or modification of IPv4 and IPv6 addresses and CIDRs.

Automatic deployment of Firewall Rule Objects is disabled by default. To enable automatic deployment:

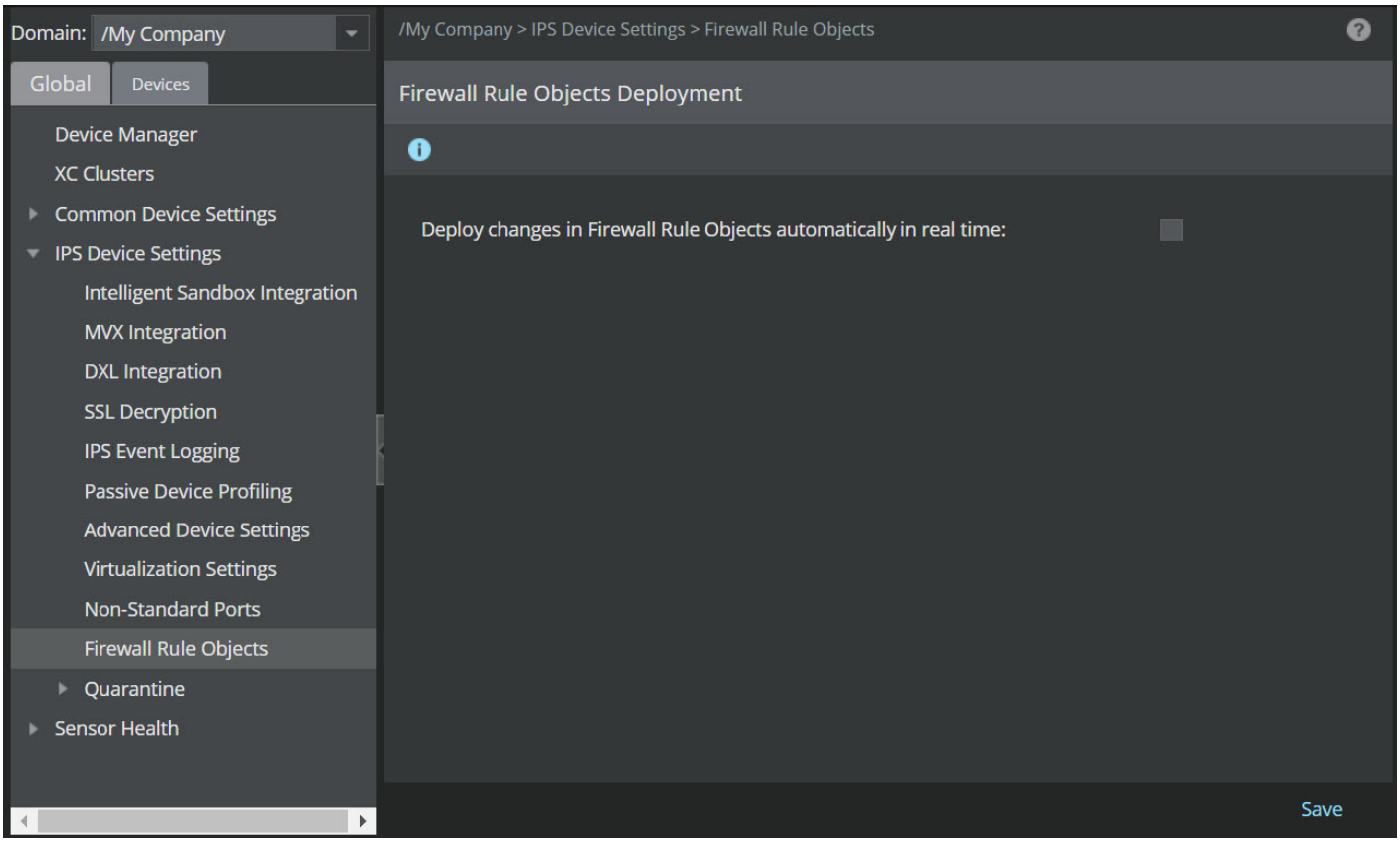
1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **Firewall Rule Objects**.
2. **Firewall Rule Objects Deployment** page appears. Select the **Deploy changes in Firewall Rule Objects automatically in real time** checkbox to enable automatic Firewall Rule Objects deployment to applicable Sensors in real-time.

> **NOTE**
>
> This is a global setting across the Manager which is applicable to all the domains.

> **NOTE**
>
> Automatic deployments are applicable only if the rule object being modified is of the following type: IPv4 Endpoint, IPv4 Network, IPv6 Endpoint, or IPv6 Network.

> **NOTE**
>
> Automatic deployments are applicable only if the rule object being modified is used in a Firewall policy and assigned to a Sensor running on software version which is later than 10.1.5.153.

Figure 542. Enable automatic deployment of Firewall rule objects



Configure the DNS server details

You must configure the DNS server details in the Manager, if you have Firewall, QoS, or Quarantine Zone rules that use Host DNS Name rule object. The Sensors use these DNS server details to resolve the Host DNS Name rule objects to IP addresses. This also applies to rules using Network Group rule objects, which in turn use a Host DNS Name rule object.

In addition to what is mentioned above, NS-series Sensors use the DNS server details to resolve the host name of the syslog server used for Firewall or Quarantine. You can configure the Sensor to forward the details of matched Firewall or Quarantine Zone rules to a syslog server. As part of this configuration, you define the syslog-server details in the Manager. If you provide the host name of the syslog server, then the Sensor uses the DNS server to resolve the syslog server's host name.

IMPORTANT

The Sensor uses only UDP and never falls back to TCP for DNS queries even if the DNS server forces for TCP.

You can configure the DNS server details at a domain level or at a device level. The DNS server at the admin domain, by default, applies to the following:

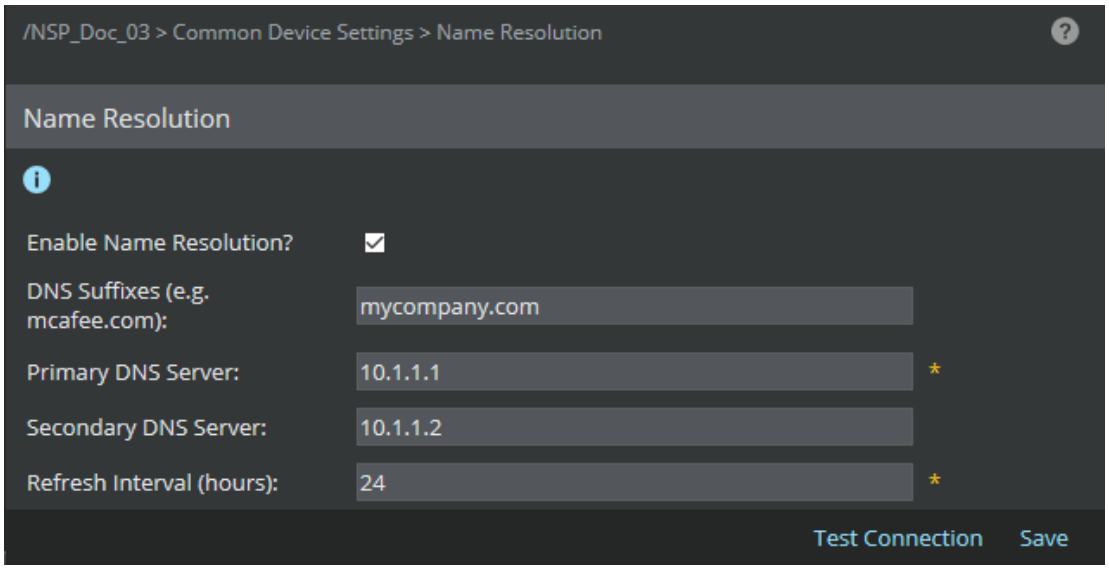
- All the corresponding child domains
- All the Sensors in this domain. This includes any interfaces delegated to other domains.

- All the Sensors in the corresponding child domains

If required, you can override the DNS server details at a child admin domain level and also at each Sensor level.

1. To configure the DNS server details for an admin domain:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. Select Global → Common Device Settings → **Name Resolution.**

Figure 543. DNS window



2. To configure the DNS server details for a Sensor:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. On the left pane, click the **Devices** tab.
   d. Select the device from the **Device** drop-down list.
   e. Select Setup → **Name Resolution.**
   f. Deselect **Inherit Settings?** to override the settings of the parent domain.
3. Enter the DNS information in the corresponding fields.

Option	Definition
Enable Name Resolution?	Select to display the fields in the **Name Resolution** page. **NOTE** If you deselect this field and click **Save**, the DNS details that you had saved earlier is lost.

Option	Definition
DNS Suffixes	You can enter multiple values separated by a space. The Sensor uses these suffixes, in the same order, to resolve non-qualified DNS host names in your Firewall rules. Consider that the DNS host name in your Firewall rule is “host1” and the DNS suffixes are “mycompany.com” and “mycompany.org”. To resolve this host name, the Sensor first tries host1.mycompany.com. If this fails, it tries host1.mycompany.org.
Primary DNS Server	Enter the IPv4 or IPv6 address of the DNS server that the Sensor must contact first.
Secondary DNS Server	Optionally, enter the IPv4 or IPv6 address of a secondary DNS server. If the primary DNS server is unreachable, the Sensor communicates with the secondary DNS server.
Refresh Interval	If you are configuring the details for an admin domain, then enter a value between 24 and 9999. Though this field is applicable only to NTBA, you must enter a value when configuring the details for an admin domain.
Test Connection	Click this button to check the connectivity to the DNS Server. The status of the connectivity test is displayed in the **Name Resolution** page.
Save	Saves the DNS server details in the Manager database. **TIP** To resolve the Host DNS Name rule objects, the Sensor management port must be able to connect to **Save** the specified DNS servers. So, to be sure, ping the DNS servers from the Sensor CLI.

4. Perform a configuration update to the relevant Sensors.

NOTE

If the Sensor is unable to communicate with a DNS server, a fault of severity **Warning** is displayed on the **Faults** tab in **Logs** page.

Configure the time zone

You need to select a time zone in the Manager if you have any Firewall or QoS rules that involve a time-based rule object. The time-based rule objects are Finite Time Period, Recurring Time Period, and Recurring Time Period Group. Time-based rules are implemented using the local time zone of the corresponding Sensor. By default, the time on the Sensor is set to the Greenwich time zone (GMT +00:00).

The Manager displays the alerts generated with respect to the time zone configured for the Manager. For example, consider the Sensor to be in the GMT-08 time zone, and the Manager in the GMT+5:30 time zone. An alert is generated from the Sensor at 11 AM (in the GMT-08 time zone), the Manager displays the time of the alert as 12:30 AM (in the GMT+5:30 time zone). A time based rule has to be configured based on the Sensor time zone, but the alert generated is displayed with reference to the time zone configured for the Manager.

You can configure the time zone at an domain level or at a device level. The time zone at the admin domain, by default, applies to:

- All the corresponding child admin domains.
- All the Sensors in this domain. This includes any interfaces delegated to other domains.
- All the Sensors in the corresponding child admin domains.

If required, you can override the time zone at a child admin domain level and also at each Sensor level.

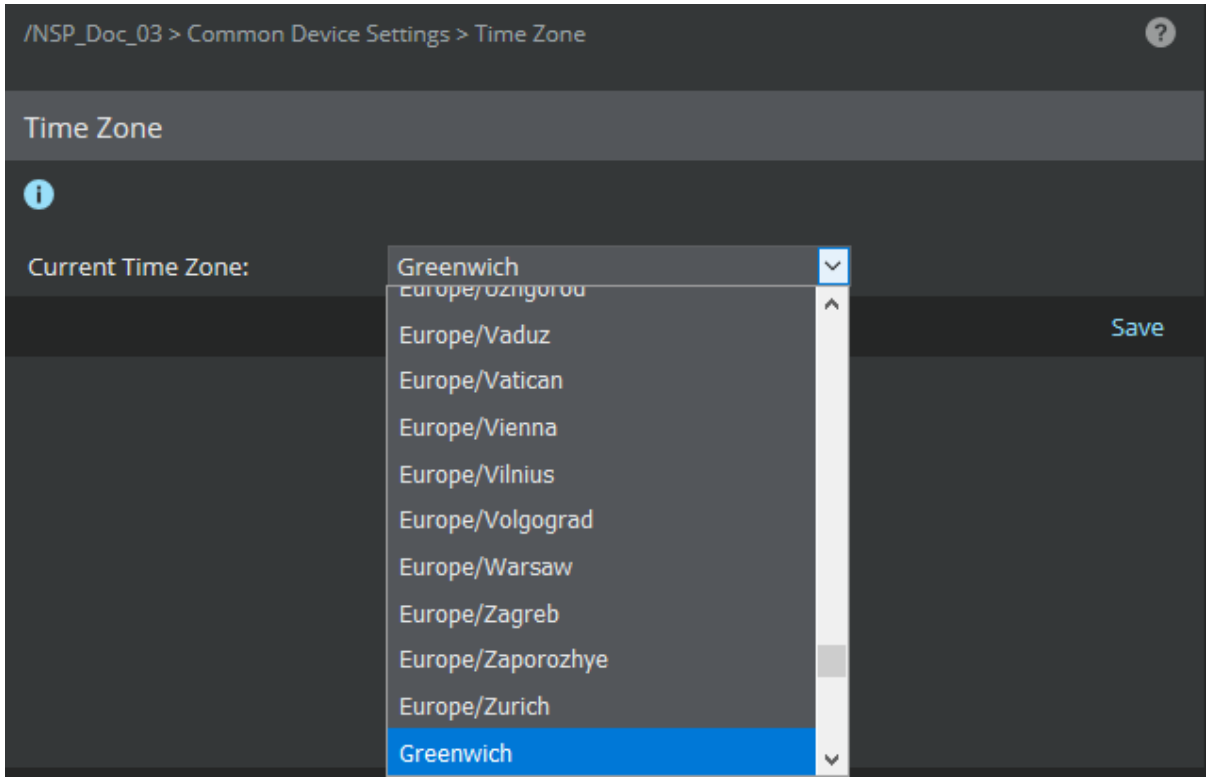
IMPORTANT

When you delegate Sensor ports to a child admin domain level, for those ports only the Sensor's time zone will apply and not the child admin domain's time zone.

When you select a time zone, Sensors interpret the time-based rule objects based on the selected time zone. They also factor in daylight savings time, if applicable.

1. To configure the time zone for an admin domain:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. Select Global → Common Device Settings → **Time Zone.**
2. To configure the time zone for a Sensor:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. On the left pane, click the **Devices** tab.
   d. Select the device from the **Device** drop-down list.
   e. Select Setup → **Time Zone.**
   f. Deselect **Inherit Settings?** to override the settings of the parent domain.
3. Select a time zone from the **Current Time Zone** drop-down.

Figure 544. Time Zone configuration



4. Click **Save.**
5. Perform a configuration update to the relevant Sensors.

   The selected time zone is applied to those Sensors.

Additional configurations for Kerberos snooping

If you require the Manager to verify the AD credentials from the Kerberos traffic or from the Guest Portal, you must configure the details of the corresponding AD and Trusted Domain Controllers.

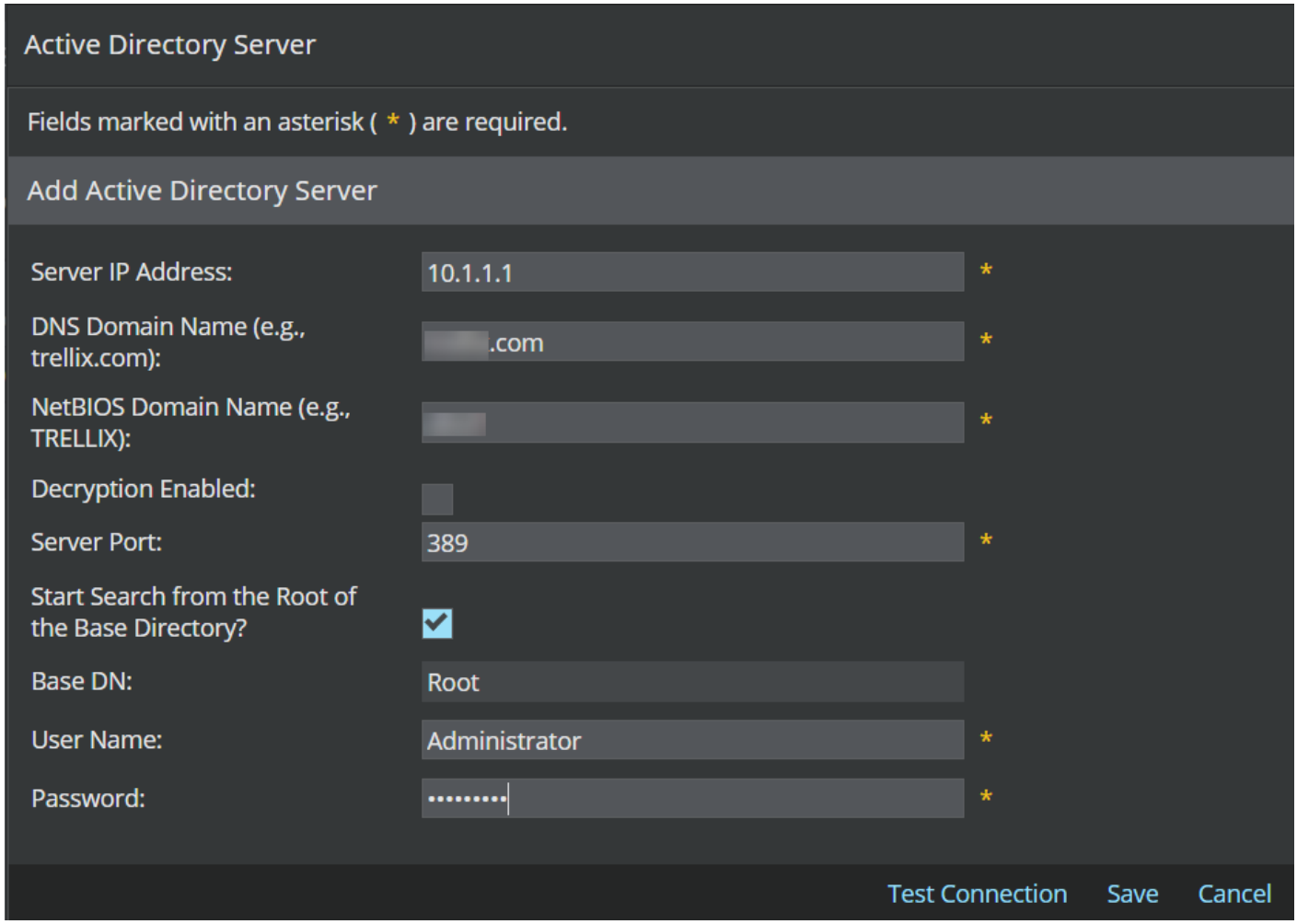
NOTE

When you modify the AD and Trusted Domain Controller settings, be aware that they apply to Firewall and QoS.

Add Active Directory servers

1. Go to, Manager → <Admin Domain Name> → Setup → Intrusion Prevention → **Active Directory Servers**.
2. Click +.

Figure 545. Add an Active Directory Server



NOTE

When the **Active Directory Servers** tab is accessed from child admin domains, the **Inherit Settings?** option is available. The + button is visible only if you deselect **Inherit Settings?**.

3. In **Add Active Directory Server** window, enter the AD server details in the appropriate fields:

Option	Definition
Server IP Address	Enter the IPv4 IP address of the Active Directory server.
DNS Domain Name	Enter the Active Directory domain name, like Trellix.com.
NetBIOS Domain Name	Enter the NetBIOS domain name of the Active Directory; for example, Trellix.

Option	Definition
Decryption Enabled	Select this option if you want to enable SSL connection for secure data communication.
Server Port	The Active Directory server port. If you select **Decryption Enabled**, the port automatically changes to the default value, 636. Else the default value is 389.
Start Search from the Root of the Base Directory?	Select this option if you want Trellix IPS to check user information from the root node of the Active Directory tree. When you select this option, the value of the next field **Base DN** is displayed as **Root**, by default.
Base DN	Base DN represents the intermediate node name in the Active Directory tree. If you want Trellix IPS to check user information from an intermediate node in the Active Directory tree, enter the corresponding node name in Base DN.
User Name	Active Directory login name for the domain.
Password	Password for the Active Directory login.
Test Connection	Click to test whether the connection with the configured Active Directory Server is working fine. If the connection is successful, a message is displayed for the same.
Save	Saves the configuration in the Manager database. The Manager attempts to verify the details that you provided before creating the record. Even if the Manager is unable to verify the details currently, you can go ahead and create the record. The added Server is listed in the **Active Directory Servers** list.

Notes:

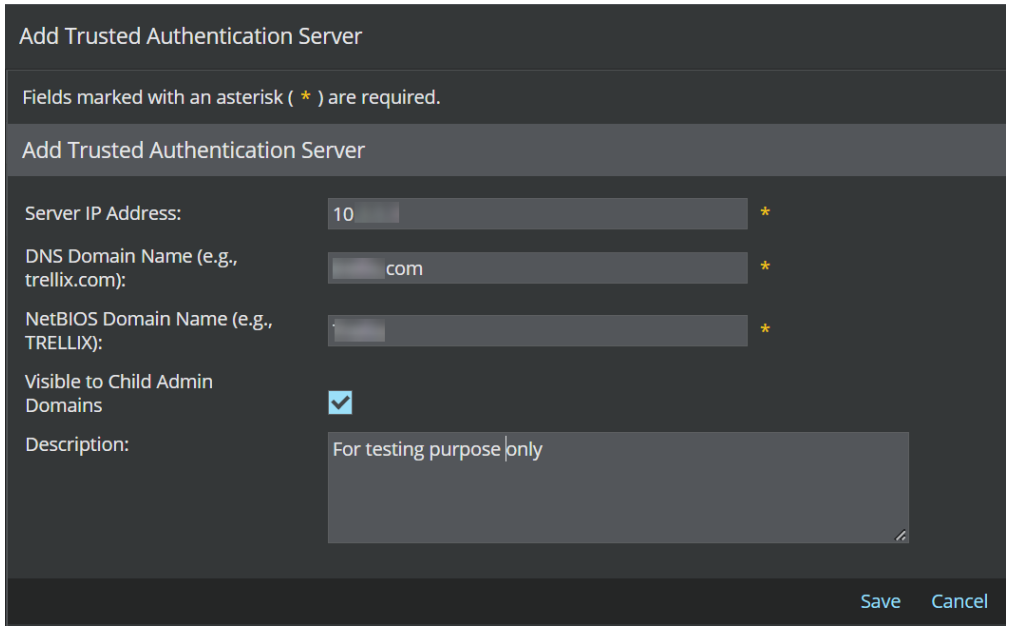
- In **Active Directory Servers** list, if the configuration needs to be inherited to the child admin domains, you can optionally check **Make Settings Visible to Child Admin Domains?** option.
- You are prompted to add the Active Directory server that you created to the list of trusted domain controllers automatically.
- If you configure multiple Active Directory servers, the Manager considers them in a top-down fashion. If two servers from the same domain are listed, the second is only consulted if the one above it cannot be reached.

Add Trusted Domain Controllers

When you add the Active Directory servers for an admin domain, you are prompted to automatically create the Trusted Domain Controllers using the same information. If you have done so, you can just verify the list of Trusted Domain Controllers.

1. Go to, Manager → <Admin Domain Name> → Setup → Intrusion Prevention → **Trusted Domain Controllers**.
2. Click  .

Figure 546. Add Trusted Domain Controllers



3. In the **Add Trusted Authentication Server** window, enter the Trusted Domain Controller details in the appropriate fields.

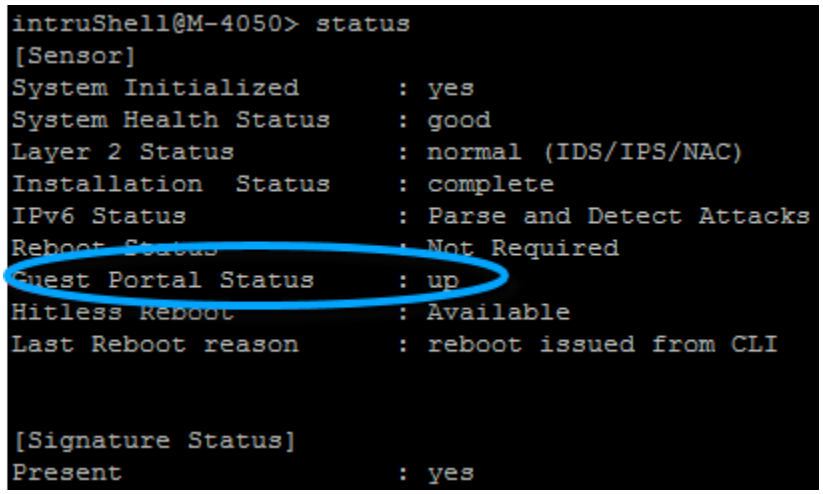
Option	Definition
Server IP Address	Enter the IPv4 IP address of the Active Directory server.
DNS Domain Name	Enter the Active Directory domain name, like Trellix.com.
NetBIOS Domain Name	Enter the NetBIOS domain name of the Active Directory; for example, Trellix.
Visible to Child Admin Domain	Select if the configuration needs to be inherited by the child admin domains.
Description	Optionally enter additional information about the Trusted Domain Controller.
Save	Saves the configuration in the Manager database.
Cancel	Clears the details you have entered in the **Add Trusted Authentication Server** window.

Configure the Guest Portal

If you have configured a require-authentication access rule, and the Sensor does not have the IP-to-user mapping for the detected traffic, it can redirect HTTP traffic from that host to the Guest Portal. This is a Web portal on the Sensor where users can enter their AD credentials. For this, you must install the Guest Portal on the Sensor. You can optionally customize the message displayed on the Guest Portal.

Install Guest Portal on the Sensor

Verify that the Guest Portal is installed on the Sensor using the **`Status`** CLI command. Guest Portal is installed by default.



If the Guest Portal is down, follow the steps in this section to install the Guest Portal.

1. Establish communication between the Sensor and Manager.
2. In the Sensor CLI, type

   `guest-portal install`
3. You must enter the following details for generating the default Guest Portal Certificate:
   - Common Name (IP Address/Domain Name)
   - Organization
   - Organization Unit
   - City
   - State
   - 2 letter Country code
4. Once the certificate is generated, type **`guest-portal status`**. This command displays all the information related to the Guest Portal.

   To uninstall the Guest Portal from the Sensor, use the **`guest-portal deinstall`** command. This command also deletes the default Guest Portal certificate that was generated when you installed the portal. You can also temporarily stop the Guest Portal on the Sensor using the **`guest-portal stop`** command. To start it again, use the **`guest-portal start`** command.

> **NOTE**
>
> Suppose you are trying to install Guest Portal on the Sensor and Sensor-Manager communication goes down. The Guest Portal cannot be hosted in such a scenario. You have to establish Sensor-Manager communication and follow the steps above to get the Guest Portal running. When Sensor-Manager communication is down, you cannot login to the installed Guest Portal.

Generate custom Guest Portal certificates

The communications between the guests and the Guest Portal are encrypted, and the Guest Portal accepts only HTTPS (HTTP over SSL/TLS) connections.

The Guest Portal uses the default *self-signed Guest Portal certificate* generated by the Sensor. The Guest Portal uses this certificate to generate standard browser messages to the guest users. You can use a custom SSL certificate and eliminate the browser warning, if required.

Generating a self-signed certificate via Sensor CLI

The Sensor CLI provides **`guest-portal install`** command which prompts the user for different fields required for Guest Portal Certificate and for creating the public/private key pair.

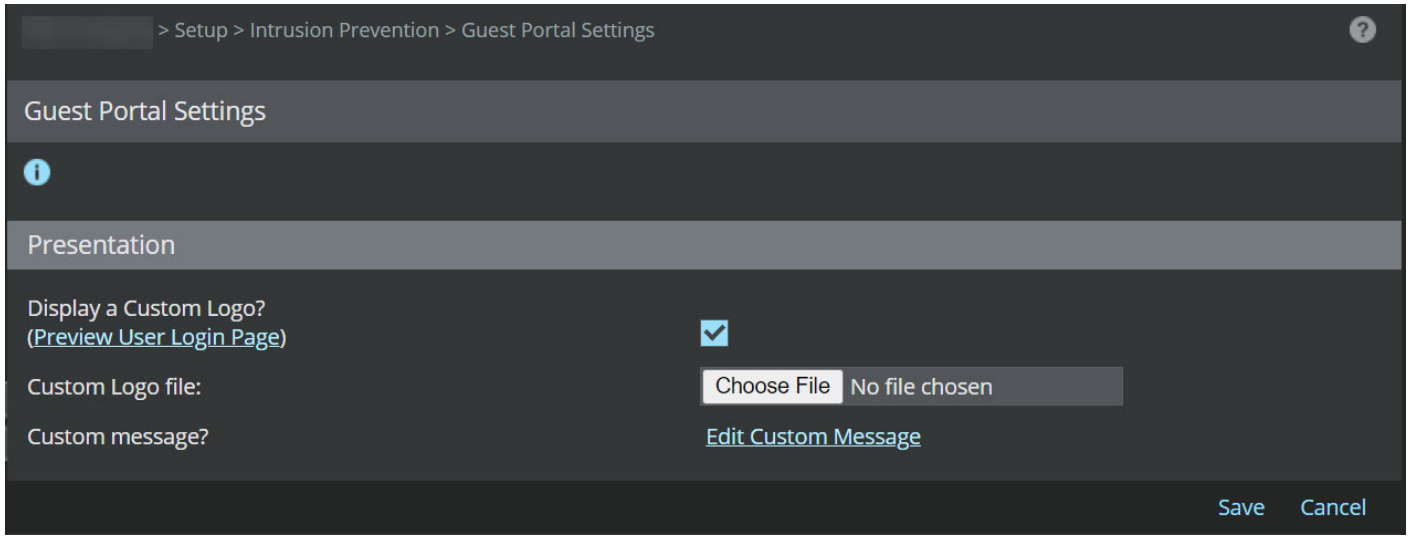
Customize Guest Portal settings for Firewall

For Firewall, the **Guest Portal Settings** page in the root admin domain allows you to specify the presentation settings for the Guest Portal. This includes your organization's logo as well as message that your users must acknowledge to access the Guest Portal.

Configuring the logo is optional. The message option is configured with a default message that you can modify or replace with your own. This message option is for you to specify your organization's policy, terms, and conditions that your users must agree to comply with. Only then they can proceed to self-register or enter their logon credentials in the Guest Portal.

1. Go to Manager → <Admin Domain Name> → Setup → Intrusion Prevention → **Guest Portal Settings.**

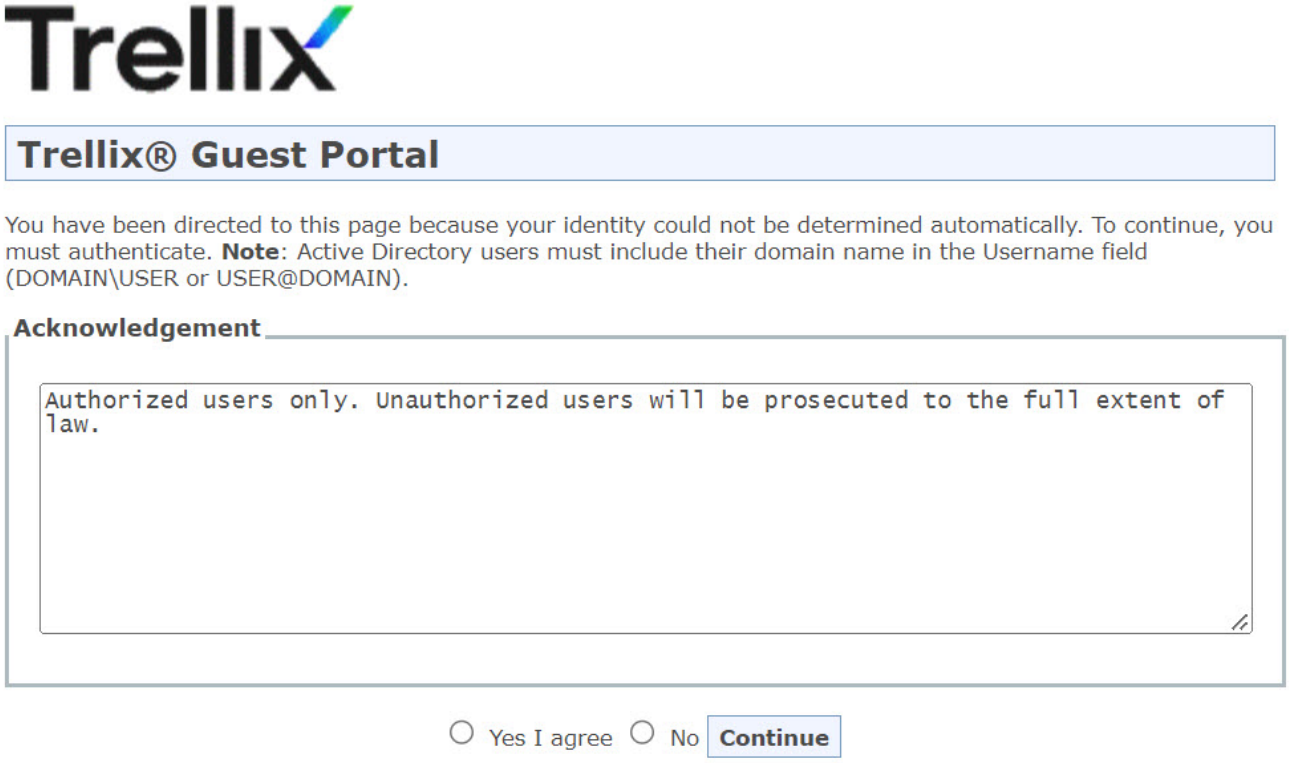
Figure 547. Guest Portal Settings for Firewall



2. Configure the required options in the **Guest Portal Settings** page.

Option	Definition
Display a Custom Logo?	Select to upload the picture file that you want to display as the logo on the Guest Portal. **NOTE** It must be a .jpg, .gif, or .bmp file that is less than 2 KB in size.

Option	Definition
Preview User Login Page	Click the hyperlink to preview how the message (terms and conditions) displays in the Guest Portal. **NOTE** **Preview User Login Page** is available only in the root admin domain. Also, if you have selected **Display a Custom Logo?** then navigate again to the Guest Portal Settings page to view the **Preview User Login Page** link.
Custom Logo file	Enables to browse to the picture file that you want to display as the logo. This field is displayed only if **Display a Custom Logo?** is selected.
Edit Custom Message	Click to view the default Guest Portal message that your users must agree to comply with. • This default message is in English. You can customize it or replace it with your own message. • This message should not exceed 1024 characters in length. • To revert to the default message, delete your custom message in the **Message Body** box, click **Save,** then click **Save** in the Guest Portal Settings page, and then restart the Manager client. • Only one message box is provided. That is, no separate boxes are provided for different languages. The message that you provide in the box is displayed first when users are redirected to the Guest Portal. • Only if your users select **Yes I agree,** they can proceed to enter the logon credentials or self-register. In the Guest Portal, if users change the language, this message (terms and conditions) is displayed again; they have to select **Yes I agree** to enter the logon credentials.
Save	Saves the **Guest Portal Settings** in the Manager.
Cancel	Clears the options you selected in the **Guest Portal Settings** page.

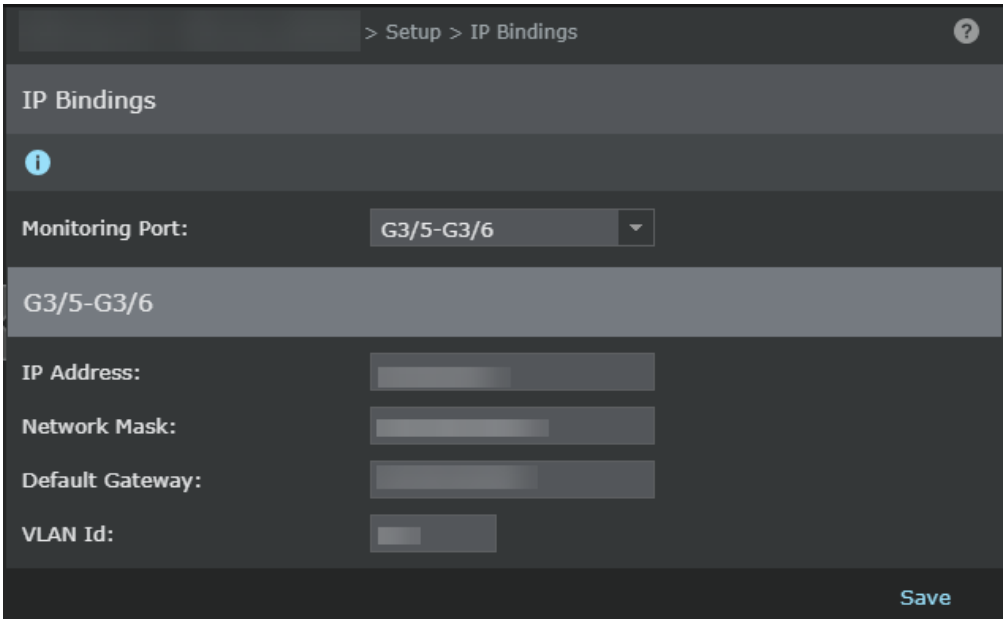


Specify IP details for monitoring ports

If your advanced Firewall policies have a require-authentication rule, the Sensor redirects the users to its Guest Portal if it cannot determine whether they have valid AD logon credentials. For this redirection, you must configure the IP address and related details to the Sensor monitoring ports.

- You can configure the IP details regardless of the port deployment mode, but redirection to Guest Portal is effective only with inline ports. These settings apply to both the ports of the monitoring port pair. The monitoring port IPs that you configure must be reachable to the hosts being monitored.
- Each monitoring port pair used for Firewall must have a unique IP address. For Sensors in failover, you must configure the IP settings separately for both the Sensors. Also, you must use unique IP addresses.

Figure 548. Configure IP details for monitoring ports



1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. For standalone Sensors, select Setup → **IP Bindings**.

   For Sensors in a stack, select Member Sensors → <Stackname-node id> → Setup → **IP Bindings**.
6. For Sensors in failover, select <Device Name> → Member Sensors → <Sensorname-node id> → Setup → **IP Bindings**.

   For a stack of Sensors in failover, select <Device Name> → Member Sensors → <Stackname-node id> → Setup → **IP Bindings**.

   In case of failover Sensors, use the steps below to configure the IP details for the corresponding ports of the peer Sensor.
7. Enter the IP details in the corresponding fields.

Option	Definition
Monitoring Port	Select the port pair for which you want to configure the IP bindings.
IP Address	Enter the IPv4 address that the Sensor can use for the monitoring port pair.
Network Mask	Enter the corresponding network mask for the IP address that you entered.
Default Gateway	Enter the corresponding network gateway for the IP address that you entered.
VLAN Id	Specify the VLAN ID only if the monitoring ports are connected to trunk ports.
Save	When you click, the Manager automatically updates the Sensor with these settings. **Save** is displayed only if you have entered valid details.
Cancel	Clears the details you have entered in the **IP Bindings** page.

8. Click **Save**.

Management of Firewall policies

You define your Firewall implementation by creating Firewall policies. After you create a policy, you need to assign it to one or more of the following Sensor resources:

- Pre-device
- Interface or subinterface
- Port
- Post-device

View Firewall policies

To view the firewall policies:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Policy Types → **Firewall**.

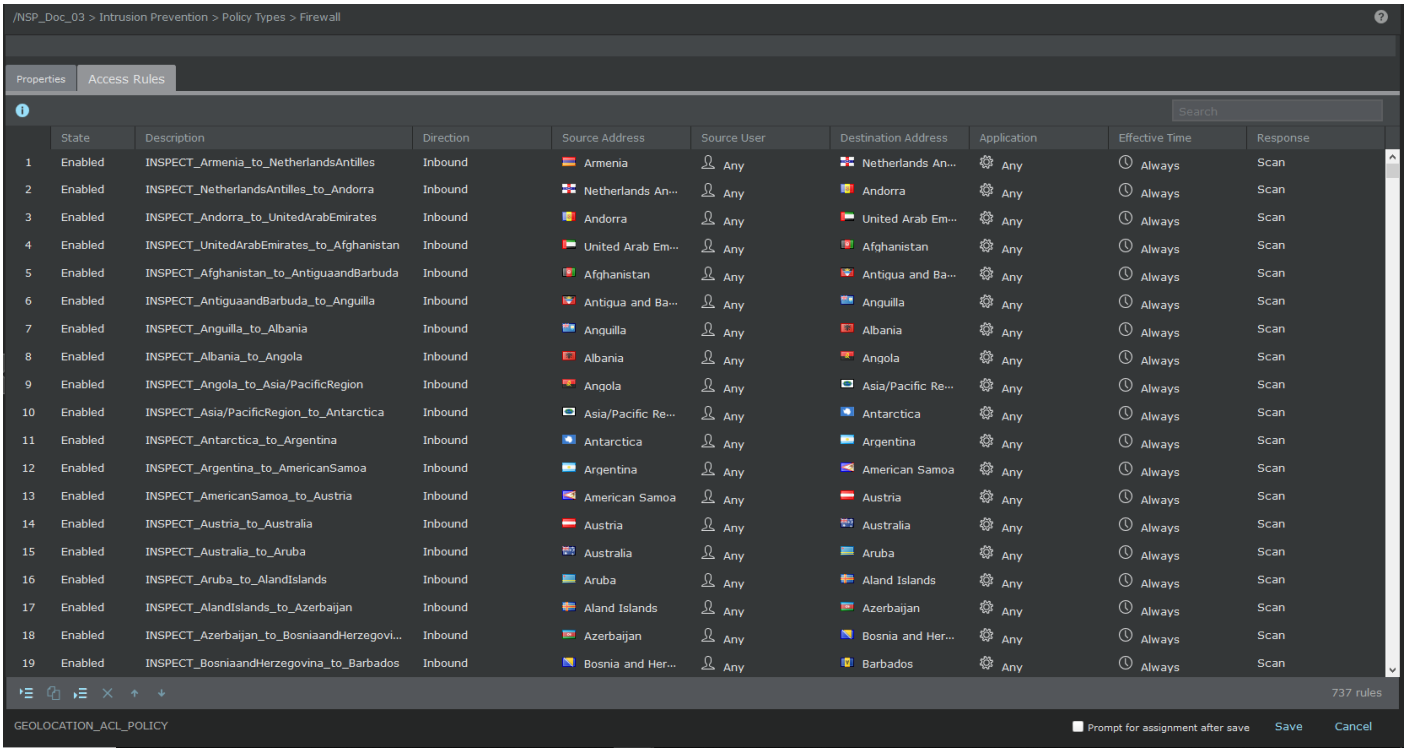
   The Firewall policies created at the selected admin domain and its parent domain are listed. The details of the firewall policies are displayed in columns.

Option	Definition
Name	Displays the name of the firewall policy.
Description	Displays the description of the firewall policy.
Ownership and Visibility	**Owner Domain** — Specifies the ownership of the domain. **Visibility** — Specifies the visibility level of the domain. **Editable Here** — The status **Yes** indicates that the policy is owned by the current admin domain.
Type	Specifies the type of policy.
Last Updated	**Time** — Displays the time when the firewall policy was last updated **By** — Displays the user who modified the firewall policy.
Assignments	Indicates the number of Sensor resources to which the policy is assigned.

   You can sort the list in ascending or descending order based on any of the columns by clicking on the column heading. You can also view the **Columns** option to enable or disable the display of the columns by selecting or deselecting the relevant checkbox.

4. Double-click on the row of the policy to view the rules of that policy.
5. On the **Access Rules** tab, type in the search text field to view the access rule for the given search criteria.

Figure 549. Viewing Firewall policies



Create Firewall policies

Prerequisite: You can create rule objects when creating the Firewall access rules. However, a systematic approach is to create the required rule objects before you create the Firewall access rules. You create a Firewall policy using access rules as the building blocks.

Be sure whether you need a classic or advanced Firewall policy. Review the [Differences between Advanced and Classic Firewall policies] section. To use advanced features such as require-authentication access rules, user-based access rules, and application-based access rules you need advanced Firewall policies.

When you create the access rules, be aware that for a given traffic, the Sensor executes the rules in a top-down fashion and stops the execution when a rule matches. The following are some recommendations that you can consider:

- As a precaution, create a rule that allows traffic to the basic network infrastructure servers such as AD, DHCP, and Trellix ePO - On-prem. Make sure this is the first rule in the list. This is to ensure that your Firewall policy does not prevent the hosts from receiving an IP address or your users from authenticating against the AD.
- If you require, create all the required authentication access rules right after the rule that allows traffic to the infrastructure servers.
- Define the specific rules above the broader rules. For example, rules for Facebook, Google, Yahoo and so on must be above the HTTP rule.

To create user-based access rules, you use user and user group rule objects. Note the following:

- You can create these rules only in Advanced Firewall policies.

- To create these rules, you must first integrate Trellix Logon Collector 3.0.11 with the Manager.
- Before you create these rules, make sure the AD server is able to authenticate the users and these details are reflected correctly in Trellix Logon Collector.
- If Kerberos snooping is required, you must configure the Active Directory server details and Trusted Domain Controllers in the respective pages of the Manager.

For the require-authentication rules to work, the Guest Portal on the Sensor must be up, and you must configure the IP address settings for the corresponding monitoring ports as well.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Policy Types → **Firewall**.
4. Click +.
5. Specify the details on the **Properties** tab.

Option	Definition
Name	Enter a unique name to easily identify the policy.
Description	Optionally describe the policy for other users to identify its purpose.
Owner	Displays the admin domain to which the policy belongs
Visibility	When selected, it makes the policy available to the corresponding child admin domains. **NOTE** However, the policy cannot be edited or deleted from the child admin domains.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Type	Select the type — **Advanced** or **Classic**. After you save the properties, you cannot change advanced to classic.
Statistics	
Lasted Updated	Displays the time stamp when the quarantine zone was last modified
Last Updated By	Displays the user who last modified the quarantine zone
Assignments	Indicates the number of Sensor resources to which the policy is assigned
Inbound Rules	Displays the number of access rules currently defined for inbound traffic
Outbound Rules	Displays the number of access rules currently defined for outbound traffic
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.

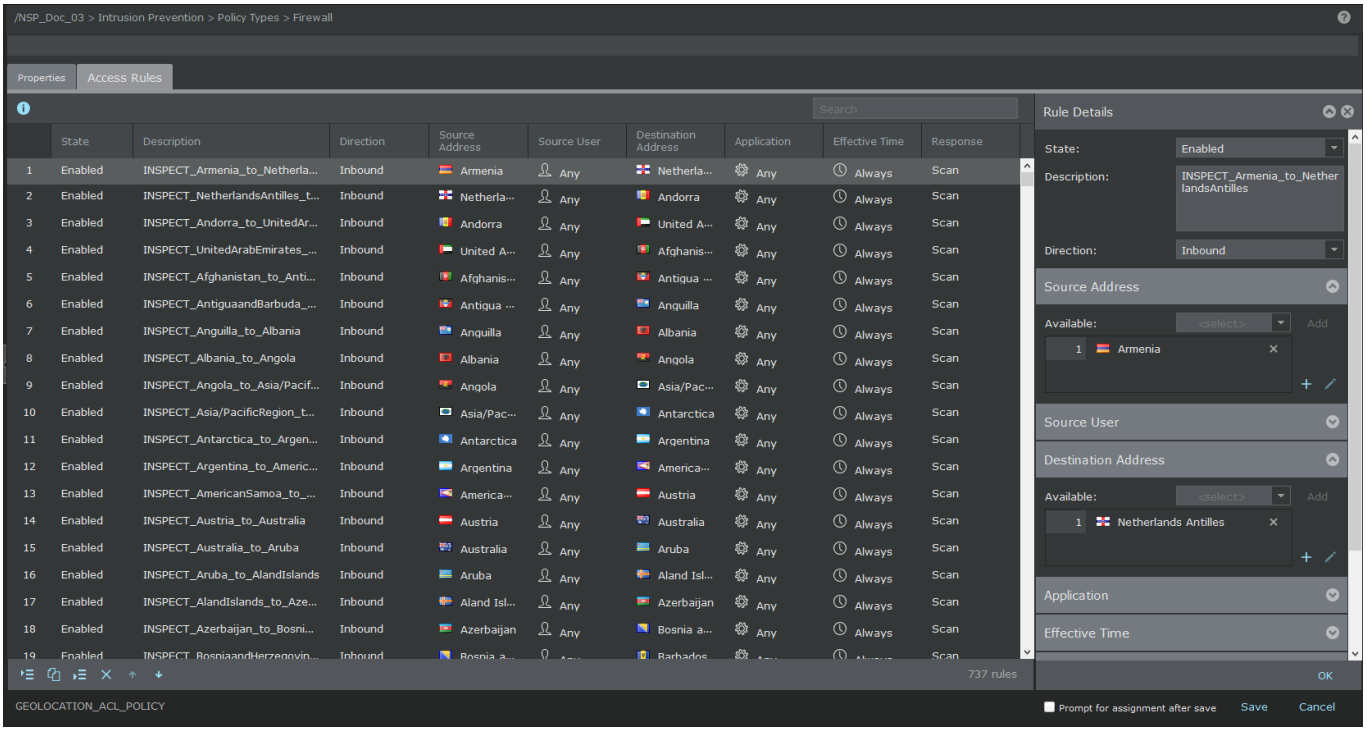
Option	Definition
Next	Click **Next** to save the changes made on the **Properties** tab and access the **Access Rules** tab. **IMPORTANT** After you click **Next** you cannot change the type from advanced to classic.
Save	Saves the changes made on the **Access Rules** tab. This is also visible when you open an existing policy.
Cancel	Reverts to the last saved configuration

6. On the **Access Rules** tab, click the appropriate button to insert a new rule.

Button	Definition
	Inserts a new rule above the currently selected rule
	Inserts a new rule below the currently selected rule
	Clones the currently selected rule
	Deletes the currently selected rule
	Moves the currently selected rule one row up
	Moves the currently selected rule one row down

7. Select the section of an access rule and specify your choices.

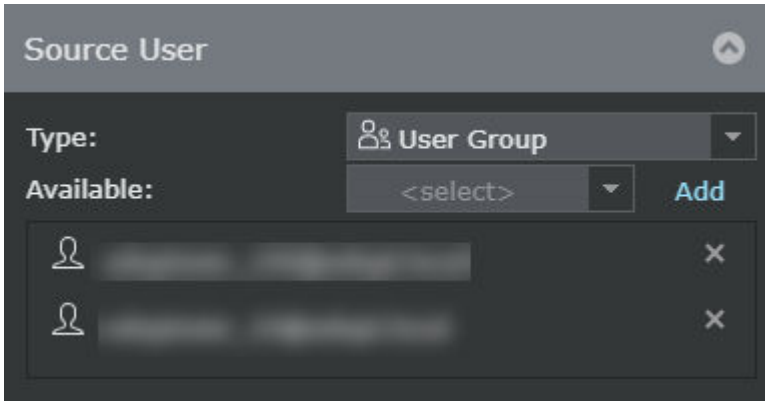
Figure 550. Adding Firewall access rules



- For advanced Firewall policies, change the values of **Source Address, Direction, Source User, Destination Address, Application**, **Effective Time** and **Response**. For classic Firewall policies, change the values of **Source Address, Destination Address, Service, Direction** and **Response**.

Option	Definition
#	Displays the serial number of the rule
State	Displays whether a rule is enabled or disabled. Sensor does not apply disabled rules. This option might help you during troubleshooting.
Description	Optionally enter additional information about the rule. This might help you to easily understand the logs forwarded to the syslog server. You can enter a description up to 64 characters long and click **OK**.
Direction	• **Inbound** — To apply this rule only to traffic seen at the outside port • **Outbound** — To apply this rule only to traffic seen at the inside port • **Any** — To apply this rule at both the ports

Option	Definition
Source Address	Select the rule objects corresponding to the source of the traffic from the **Available** list. Click **Add** to add a rule object. Click to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.
Destination Address	Select the rule objects corresponding to the destination of the traffic from the **Available** list. Click **Add** to add a rule object. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.
Application	Select the rule objects corresponding to the application from the **Available** list. Click **Add** to add a rule object. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.

Option	Definition
Source User	This option is for user-based rules. Recall that the Manager receives users and user groups from Logon Server and automatically displays them as rule objects. User groups are listed by default. User groups are listed by default. Select the user group from the **Available** drop-down list. Click **Add** to add the selected user group to the list. Click to remove the user group from the list. To select the user: 1. Select **User** from the **Type** drop-down list.  2. In the **Search User** text field, type the fist few letters of the name you want to find and click the **Find** button. The list of users with the searched criteria is listed in the **Available** drop-down list. 3. Click **Add** to add the selected user to the list. 4. Click to delete user from the list.
Service	Select the Application or Service-related rule objects from the **Available** list. Click **Add** to add the selected service. **NOTE** This option is available only for classic firewall policies. Click to create a new rule object. Click to edit or view a rule object. Click to remove the rule object from the list. You can have Service or Application-related rule objects in a rule but not both.

Option	Definition
Effective Time	Select the time-based rule objects to specify the time when the Sensor should implement the rule, from the **Available** list. Click **Add** to add the selected service. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list. **NOTE** Time-based rules are implemented using the local time zone of the corresponding Sensor.

Option	Definition
Response	Specify the response action the Sensor should take on the traffic that matched the rule. **Primary Action**: **NOTE** To configure stateful access rules, use the response actions **Deny**, **Drop**, **Ignore**, **Scan**, **Scan with Priority**, or **Require Authentication**. • **Deny** — Discards the traffic and resets the connection with the source of the traffic. • **Drop** — Discards the traffic. • **Ignore** — Allows the traffic to pass through without any further inspection. • **Scan** — Allows the traffic but inspect it for attacks. • **Scan with Priority** — Allows you to prioritize critical network traffic. The prioritization increases the usable bandwidth for high priority packets to optimize performance. Consider you have a traffic comprising of HTTP, SMTP, FTP, POP, and so on and you have configured a priority access rule for HTTP traffic. In this case, during heavy network load conditions, the HTTP traffic is always put in the priority queue and processed and non-HTTP traffic is dropped. In case of a heavy network load condition comprising of HTTP traffic only, some HTTP packets might be forwarded or dropped. In case of High priority traffic is latency sensitive, that is, it has lower latency compared to other traffic. **NOTE** This option is available only for advanced Firewall policies. • For information on **Require Authentication**, see the following step. • For information on **Stateless Drop** and **Stateless Ignore**, see [Using stateless access rules]. **Log to Syslog** — Select if you want to log the details of the traffic that matched the rule.
Prompt for assignment after save	If you clear this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the **Assignments** window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Save	Saves the access rules in the Manager database. The Firewall policy is listed in the **Firewall** list.

8. To create a require-authentication rule, do the following:
   a. In the **Description** field, enter a description.
   b. In the **Response** field of a rule, select **Require Authentication**, and click **OK**.
   c. In the **Application** field, select only the default HTTP Service rule object.

Even the HTTP Application rule object or a custom HTTP Service rule object are not valid in a require-authentication rule.

d. Specify the values for **Source Address**, **Destination Address**, **Effective Time**, and **Direction**.

You must leave the **Source User** as **Any**.

9. Repeat the steps to add more access rules.

Following these steps, you can clone and edit Firewall policies.

Assign a Firewall policy to Sensor resources

Prerequisite: Make sure you have created a Firewall policy with the required access rules.

A Firewall policy is useful for maximizing a Sensor's detection and prevention capabilities by denying specified traffic without requiring full inspection, while also permitting certain traffic to pass without inspection.

At the Sensor level, you can assign a Firewall policy for the entire Sensor as well as those for specific ports/port pairs of the Sensor. Policy assigned at the Sensor level for a specific port/port pair are inherited by all the ports/interfaces/subinterfaces, while policy assigned is inherited by the corresponding interface and, if applicable, subinterfaces. In the case of Firewall policies, an interface is a subset of the corresponding port or port pair. That is, access rules configured for a port/port pair at the Sensor level are inherited by the corresponding interface as well as any subinterfaces. However, rules created at the interface level are not inherited by corresponding subinterfaces due to the rule of separating interface traffic flows from subinterface traffic flows based on the following policy application rule:

If you configure multiple access rules, note the order as access rules are executed in top-down sequence: the rule at the top of the list is checked first, followed by subsequent rules down to the bottom-most rule. Trellix IPS employs a first-match process; the first rule matched in sequence is enforced.

If you apply a policy to a subinterface that is different than the inherited policy, the policy enforced at the interface level protects all traffic not specific to the subinterface. Thus, for access rules, the rule of inheritance requires you to create global rules at the Sensor or physical port/port pair level: interface rules only apply to interfaces, and subinterface rules only apply to subinterfaces.

Access rules applied at the Sensor level are inherited by all interfaces and subinterfaces of the Sensor. You can add more rules at the interface and subinterface levels; however, you cannot delete inherited rules at the child levels. Even if no rules have been assigned at the Sensor level, you can assign rules at the interface and subinterface levels.

In a Firewall policy, you can create unique access rules for inbound and outbound traffic, respectively. Inbound refers to any traffic destined for the internal network from an external source. Outbound refers to any traffic that originated from your internal network.

You assign rules to a Sensor/port/interfaces or subinterfaces using the **Policy Manager** panel and view the order of the rules at the ports, interfaces, or subinterfaces by clicking **Inbound** or **Outbound** in the **Effective Rules** field of the corresponding **Policy Manager** panel.

For a Sensor, ports, and interfaces, or subinterfaces, you can choose rules created at admin domain and apply them to the entity.

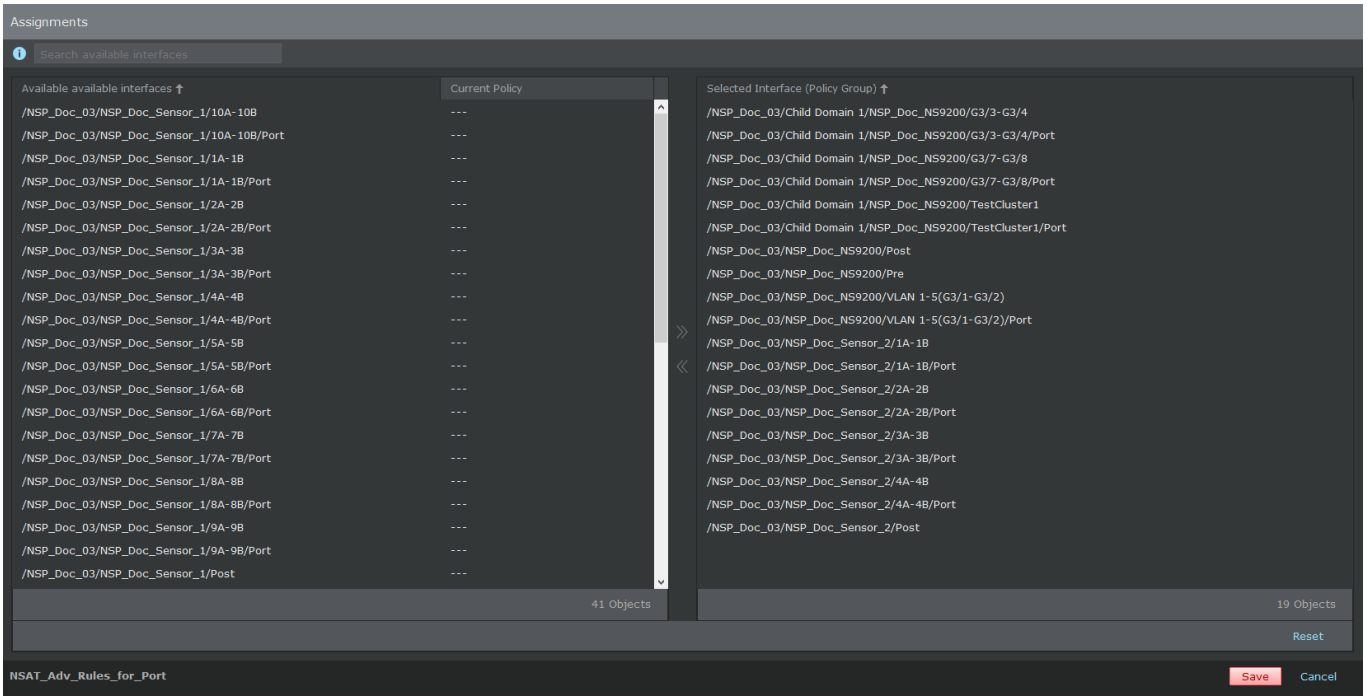
1. Select Intrusion Prevention → Policy Types → **Firewall Policies**.
2. Click the **Assignments** value of the policy that you want to assign.

Last Updated		Assignments
Time	By	
Sep 27, 2019 15:25:05	admin	0
Sep 27, 2019 15:25:08	admin	2

The **Assignments** window displays. It lists the available resources for the admin domain.

3. Assign the policy to the required Sensor resources.

Figure 551. Assignments window



Option	Definition
Search Interfaces	To filter the list of available resources and selected resources, enter a string that is part of the **Available Interfaces** or **Selected Interface**.

Option	Definition
Available Interfaces	Lists the Sensor resources for the admin domain. For example, if an admin domain has only Sensor ports allocated from the parent domain but no Sensor of its own, then no device-level resource is listed. Also, the items in this list are filtered based on your filter criteria. **NOTE** In case of Sensors in failover, the ports used for interconnection of the Sensors are not displayed. If you have assigned the Firewall policy to an interconnect port, the assignment is automatically removed when you create the failover. Select a resource and click » to move it to **Selected Interface**.
Current Policy	The Firewall policy that is currently assigned to a resource. To replace that policy with the policy that you are currently assigning, move the resource to **Selected Interface**.
Selected Interface (Policy Group)	Lists the Sensor resources to which you have assigned the policy.
Reset	Reverts to last saved configuration.
Save	Saves the changes to the Manager database.
Cancel	Closes the **Assignments** window without saving the changes.

4. Verify the list of effective inbound and outbound rules at the corresponding ports, interfaces, or subinterfaces.

   Note that the Sensor checks the traffic against the effective rules in a top-down fashion.

   You can view the **Effective Rules** in the **Policy Manager** panel at the interface and sub-interface levels.

5. Do a configuration update for the Sensor to enforce the policy.

Example 1. Alternative ways to assign Firewall policies

There are many options to assign Firewall policies to Sensor resources. You can also go to the **Policy Manager** page of a specific Sensor resource and select a Firewall policy for that resource. These options are described here. Ensure you do not assign the same Firewall policy to more than one resource of a Sensor.

To assign a Pre-device or Post-device Firewall policy:

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Navigate to Intrusion Prevention → **Policy Manager**.
4. Select the **Devices** tab and double-click the Sensor to which you would like to assign the Firewall policy.

   The **<Sensor Name>** panel opens.

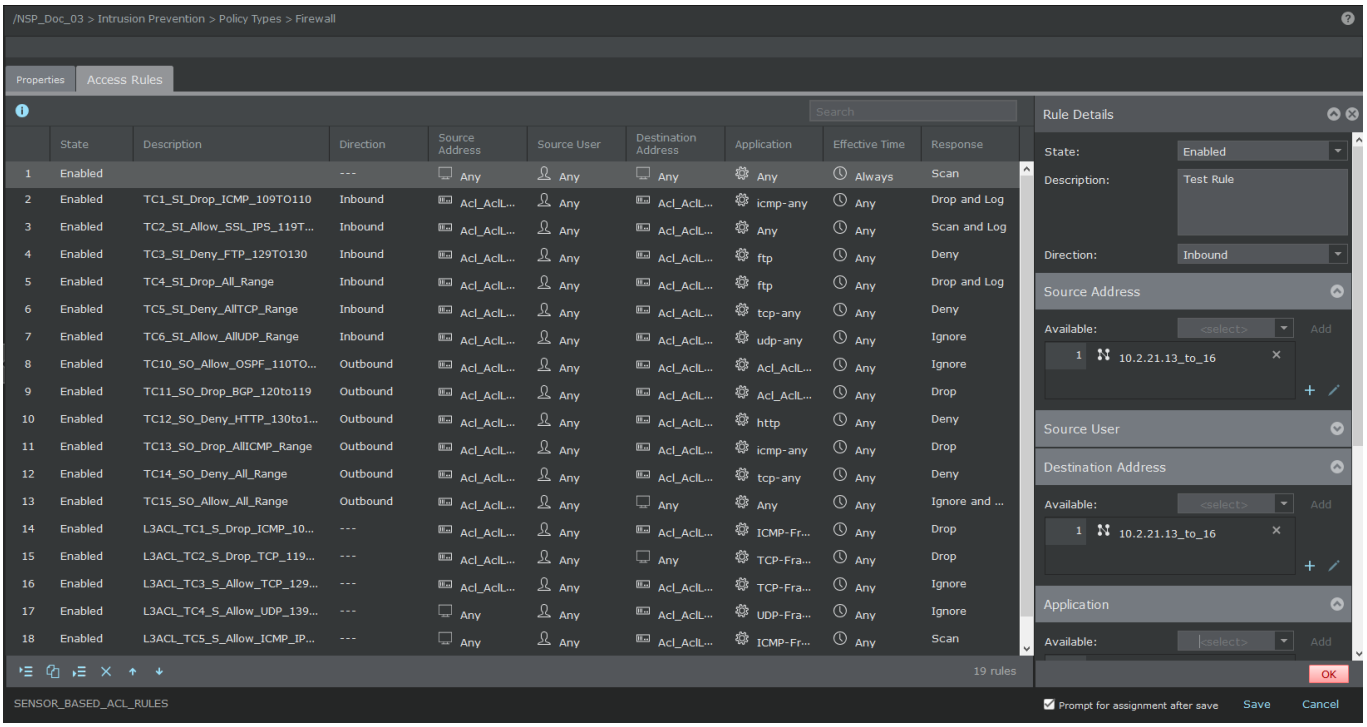
5. Under the **Firewall-Device First** and **Firewall-Device Last** sections, select the policy to be assigned from their respective **Policy** drop down lists.
6. To create a new policy, click the + icon or click the ✎ icon to edit an already assigned policy.

   If you are creating a new policy, proceed to step 7. If you are editing an existing policy, proceed to step 8.

7. The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and **Type**. Click **Next**.

   The **Access Rules** page opens.

Figure 552. Assigning Firewall policy



8. Click the icon to insert a new rule or double-click the existing rule to edit.

   In both cases the **Rule Details** panel opens.

9. Select the necessary rules under the **Source Address**, **Source User**, **Destination Address**, **Application**, **Effective Time**, and **Response** sections.

10. Click **OK** and then **Save** the changes.

11. Do a configuration update for the Sensor to enforce the policy.

To assign a Firewall policy to port or interface and sub-interfaces:

1. Navigate to Policy → Intrusion Prevention → **Policy Manager**.

2. In the **Interface** tab, double-click the interface/sub-interface to assign the firewall policy.

   The **<Device name/Interface>** panel opens.

3. In the **Firewall** section, select the policy from the **Interface Policy** drop down list.

   To create a new policy, click the icon or click the icon to edit an already assigned policy.

   If you are creating a new policy, proceed to step 6. If you are editing an existing policy, proceed to step 7.

4. The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and **Type**. Click **Next**.

   The **Access Rules** page opens.

5. Click the icon to insert a new rule or double-click the existing rule to edit.

In both cases the **Rule Details** panel opens.

6. Select the necessary rules under the **Source Address**, **Source User**, **Destination Address**, **Application**, **Effective Time**, and **Response** sections.
7. Click **OK** and then **Save** the changes.
8. Click **Save** to save the configuration changes updated.

Modify Firewall policies

On the **Firewall Policies** page, you can change the assignments for any of the listed policies, but you can modify the access rules only for the policies that are created at the selected admin domain. Such policies have the **Editable here** field displays the status as **Yes**.

Steps:

1. Select Intrusion Prevention → Policy Types → **Firewall**.

   The **Firewall** page is displayed.
2. To change the assignments:
   a. Click the **Assignments** value of a policy.
   b. In the Assignments window, select from the **Available Interfaces** list and click . Click **Reset** to cancel the assignments that you made in the current session.

      NOTE

      You can select multiple interfaces by pressing the **Shift** key (for continuous selection) and **Ctrl** key for (discontinuous selection) and click .
   c. Click **Save** to save and exit the **Assignments** window.
3. To modify the properties, rules, or assignments of a policy, double-click on the policy.
4. On the **Access Rules** tab, click the appropriate button to manage rules.

Table 65. Access rule button definitions

Option	Definition
	Inserts a new rule above the currently selected rule
	Inserts a new rule below the currently selected rule
	Clones the currently selected rule
	Deletes the currently selected rule

Option	Definition
	Moves the currently selected rule one row up
	Moves the currently selected rule one row down

5. Modify the values for the required rules.
6. Click **Save**.

   If you selected **Prompt for assignment after save**, the **Assignments** window opens where you can modify the current assignments.
7. For the changes to take effect, perform a configuration update.

Convert classic Firewall policies to advanced

You can convert a classic Firewall policy to advanced. However, you cannot convert an advanced to classic.

Steps:

1. Select Intrusion Prevention → Policy Types → **Firewall**.
2. Double-click the required classic Firewall policy.

   Make sure the **Editable here** column displayed as **Yes** for the policy. If not, go to the domain which owns the policy to convert it.
3. On the **Properties** tab, select **Advanced** from the **Type** drop-down.
4. Click the **Access Rules** tab to view the corresponding rules.

   The additional parameters applicable only to advanced Firewall policies are now available for these rules.
5. For each access rule, review and specify the required criteria.
6. Do a configuration update to the corresponding Sensors for the changes to take effect.

Export Firewall policies

You can export the Firewall policies to a local file system.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Advanced → Policy Export → **Firewall.**
4. Select the policies to export and click **Export**. The selected policies are all exported as one .xml file. You can then import this .xml file into a Manager of the same version.

NOTE

Using this export feature, you can only export Firewall policy definitions. If a policy is assigned to a Sensor, ports, interfaces, or subinterfaces, and if you want to export this assignment as well, then you need to do a Sensor configuration export.

Import Firewall policies

Between the same versions of the Manager, you can export and import Firewall policies. When you export, the selected Firewall policies are exported into a .xml file. You can then import this .xml file into a Manager to create the Firewall policies contained in that .xml file.

Steps:

1. Select Intrusion Prevention → Advanced → Policy Import → **Firewall.**
2. Specify the required options to import the Firewall policies.

Option	Definition
Skip duplicate policy definitions	When selected, the Manager imports only those policies that are not present in the Manager already.
Import File	Click **Choose File** to locate the file to import.
Import	Begins the import process.

Configure access rules for fragmented traffic

L3 Firewall access rules allow you to selectively specify rules for a host (or network) based on which Trellix IPS skips reassembly handling of the fragmented traffic. This helps in decreasing the latency of the fragmented traffic for the specified network or host.

L3 Firewall access rules do not apply to non-fragmented traffic.

It is advisable to use this feature only with a trusted host and only if you are receiving extremely a high amount of fragmented traffic. For example, you could use L3 Firewall access rules if your NFS server is sending a huge amount of fragmented traffic through a Sensor. Note that using this feature while receiving traffic from an unknown host can mean evasion using IP address fragments.

In Trellix IPS, the rules that can be set for L3 Firewall access rules are as follows:

- *Ignore*: Fragmented traffic that matches the L3 Firewall access rules applied is sent inline without reassembly.
- *Scan*: Fragmented traffic that matches the L3 Firewall access rules applied is reassembled prior to IPS processing.
- *Drop*: Fragmented traffic that matches the L3 Firewall access rules applied is dropped by the Sensor.

All fragmented traffic is reassembled before IPS processing if traffic does not match any L3 ACL rules.

In Trellix IPS, three default Service rule objects are provided to support fragmented ICMP, TCP, and UDP. They are ICMP-Fragmented, TCP-Fragmented, and UDP-Fragmented. The user-specified protocol numbers are not supported.

From Manager, you can configure the access rules for fragmented traffic.

Steps:

1. Select Intrusion Prevention → Policy Types → **Firewall**.
2. Click  .

3. On the **Properties** tab, enter a **Name** and **Description** for the policy.

   The **Owner** field corresponds to the admin that you selected.
4. In the **Visibility** field, select **Owner and Child Domains**.
5. From the **Type** drop-down, select **Advanced** or **Classic**.
6. Click **Next** to view the **Access Rules** tab.
7. Click the relevant button to insert a new access rule at the appropriate location within the list of access rules.
8. In the **Application** section, select the required option from the list.
9. Select a protocol — ICMP- Fragmented, TCP - Fragmented, or UDP- Fragmented.

   When L3 Firewall Access Rules are configured, set **TCP Flow Violation** to **Permit out-of-order** (the default setting).

   a. Click the **Devices** tab.

   b. Select the domain from the **Domain** drop-down list.

   c. In the left pane, click the **Devices** tab.

   d. Select the device from the **Device** drop-down list.

   e. Select Setup → Advanced → **Protocol Settings**.

   f. In the **Protocol Settings** page, from the **TCP Flow Violation** drop-down list, select **Permit out-of-order**.

   g. Click **Update** that corresponds to **TCP Flow Violation**.

Limitations

- You can use access rules for fragmented traffic only with **TCP flow violation** set to **Permit out-of order.**
- Syn-cookie should not used when access rules for fragmented traffic are applied.
- Firewall logging is not supported for access rules for fragmented traffic.

Using stateless access rules

You can use stateless access rules to allow or block certain traffic without deeper inspection. These rules can prevent you from spending time or valuable Sensor resources on traffic that you completely trust or traffic that you want to completely avoid. You can use stateless access rules to bypass IPS inspection for trusted high-throughput applications like database backups. For asymmetric traffic, the traffic flowing in and out of the network may not be inspected by a Sensor. In such cases, you can configure the stateless access rules where each packet is inspected by the Sensor and not the complete traffic flow. The Sensor allows or blocks packets just based on L3 and L4 information in those packets.

> **NOTE**
>
> In stateless access rules, the Sensor inspects the traffic on per-packet basis. Post-inspection, the packets are either dropped or ignored depending on the response action configured. Due to per-packet inspection of the traffic flow, the stateless access rules results in noticeable drop in Sensor performance.

You can create stateless access rules in both advanced and classic Firewall policies. When compared to the regular access rules, the stateless access rules allow or drop traffic in a stateless manner. That is, for stateless rules the Sensor considers the traffic on

a per-packet basis, whereas for service-based and application-based regular access rules it considers the entire flow. So, if you set the response as *drop* for stateless rules, the Sensor drops the packets, but for the regular rules, it drops the flow. You can use the stateless access rules during troubleshooting, where you might want the Sensor to drop packets of only one direction in a flow.

Notes:

- When using stateless access rules, if IPv4 Address Range or IPv6 Address Range Rule Objects are used in the stateless or the stateful access rules, there can be a drop in the Sensor's performance. So, Trellix recommends that you avoid using these Rule Object types with stateless access rules.
- You create a stateless access rule just like any other Firewall access rule but with the following differences:
  - Except for the response and application, all other columns are similar to the regular access rules in terms of functionality and usage.
  - In the response column of the rule, you select **Stateless Ignore** or **Stateless Drop**. The Sensor identifies a stateless access rule based on this selection only.
    - Stateless ignore – This is the same as ignore option. That is, the Sensor permits the packet without inspection for intrusions.
    - Stateless drop – The Sensor discards the packet.
    - In addition to inline mode, you can use the stateless access rules in SPAN and tap modes as well. However, in SPAN and tap, the stateless drop response action has no effect.
  - For the **Application** column, you can only select the following for stateless access rules:
    - You should leave it as **Any**.
    - You can select custom or default Service rule objects except for custom Service rule object with **Port/Number** set to 89. IP protocol number 89 relates to OSPF (RFC 1583), which is a routing protocol; this traffic bypasses the stateless access rules on the Sensor.
    - Custom Service Group rule object that uses Service rule objects except for ones where the **Port/Number** is 89.
  - The Sensor cannot log matched traffic to a syslog server. You cannot create a stateless access rule with logging enabled.
- The stateless access rules generally target traffic that must be allowed or blocked on a priority basis (is allowed or blocked across your network). Also, the Sensor takes less time to process these rules. For these reasons, it is recommended that you define the stateless rules ahead of other similar regular rules and assign them at the pre-device level.

Configure stateless access rules

Prerequisites:

- You have created an advanced or classic Firewall policy to which you want to add stateless access rules.
- You have created the rule objects, especially the service or service group rule objects, required to create your stateless access rules.

Create stateless access rules to allow or block certain traffic without deeper inspection.

1. Select Intrusion Prevention → Policy Types → **Firewall**.

2. Double-click the Firewall policy in which you want to add the stateless rules.
3. In the **Firewall** window, click **Access Rules**.
4. Select the top-most rule and click  .

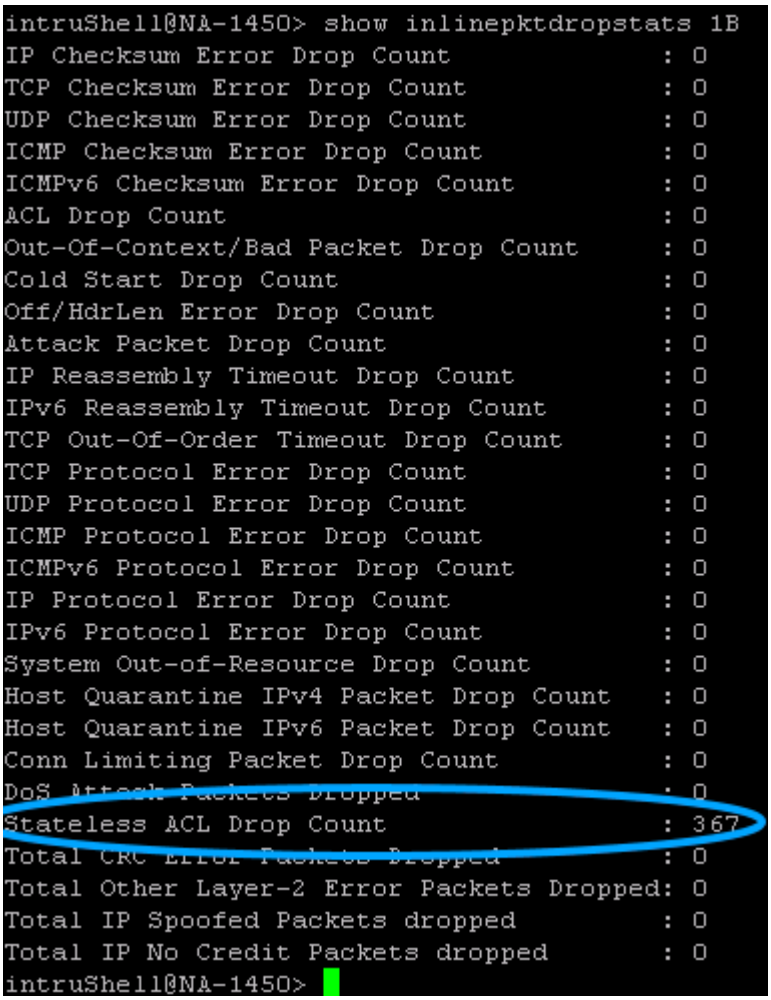
   NOTE

   It is recommended to have the stateless rules above any of the other rules.

5. Optionally, double-click the **Description** field to describe the rule.
6. Select the appropriate values for **Source Address, Source User, Destination Address, Effective Time,** and **Direction.**
7. For **Application**, select the required Service and Service Group rule objects.
8. In the **Response** column, select **Stateless Drop** or **Stateless Ignore**.
9. Click **Save**.
10. Update the Sensor configuration for the rule to be enforced.

    You cannot log the packets that matched a stateless access rule. However, you can view the number of packets dropped by using the **`show inlinepktdropstats <monitoring port>`** command on the Sensor CLI. You cannot view the number of packets that were ignored according to stateless access rules.

Figure 553. Count of packets dropped according to stateless access rules



How to view the details of matched traffic

For all traffic that matched an Access Rule, the Sensor can forward the details to a syslog server. You can use these details for analysis and reporting purposes. For example, you can view all the hosts that tried to access social networking sites during a specific time period. You can also log the packets that matched your Firewall Access Rules.

To view the details of matched traffic you need to configure the following:

- Configure a syslog server and ensure that it is accessible to the Sensor's Management port if you want the Sensor to send the logged details directly to the syslog server. Alternatively, if you want the Sensor to send the details through the Manager, then the Manager must be able to communicate to the syslog server. In this case, the Sensor forwards the logs to the Manager, which formats and converts them to syslog messages and sends them to the configured syslog server.

> **NOTE**
>
> Only NS-series Sensors can directly send logs to a syslog server.

You can then view the log from a third-party Syslog application.

NOTE

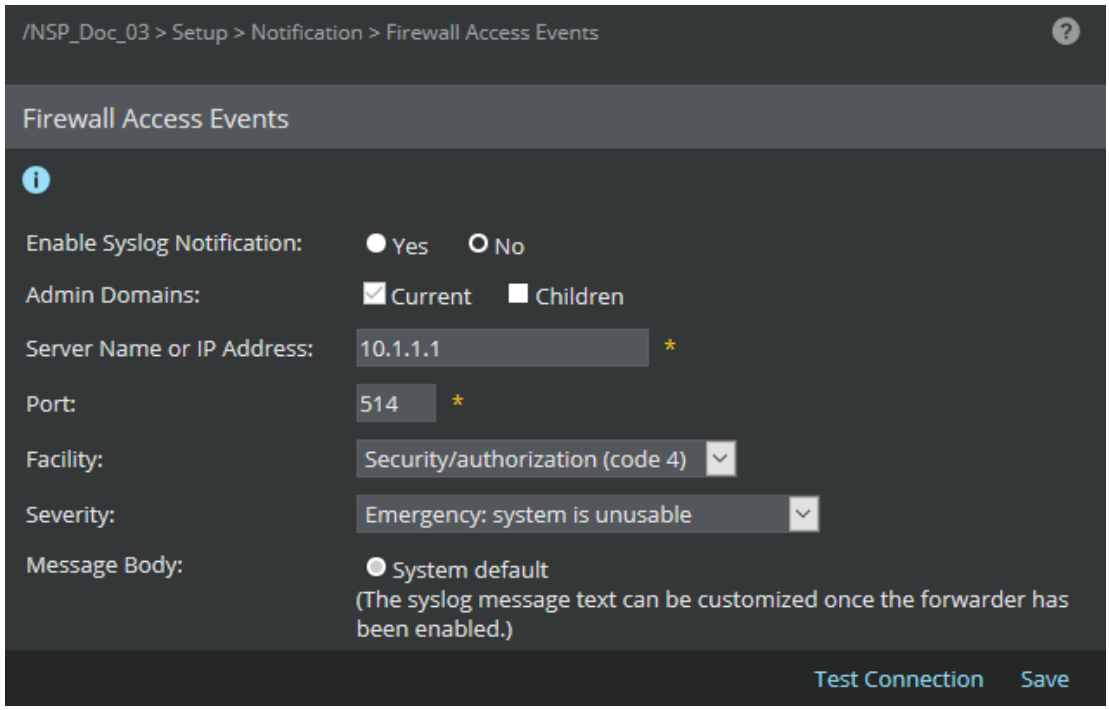
For syslog forwarding, the admin domains have the option to include the logs from the corresponding child domains.

- Enable Firewall Rule Match Notification at the admin domain level.
- Enable Firewall Logging at the Sensor level.

Enable rule match notification

1. Click the **Manager** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Setup → Notification → **Firewall Access Events**.
4. Specify the domain-level syslog details in the corresponding fields.

Figure 554. Syslog server details for Quarantine



Option	Definition
Enable Syslog Notification	If you select **Yes,** the details of the traffic that matched an access rule is forwarded to a syslog server. You can also configure the details now and enable it at a later time.

Option	Definition
Admin Domains	• **Current** — The syslog configuration applies only to the current domain. This is always enabled for the current domain. • **Children** — The syslog configuration applies to child domains as well. You can also modify this syslog configuration at a child domain if required.
Server Name or IP Address	Enter the syslog server name or its IP (IPv4 or IPv6) address. If you specify the syslog server name: • The Manager uses the DNS servers configured in its TCP/IP properties. • If you choose the Sensor to forward the logs to a syslog, then the Sensor uses the DNS servers that you configured in the **Name Resolution** page for the Sensor. **NOTE** The length of server name has been increased to support up to 255 characters from 40 characters.
Port	Enter the communication port number on the target server which is authorized to receive syslog messages. The standard port for syslog, which is 514, is pre-filled in the field. If you are using a non-standard port, then replace 514 with that number.
Facility	Lists the syslog prioritization values. By default, the syslog messages forwarded to a syslog server are of **Security authorization** prioritization value.
Severity	Lists the syslog priority values. By default, the syslog messages forwarded to a syslog server are of **Debug** severity.
Message Body	Optionally, customize the default syslog message. There are two types: • **System Default** — The default message is a quick summary for easy recognition. A default message reads: `"$IV_SENSOR_NAME$$IV_ACL_ID$$IV_ACL_ACTION$$IV_APPLICATION_PROTOCOL$$IV_SOURCE_IP$$IV_SOURCE_PORT$ $IV_DESTINATION_IP$$IV_DESTINATION_PORT$"` • **Customized** — You can customize the message after you successfully save the syslog configuration details. Click **Test Connection** to view the option to edit the default message.

Option	Definition
Test Connection	Checks if the Manager is able to send logs to the syslog server. Check your syslog server if it has received the test message from the Manager. If not, check the syslog server name or IP address that you had provided. Ping the syslog server from the Manager server to see if the Manager is able to reach the syslog server. If you plan to configure NS-series Sensors to directly send the messages to the syslog server, ping the syslog server from the Sensor's CLI. This option is available in the **Firewall Logging** page. **NOTE** You can use the test connection feature, even if you have set **Enable Syslog Forwarding?** to no.
Save	Saves the syslog configuration changes in the Manager database. Once you click **Save**, you will be able to customize the message format sent to the syslog server. **NOTE** If you have modified the syslog configuration, then do a configuration update of the Sensors for the changed settings to take effect.

5. Click **Save**.

NOTE

Once you click **Save**, you will be able to customize the message format sent to the syslog server.

6. Do a Configuration Update for the Sensors for the notification settings to take effect.

NOTE

Use the `show acl stats` command in the Sensor's CLI to see the count of ACL logs sent through the Manager.

Customize the syslog forwarder message

Prerequisite: You must have saved the syslog server details successfully in the **Syslog** page.

Steps:

1. To access the **Syslog** page from the **Manager** tab, do the following.
   a. Click the **Manager** tab.
   b. From the **Domain** drop-down list, select the domain you want to work in.
   c. Select Setup → Notification → **IPS Quarantine Access Events**.

Option	Definition
Enable Syslog Logging?	Select **Yes** to enable syslog and **No** to disable syslog.
Applicable Admin Domains	**Current** — Refers the admin domain currently selected. This is enabled by default. **Children** — Refers the child admin domains of the current domain.
Target Syslog Server Name or IP Address	The IP address or name of the syslog server which becomes the destination of the alert notifications sent by all devices. **NOTE** The length of server name has been increased to support up to 255 characters from 40 characters.
Target Syslog Server UDP Port	Port on the target syslog server that is authorized to receive syslog messages. The default protocol for syslog forwarding from Sensors is UDP. Therefore, this port must not be altered.
Syslog Facility	Standard syslog prioritization value. The choices are as follows: • **Security/authorization (code 4)** • **Security/authorization (code 10)** • **Log audit (note 1)** • **Log alert (note 1)** • **Clock daemon (note 2)** • **Local user 0 (local0)** • **Local user 1 (local1)** • **Local user 2 (local2)** • **Local user 3 (local3)** • **Local user 4 (local4)** • **Local user 5 (local5)** • **Local user 6 (local6)** • **Local user 7 (local7)**

Option	Definition
Syslog Priority	You can map each severity (Informational, Low, Medium, or High) to one of these standard syslog severities: • **Emergency** – System is unusable • **Alert** – Action must be taken immediately • **Critical** – Critical conditions • **Error** – Error conditions • **Warning** – Warning conditions • **Notice** – Normal but significant condition • **Informational** – Informational messages • **Debug** – Debug-level messages
Message Body	**System default** — The default message is a quick summary of an event. **Customized** — Personalized message of an event.

2. Click **Test Connection** in the **Syslog** page.
3. Click **Edit** in the **Message Body** field in the **Syslog** page.

   The **Customize Syslog Forwarder Message** page displays.
4. Customize the format for the syslog forwarder message.

Option	Definition
Message	Form the message by typing in the required text and by clicking on the parameters provided below this field. **IMPORTANT** For Syslog information to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each element. Example: $SENSOR_NAME$
Save	Saves the message you created. Displays the **Syslog** page when you click.
Cancel	Cancels the changes you made to the message.
Reset to System Default	After you customize the syslog message, the **Reset to System Default** button appears in the **Customize Syslog Forwarder Message** page. Click this button to revert to the system default message.

5. Click **Save** in the **Syslog** page.

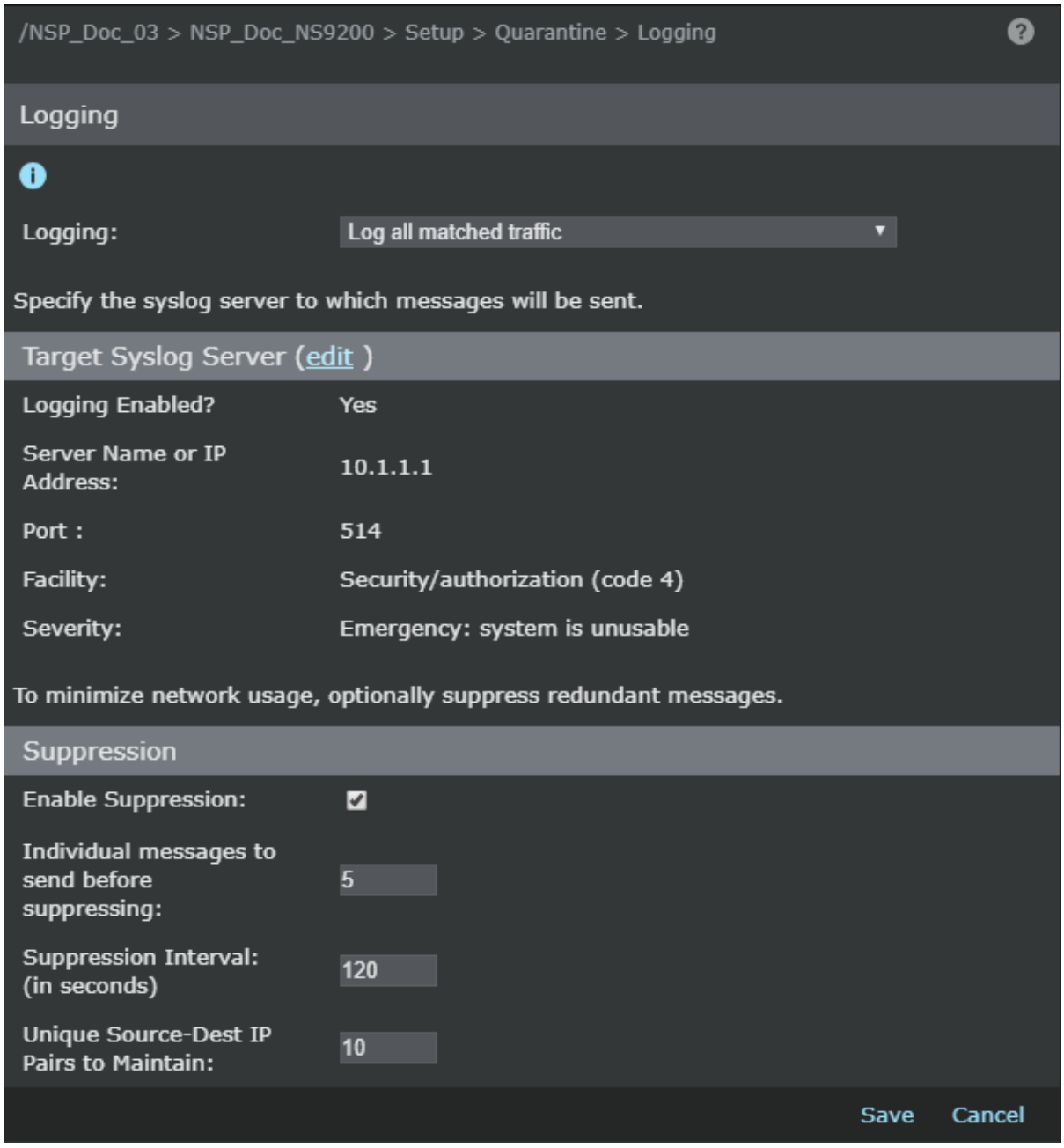
Enable syslog forwarding for Firewall at Sensor level

Steps:

1. Click the **Devices** tab.

2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Logging → **Firewall Access Logging**.

Figure 555. Enabling syslog forwarding for a Sensor



6. Specify the Sensor-level syslog details in the corresponding fields.

Option	Definition
Logging	Sets the condition when the Manager or the Sensor should send the log message to the syslog server. The options are: • **Disabled on this device** — This disables logging on the device. This option overrides the setting on the individual access rules. The remaining options in the **Logging page** are not displayed if you choose this option. • **Log all matched traffic** — Logs all traffic that matched a rule regardless of whether it was dropped/denied or permitted. This option overrides the setting on the individual access rules. • **Log all dropped/denied traffic** — Logs all traffic that was either dropped or denied according to an access rule. This option overrides the setting on the individual access rules. • **Log all permitted traffic** — Logs all traffic that was permitted according to an access rule. This option overrides the setting on the individual access rules. • **Log traffic only if the matched rule is configured to log** —Logs only if you had configured logging for the corresponding access rule.
Delivery	Applicable only for NS-series Sensors. If you choose the Sensor to forward the logs to a syslog, then the Sensor uses the DNS servers that you configured in the **Name Resolution** page for the Sensor. **NOTE** Make sure the Sensor management port is able to reach the DNS servers by pinging them from the Sensor CLI.
Target Syslog Server	Displays the syslog server details that you have configured at the corresponding admin domain. Click **Edit** to go to the **Syslog** page and modify the required details.
Enable Suppression	Option to suppress redundant messages. Only if you select it, the remaining fields in the **Suppression** table are displayed. Suppressing log entries causes the Sensor to send initial log entries representing the first instance of an event (the number of which is configurable), and then suppress further instances of the same event for a configurable number of seconds. This is a useful tool in keeping the log file size under control.
Individual messages to send before suppressing	Indicates the number of messages to be sent within the seconds specified in the **Suppression Interval** field for suppression to begin.
Suppression Interval (in seconds)	Time span in which you accumulate instances of the same rule match. This value acts as a timer; when the timer expires, the current instance is cleared to make room for a new suppression instance.

Option	Definition
Unique Source-Dest IP Pairs to Maintain	Determines the number of unique suppression instances to maintain at a given time. For example, if you enter the number 10, then 10 unique instances can be tracked at a given time. Once 10 is reached, all other cases are kept in a single "wildcard" instance; thus, other unique combinations that occur outside of the 10 uniquely maintained instances are maintained as one instance, and source and destination IP do not appear in the summary since multiple addresses may be involved. An entry is removed after the time limit (Suppression interval) expires.
Save	Saves the configuration in the Manager database. **NOTE** Do a configuration update to the applicable Sensors for the configuration to take effect.
Cancel	Reverts to the last saved configuration.

7. Do a configuration update to the Sensors for the configuration to take effect.

Run the Firewall Policy Definitions configuration report

The **Firewall Policy Definitions** configuration report provides the details of the selected Firewall policy, its component access rules, and the Sensor resources to which the policy is applied. This report carries the source user and source user group that you have selected for each rule.

Steps:

1. Click the **Manager** tab.
2. Select Reporting → **Configuration Reports** and click **Firewall Policy Definitions**.
3. Select the **Admin Domain**, **Firewall Policy Name**, and **Output Format** and then click **Submit**.

NOTE

The admin domain filter in the main **Manager** page (provided in the left pane) does not impact the report generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

For more information on this report, see Generate Firewall Policy Definition report (page 249).

Firewall-related capacity values

The following table provides the Firewall-related capacity values for the various NS-series Sensor models.

Model	Effective Access Rules	Cumulative rule object member count of all the rule objects selected	DNS Rule Objects	Rule Object Groups (such as Application Groups and Service Groups)	Custom Rule Objects
NS9500 stack - 100 Gbps throughput	20000	240000	5000	1000	2000
NS9500 stack - 60 Gbps throughput	20000	240000	5000	1000	2000
NS9500 stack - 40 Gbps throughput	20000	170000	5000	1000	2000
NS9500 standalone - 30 Gbps throughput	20000	240000	5000	1000	2000
NS9500 standalone - 20 Gbps throughput	20000	240000	5000	1000	2000
NS9500 standalone - 10 Gbps throughput	10000	170000	2500	500	1000
NS9300	20000	240000	5000	1000	2000
NS9200	20000	240000	5000	1000	2000
NS9100	10000	170000	2500	500	1000
NS7600 - 15 Gbps throughput	4000	135000	1250	400	500
NS7600 - 10 Gbps throughput	4000	135000	1250	400	500
NS7600 - 5 Gbps throughput	4000	135000	1250	400	500
NS7500 - 7.5 Gbps throughput	4000	135000	1250	400	500
NS7500 - 5 Gbps throughput	4000	135000	1250	400	500
NS7500 - 3Gbps throughput	4000	135000	1250	400	500
NS7350	4000	135000	1250	400	500
NS7250	3000	121000	1000	300	500
NS7150	3000	121000	1000	300	500
NS7300	5000	135000	1250	400	500
NS7200	3000	121000	1000	300	500
NS7100	3000	121000	1000	300	500
NS5200	2000	34000	750	200	250
NS5100	2000	34000	750	200	250
NS3600 - 5 Gbps throughput	4000		1250	400	500
NS3600 - 3 Gbps throughput	4000		1250	400	500
NS3600 - 1 Gbps throughput	4000		1250	400	500
NS3500	1000	17000	500	100	150

Model	Effective Access Rules	Cumulative rule object member count of all the rule objects selected	DNS Rule Objects	Rule Object Groups (such as Application Groups and Service Groups)	Custom Rule Objects
NS3200/NS3100	1000	17000	500	100	150

Notes:

- Config Update of Sensors fail if you exceed the limits in the table above.
- At a Sensor level, there are limits to the number of entities that you can refer to in the Firewall policies. For a given Sensor model, these limits are the same as the limit for Effective Access Rules
- The Sensor derives the limit by totaling rules in all the policies assigned to it. The number of rules in each policy is derived by totaling the rules assigned to each interfaces.
- Even if you refer to the same rule in all your policies, each reference is counted. For example, a policy with the following rule lines are applied to the Sensor interface.
    1. Source 10.1.1.10 | Destination 20.1.1.10 | Application: Gmail
    2. Source 10.1.1.10 | Destination 20.1.1.20 | Application: Gmail
    3. Source 10.1.1.10 | Destination 20.1.1.10 | Application: Gmail

  Though the first and third rule line are same in the above policy, both the references are counted. So, the number of policies here is 1 and the number of rule lines is 3.
- If you use a Group Rule Object such as Network Group, then entire Group is counted as one rule. Consider that a rule refers to a Network Group as the Source. This Network Group contains 3 HostIPv4 Rule Objects. These 3 Rule Objects refer to 10 IPv4 addresses each. In this case, the count for Source remains as one and the rule line is considered as single entity.

Viewing effective Firewall rules

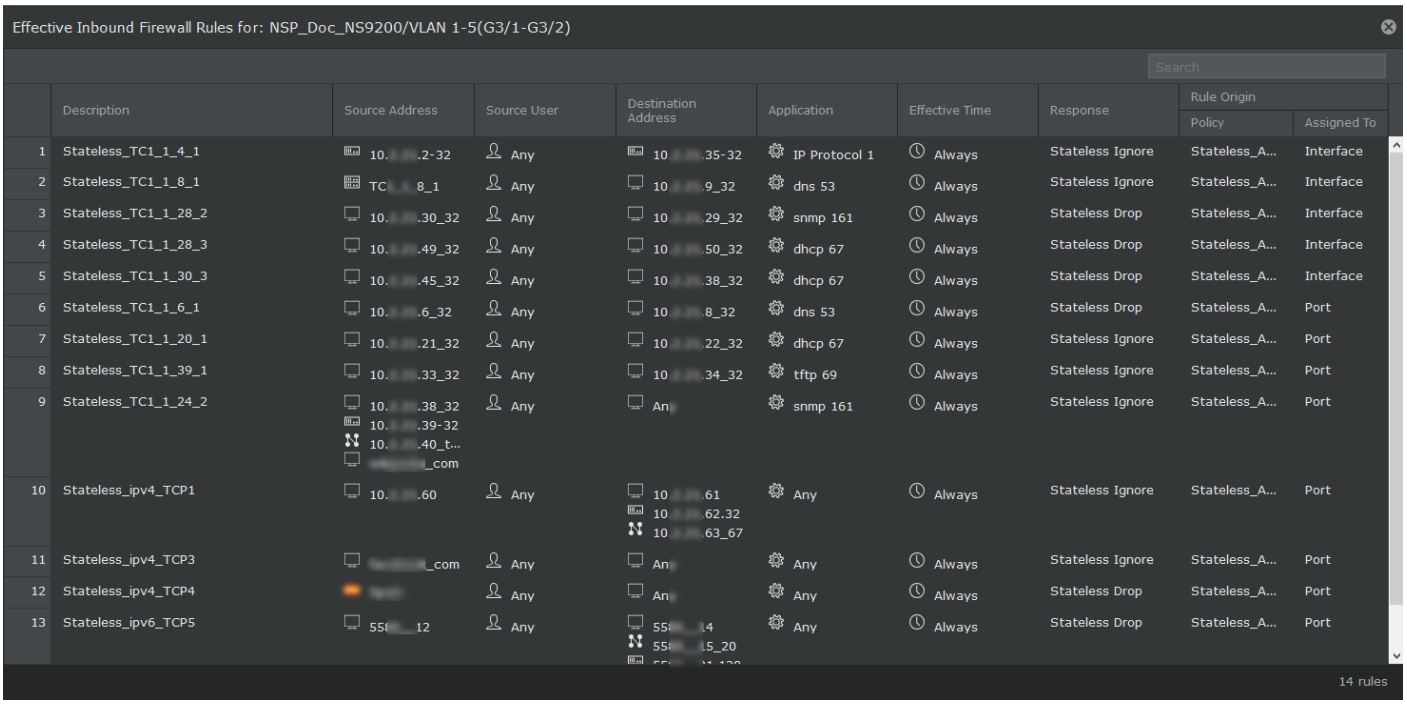
Effective Firewall rules is a sequential list of access rules that a Sensor checks in a top-down fashion against the traffic that it sees at a port/port pair, interface, or subinterface. Afer you assign Firewall policies to the required Sensor resources, the Manager collates all the rules from these policies and creates the list of effective Firewall rules for each port/port-pair, interface, and subinterface. It creates separate lists for inbound and outbound traffic.

NOTE

In all effective Firewall rules list, the Manager adds a default entry at the bottom that allows all traffic with IPS inspection. You cannot modify or delete this default entry. If you do not assign any Firewall policy to any of the resources of a Sensor, this default entry is applied at all ports/port pairs, interfaces, and subinterfaces. Firewall logging is not applicable to this entry.

The order of the rules in the list of effective Firewall rules is based on the hierarchy of Sensor resources. That is, the rules of the pre-device Firewall policy are listed on top followed by the rules of the interface or subinterface policy, then followed by the port-level policy, and finally the post-device level policy. You can view the inbound and outbound effective Firewall rules for a port/port-pair, interface, and subinterface.

Figure 556. Viewing Effective Firewall access rules



The fields displayed are:

Field	Description
#	The order of the rule in the policy.
Description	Description of the rule, if available.
Source Address	The source of the traffic. In case of Advanced Firewall policies, it is based on country, host name, IPv4 or IPv6 address, IPv4 or IPv6 address range, IPv4 or IPv6 network, or Network Group. For Classic policies, it is based on IPv4 address or network.
Source User	This is displayed only for Advanced Firewall policies. Indicates the AD user name and AD user group for the user logged on the source host.
Destination Address	The destination of the traffic. In case of Advanced Firewall policies, it can be country, host name, IPv4 or IPv6 address, IPv4 or IPv6 address range, IPv4 or IPv6 network, or Network Group. For Classic policies, it can be IPv4 address or network.
Application	It indicates the Application, Application Group, Application on Custom Port, Service, or Service Group.
Effective Time	Indicates the time period when the rule is effective. Shows as Always for rules belonging to Classic policies.
Service	This is displayed only if Classic policies are applied. It indicates the service defined for the rule.
Response	The response action to be taken by the Sensor on traffic that matches the rule.
Rule Origin	**Policy** — Name of the Firewall policy to which the rule belongs. **Assigned to** — Name of the interface to which the policy is assigned to.

To view the Effective Rules:

1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Select **Policy Manager**. List of interfaces for the Sensors configured is displayed.
4. Double-click the interface of a Sensor for which you wish you view the Effective Rules. The **<Device Name/Interface>** panel opens.
5. In the **Firewall** section, click **Inbound** or **Outbound** option under **Effective Rules** to view the rules configured.

Computing the number of access rules utilized per Sensor

You can calculate the number of Firewall access rules being utilized per Sensor by adding all the rules configured at the Sensor-level, port-level, and interface or subinterface level.

Example: Computing access rules utilized per Sensor

On an NS7200 Sensor, if you configure 8 rules at the Sensor level, 20 rules on port pair G3/1-G3/2, and 10 rules on the subinterface of G3/3-G3/4, you would have utilized 38 out of the 3000 limit.

You can also calculate the number of access rules utilized by adding the number of rules displayed under Inbound Rules and Outbound Rules link at each port, interface, and subinterface level of the Sensor.

Computing the number of access rules utilized during port clustering

When port clustering (interface grouping) is used, and port-level access rules are configured, the number of access rules utilized (for each port-cluster-level access rule) will be different based on the participant port-types of the cluster. One rule will be consumed per each inline port-pair member, and one rule will be consumed per each SPAN port member of the port cluster.

Examples: Computing the effective access rule utilization for each port-level access rule defined for a port-cluster

Port cluster 1: If your port cluster consists of G3/1-G3/2 (inline, fail-open), G3/3 (SPAN), and G3/5-G3/6 (inline, fail-close), 3 rules will be consumed for each rule configured at the port level.

Port cluster 2: If your port cluster consists of G3/1 (SPAN), G3/3 (SPAN), G3/5 (SPAN), G3/7-G3/8 (inline, fail-close), 4 rules will be consumed for each rule configured at the port level.

Quality of Service policies

Quality of Service (QoS) policies help in avoiding traffic congestions, controlling the actual traffic flow within the permissible limit of the network, and limiting traffic surges in your network. Trellix IPS provides two traffic management features — *DiffServ tagging* and *IEEE 802.1p (VLAN) tagging*.

- Differentiated services, or DiffServ, operates on the principle of traffic classification, where each data packet is classified and placed into a limited number of traffic classes. You can configure network devices which support DiffServ, such as a router, to differentiate traffic based on its class. So, you can manage each traffic class differently, ensuring preferential treatment for higher-priority traffic on the network. The Sensor provides DiffServ tagging of packets. The tagged packets are used by DiffServ-compliant external network devices for traffic management.
- IEEE 802.1p specification enables network devices to prioritize traffic at the media access control (MAC) layer, and perform dynamic multi-cast filtering. The 802.1p header includes a three-bit field for prioritization, which allows packets to be grouped into various traffic classes. The three-bit prioritization field provides eight different classes of service to the user.

The way the traffic is treated when assigned to any particular class is undefined, and left to the implementation on your network. The Sensor provides VLAN 802.1p tagging of packets, which are sent to VLAN 802.1p-compliant external network devices for traffic management.

NOTE

For DiffServ tagging and VLAN 802.1p tagging, the Sensor's role is limited to just tagging the traffic. You must configure the corresponding network devices like switches and routers to provide QoS based on these tags.

QoS features

- Configuring the QoS feature is to some extent similar to the Firewall feature. You define the QoS policy and the component rules for DiffServ tagging and VLAN 802.p tagging. Then you assign this policy to inline ports. These QoS rules are similar to Firewall access rules in the way the Sensor executes them.
- You can configure the following as the criteria in a QoS rule:
  - Source of the traffic:
    - Country
    - Host name
    - IPv4 or IPv6 addresses, address ranges, or networks
    - Windows Active Directory user names or user groups
  - Destination of the traffic:
    - Country
    - Host name
    - IPv4 or IPv6 addresses, address ranges, or networks
  - Applications such as Facebook, Yahoo! Instant Messenger, and Gmail. You can specify a group of applications. You can also specify features of an application, such as the file transfer feature of Yahoo! Messenger.
  - Services or groups of services
  - You can also set a time period during which the Sensor should apply a QoS rule.
- You define separate sets of rules for DiffServ and 802.1p that the Sensor executes in a top-down fashion. When the traffic matches a rule, the Sensor tags the traffic with the corresponding DiffServ or 802.1p value specified in the rule.

Advantages

- You can identify traffic at a very granular level and provide QoS accordingly. For example, you can restrict social-networking traffic to a very low bandwidth so that it does not affect the QoS of your business applications.
- You can enforce different policies based on time. For example, you can have a higher bandwidth for gaming applications on weekends but a low one during weekdays.
- You can provide QoS based on geographical locations.
- You can provide QoS based on the phase of an application. For example, you can differentiate chatting through Yahoo! Messenger from file transfers through Yahoo! Messenger.

- You can provide differential QoS based on the sub-networks within your enterprise network. For example, you can have a bigger bandwidth for your engineering subnet when compared to your finance subnet. For environments where the IPs are likely to change frequently, you can base QoS on Windows Active Directory user names.
- You can enable or disable each rule in your QoS policies. This can help you to narrow down on the rules when troubleshooting.
- The modular design of the QoS feature greatly facilitates reusability:
  - You can define the criteria as rule objects and use them for Firewall, Ignore Rules, and QoS.
  - You can define a QoS policy with the component rules and assign it to multiple monitoring ports.

Component of the QoS feature

At the highest level, QoS policy is considered as the component of QoS feature.

QoS policy — QoS is basically about classifying your network traffic and then giving it a preferential treatment accordingly. For example, it can involve classifying the traffic that is critical to your business operations and provide this class of traffic the highest preference in your network. To enable the Sensor to classify traffic, you define a set of rules that are similar to Firewall access rules. A QoS rule contains a set of criteria. The Sensor matches the detected traffic against these rules. So, it is possible to match all the traffic to be added to a specific QoS rule.

Similar to how a Firewall policy contains the Firewall access rules, a QoS policy contains the QoS rules. A QoS policy contains separate sets of QoS rules for each of the traffic management techniques - DiffServ tagging and IEEE 802.1p (VLAN) tagging.

Types of QoS policies — Two types of QoS policies are available in Trellix IPS. They are advanced and classic QoS policies. Functionally, these two types are similar. However, as the names may suggest, advanced QoS policies provide you more options to identify traffic when compared to classic.

NOTE

None of the NS-series or Virtual IPS Sensor models supports traffic management.

Components of a QoS policy

To effectively use QoS policies, familiarize yourself with its components.

QoS policies — A Sensor applies a QoS policy on the egress traffic to classify the traffic for QoS. As explained in the earlier sections, there are two types of QoS policies — advanced and classic.

QoS rules — QoS rules are the building blocks of a QoS policy. QoS rules are an ordered set of rules, which enable the Sensor to classify traffic.

Rule objects — You use rule objects to define QoS rules. Rule objects are mappings to one or more components related to your network traffic. Examples of rule objects are applications, source and destination hosts, source and destination networks, and so on. For example, you can group a set of IPv6 addresses to create a rule object. Then you can create a QoS rule in which you specify this rule object as the source or destination of traffic. Every time you want to refer to this set of IP addresses in your rules, you just use this rule object.

Rule objects are common to Ignore Rules, Firewall access rules, QoS, and Quarantine. With respect to a domain and its child domains, the rule objects that you create for one of these features is automatically available for other applicable features. For example, if you create a IPv4 Endpoint rule object for QoS, it is available for use in Ignore Rules, Firewall Access Rules, QoS, and Quarantine.

The Service rule object is available for both classic and advanced QoS policies. Except for Service, all of the following rule objects are available only for advanced QoS policies.

- **Applications** — These are the various software programs that the Sensor can detect. The Manager derives the list of applications from the signature set. You cannot modify the list of available applications.

  IMPORTANT

  If Trellix Advanced Research Center deprecate an application that you have used in a QoS policy, a fault message of *warning* severity is raised. You will then have to delete those rules from the policies or modify them; if not, signature set push to Sensors will fail.

- **Application on Custom Port** — You can use rule object to detect applications when they are communicated over specific ports. For example, you might want the Sensor to detect FTP, when it is over port 2021.
- **Application Group** — If the pre-defined Application Groups do not meet your requirements, you can create one. You create an Application Group to combine more than one application and Application on Custom Port rule objects. Typically, you create an Application Group for those applications that you want the Sensor to handle in a similar fashion. For example, you can combine all applications related to Internet games to form one Application Group. You can group up to 10 items in an Application Group.

  NOTE

  You can combine Application and Application on Custom Port rule objects to form an Application Group. You cannot include Application Group within another Application Group.

- **Country** — The Country rule object enables you to identify traffic based on the source or destination country for QoS. The Sensor identifies the traffic originating or destined to these countries based on the CIDRs mapped to the countries.

  The country-to-CIDRs mapping information is sourced from the geolocation database of Digital Envoy. You cannot modify or update this list of countries manually. Trellix updates this list of country-to-CIDRs mapping through signature sets. Use the **`status`** command in a Sensor's CLI to check if the geolocation database is present on the Sensor.

  NOTE

  If the Manager and Sensor are on software versions prior to 10.1 Update 7, it is recommended to upgrade them to later versions to continue receiving the updated geolocation databases. For more information, refer to KB95636. Always ensure to maintain the latest software versions of the Manager, Sensor, and Signature Sets.

- **IPv4 Endpoint** — You can create a list of source and destination IPv4 addresses that you want to use in a QoS rule. You can specify up to 10 addresses in a rule object.
- **IPv6 Endpoint** — You can create a list of source and destination IPv6 addresses that you want to use in a QoS rule. You can specify up to 10 addresses in a rule object.
- **Host DNS Name** — You can create the list of source and destination host names that you want to use in a QoS rule. For example, you can create a Host DNS Name rule object for facebook.com, faceparty.co.uk, and ibibo.com. You can add 10 Host DNS Names in a rule object. The Sensor contacts the DNS servers that you configure in the **Name Resolution** page to resolve these names to IP addresses. To go to the **Name Resolution** page of a Sensor, under the **Devices** tab, select <Admin Domain Name> → Devices → <Device Name> → Setup → **Name Resolution**.

IMPORTANT

The Sensor uses only UDP and never falls back to TCP for DNS queries even if the DNS server forces for TCP.

- **IPv4 address range** — You can create the list of IPv4 addresses to use in a QoS rule. In the rule, you can specify an IPv4 address range as the source or destination of traffic. For example, you may want to apply a rule to traffic from IPs ranging from 10.1.1.1 to 10.1.1.25. You can specify up to 10 ranges in a rule object.
- **IPv6 address range** — You can create the list of IPv6 addresses to use in a QoS rule. In the rule, you can specify an IPv6 address range as the source or destination of traffic. You can specify up to 10 ranges in a rule object.
- **IPv4 Network** — You can create a list of IPv4 CIDRs to use in a QoS rule. In the rule, you can specify a CIDR as the source or destination of traffic. For example, you might want to apply a rule on the traffic targeted for 172.16.225.0/24 network. The three reserved IPv4 ranges according to RFC 1918 are provided as default networks. You can specify up to 10 CIDRs in one rule object.
- **IPv6 Network** — You can create a list of IPv6 CIDRs to use in a QoS rule. In the rule, you can specify a CIDR as the source or destination of traffic. You can specify up to 10 CIDRs in one rule object.
- **Network Group** — You can combine one or more Country, Host IP, Host Name, IP range, or Network to form a Network Group. For example, you can combine all the North American countries and multiple IP ranges to form a Network Group rule object. You can specify up to 10 items in one Network Group rule object.

NOTE

The Network Group rule object that you create can contain either IPv4-based rule objects or IPv6-based rule objects. You cannot combine IPv4 and IPv6 rule objects in one Network Group rule object.

- **Finite Time Period** — You can configure the Sensor to enforce a QoS rule continuously just for a specific time period. For example, you might want to enforce a rule from 9 am on June 10 to 10 am on June 11. For this, you need to create a Finite Time Period rule object specifying the start time and date along with the end time and date. The start and end time are both inclusive. You can specify only one Finite Time Period rule object in a QoS rule. Time-based rules are implemented using the local time zone of the corresponding Sensor.
- **Recurring Time Period** — This rule object enables you to enforce a QoS rule at a certain frequency. For example, you can enforce a rule from 9 am to 5 pm on all weekdays. To enforce a rule just once, use the Finite Time Period rule object.

  When you use a time-based rule object, make sure you have configured the corresponding Time Zone. Time-based rules are implemented using the local time zone of the corresponding Sensor. Note that the Sensor automatically factors in the daylight savings time, where applicable. GMT is the default Time Zone in the Manager.
- **Recurring Time Period Group** — You can group up to 10 Recurring Time Periods to form a Recurring Time Period Group rule object.

NOTE

You can use the Finite Time Period rule object along with Recurring Time Period and Recurring Time Period Group rule objects. In such a case, the Finite Time Period takes precedence. Also, for the Sensor to check for that QoS rule, the Finite Time Period and at least one Recurring Time Period must be active.

- **Service** — To classify traffic based on the IP protocol, ICMP codes, or the TCP/UDP port numbers, use the Service rule object. You can create Service rule objects or use the default ones. The well-known services on standard TCP and UDP ports,

as well as ICMP codes are pre-defined. For example, telnet is predefined as TCP on port 23. Similarly, ICMP codes such as ICMP echo reply and ICMP request are pre-defined.

NOTE

ICMP-Fragmented, TCP-Fragmented, and UDP-Fragmented Service rule objects are not relevant for QoS.

When you create a Service rule object, the options are to specify the protocol number, TCP port, or UDP port. You can define only one IP protocol specification per rule object.

NOTE

For QoS rules that use Service rule objects, the Sensor factors in any non-standard ports that you have configured for IPS. For example, if you have specified port 2023 as the non-standard port for FTP, and if you have used the FTP Service rule object in a rule, then the Sensor considers FTP on both ports 21 and 2023.

For certain traffic, you can use more than a type of rule object. For example, for FTP and HTTP, you can use the Application rule object or the Service rule object. If you use the Application rule object, the Sensor does not consider the port number when detecting the traffic, and relies only on the application signatures. This means that the Sensor can detect a protocol regardless of the port used in case of Application rule objects. If you use the Service rule object, the port number matters when detecting a protocol. The Sensor considers all the standard ports as well as non-standard port numbers that you have defined in the **Non-Standard Ports** page.

In case of Service rule object, the Sensor can classify the traffic using even the SYN packet. In case of Application rule object, the Sensor can classify the traffic only after the three-way handshake. This is because, only after the handshake, the Sensor identifies the application.

NOTE

A Sensor processes the QoS rules in a top-down fashion. So, if you want to classify traffic based on Services, define those rules high up in the policy.

Note the following if you use classic QoS policies:

- It is not advisable to create rules for protocols such as FTP, TFTP, and RPC services that negotiate ports dynamically. For RPC services, you can configure rules for RPC as a whole, but not its constituents, such as statd and mountd.
- Multimedia protocols such as H.323 and services such as instant messaging and peer-to-peer communication either negotiate the data channel separate from the control channel or negotiate ports that do not follow a standard. However, you can define rules to classify these dynamic protocol instances by denying the fixed control port.

- **Service Group** — You can group the services that you want to be handled in a similar manner. This enables you to easily manage your QoS policies. You can group up to 10 services in one Service Group rule object. You cannot add Service Range objects in a Service Group.
- **Service Range** — You can define a Service Range rule object by defining the TCP or UDP port range. You can define up to 10 services ranges in one rule object. You can combine TCP ranges and UDP ranges in a Service Range rule object. Service Range is available only for QoS policies.

NOTE

The Service Range rule object is available only for QoS policies.

How QoS works

The following are the high-level steps involved in the configuration and implementation of QoS using Trellix IPS:

1. Make sure you have deployed Trellix IPS according to your requirement. See [Trellix Intrusion Prevention System Installation Guide] for details.
2. Make sure you have connected the monitoring ports to the networks that you want to monitor in inline mode. QoS is not applicable to SPAN or tap mode.
3. Create the rule objects that you plan to use in your QoS rules. For example, identify the IPv4 and IPv6 addresses and address ranges and create the corresponding rule objects. Similarly, verify if rule objects are available for the applications for which you want to provide QoS.
4. If you plan to use the Host DNS Name rule object, make sure you configure the DNS server details in the Manager. Also, make sure these servers are accessible to the Sensor's management port. If the DNS servers are not accessible, a fault message is raised.

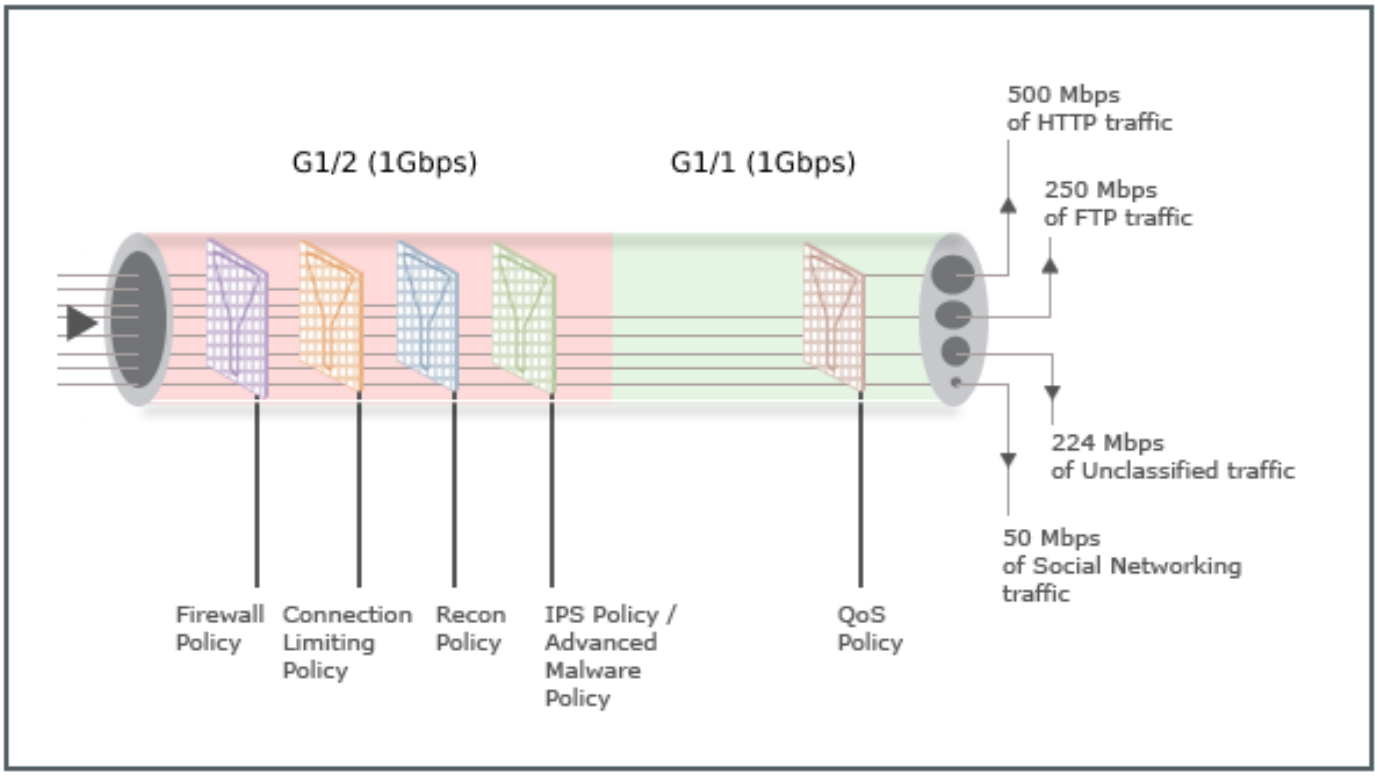
   NOTE

   The DNS server details apply to Firewall, QoS, integration with GTI for File Reputation, and NTBA.
5. If you plan to use user name or user group rule objects, make sure you have integrated the Manager with Trellix Logon Collector version 3.0.11 or above.
6. If you are using any time-based rule objects, make sure you have configured the Time Zone in the Manager. Time-based rules are implemented using the local time zone of the corresponding Sensor. The pre-configured Time Zone is GMT.
7. Create the required QoS policies at the corresponding admin domain. When you create a QoS policy, you define the QoS rules separately for DiffServ tagging and VLAN 802.1p tagging.
8. After you create a QoS policy, you must assign them to the corresponding inline port pairs.
   - You assign the QoS policies separately for inbound and outbound directions of a port pair.
   - You can assign only one QoS policy per direction (inbound/outbound) of a port pair.
   - You can assign a QoS policy to any number of port pairs.
   - You can assign the same QoS policy to both inbound and outbound directions.
9. After you complete assigning the QoS policies to the required Sensor resources, do a configuration update. The Sensor assigns the QoS policy to the corresponding Sensor monitoring ports. Consider port pair G1/1-G1/2 with a port speed of 1 Gbps in either direction. Assume G1/1 is connected to the outside network. Then the QoS policy that you assigned to G1/1-G1/2/Outbound is assigned to port G1/1. The QoS policy that you assigned to G1/1-G1/2/Inbound is assigned to port G1/2.

Notes and examples

- The important thing to note about QoS is that the policies are applied only to the traffic exiting the port-pair. Consider the example in the previous point. The traffic originating from your inside network is detected at G1/2. The Sensor applies the

Firewall, Connection Limiting, Recon, Advanced Malware, and IPS policies assigned to port G1/2 on this traffic but not the QoS policy. The traffic that is allowed to pass through according to these policies reaches G1/1 and about to egress out through G1/1. At this point, the QoS policy assigned to G1/1 is applied on this traffic. Similarly, the traffic from the outside network enters through G1/1 and is subjected to the other IPS features. The QoS policy assigned to G1/2 is applied on this traffic when it exits through G1/2.



- When the Sensor applies a QoS policy, it matches the traffic against the Diff Serv and 802.1p rules simultaneously. That is, it applies the Diff Serv and 802.1p rules in a top-down fashion on the traffic. When a rule matches the traffic, the Sensor does not consider the remaining rules of the same type.
- To understand how the DiffServ technique works:
  - Consider you have created a QoS policy named QoS_Policy. You have made sure you have the required rule objects to create this policy.
  - Consider port G1/2 which is connected to your inside network. Assume that the port speed of G1/2 is 1 Gbps
  - To keep it simple, consider the policy QoS_Policy assigned to G1/2.
  - The first Diff Serv rule is to identify SSL traffic. So, in the **Application** column, you select the SSL Service rule object. In the **Diff Serv Tag** column, you specify 60.
  - The second rule is to identify HTTP traffic. So, in the **Application** column, you select HTTP service rule object. In the **Diff Serv Tag** column, you specify 50.
  - The third rule is to identify FTP traffic. So, in the **Application** column, you select FTP service rule object. In the **Diff Serv Tag** column, you specify 40.
- Again, to understand how 802.1p tagging works, consider the same example. Assume that the first 802.1p rule is assigned a 802.1p VLAN priority value of 6, the second a 802.1p VLAN priority value of 5, and the third rule a 802.1p VLAN priority value of 4.

- The SSL traffic going out through port G1/2 is tagged 60 for DiffServ; tagged with 6 for 802.1p; and restricted to 300 Mbps.
- In case of DiffServ and 802.1p, you can specify if you want the Sensor to tag value of zero for unclassified traffic.

  Suppose you have specified the DiffServ tag value to be set to zero for unclassified traffic. In our example, there is no DiffServ rule to identify Telnet. So, the Telnet traffic exiting through G1/2 is treated as unclassified. If, for example, this Telnet traffic reaches the Sensor with a DiffServ tag value of 10, then the Sensor tags the Telnet traffic with a zero value, and then passes it on to the external network device for DiffServ categorization.

  On the other hand, you have opted for the tag value as seen on the wire. Now the telnet traffic exiting out of G1/2 reaches is sent out with the tag value of 10. That is the Sensor does not alter the tagging.
- The user-based rule objects and application-related rule objects work the same way as in the case of Firewall policies. Refer to the Firewall policies section to understand how these features work.
- You can view the number of bytes and packets that the Sensor dropped for a specific class of traffic under **Traffic Statistics**.

Configuring QoS

The high-level steps to configure QoS are as follows:

1. Create the required rule objects.
2. Define the QoS policy with the component rules for DiffServ and 802.1p.
3. Assign the QoS policy to the required inline port pairs.

The **QoS Policy** configuration report details the configuration information for each port on the Sensor. To access this report, select the domain on the **Manager** tab. Then select Reporting → Configuration Reports → **QoS Policy**. See [Trellix Intrusion Prevention System Product Guide] for information on how to generate this report.

Manage rule objects

You use rule objects to define Firewall and QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones, and NTBA Communication Rules. To manage the rule objects, go to Policy → <Admin Domain Name> → Intrusion Prevention → Objects → **Rule Objects**.

Option	Definition
Rule Objects	Displays the rule objects according to the filter criteria. Click a column heading to sort the table in ascending or descending order. • **Name** — Indicates the name of the rule objects • **Description** — Indicates the description of the rule object • **Type** — Indicates the rule object type • **Owner Domain** — Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain. • **Visibility** — Indicates the visibility settings of settings to the domains, whether it is visible only to the owner domain or to both owner and child domains • **Editable here** — **Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.
Object Type	Filters rule objects in the list. • **Default Objects Only** — Trellix pre-defined these rule objects. For example, the Application and Country are default rule objects. You cannot define these rule objects. • **Custom Objects Only** — You need to define these rule objects. For example, you need to define the Host DNS Name rule object. • **Custom and Default Objects** — When selected, it displays both the predefined and user defined rule objects. For example, IPv4 Network Rule Object has the 3 reserved private networks pre-defined, but you can also create your Network rule objects.
Rule Object Type	Select the rule object type that you want to view.
Search	Type your search criteria in the field to find rule objects with matching elements. For example, type **`google`** to list the rule objects containing *google* as part of their names.
 icon	Creates a custom rule object
 icon	Clones a rule object. You cannot clone default rule objects other than the IPv4 network rule objects.
 icon	Deletes a custom rule object belonging to the current admin domain
Save as CSV	Saves the rule objects for the rule object type selected
To view or edit a rule object	Double-click the rule object belonging to the current admin domain.

In the Manager, each rule object type has an associated icon for easy identification. The following table lists the rule objects and the corresponding icons.

Table 66. Rule object icons

Icon	Rule Object
	Application
	Application Group
	Application on Custom Port
	Country (displays the country's flag. So, the icon varies for each country)
	Finite Time Period
	Host DNS Name, IPv4 Endpoint, and IPv6 Endpoint
	IPv4 Address Range and IPv6 Address Range
	IPv4 Network and IPv6 Network
	Network Group (Network Group for Exception Object)
	Recurring Time Period
	Recurring Time Period Group
	Service
	Service Group and Service Range (Service Range is applicable only to QoS policies).

You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

Notes on IPv4 and IPv6 rule objects

For Firewall and QoS, IPv6 addresses are supported for the following rule objects:

- Host
- Address range
- Network

The default Service rule object for ICMPv6 is also now available.

- You use the above-listed, IPv6-based rule objects to create a Network Group rule object. However, you cannot use a combination of IPv4 and IPv6 based rule objects in one Network Group rule object.
- In a Firewall access rule or QoS rule, you cannot specify an IPv4-based rule object for one field and IPv6-based rule objects for other applicable fields. For example, if you select an IPv6-based rule object in the **Source Address** field, then you cannot specify IPv4-based rule objects for **Destination Address** or **Source User** fields. For this example, you can specify only an IPv6-based rule object or *other* as the value for **Destination Address** and *any* for **Source User**. Recall that User and User Group rule objects are considered as IPv4 based rule objects because Trellix Logon Collector does not collect user information from IPv6 hosts. Similarly, Country and Host DNS Name are also IPv4-based rule objects.

The following table classifies IPv4 and IPv6 rule objects:

Type	Rule objects
IPv4	IPv4 Endpoint, Host DNS Name, IPv4 Address Range, IPv4 Network, User, User Group, Country
IPv6	IPv6 Endpoint, IPv6 Address Range, IPv6 Network

You configure user-based Firewall access rules using the user and user group rule objects. It is important to note the following regarding these rule objects:

- You cannot create, modify, or delete the User or User Group rule objects. The Manager manages these rule objects according to the updates from Trellix Logon Collector.
- You can view these rule objects only n the **Access Rules** tab of the **Firewall** page. You cannot view these rule objects in the **Rule Objects** page.
- The user names verified through Kerberos snooping or the Sensor's Guest Portal are not displayed in the Manager.

View the rule objects

You can view existing rule objects in a selected domain.

For a rule object to be listed, it must meet one of these conditions:

- It is a default rule object.
- It is created at a parent admin domain, but it is set to be visible to the child admin domains.
- The rule object was created at the current admin domain.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

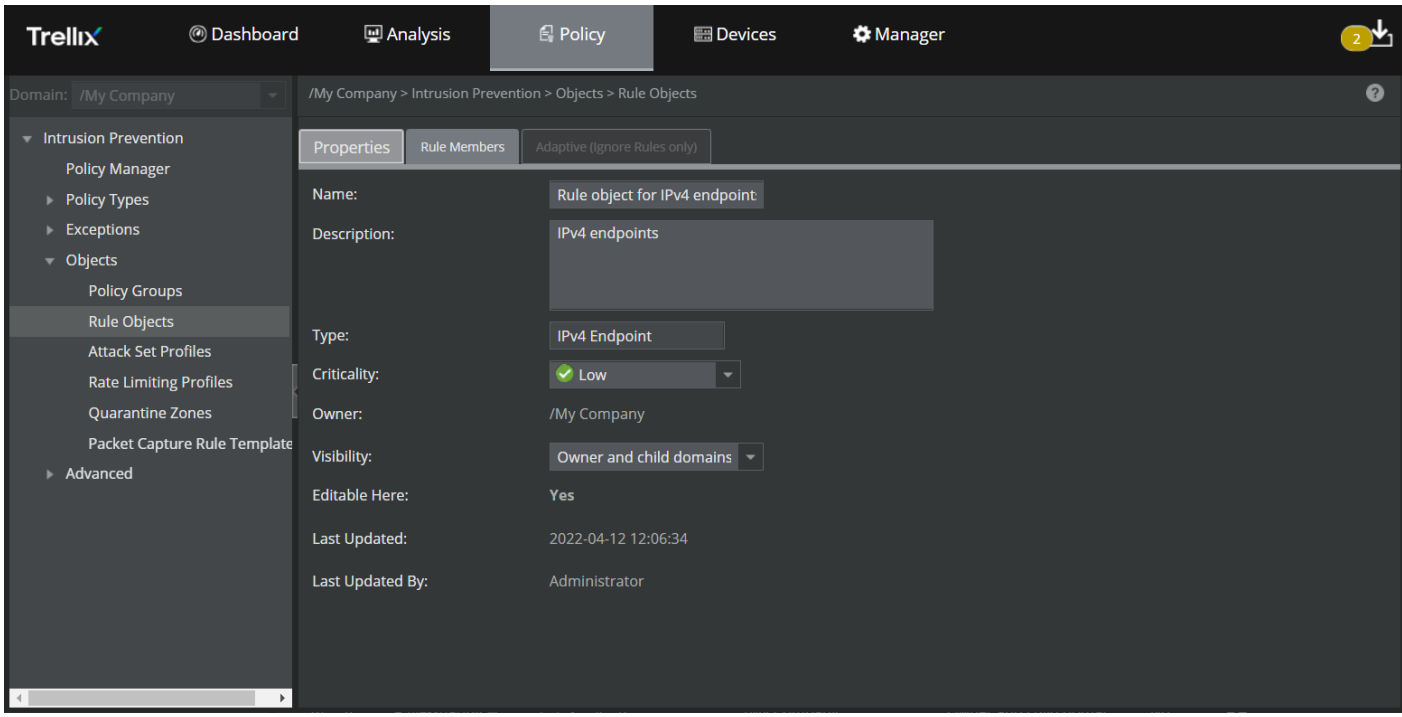
   Rule Objects for the selected admin domain are listed.

   - To locate specific rule objects, enter a string in the **Search** text box. For example, type “google” in the **Search** text box to list the rule objects containing “google” as part of their Names.
   - Select the **Custom Objects Only** or **Default Objects Only** or **Custom and Default Objects** from the drop-down list as required.

- Select the rule object type in the drop-down list.
- To view limited details of a rule object, point to the object. To view complete details, select and double-click the rule object.
- The rule object details appear under the **Properties** tab, and the rule members (rule object items) appear under the **Rule Members** tab.

> **NOTE**
>
> An additional tab named **Adaptive (Ignore Rules only)** appears while viewing IPv4 and IPv6 based rule objects.

Figure 557. Viewing Rule Objects



Add a rule object

You can create custom rule objects to use within the Firewall and QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones, and NTBA Communication Rules.

Following table lists the maximum count of rule object items (**Rule Members**) that can be added under each rule object type:

Rule Object type	Rule Members (Maximum count)
Host DNS Name	5000
IPv4 Address Range	20000
IPv4 Endpoint	140000

Rule Object type	Rule Members (Maximum count)
IPv4 Network	140000
IPv6 Address Range	20000
IPv6 Endpoint	140000
IPv6 Network	140000
Application Group, Application on Custom Port, Finite Time Period, Network Group, Network Group for Ignore Rules, Recurring Time Period, Recurring Time Period Group, Service, Service Group, Service Range	10

NOTE

The rule member count specified in the above table is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object.

NOTE

If you are using a Manager running on or before version 10.1.7.55 and a Sensor running on or before 10.1.5.153, the maximum count of rule members you can add under each rule object type is 10.

NOTE

The above rule object count specified for IPv4/IPv6 based rule objects is also applicable for Central Managers. Central Managers running on or before version 10.1.7.55, however, support only 10 rule members per each rule object.

NOTE

If you are using a Central Manager, do not add more than 10 entries in the Central Manager Rule Objects which are associated with QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones or Quarantine Exceptions in a Manager.

Steps:

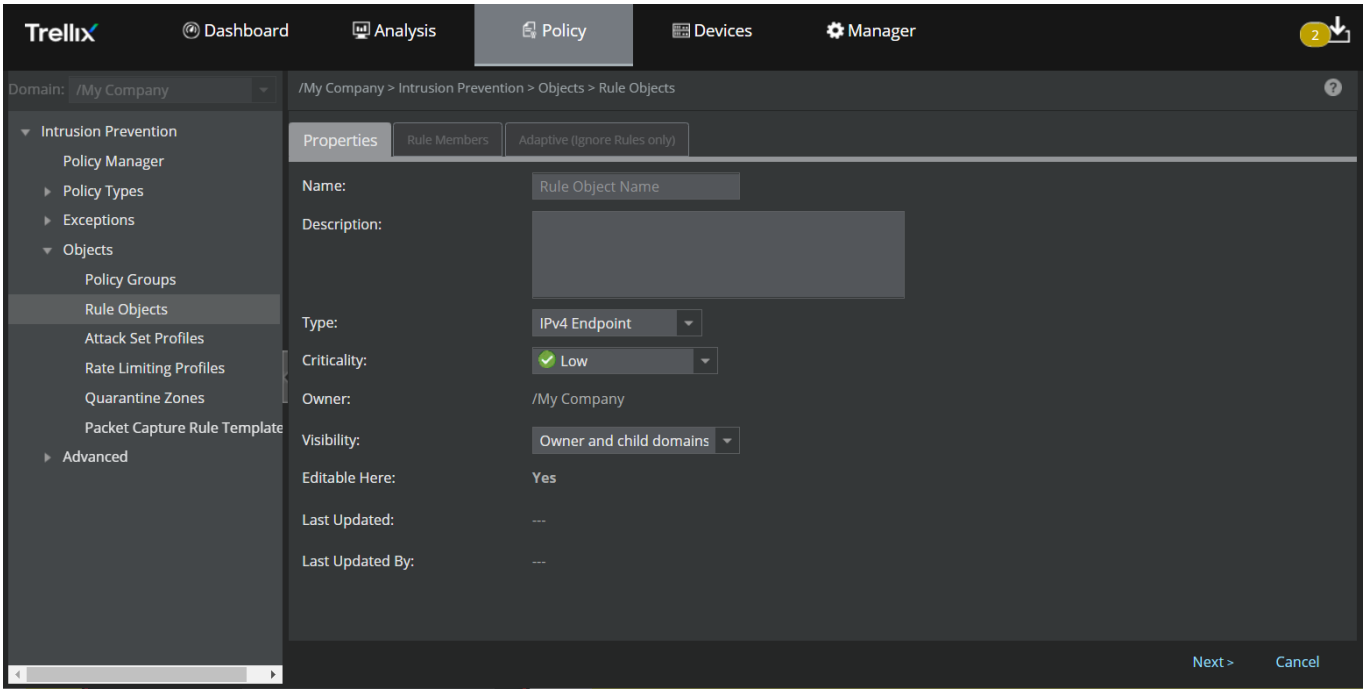
1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.
4. Click . This displays two tabs, namely the **Properties** tab and the **Rule Members** tab.

   NOTE

   An additional **Adaptive (Ignore Rules only)** tab appears while adding IPv4 and IPv6 based rule objects.

Figure 558. Selecting Criticality for each of your assets

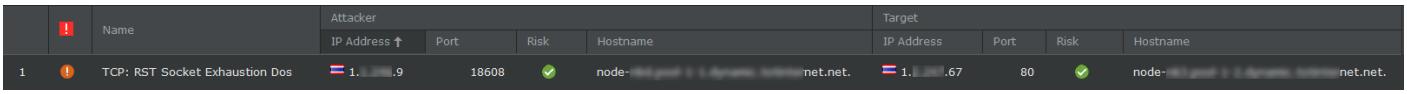


The following table describes the options in the **Properties** tab that are common to all rule objects.

Option	Definition
Name	Enter a unique name to easily identify the rule object.
Description	Enter the description for the rule object.
Type	From the drop-down list, select the type of rule object you want to create. For information on a specific object type, refer to the corresponding sub-section.
Criticality	[Optional] If you have chosen rule object type as IPv4 Endpoint or IPv6 Endpoint, you can specify the **Criticality** of that host by selecting **Low**, **Medium** or **High** from the drop-down list. By default, criticality is **Low**. Determining criticality of a host enables you to categorize all IPv4 Endpoint and IPv6 Endpoint addresses based on their importance to your organization.
Owner	Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain.
Visibility	From the drop-down list, select the option for the visibility level of the rule object. The available options are **Owner and child domains** and **Owner domain only**.
Editable Here	**Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.
Last Updated	Displays the date and time when a rule object was last updated
Last Updated By	Displays the user who modified a rule object

Once you assign criticality to a rule object and an alert involving it is raised, the criticality that you assigned shows up under specific columns in Attack Log. These columns are labeled **Attacker Risk** and **Target Risk**. **Attacker Hostname** and **Target Hostname** displays the names of the rule object.

Figure 559. Display of attacker risk



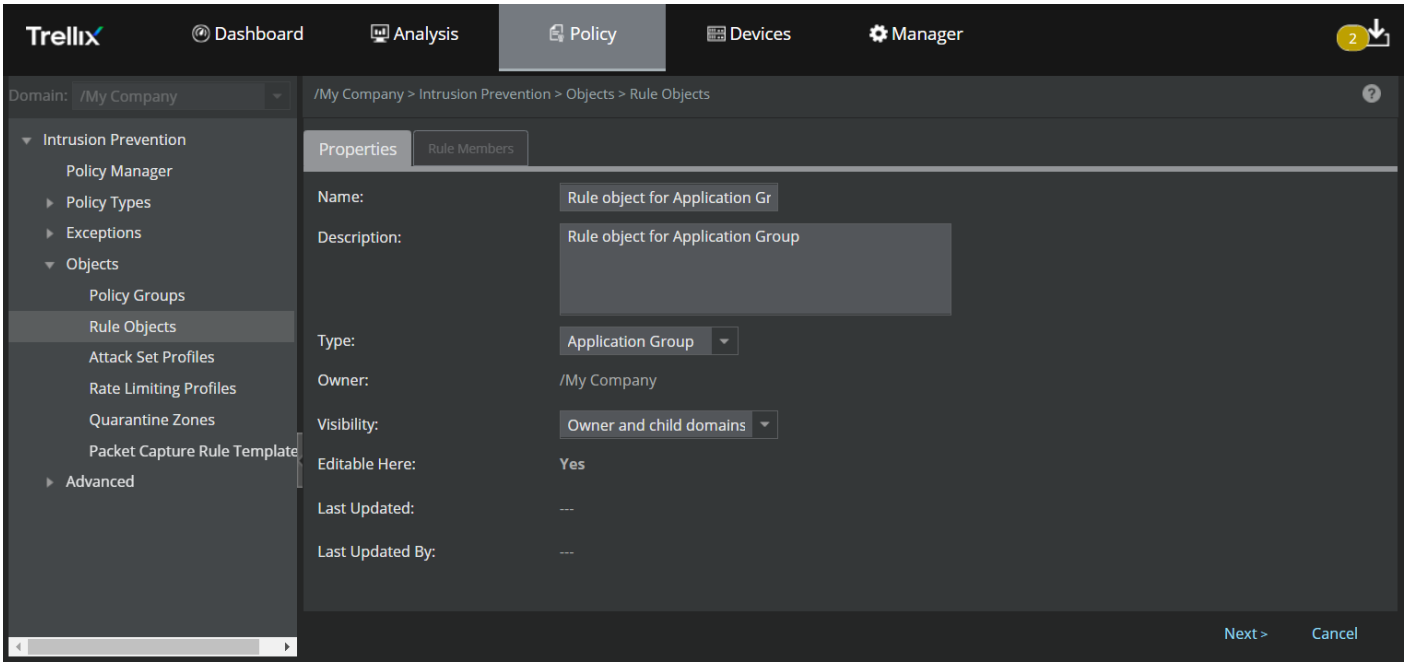
5. Enter the rule object options based on rule object you have selected in the **Type** drop-down list. For information on the subsequent steps to add a rule object, refer to the corresponding sub-sections.

Add an Application Group rule object

Follow these steps to add **Application Group** rule object:

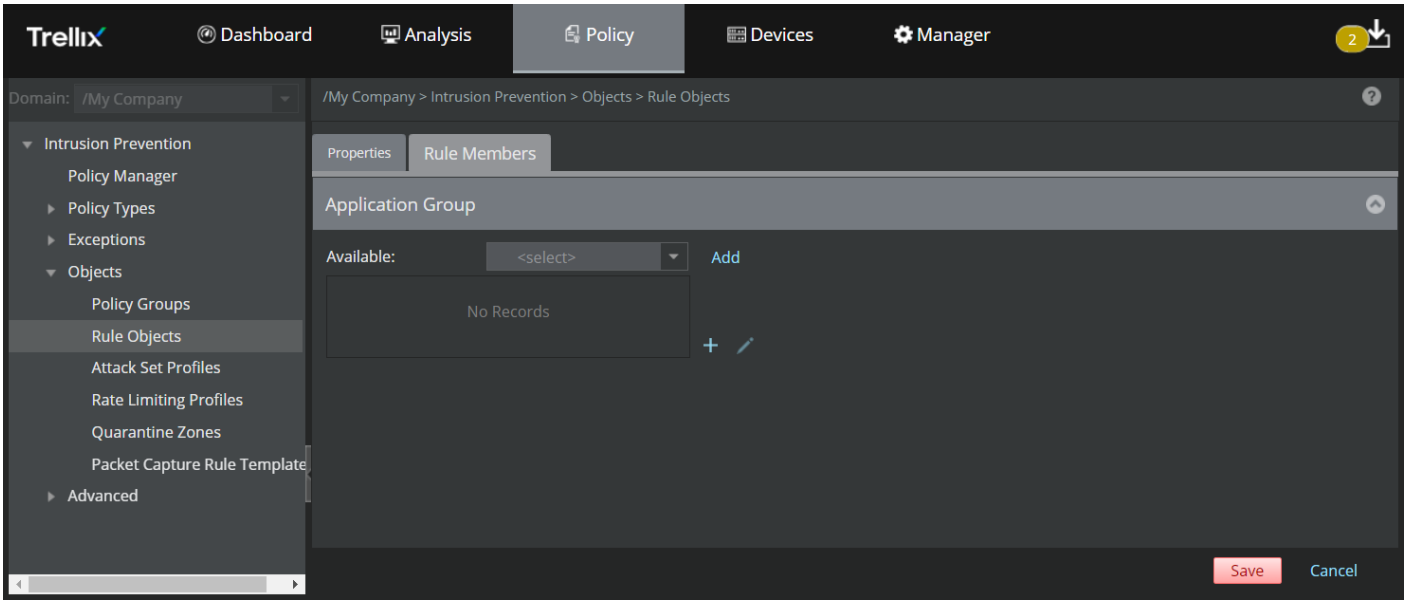
1. Upon specifying the options in the **Properties** tab and selecting **Application Group** from the rule object **Type** drop-down, click **Next**.

Figure 560. Create an Application Group rule object



The **Rule Members** tab is displayed.

Figure 561. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select a pre-defined application or an existing **Application on Custom Port** rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Members** list
	Click this icon to edit a rule member in the list
	Click this icon to add a new **Application on Custom Port** rule object
	Click this icon to remove a rule member from the list

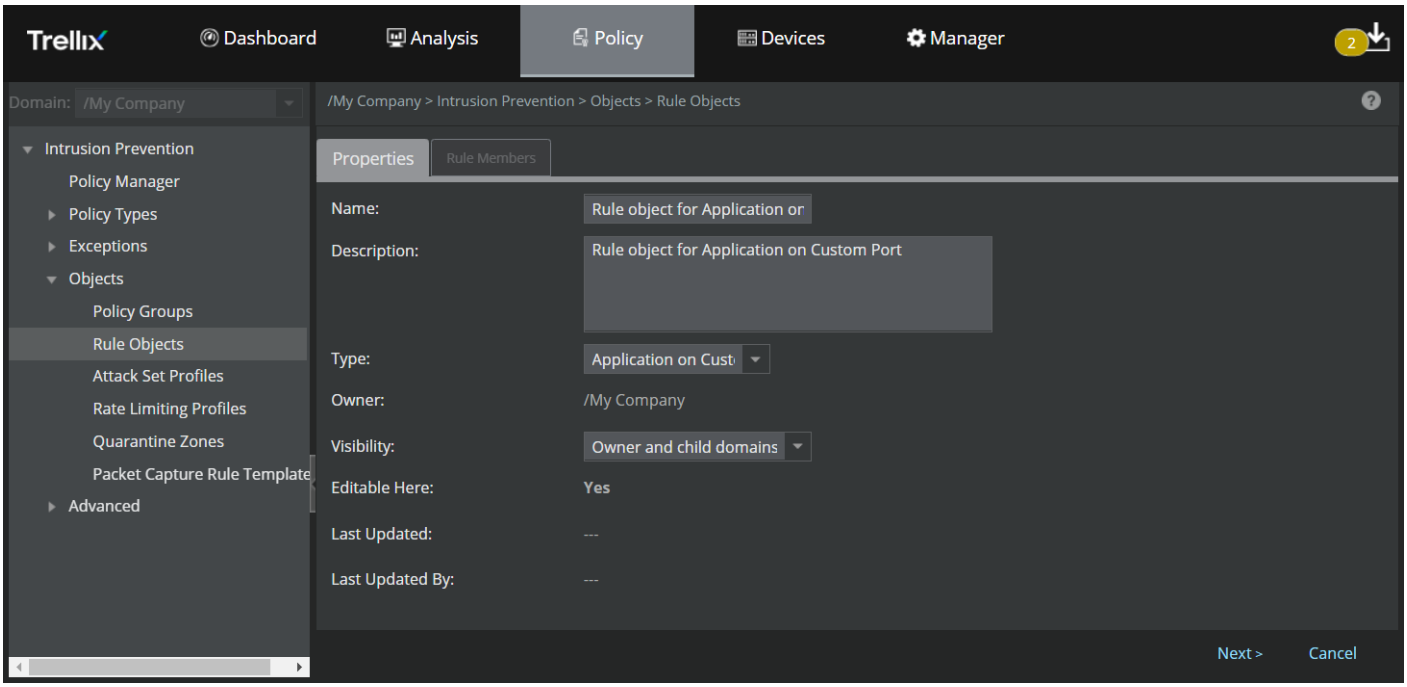
2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Add an Application on Custom Port rule object

Follow these steps to add **Application on Custom Port rule** rule object:

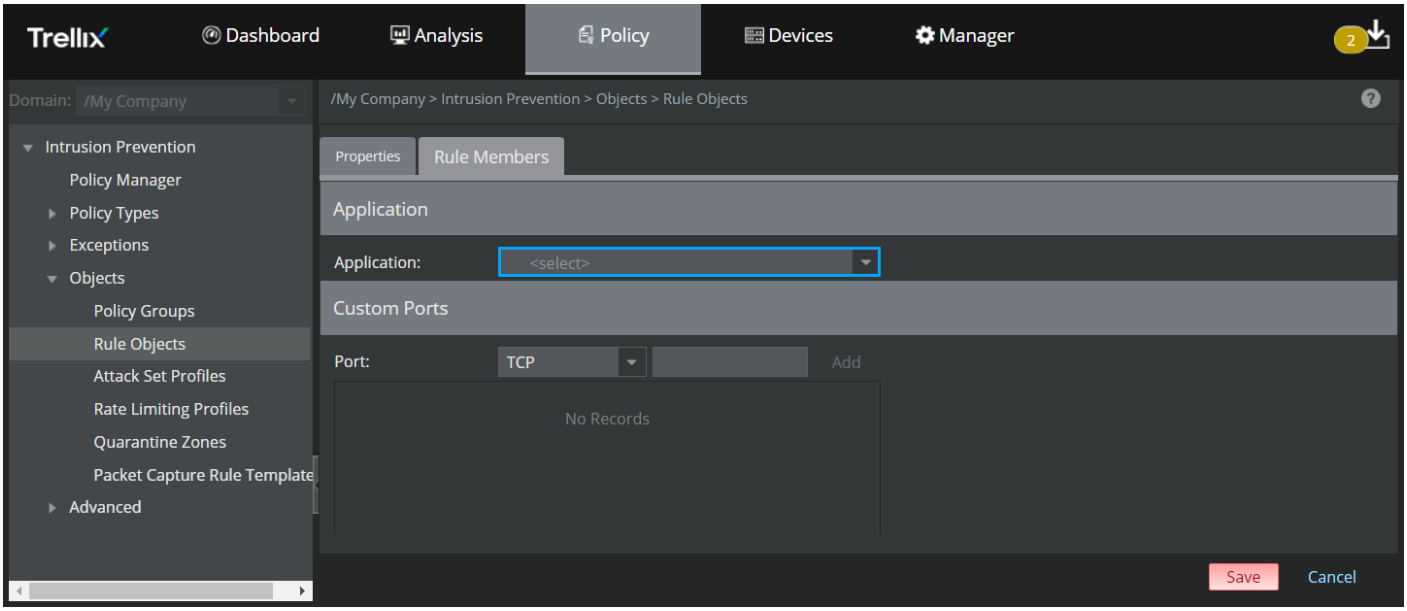
1. Upon specifying the options in the **Properties** tab and selecting **Application on Custom Port rule** from the rule object **Type** drop-down, click **Next**.

Figure 562. Create an Application on Custom Port rule object



The **Rule Members** tab is displayed.

Figure 563. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Application	Lists the pre-defined Application rule objects

Option	Definition
Custom Ports	Select TCP or UDP and type the port number (from 1 to 65534) in the adjacent text box.
Add	Click this button to add the selected IP protocol and the port number to the list. You can define up to 10 port numbers per Application.
	Click this icon to delete the selected IP protocol from the list.

2. Based on the above options, you can select an **Application** from the pre-defined list of applications and assign up to **10** TCP and UDP ports.
3. Click **Save**.

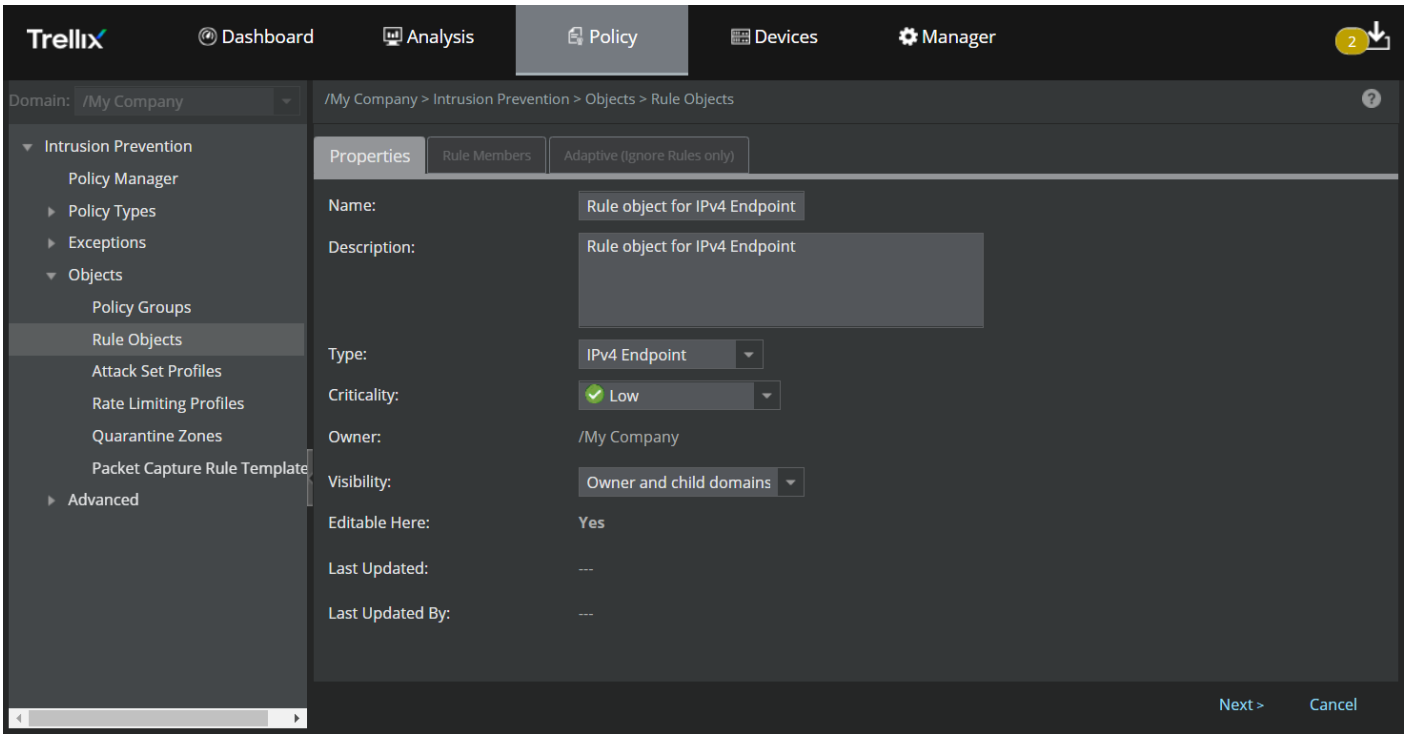
Add IPv4 Endpoint and IPv6 Endpoint rule objects

For quarantine zone access rules, only IPv4 Endpoint rule objects are supported. Also, only one rule member per rule object is applicable for quarantine zone.

The steps to add **IPv4 Endpoint** and **IPv6 Endpoint** rule objects are identical. Follow these steps to add **IPv4 Endpoint** or **IPv6 Endpoint** rule objects:

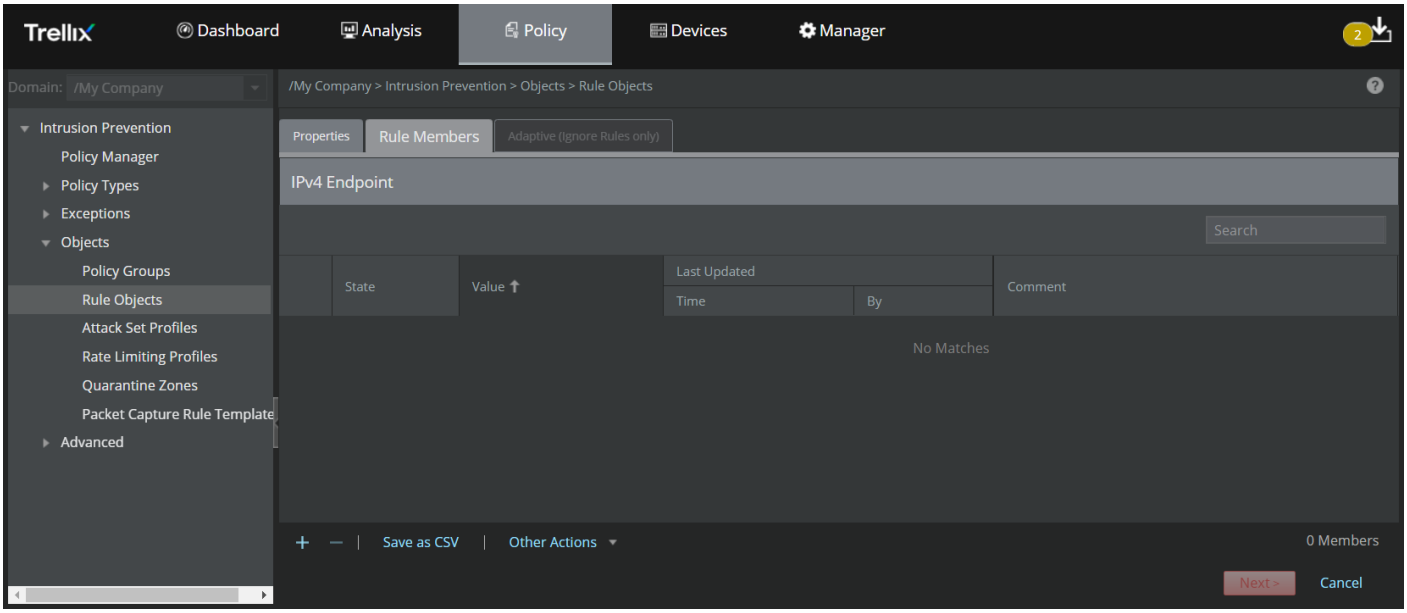
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Endpoint** or **IPv6 Endpoint** from the rule object **Type** drop-down, click **Next**.

Figure 564. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 565. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 67. Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 endpoint based on the rule object type selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 addresses
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address.
−	Click this icon to delete single or multiple IPv4 or IPv6 addresses.
Save as CSV	Click this button to export all the rule members displayed in the grid to a CSV file.
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 addresses • **Export All** — Allows you to export all the IP addresses from the Manager to the local system

2. There are two ways to add the IP addresses — add individual IP addresses using the + icon or import a list of IP addresses from a CSV file using the Other Actions → **Import** option.

3. To add an individual IPv4 or IPv6 address:

   a. Click the + icon.

   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

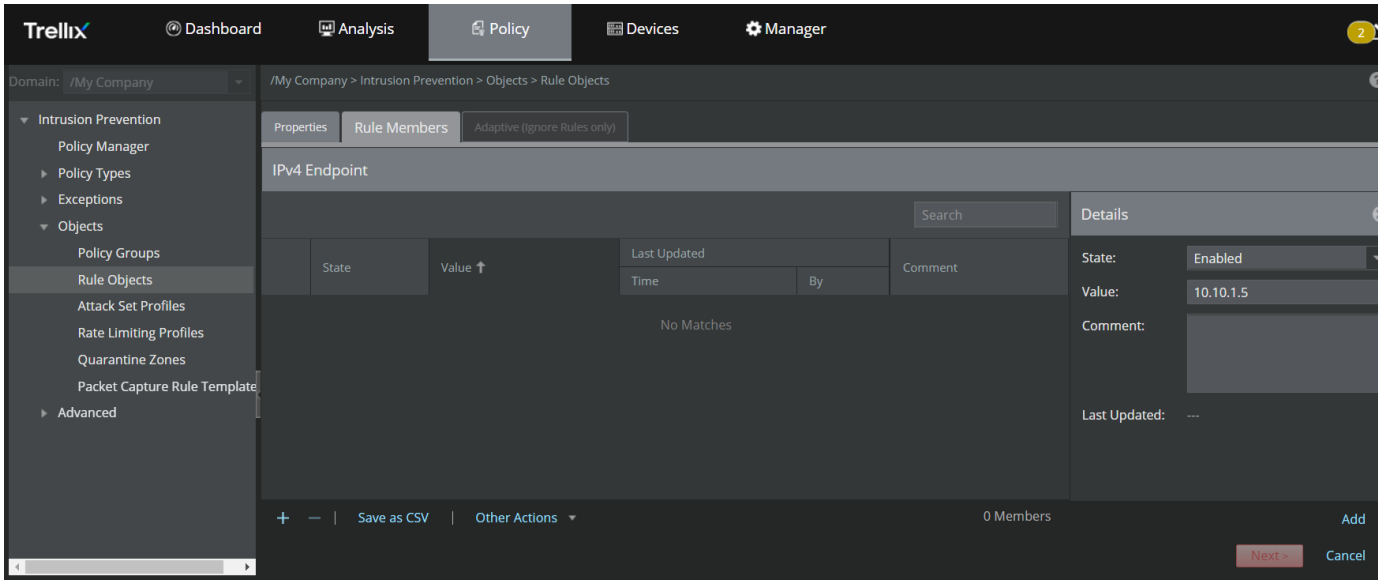
   For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object].

   Select the **State**, enter the IPv4 or IPv6 address in the **Value** field, enter a **Comment** if required and click **Add**.

   NOTE

   - Do not specify the CIDR prefix (32) when entering an IPv4 address.
   - You can enter an IPv6 address such as 5507:c0d0:2002:0071:0000:0000:0000:0003. The same address can be represented as 5507:c0d0:2002:0071::0003.
   - You can enter up to 140000 IPv4 or 140000 IPv6 addresses in a single rule object.
   - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
   - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 addresses in any rule object.

   Figure 566. Add individual IP addresses



   c. Upon adding all the required IP addresses, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add an IP address to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove an IP address from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of IP addresses from a CSV file using the **Import** option:

a. Click Other Actions → **Import**.

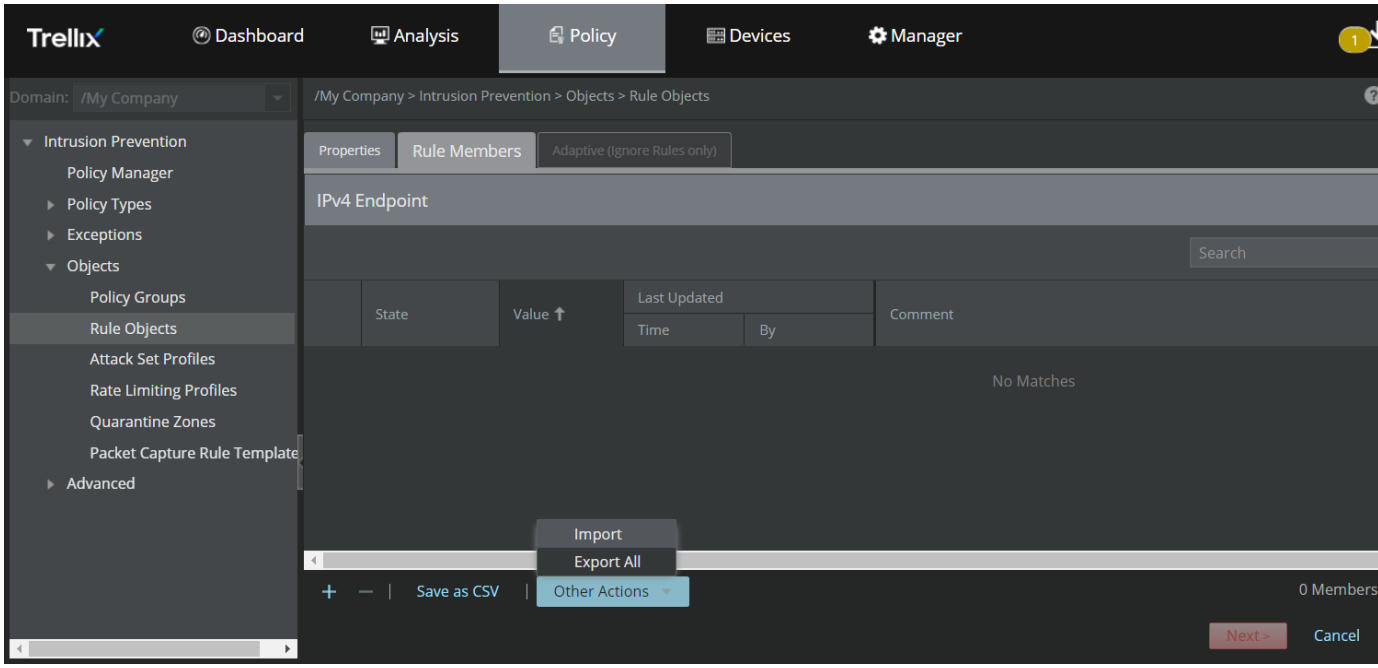
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10 entries.

Figure 567. Import IP addresses from a CSV file

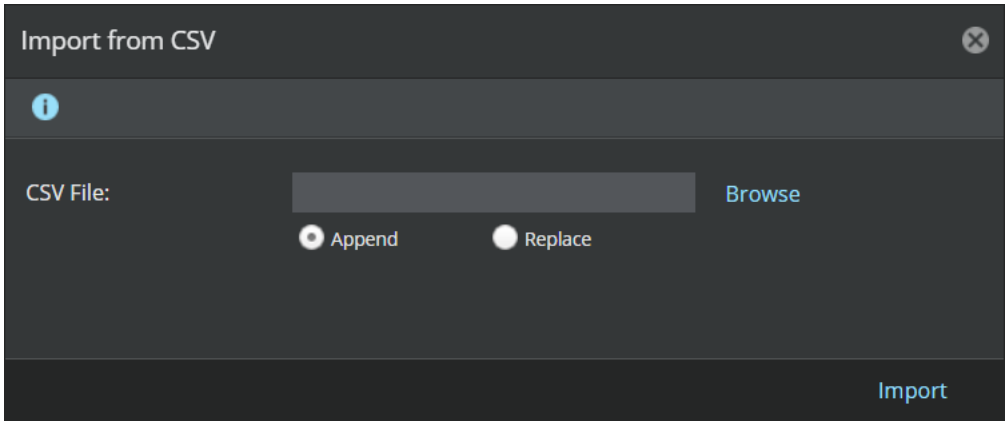


b. **Import from CSV** window appears. Use the **Append** option to add a new list of IP addresses or to append a list of IP addresses to an existing list. Use the **Replace** option to remove the existing list of IP addresses and add a new list from the file being imported.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IP addresses that you plan to import.

Figure 568. Import IP addresses from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 address>,<Comment>

Example file format: 10.10.1.1,textual description

The following is a sample for a CSV file with multiple IPv4 addresses:

Figure 569. CSV file format for IPv4 or IPv6 Endpoints

```
1  1    ..10,textual description
2  1    ..11,
3  1    ..12,
4  1    ..13,
5  1    ..14,
```

The following table describes the details of the IP addresses to be imported in the CSV file format.

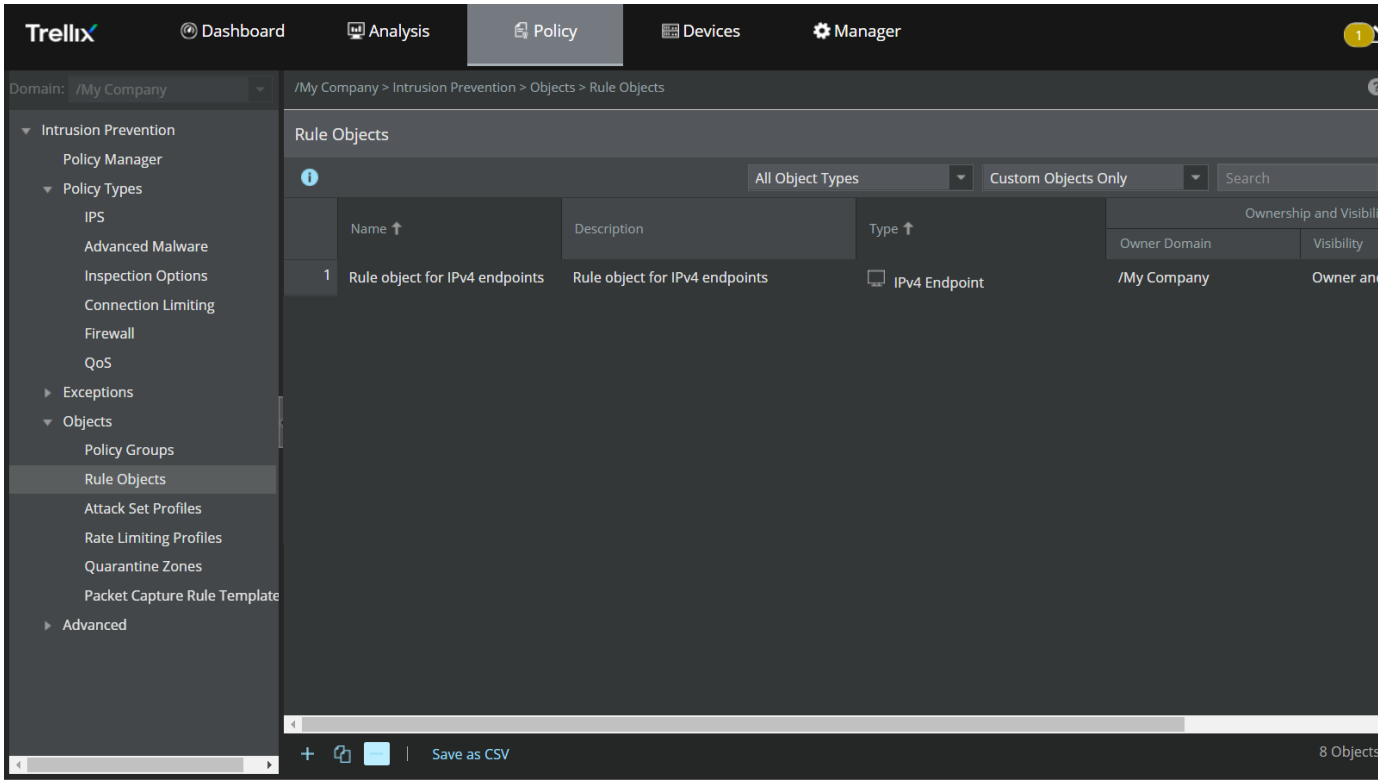
Format	Description
<IPv4 or IPv6 address>	Specifies the IP address to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (,) next to the entry and leave it.

d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

> **NOTE**
>
> The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

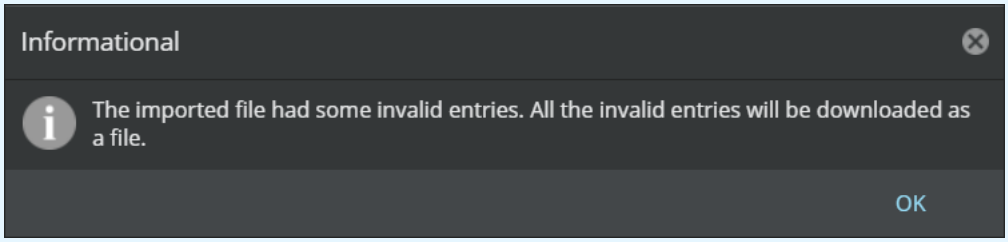
Figure 570. Rule object for IPv4/IPv6 endpoint successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 571. Information dialog-box for invalid entries

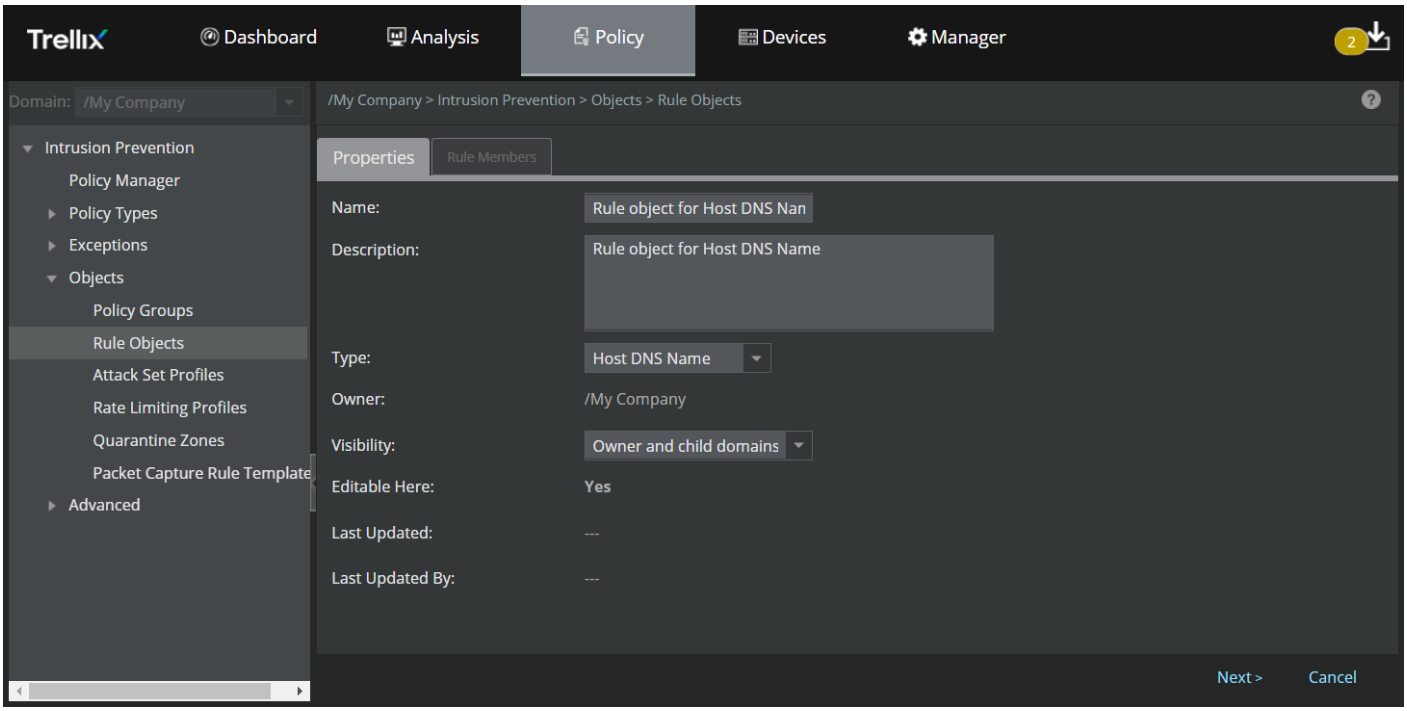


Add a Host DNS Name rule object

Follow these steps to add **Host DNS Name** rule object:

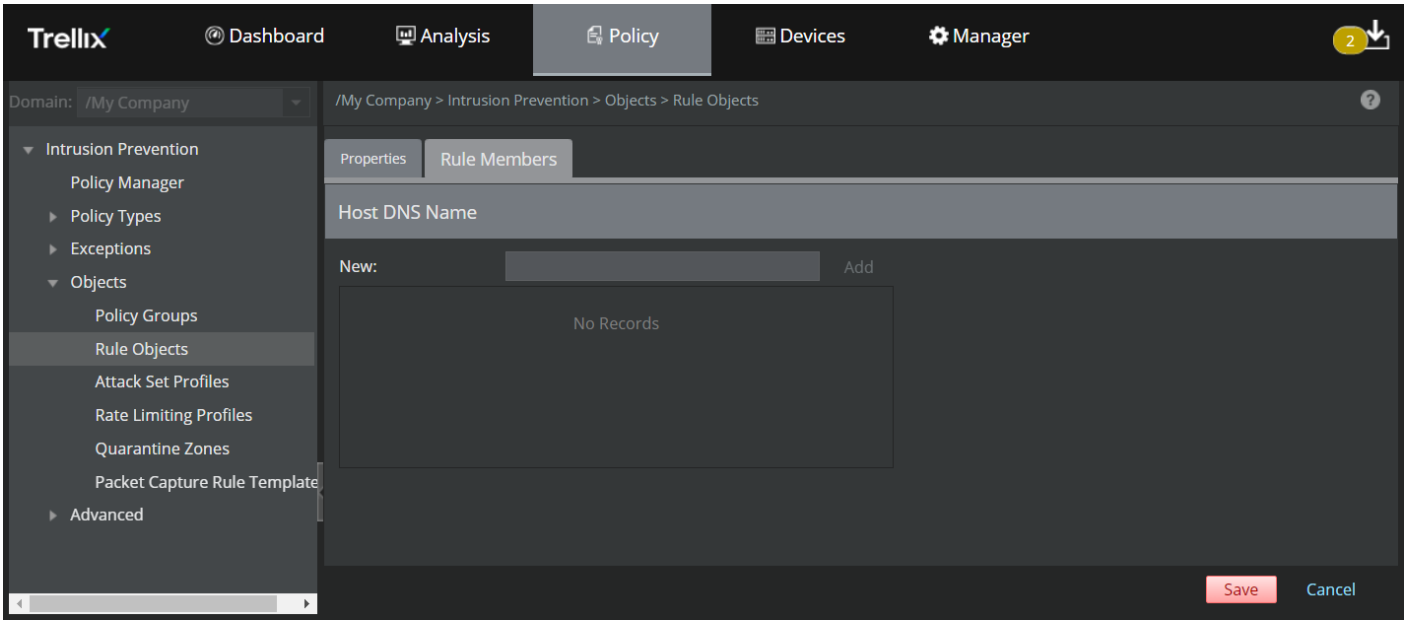
1. Upon specifying the options in the **Properties** tab and selecting **Host DNS Name** from the rule object **Type** drop-down, click **Next**.

Figure 572. Create a Host DNS Name rule object



The **Rule Members** tab is displayed.

Figure 573. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
New	Enter a fully-qualified domain name. If the domain name is not fully-qualified, the Sensor tries to resolve it using the DNS suffixes provided in the **Name Resolution** page. It communicates with the DNS server IPs configured in the **Name Resolution** page.
Add	Click this button to add the host name to the Host DNS Name list. You can add up to 5000 domain names. **NOTE** The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. **NOTE** If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 domain names in any rule object.
	Click this icon to remove the host name from the host names list

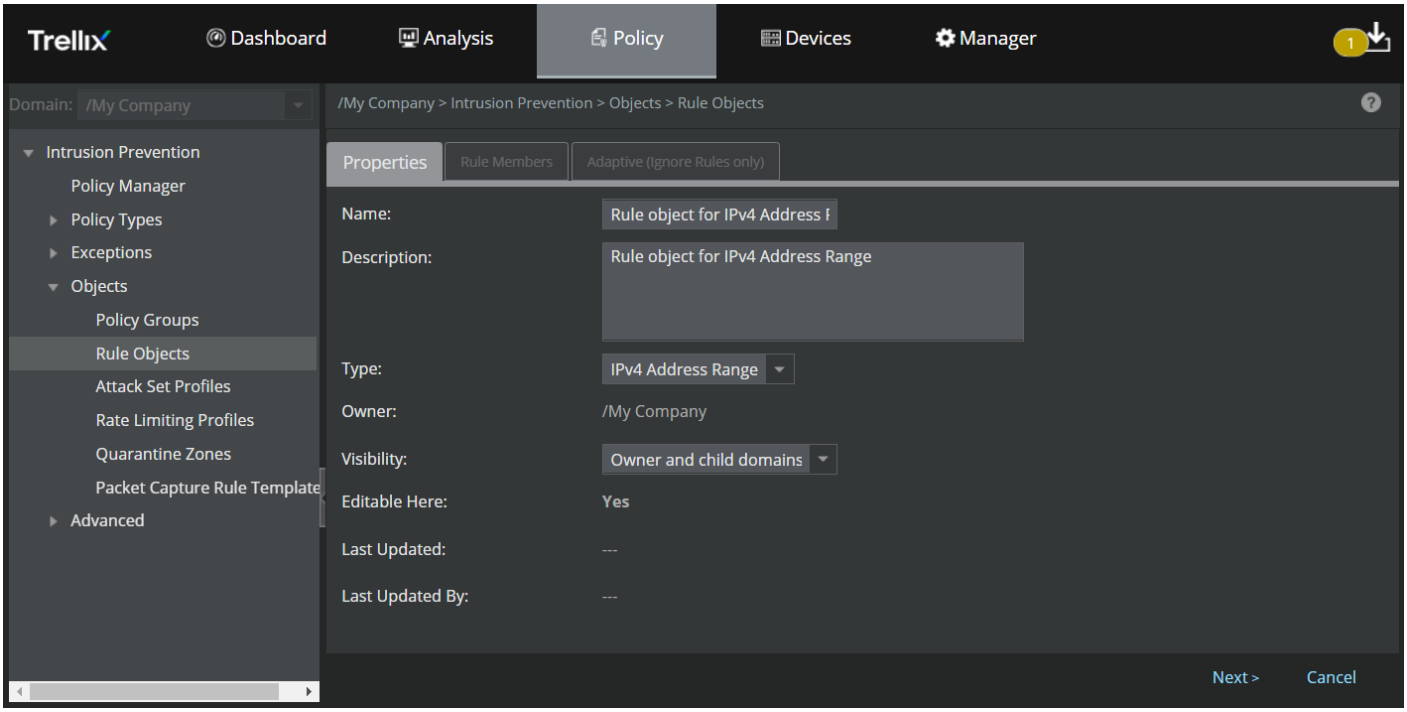
2. Based on the above options, you can add the domain names and click **Save**.

Add an IPv4 or IPv6 Address Range rule object

The steps to add **IPv4 Address Range** and **IPv6 Address Range** rule objects are identical. Follow these steps to add **IPv4 Address Range** or **IPv6 Address Range** rule objects:

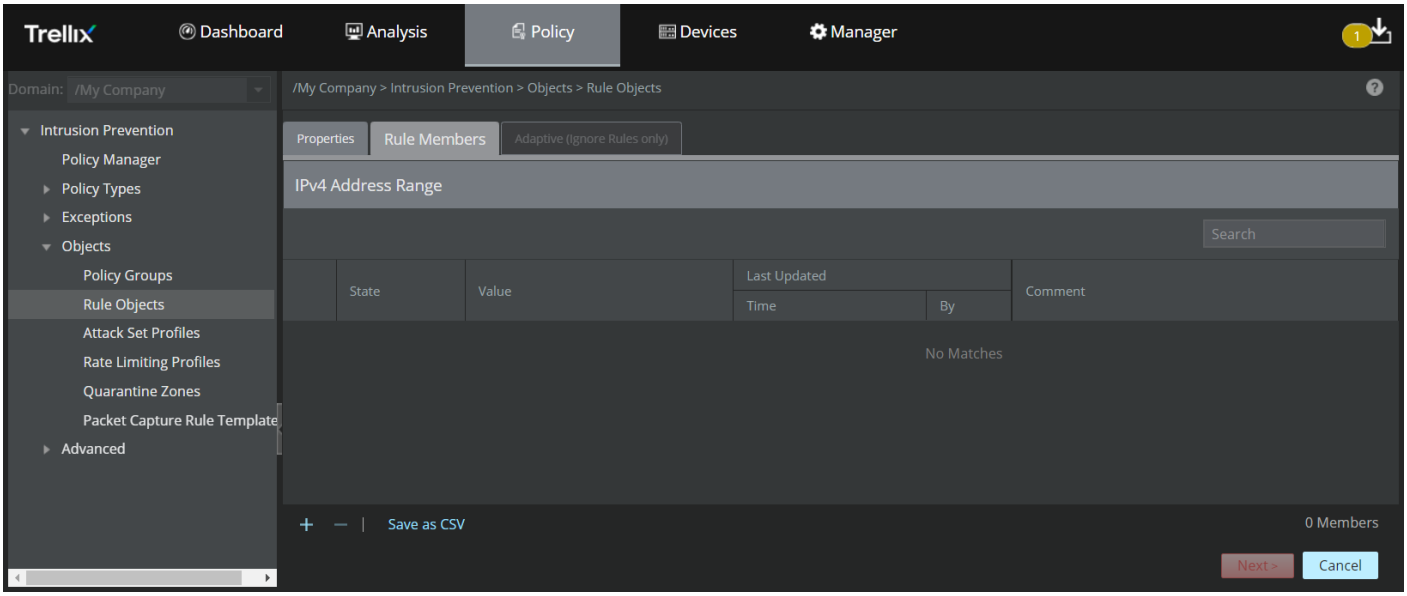
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Address Range** or **IPv6 Address Range** from the rule object **Type** drop-down, click **Next**.

Figure 574. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 575. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 68. Column details in the Rule Members tab - IP Address Range rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 address range based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 address range
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address range.
−	Click this icon to delete single or multiple IPv4 or IPv6 address ranges
Save as CSV	Click this icon to remove a rule object from the list

2. To add an IPv4 or IPv6 address range:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

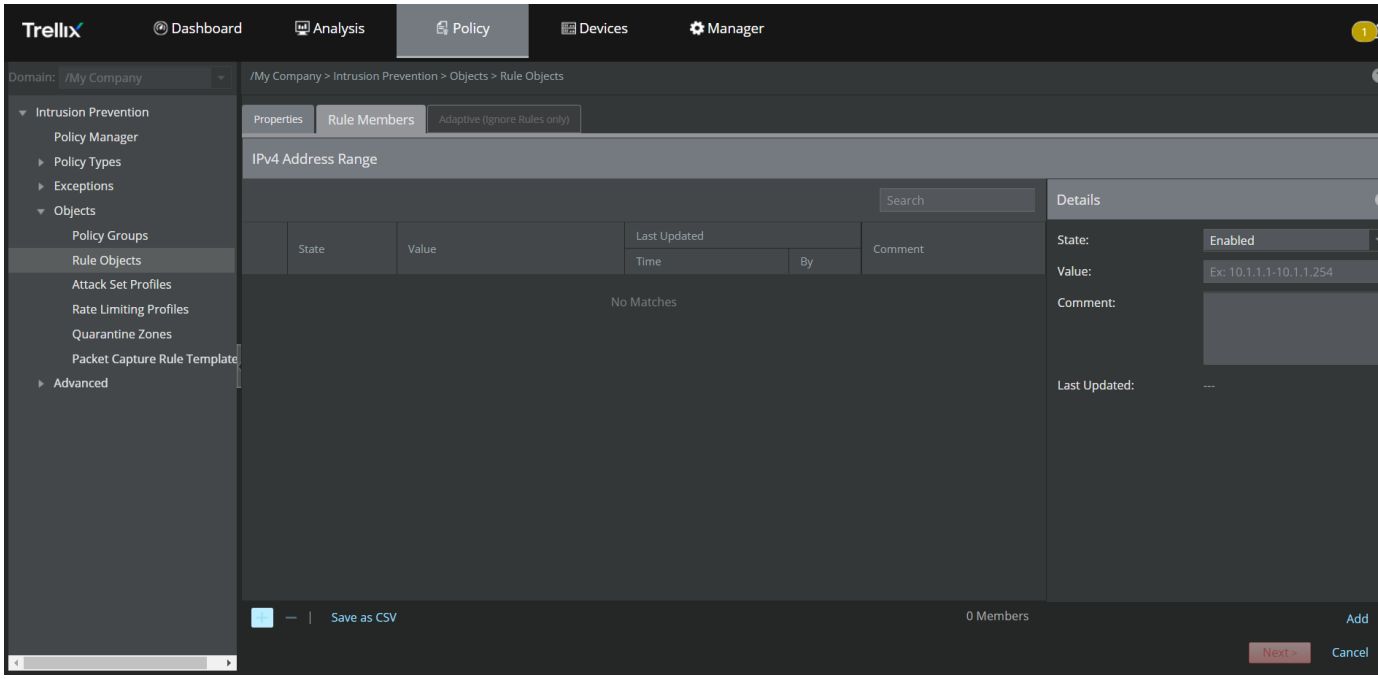
      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Address Range rule object].

Select the **State**, enter a valid IPv4 or IPv6 starting and ending address range in the **Value** field, enter a **Comment** if required and click **Add**.

NOTE

- Make sure to enter a hyphen between the starting and ending range (example: 10.1.1.1-10.1.1.25).
- You can enter up to 20000 IPv4 or 20000 IPv6 address ranges in a single rule object.
- The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
- If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 address ranges in any rule object.

Figure 576. Add individual IP addresses



3. Upon adding all the required IP addresses, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Rule Members** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values.

Option	Definition
Resource to Customize	Select the resource to customize from the drop-down list. **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**.
Add	Click this button to add the IP address range to the **Customizations** list.
Search	Type the search criteria to search for a resource.
	Click this icon to remove an address range from the list.

4. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

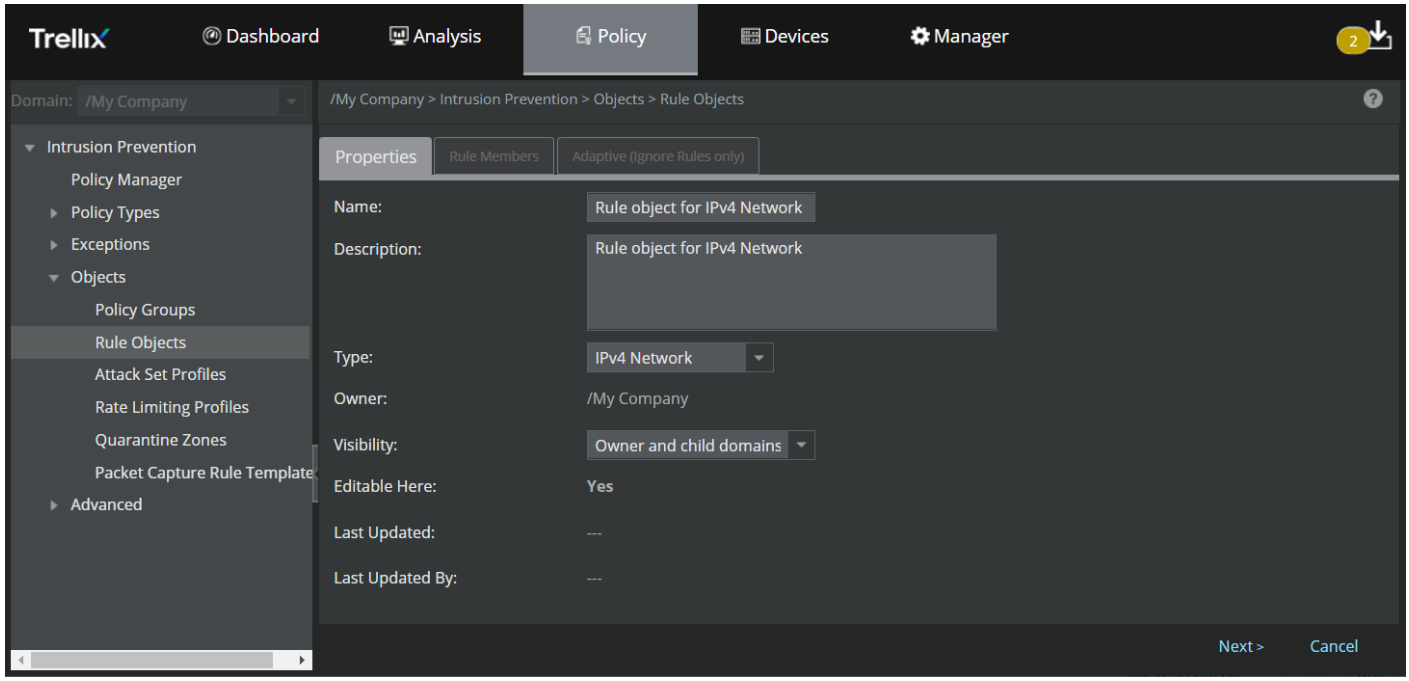
Add IPv4 Network and IPv6 Network rule objects

IPv6 Network is not supported for Quarantine. Also, only one IPv4 Network item per Rule Object is allowed for quarantine zone.

The steps to add **IPv4 Network** and **IPv6 Network** rule objects are identical. Follow these steps to add **IPv4 Network** or **IPv6 Network** rule objects:

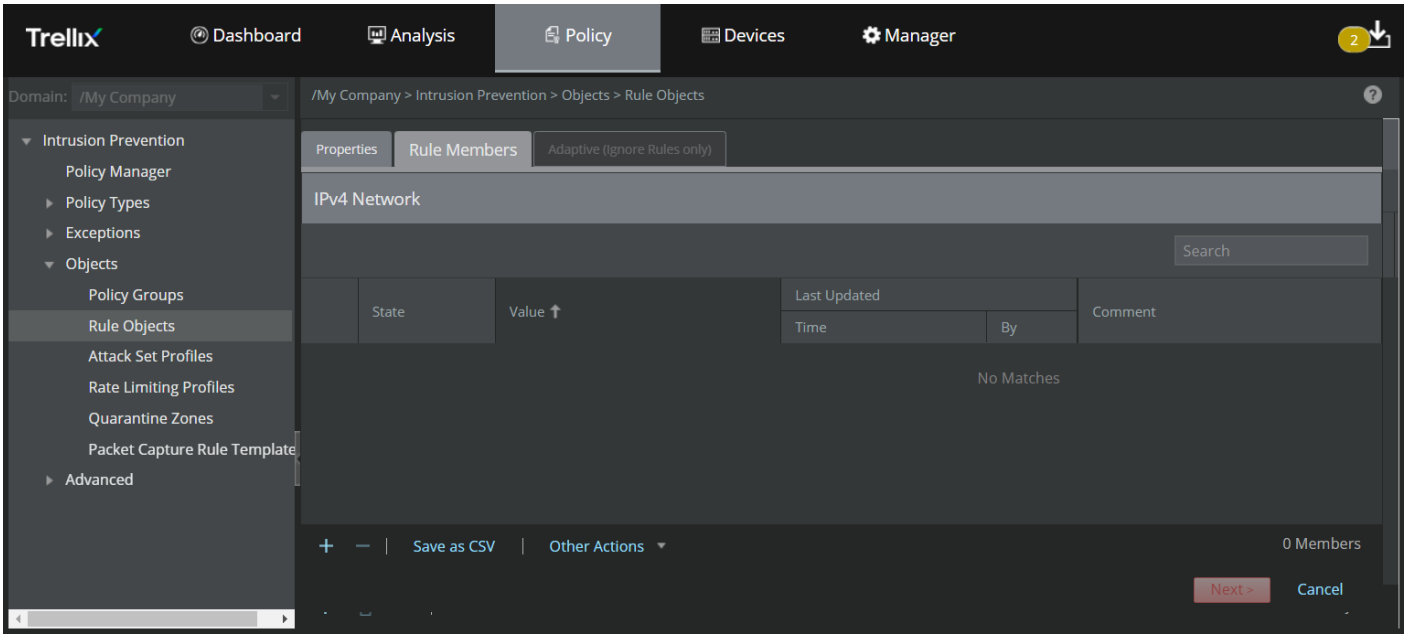
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Network** or **IPv6 Network** from the rule object **Type** drop-down, click **Next**.

Figure 577. Create an IPv4 Network or IPv6 Network rule object



The **Rule Members** tab is displayed.

Figure 578. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 69. Column details in the Rule Members tab - IP Network rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 CIDR block based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 CIDR blocks
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add a valid IPv4 or IPv6 CIDR block. For example, enter 172.16.200.0/24 for IPv4 Network, or 3003:0AB8::/48 for IPv6.
−	Click this icon to delete single or multiple IPv4 or IPv6 CIDR blocks
Save as CSV	Click this icon to remove a rule object from the list
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 CIDRs • **Export All** — Allows you to export all the CIDRs from the Manager to the local system

2. There are two ways to add the IP CIDR blocks — add individual IP CIDR block using the + icon or import a list of IP CIDR blocks from a CSV file using the Other Actions → **Import** option.

3. To add an individual IPv4 or IPv6 CIDR block:

   a. Click the + icon.

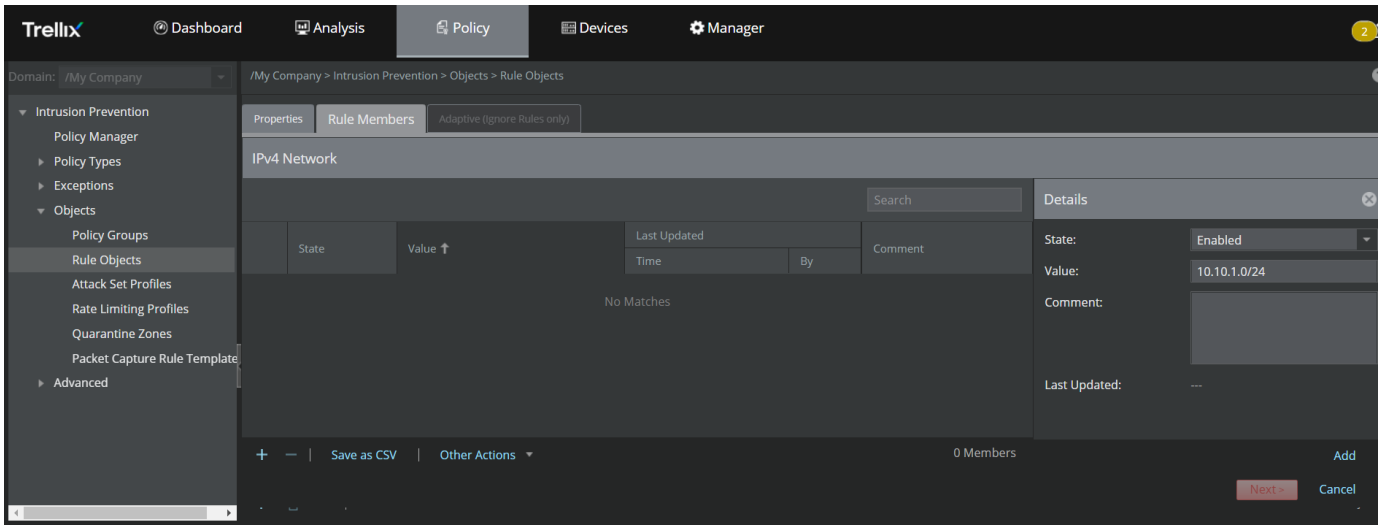
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

   For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Network rule object].

   Select the **State**, enter the IPv4 or IPv6 CIDR block in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - You can enter up to 140000 IPv4 or 140000 IPv6 CIDRs in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 CIDRs in any rule object.

Figure 579. Add individual IP CIDR block



   c. Upon adding all the required IP CIDR blocks, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values

Option	Definition
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add a CIDR block to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove a CIDR block from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of CIDR blocks from a CSV file using the **Import** option:

a. Click Other Actions → **Import**.

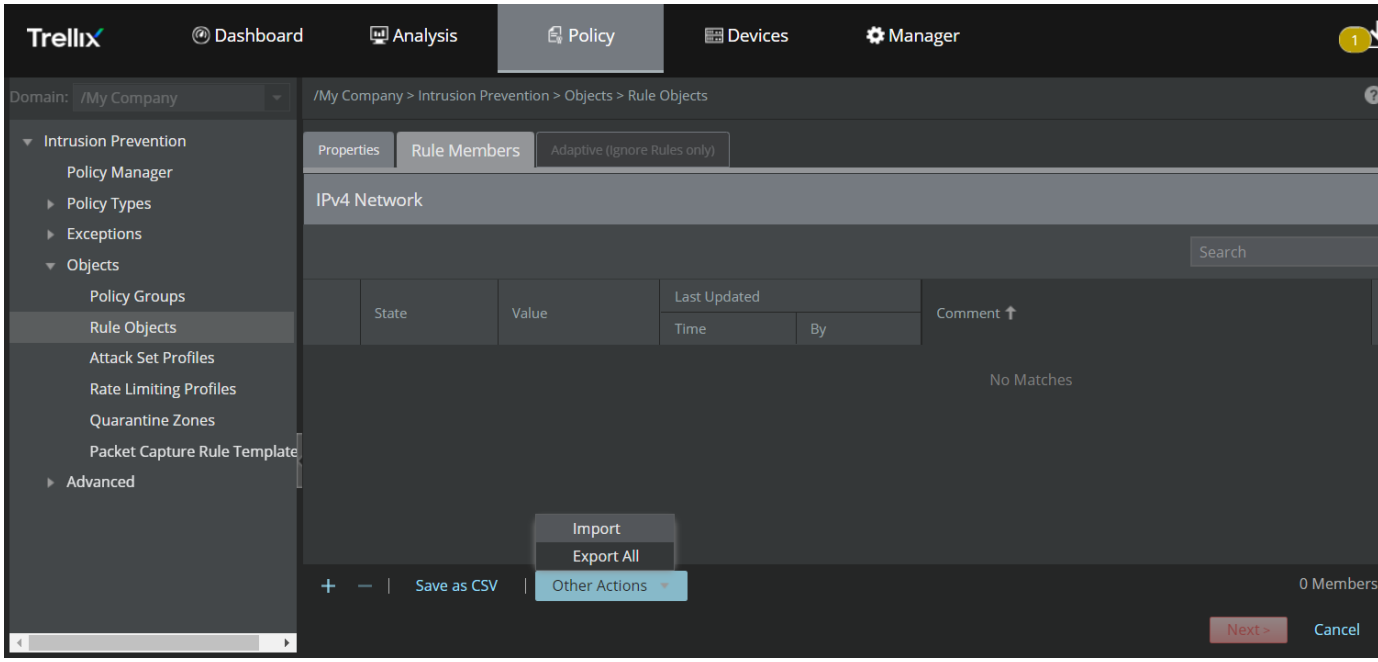
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10.

Figure 580. Import IP CIDRs from a CSV file

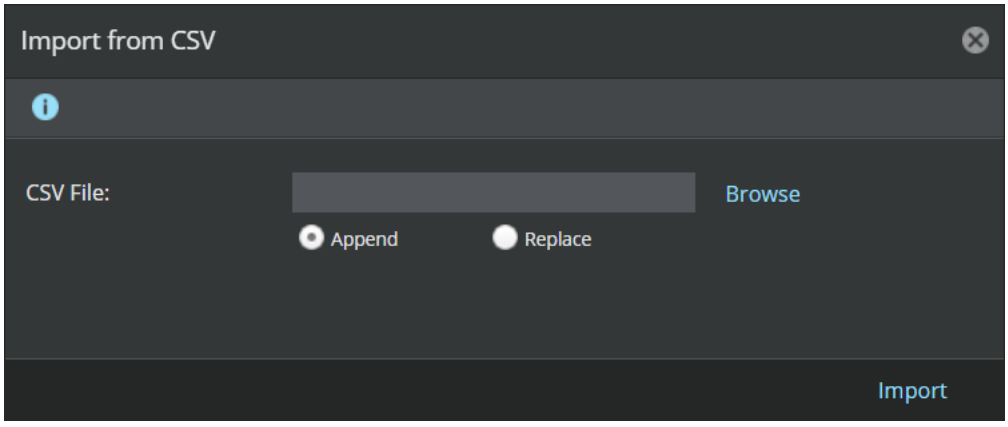


b. **Import from CSV** window appears. Use the **Append** option to add a new list of CIDR blocks or to append a list of CIDR block to an existing list. Use the **Replace** option to replace an existing list of CIDRs with a new list.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IPv4 or IPv6 CIDRs that you plan to import.

Figure 581. Import IP CIDRs from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 CIDR>,<Comment>

Example file format: 10.10.1.0/24,textual description.

The following is a sample for a CSV file with multiple IPv4 CIDRs:

Figure 582. CSV file format for IPv4 or IPv6 Networks

```
134.        .100/7,textual description
134.        .100/8,textual description
134.        .100/9,textual description
134.        .100/10,textual description
134.        .100/11,
134.        .100/12,
```

The following table describes the details of the IP CIDR blocks to be imported in the CSV file format.

Format	Description
<IPv4 or IPv6 CIDR>	Specifies the IPv4 or IPv6 CIDR to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (**,**) next to the entry and leave it.

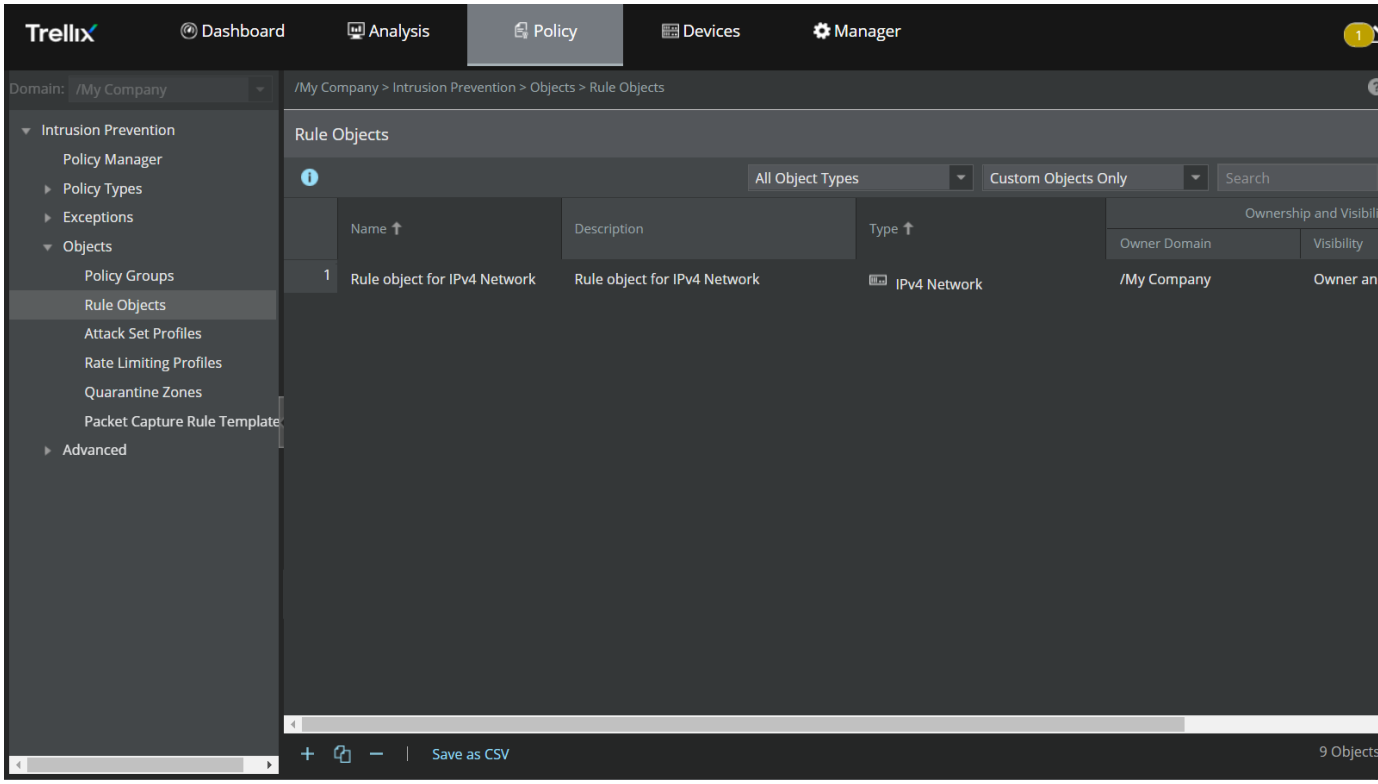
d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

NOTE

The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

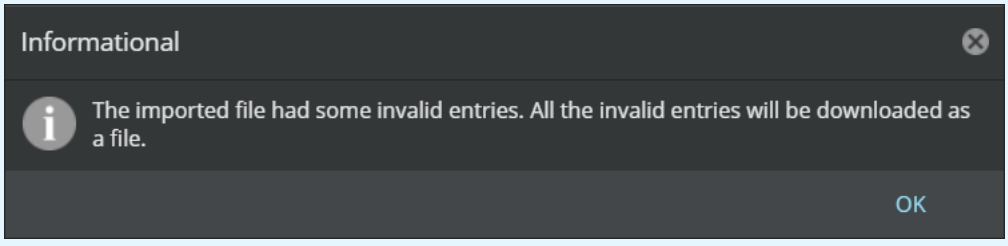
Figure 583. Rule object for IPv4/IPv6 network successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 584. Information dialog-box for invalid entries

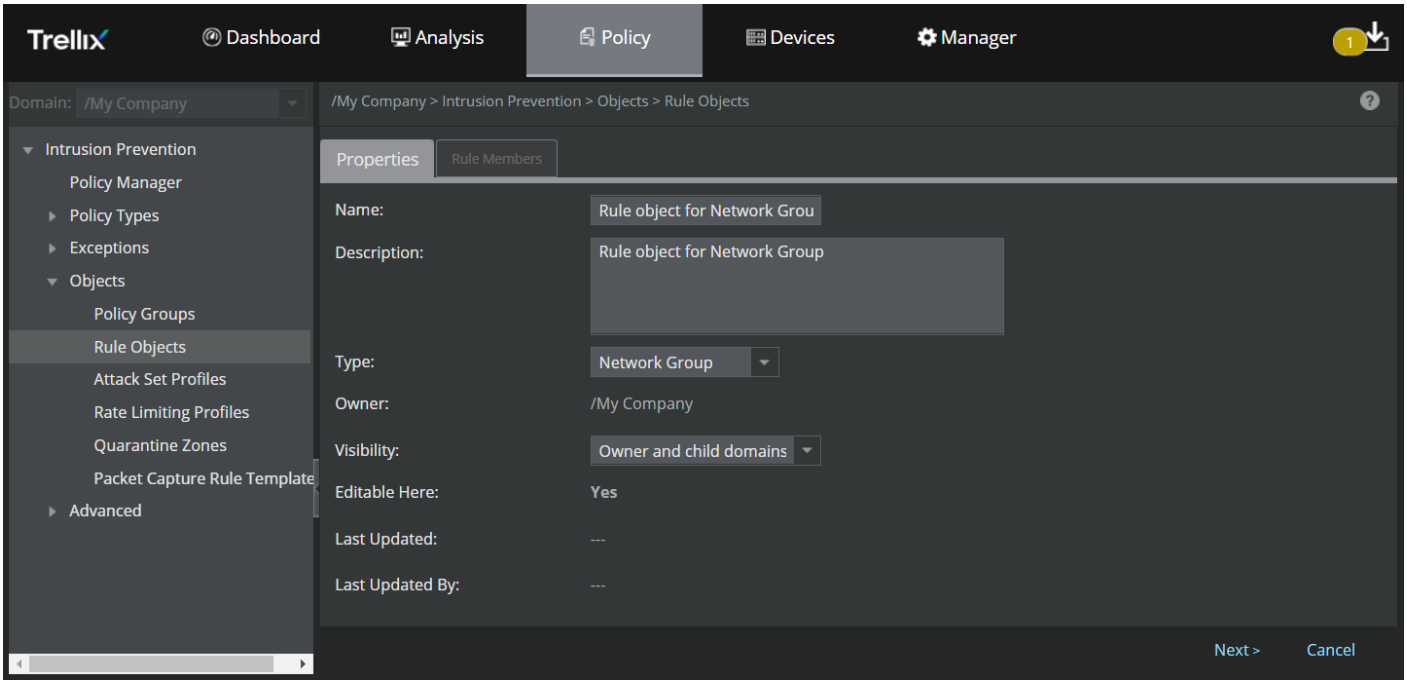


Add a Network Group rule object

Follow these steps to add a **Network Group** rule object:

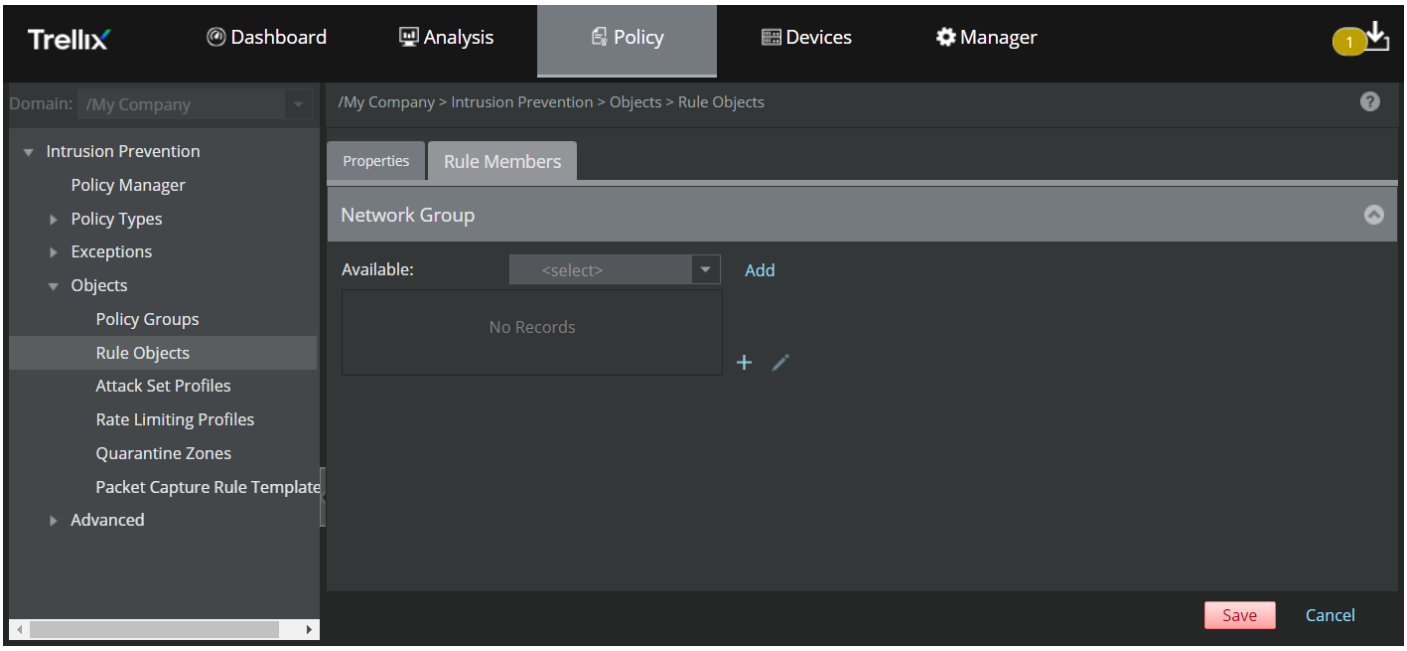
1. Upon specifying the options in the **Properties** tab and selecting **Network Group** from the rule object **Type** drop-down, click **Next**.

Figure 585. Create a Network Group rule object



The **Rule Members** tab is displayed.

Figure 586. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select the rule object from the **Available** drop down list.
Add	Click this button to add the rule object to the list.
	Click this icon to add a new rule object.
	Click this icon to edit the existing rule object.
	Click this icon to remove the rule object from the list.

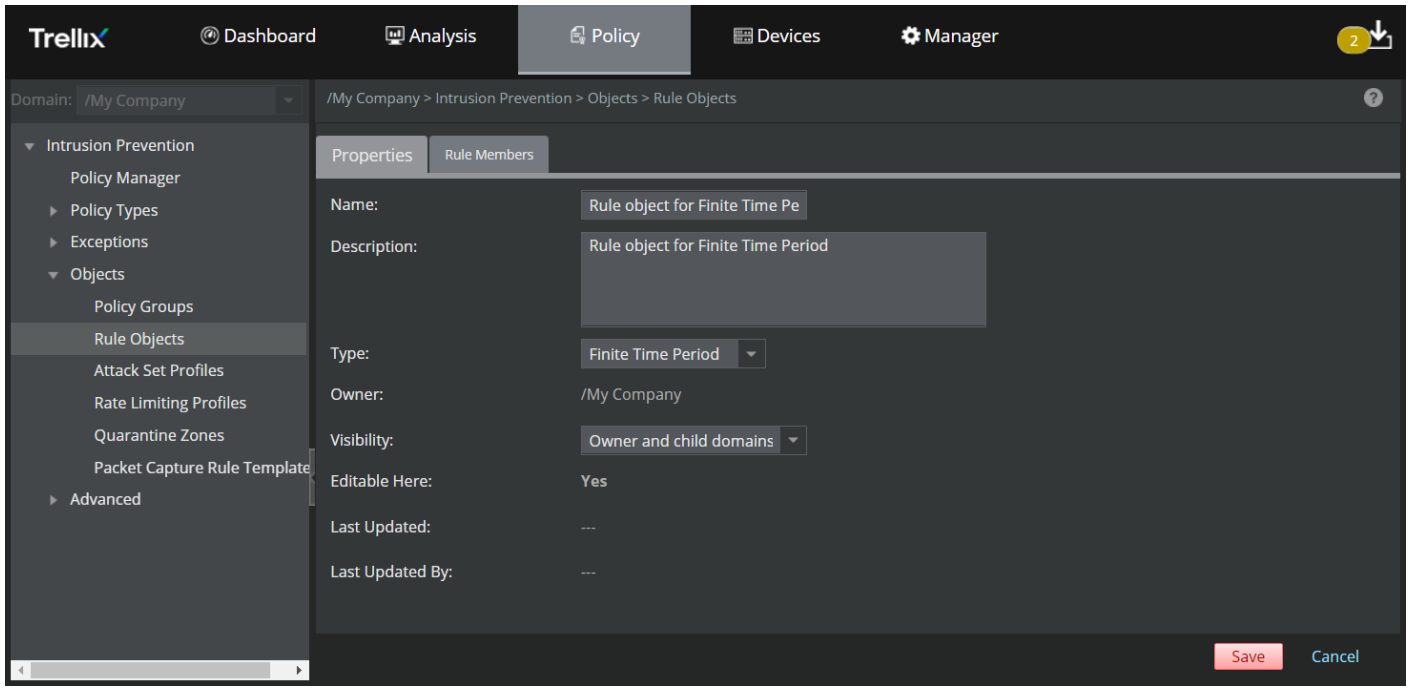
2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Add a Finite Time Period rule object

Follow these steps to add **Finite Time Period** rule object:

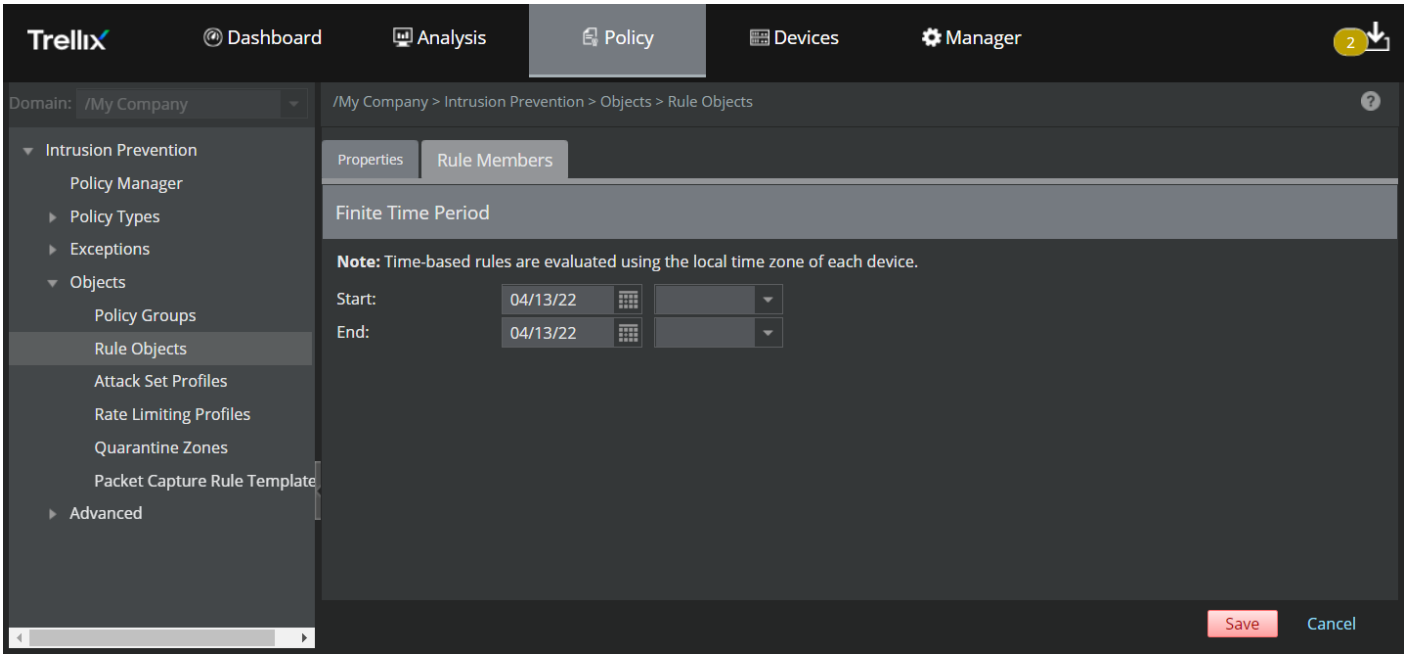
1. Upon specifying the options in the **Properties** tab and selecting **Finite Time Period** from the rule object **Type** drop-down, click **Next**.

Figure 587. Create a Finite Time Period rule object



The **Rule Members** tab is displayed.

Figure 588. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Start and **End**	Select the **Start** date and time and the **End** date and time in the corresponding fields. Time-based rules are implemented using the local time zone of the corresponding Sensor. **NOTE** **Start** date and time must be before **End** date and time.

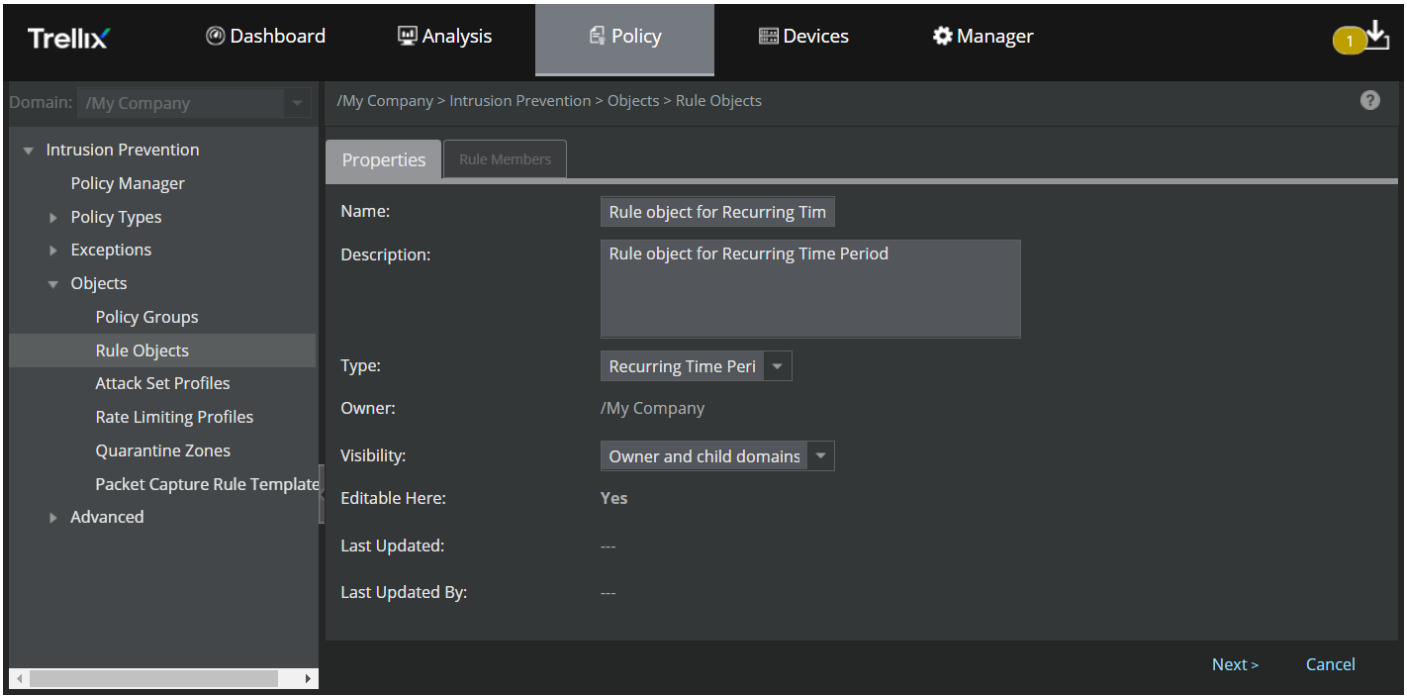
2. Based on the above option, you can select the **Start** date and time and the **End** date and time, and click **Save**.

Add a Recurring Time Period rule object

Follow these steps to add **Recurring Time Period** rule object:

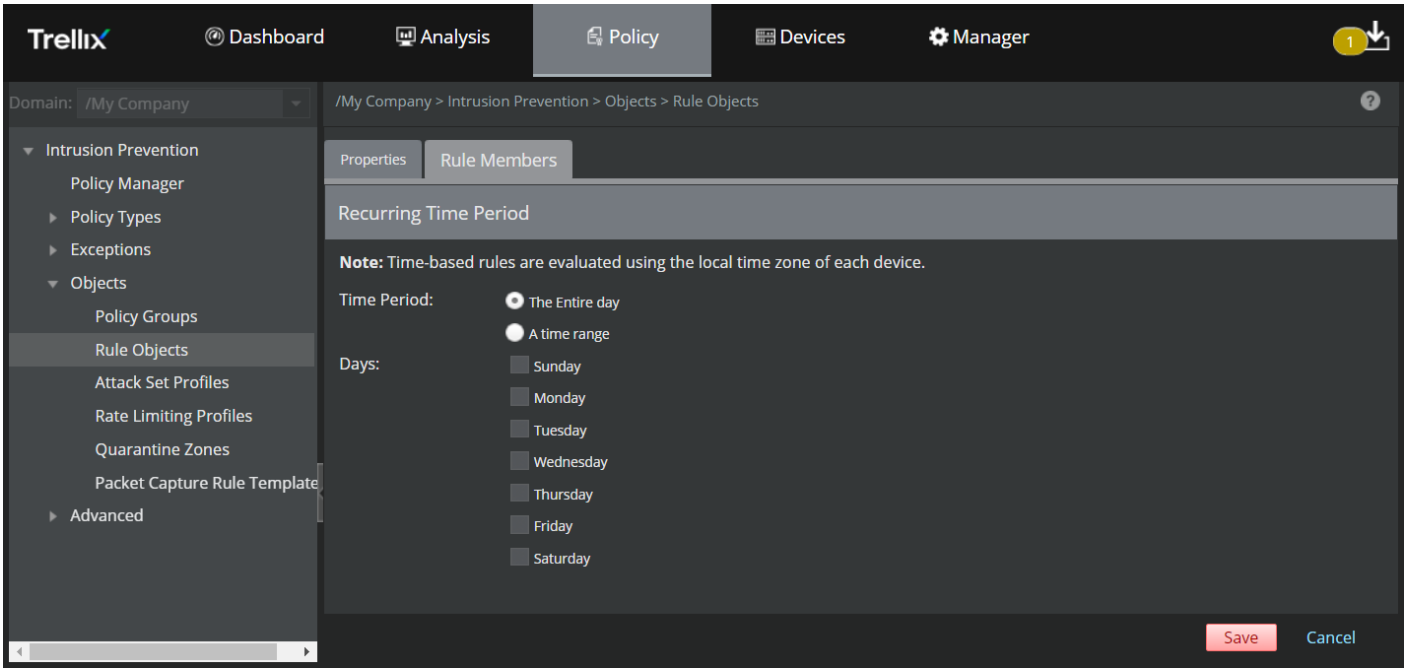
1. Upon specifying the options in the **Properties** tab and selecting **Recurring Time Period** from the rule object **Type** drop-down, click **Next**.

Figure 589. Create a Recurring Time Period rule object



The **Rule Members** tab is displayed.

Figure 590. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Time Period	Select the time when the Sensor must enforce the corresponding rule. Time-based rules are implemented using the local time zone of the corresponding Sensor. You can select the option **The Entire day** or **A time range** for a specific time period.
Time Range	To modify the hour or minute values, place the cursor on the **Time Range** field and type the hour value. Then, click on the drop-down list and select the relevant minute value. Also select the **to** range by selecting the value from the drop-down list.
Days	Select the days when the Sensor must enforce the corresponding rule. You must select at least one of the days.

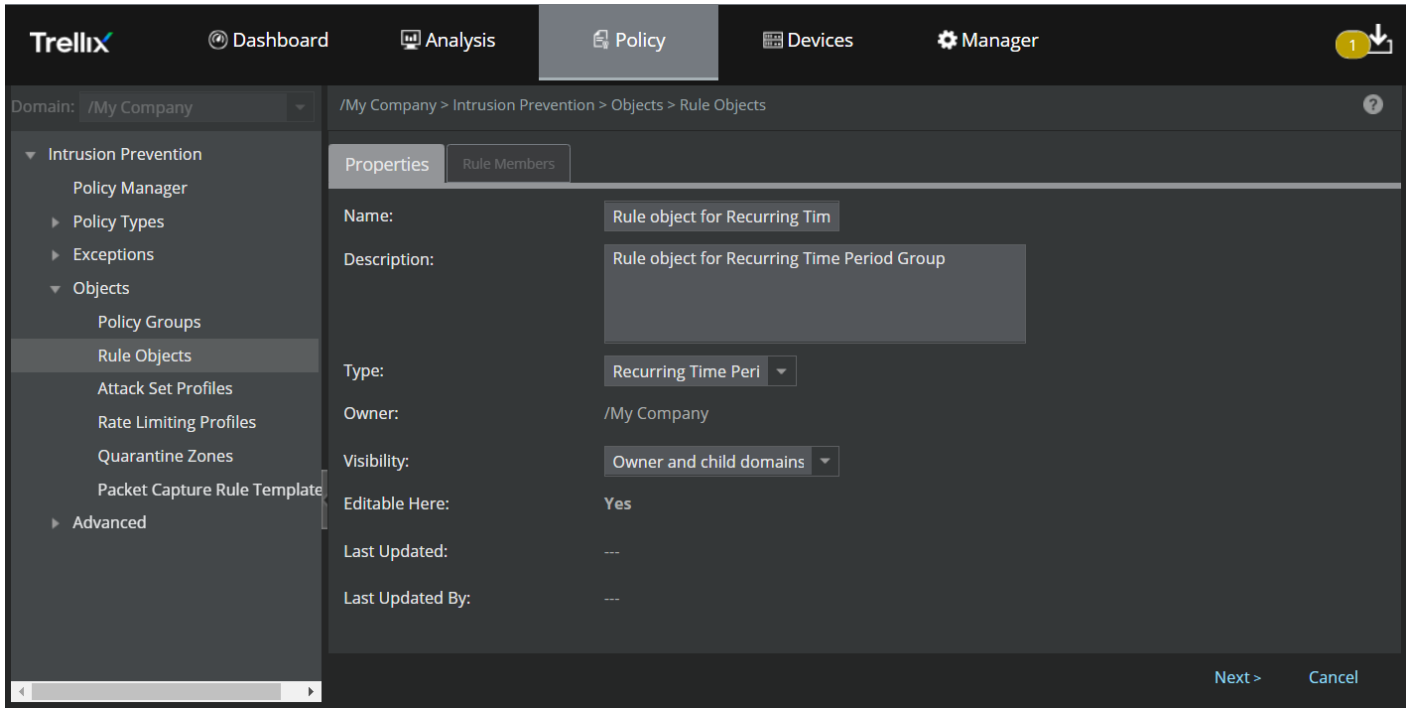
2. Based on the above options, you can select the **Time Period** and the **Days** when the Sensor must enforce the corresponding rule.
3. Click **Save**.

Add a Recurring Time Period Group rule object

Follow these steps to add **Recurring Time Period Group** rule object:

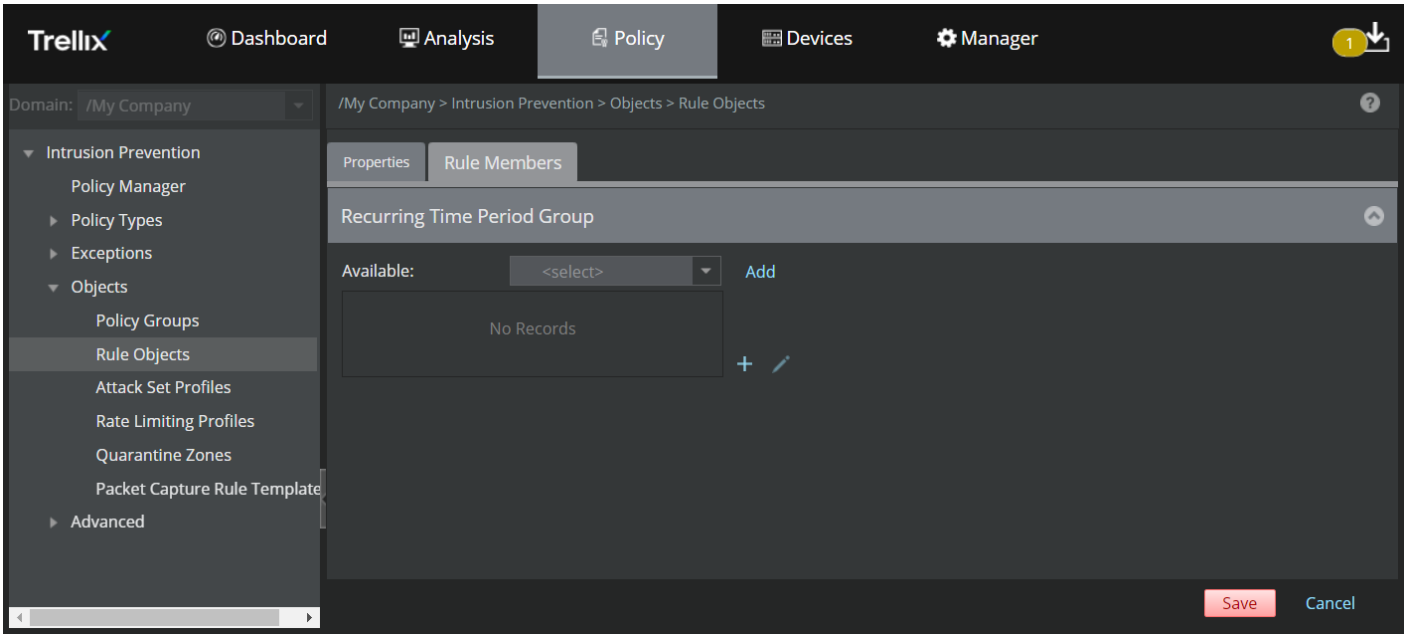
1. Upon specifying the options in the **Properties** tab and selecting **Recurring Time Period Group** from the rule object **Type** drop-down, click **Next**.

Figure 591. Create an Recurring Time Period Group rule object



The **Rule Members** tab is displayed.

Figure 592. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select an existing **Recurring Time Period Group** rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Members** list
	Click this icon to edit a rule member in the list
	Click this icon to add a new **Recurring Time Period Group** rule object
	Click this icon to remove a rule member from the list

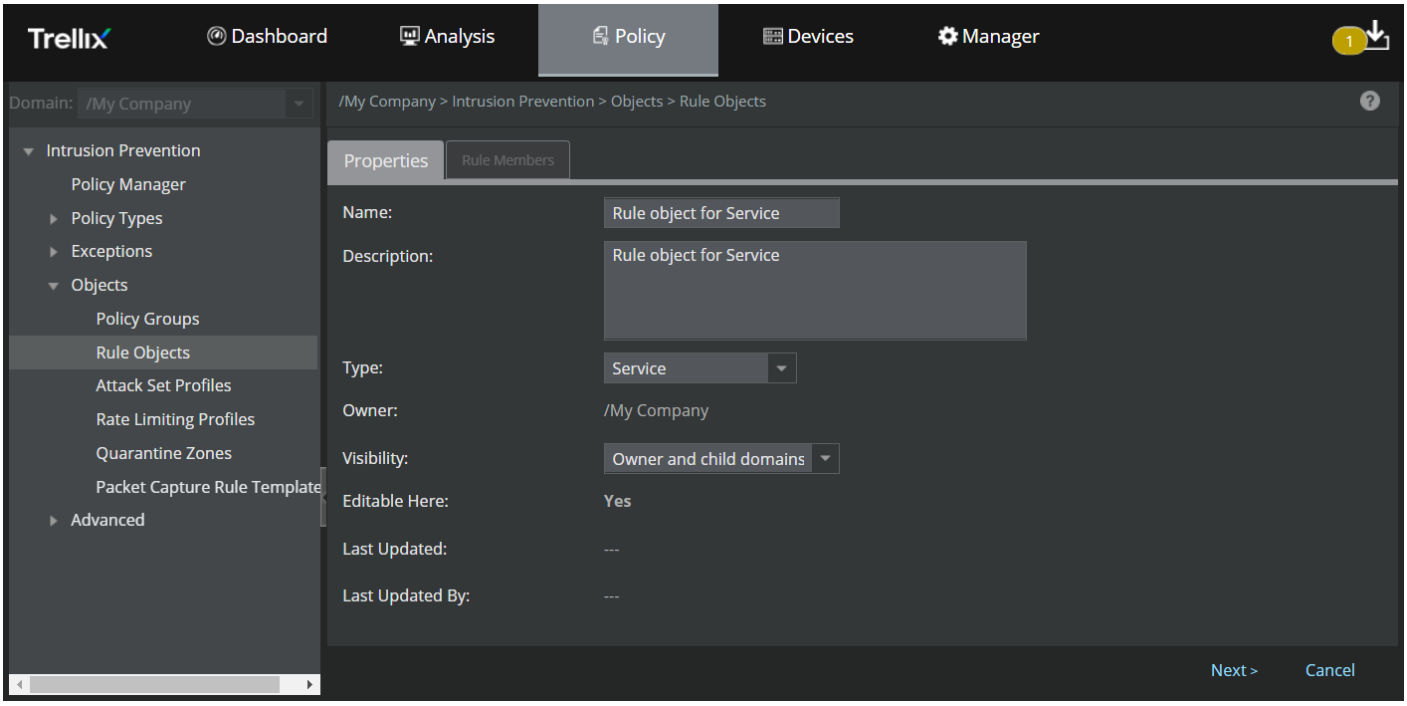
2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Add a Service rule object

Follow these steps to add **Service** rule object:

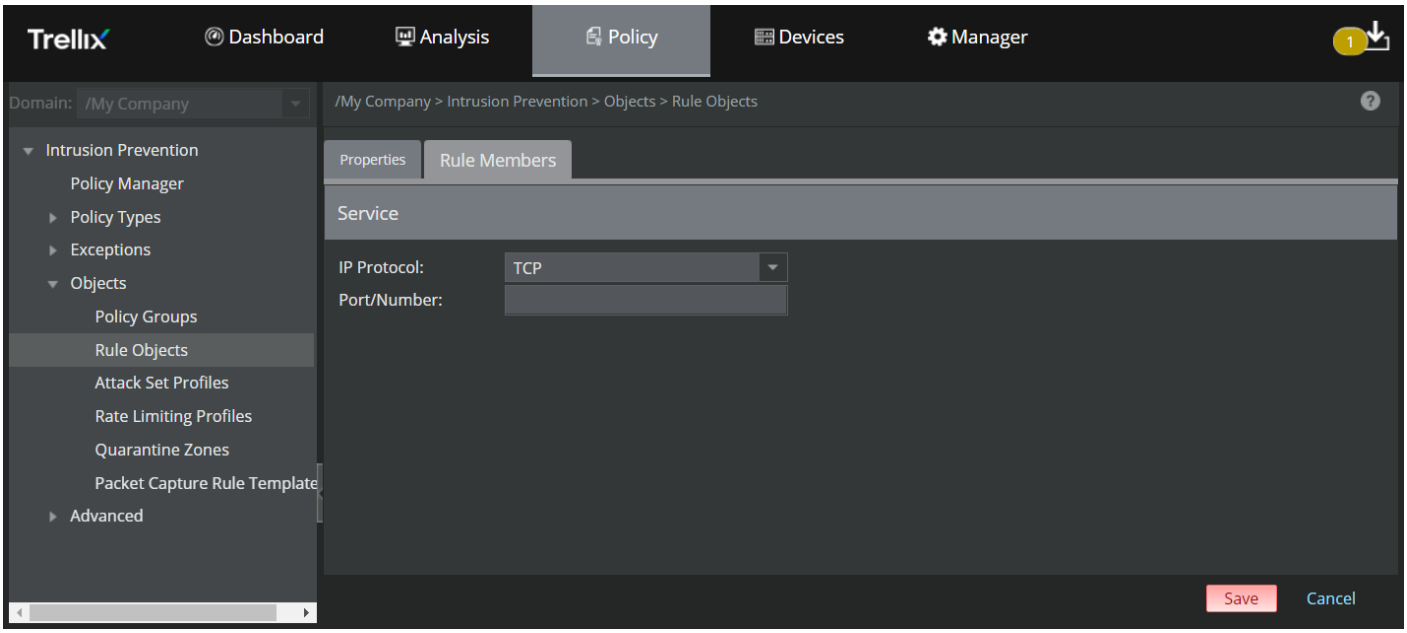
1. Upon specifying the options in the **Properties** tab and selecting **Service** from the rule object **Type** drop-down, click **Next**.

Figure 593. Create a Recurring Time Period rule object



The **Rule Members** tab is displayed.

Figure 594. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
IP Protocol	Select the required protocol from the drop-down list. The options are **TCP**, **UDP** and **Protocol Number**.
Port/Number	If you select **TCP** or **UDP** as the **IP Protocol**, you can optionally enter a port number between from 1 to 65534. Alternatively, you can specify a protocol number between from 0 to 255.

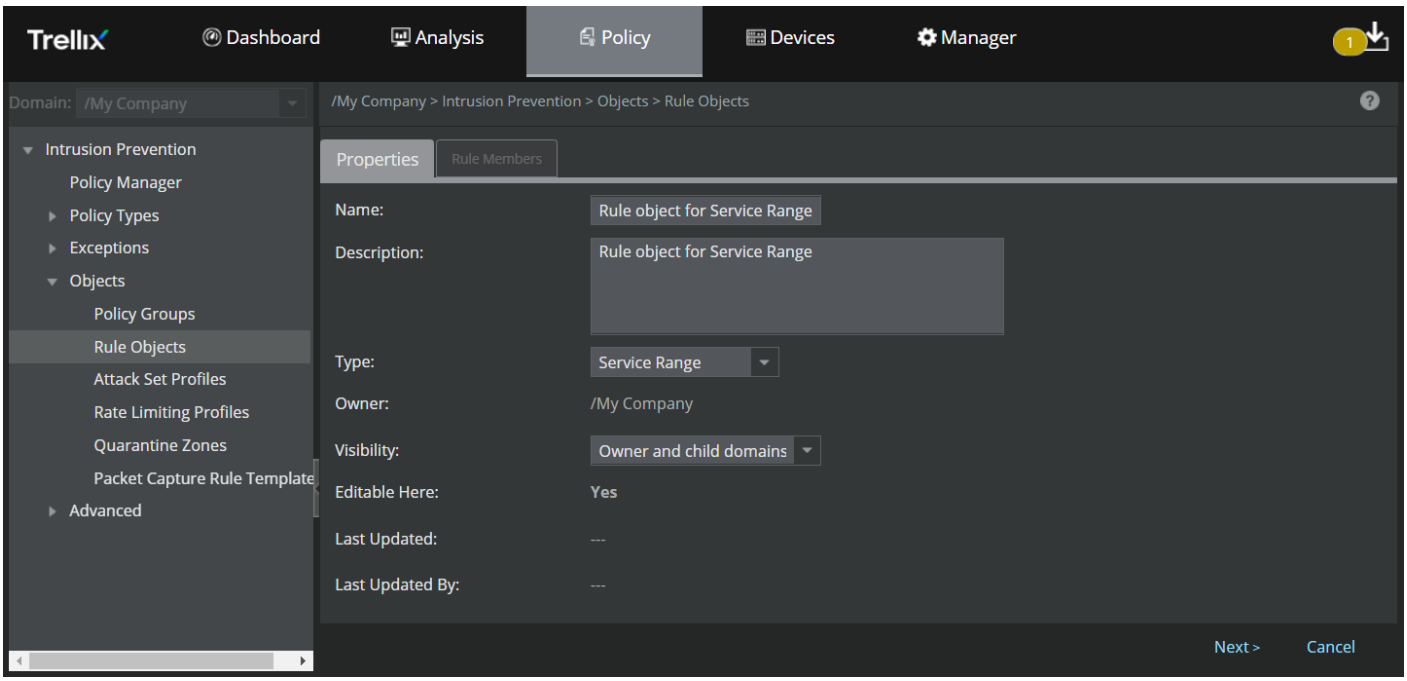
2. Based on the above options, you can select the **IP Protocol** and specify a **Port/Number**.
3. Click **Save**.

Add a Service Range rule object

Follow these steps to add **Service Range** rule object:

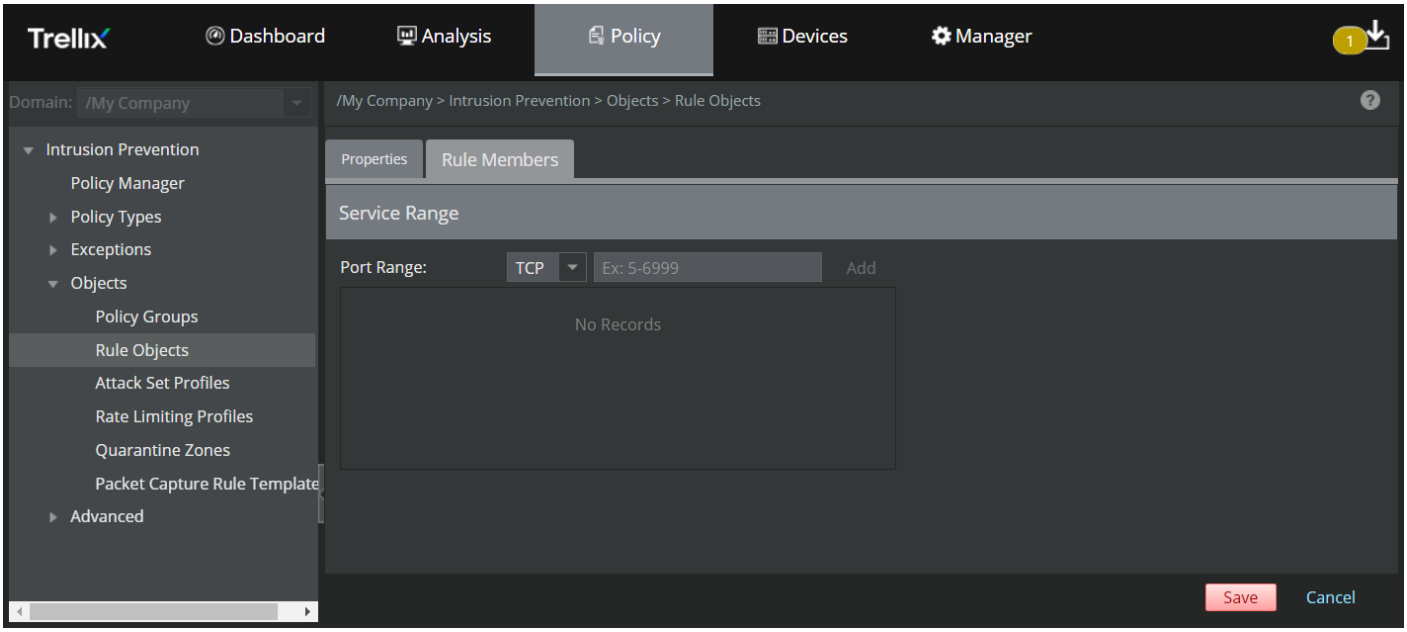
1. Upon specifying the options in the **Properties** tab and selecting **Service Range** from the rule object **Type** drop-down, click **Next**.

Figure 595. Create a Service Range rule object



The **Rule Members** tab is displayed.

Figure 596. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Port Range	Select **TCP** or **UDP** from the drop-down list. Enter the beginning and end port range (Example: 1-65534) in the text box. **NOTE** Ensure to enter a hyphen between the beginning and end port range.
Add	Click this icon to add the Port range to the list.
	Click this icon to remove the Port range from the list.

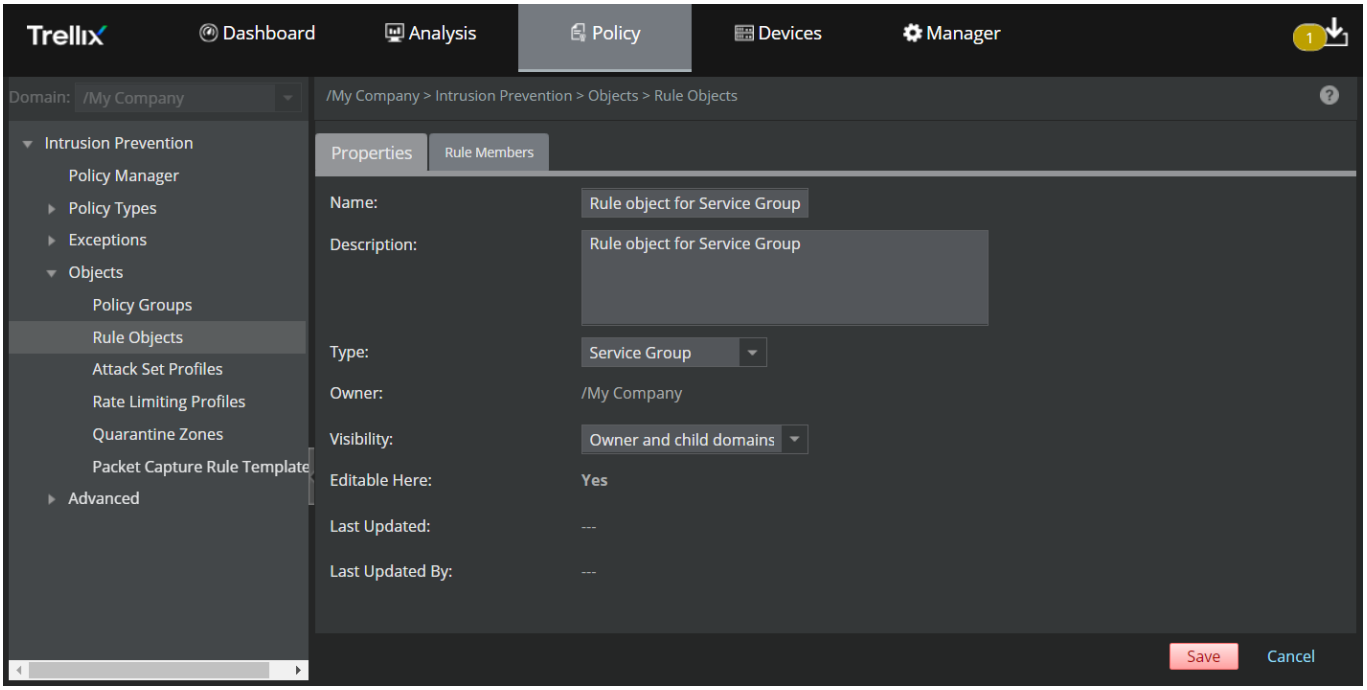
2. Based on the above options, you can assign up to **10** TCP and UDP port ranges.
3. Click **Save**.

Add a Service Group rule object

Follow these steps to add **Service Group** rule object:

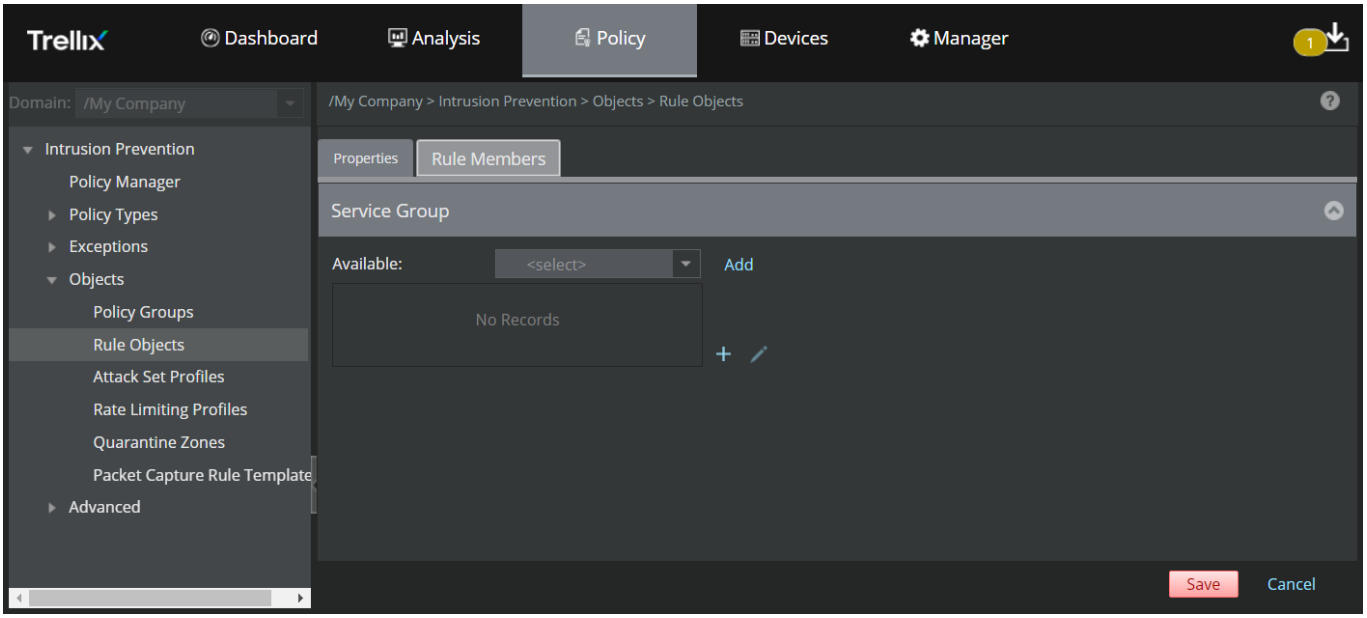
1. Upon specifying the options in the **Properties** tab and selecting **Service Group** from the rule object **Type** drop-down, click **Next**.

Figure 597. Create an Service Group rule object



The **Rule Members** tab is displayed.

Figure 598. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Available	Select a pre-defined service or an existing **Service** rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Members** list
	Click this icon to add a new **Service** rule object
	Click this icon to edit a rule member in the list
	Click this icon to remove a rule member from the list

2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Clone a rule object

You can clone custom rule objects.

- You cannot clone a default rule object except for Network.
- You can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule objects for the selected admin domain are listed.
4. Locate the Rule Object that you want to clone.

TIP

You can use the search function to more easily find the rule object.

5. Select the rule object and click  .
6. Make the required changes and click **Save**.

Modify a custom rule object

You can modify custom rule objects.

- You cannot modify or delete a default rule object.
- You can modify or delete a custom rule object only at the admin domain where it was created. If required, you can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.
- You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.
4. Locate the rule object that you want to modify.
   - You can use the search function to easily find the rule object.
   - Make sure the **Editable here** column displays **Yes** for the rule object you want to modify. If the **Editable** column displays **No**, the rule object belongs to a parent admin domain.
5. Double-click the rule object.
6. Make the required changes and click **Save**.

NOTE

If the rule object that you modified is part of a policy that is in use, you must do a configuration update to the Sensor for the changes to take effect.

Delete a custom rule object

Delete a custom rule object that you no longer use. You can delete a custom rule object only at the admin domain where it was created.

- You cannot delete a default rule object.
- You cannot delete a rule object that is used in a Firewall policy, QoS policy or, in a group rule object.
- You can delete a rule object only at the admin domain where it was created.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule objects for the selected admin domain are listed.
4. Locate the Rule Object that you want to modify.
   - You can use the search function to easily find the rule object.
   - Make sure the **Editable here** column displays **Yes** for the rule object you want to delete. If the **Editable here** column displays **No**, the rule object belongs to a parent admin domain.
5. Select the rule object and click −. Then click **Yes** to confirm deletion.

> **NOTE**
>
> To delete rule objects in bulk, press **Shift** key (for continuous selection) or press **Ctrl** key (for discontinuous selection) and then select the rule objects. The selected items are highlighted. Click − and then click **Yes** to confirm deletion.

Configure the DNS server details

You must configure the DNS server details in the Manager, if you have Firewall, QoS, or Quarantine Zone rules that use Host DNS Name rule object. The Sensors use these DNS server details to resolve the Host DNS Name rule objects to IP addresses. This also applies to rules using Network Group rule objects, which in turn use a Host DNS Name rule object.

In addition to what is mentioned above, NS-series Sensors use the DNS server details to resolve the host name of the syslog server used for Firewall or Quarantine. You can configure the Sensor to forward the details of matched Firewall or Quarantine Zone rules to a syslog server. As part of this configuration, you define the syslog-server details in the Manager. If you provide the host name of the syslog server, then the Sensor uses the DNS server to resolve the syslog server's host name.

> **IMPORTANT**
>
> The Sensor uses only UDP and never falls back to TCP for DNS queries even if the DNS server forces for TCP.

You can configure the DNS server details at a domain level or at a device level. The DNS server at the admin domain, by default, applies to the following:

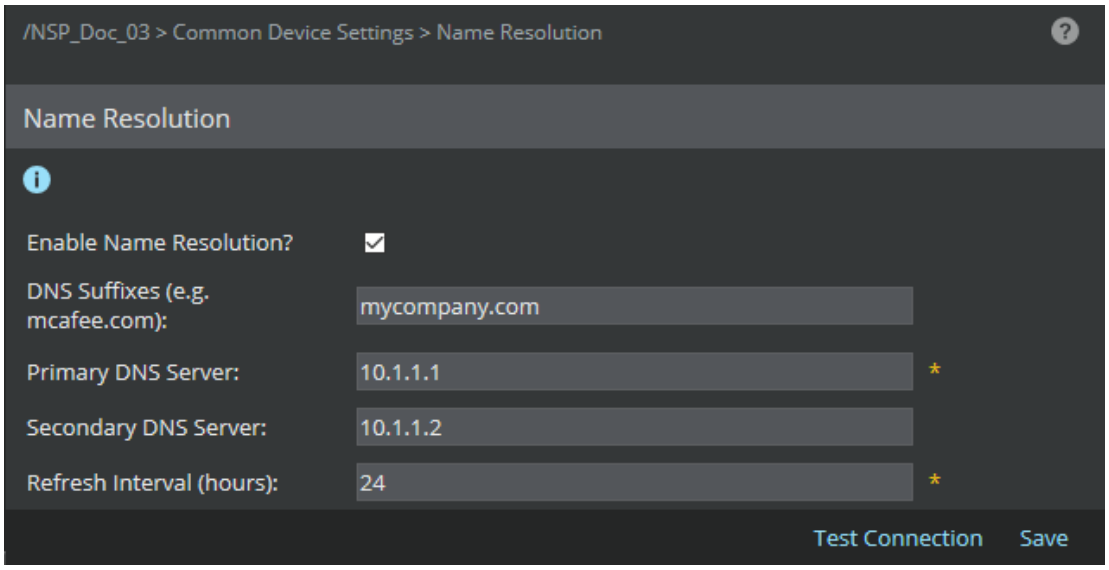
- All the corresponding child domains
- All the Sensors in this domain. This includes any interfaces delegated to other domains.
- All the Sensors in the corresponding child domains

If required, you can override the DNS server details at a child admin domain level and also at each Sensor level.

1. To configure the DNS server details for an admin domain:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.

c. Select Global → Common Device Settings → **Name Resolution.**

Figure 599. DNS window



2. To configure the DNS server details for a Sensor:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. On the left pane, click the **Devices** tab.
   d. Select the device from the **Device** drop-down list.
   e. Select Setup → **Name Resolution.**
   f. Deselect **Inherit Settings?** to override the settings of the parent domain.
3. Enter the DNS information in the corresponding fields.

Option	Definition
Enable Name Resolution?	Select to display the fields in the **Name Resolution** page. **NOTE** If you deselect this field and click **Save**, the DNS details that you had saved earlier is lost.
DNS Suffixes	You can enter multiple values separated by a space. The Sensor uses these suffixes, in the same order, to resolve non-qualified DNS host names in your Firewall rules. Consider that the DNS host name in your Firewall rule is “host1” and the DNS suffixes are “mycompany.com” and “mycompany.org”. To resolve this host name, the Sensor first tries host1.mycompany.com. If this fails, it tries host1.mycompany.org.
Primary DNS Server	Enter the IPv4 or IPv6 address of the DNS server that the Sensor must contact first.

Option	Definition
Secondary DNS Server	Optionally, enter the IPv4 or IPv6 address of a secondary DNS server. If the primary DNS server is unreachable, the Sensor communicates with the secondary DNS server.
Refresh Interval	If you are configuring the details for an admin domain, then enter a value between 24 and 9999. Though this field is applicable only to NTBA, you must enter a value when configuring the details for an admin domain.
Test Connection	Click this button to check the connectivity to the DNS Server. The status of the connectivity test is displayed in the **Name Resolution** page.
Save	Saves the DNS server details in the Manager database. **TIP** To resolve the Host DNS Name rule objects, the Sensor management port must be able to connect to **Save** the specified DNS servers. So, to be sure, ping the DNS servers from the Sensor CLI.

4. Perform a configuration update to the relevant Sensors.

NOTE

If the Sensor is unable to communicate with a DNS server, a fault of severity **Warning** is displayed on the **Faults** tab in **Logs** page.

Configure the time zone

You need to select a time zone in the Manager if you have any Firewall or QoS rules that involve a time-based rule object. The time-based rule objects are Finite Time Period, Recurring Time Period, and Recurring Time Period Group. Time-based rules are implemented using the local time zone of the corresponding Sensor. By default, the time on the Sensor is set to the Greenwich time zone (GMT +00:00).

The Manager displays the alerts generated with respect to the time zone configured for the Manager. For example, consider the Sensor to be in the GMT-08 time zone, and the Manager in the GMT+5:30 time zone. An alert is generated from the Sensor at 11 AM (in the GMT-08 time zone), the Manager displays the time of the alert as 12:30 AM (in the GMT+5:30 time zone). A time based rule has to be configured based on the Sensor time zone, but the alert generated is displayed with reference to the time zone configured for the Manager.

You can configure the time zone at an domain level or at a device level. The time zone at the admin domain, by default, applies to:

- All the corresponding child admin domains.
- All the Sensors in this domain. This includes any interfaces delegated to other domains.
- All the Sensors in the corresponding child admin domains.

If required, you can override the time zone at a child admin domain level and also at each Sensor level.

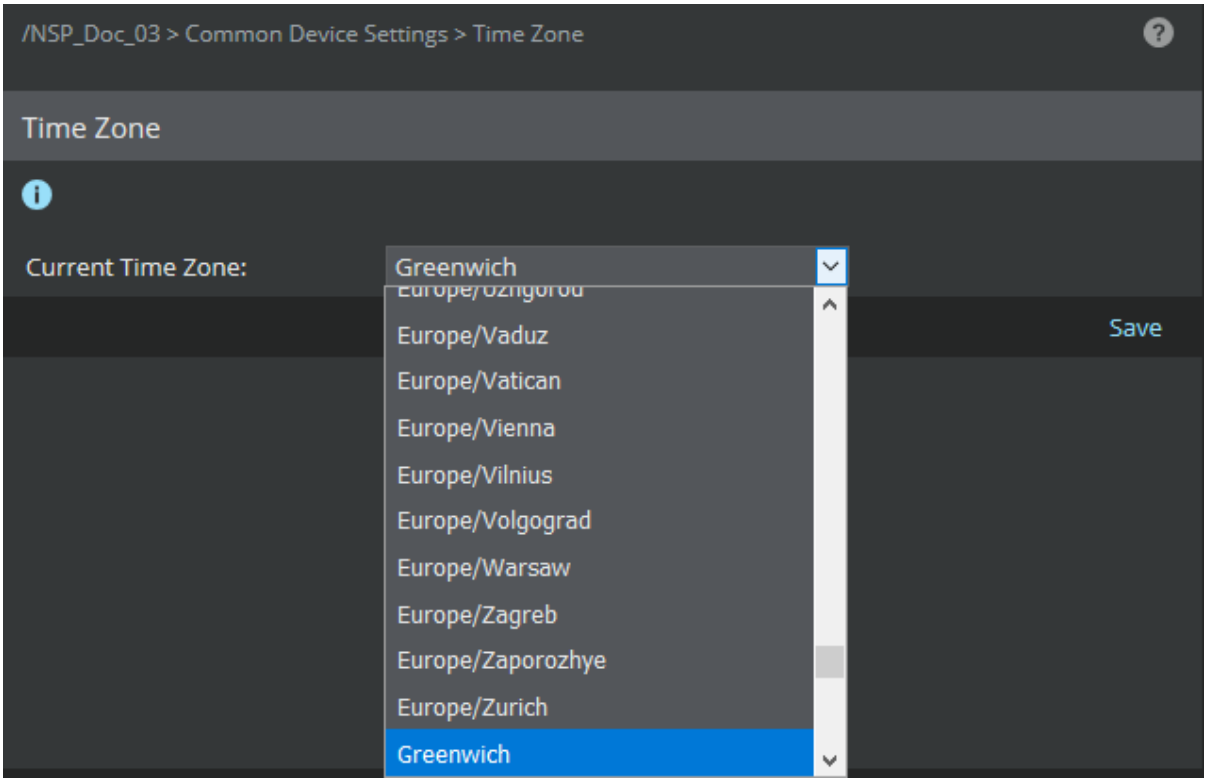
IMPORTANT

When you delegate Sensor ports to a child admin domain level, for those ports only the Sensor's time zone will apply and not the child admin domain's time zone.

When you select a time zone, Sensors interpret the time-based rule objects based on the selected time zone. They also factor in daylight savings time, if applicable.

1. To configure the time zone for an admin domain:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. Select Global → Common Device Settings → **Time Zone.**
2. To configure the time zone for a Sensor:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. On the left pane, click the **Devices** tab.
   d. Select the device from the **Device** drop-down list.
   e. Select Setup → **Time Zone.**
   f. Deselect **Inherit Settings?** to override the settings of the parent domain.
3. Select a time zone from the **Current Time Zone** drop-down.

Figure 600. Time Zone configuration



4. Click **Save.**
5. Perform a configuration update to the relevant Sensors.

   The selected time zone is applied to those Sensors.

Create a QoS policy

Prerequisite: For the sake of usability, an option is provided for you to create rule objects when creating the QoS rules. However, a systematic approach is to create the required rule objects before you create the QoS policy.

You create a QoS policy using the QoS rules as the building blocks. Then you need to assign the policy to the required Sensor ports.

NOTE

Import or export of QoS policies is not supported.

1. Select Intrusion Prevention → Policy Types → **QoS**.

   The currently available QoS policies for the domain are listed. This includes the policies inherited from the parent domain. You cannot edit the inherited policies.
2. Click .

   The **QoS** page displays.
3. Specify the details on the **Properties** tab.

Table 70. Properties option definitions

Option	Definition
Name	Enter a unique name to easily identify the policy.
Description	Optionally describe the policy for other users to identify its purpose.
Owner	Displays the admin domain to which the policy belongs
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are **Owner and child domains** and **Owner domain only**.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Type	Select the type — advanced or classic. After you save the properties, you cannot change the type.
Statistics	
Lasted Updated	Displays the time stamp when the policy was last modified
Last Updated By	Displays the user who last modified the policy
Assignments	Indicates the number of inline ports to which the policy is assigned

Option	Definition
Diff Serv Tagging Rules	Displays the number of DiffServ tagging rules currently defined in the policy
802.1P Tagging Rules	Displays the number of 802.1P tagging rules currently defined in the policy
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.
Save	Saves the changes made on the **Properties** tab. **NOTE** This option is visible only when you open an existing policy.
Next	Click this to save the changes made on the **Properties** tab and to access the **Diff Serv Rules** tab. This button is available only when you create a policy. **IMPORTANT** After you click **Next**, you cannot change the policy type.
Cancel	Reverts to the last saved configuration

4. Define the QoS rules for Diff Serv and 802.1P in the corresponding tabs.

   You use the rule objects as building-blocks to create a rule. Recall that the Sensor matches the rules in a top-down fashion and does not processes a set of rules after the first match. So make sure the specific rules are defined at the top, and the rules with a broader scope are defined towards the end of the list.

5. On the **Diff Serv Rules** and **802.1P Rules** tabs, click the appropriate button to insert a new rule.

Table 71. QoS rule button definitions

Option	Definition
	Inserts a new rule above the currently selected rule
	Inserts a new rule below the currently selected rule
	Clones the currently selected rule
	Deletes the currently selected rule
	Moves the currently selected rule one row up

Option	Definition
	Moves the currently selected rule one row down

On the **Diff Serv Rules** tab, you can select any of the following options for **Unclassified Traffic - Diff Serv Value** :

- **Set to Zero** — To re-tag the unclassified traffic with a zero-value tag
- **Keep the value seen on the wire** — To retain the tag that was originally present

On the **802.1P Rules** tab, you can select any of the following options for **Unclassified Traffic - 802.1P Value** :

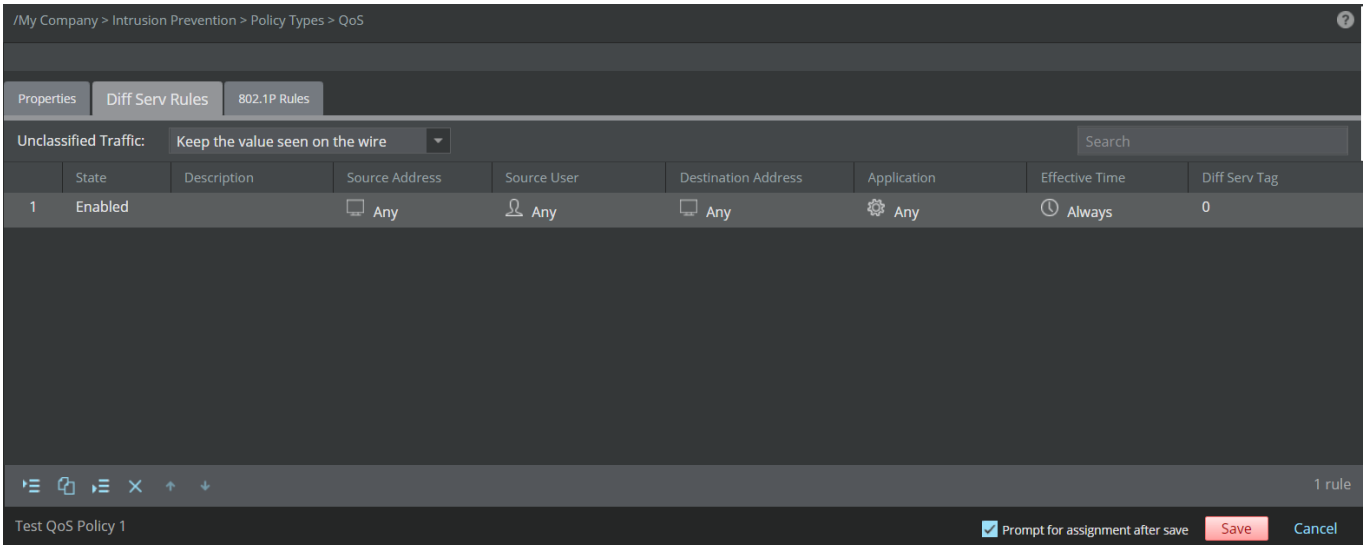
- **Set to Zero** — To re-tag the unclassified traffic with a zero-value tag
- **Keep the value seen on the wire** — To retain the tag that was originally present

NOTE

To search for a specific rule, type the first few letters of the description of the rule in the **Search** field. The rule containing the description of the typed letter(s) is displayed.

6. Double-click on the row of an access rule and specify your choices.

Figure 601. The default Diff Serve rule



- For advanced QoS policies, change the values of **Source Address, Source User, Destination Address, Application**, and **Effective Time**. For classic QoS policies, change **Service.**

NOTE

In a Firewall access rule or QoS rule, you cannot specify an IPv4-based rule object for one field and IPv6-based rule objects for other applicable fields. For example, if you select an IPv6-based rule object in the **Source Address** field, then you cannot specify IPv4-based rule objects for **Destination Address** or **Source User** fields. You can specify only an IPv6-based rule object or *any* as the value for **Destination Address** and *any* for **Source User.** Recall that User and User Group rule objects are considered as IPv4 based rule objects because Logon Collector does not collect user information from IPv6 hosts. Similarly, Country and Host DNS Name are also IPv4-based rule objects.

- In the QoS rules, you can generally add up to 10 rule objects per field.

Table 72. QoS rules option definitions

Option	Definition
State	Displays whether a rule is **Enabled** or **Disabled**. Sensor does not apply disabled rules. This option might help you during troubleshooting.
Description	Optionally enter additional information about the rule. You can enter a description up to 64 characters long and click **OK**.
Source Address	Select the rule objects corresponding to the source of the traffic from the **Available** list. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in QoS policy is 10. Click **Add** to add a rule object. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.
Source User	Select the type of user from the **Type** drop-down list and then select the rule objects corresponding to the user from the **Available** list. Click **Add** to add the selected rule object. **NOTE** This option is for user-based rules. Recall that the Manager receives users and user groups from Logon Server and automatically displays them as rule objects. User groups are listed by default.

Option	Definition
Destination Address	Select the rule objects corresponding to the destination of the traffic from the **Available** list. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in QoS policy is 10. Click **Add** to add a rule object. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list.
Application	Select the rule objects corresponding to the application from the **Available** list. Click **Add** to add a rule object. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list. You can have Service or Application-related rule objects in a rule but not both.
Effective Time	Select the time-based rule objects to specify the time when the Sensor should implement the rule, from the **Available** list. Click **Add** to add a rule object. Click  to create a new rule object. Click  to edit or view a rule object. Click  to remove the rule object from the list. **NOTE** Time-based rules are implemented using the local time zone of the corresponding Sensor.
Diff Serv Tag	This option is seen when you select the **Diff Serv Rules** tab. Select the required DiffServ tag from the drop-down list and click **OK**.

Option	Definition
802.1P Tag	This option is seen when you select the **802.1P Rules** tab. Select the required 802.1P tag from the drop-down list and click **OK**.
Prompt for assignment after save	If you clear this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the **Assignments** window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Save	Saves the access rules in the Manager database. The QoS policy is listed in the **Quality of Service (QoS) Policies** list.
Cancel	Reverts to the last saved configuration

You can follow these steps to clone and edit QoS policies.

Assign a QoS to inline port pairs

Make sure you have created a QoS policy with the required access rules.

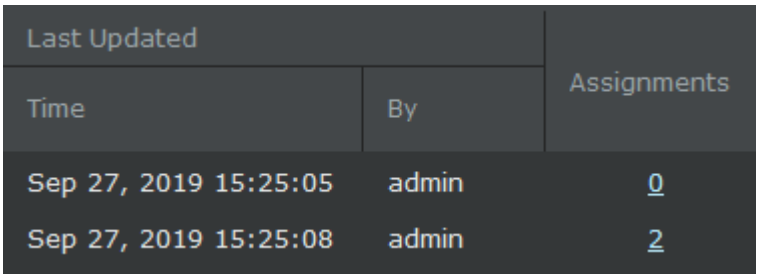
From the domain level, you assign a QoS policy to the required inline port pairs of that domain. You have to assign a QoS policy separately for inbound and outbound. Only when you assign a QoS policy, the Sensor is aware of the rules against which it should match the traffic and corresponding bandwidth that it should allow for the matching traffic. You can assign the same QoS policy to any number of inline ports that belong to the domain.

The QoS policy that you assign might belong to the domain or inherited from a parent domain. For delegated Sensor ports, you can only assign the QoS policy from the domain that owns the Sensor.

1. Select Intrusion Prevention → Policy Types → **QoS.**
2. Click the **Assignments** value of the policy that you want to assign.

   The **Assignments** window displays. It lists the available resources for the admin domain.

Figure 602. Option to assign a QoS Policy



3. Assign the policy to the required Sensor resources.

Figure 603. Assignments page for a QoS policy

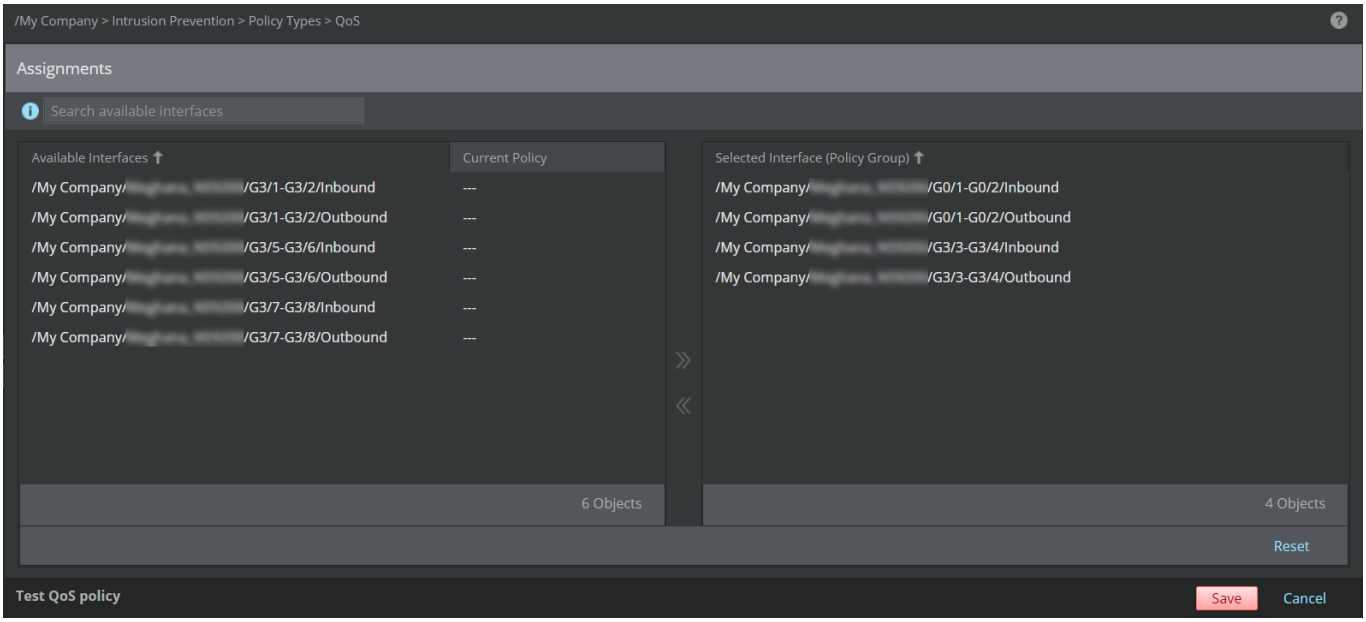


Table 73. Option definitions - assigning QoS policies to Sensor resources

Option	Definition
Search Interfaces	To filter the list of available resources, enter a string that is part of the **Available Interfaces**.
Available Interfaces	Lists the Sensor resources for the admin domain. For example, if an admin domain has only Sensor ports allocated from the parent domain but no Sensor of its own, then no device-level resource is listed. Also, the items in this list are filtered based on your filter criteria. **NOTE** In case of Sensors in failover, the ports used for interconnection of the Sensors are not displayed. If you have assigned the QoS policy to an interconnect port, the assignment is automatically removed when you create the failover. Select a resource and click » to move it to **Selected Interface**.
Current Policy	The QoS policy that is currently assigned to a resource. To replace that policy with the policy that you are currently assigning, move the resource to **Selected Interface**.
Selected Interface (Policy Group)	Lists the Sensor resources to which you have assigned the policy.
Reset	Reverts to last saved configuration.
Save	Saves the changes to the Manager database.
Cancel	Closes the **Assignments** window without saving the changes.

4. Do a configuration update to the Sensor.

Assign QoS policies – alternatives

There are many options to assign a QoS policy to Sensor ports. You can assign a QoS policy to multiple Sensor ports. You can also go to the **Policy Manager** page of a specific Sensor port pair and select a QoS policy for that port. These options are described here.

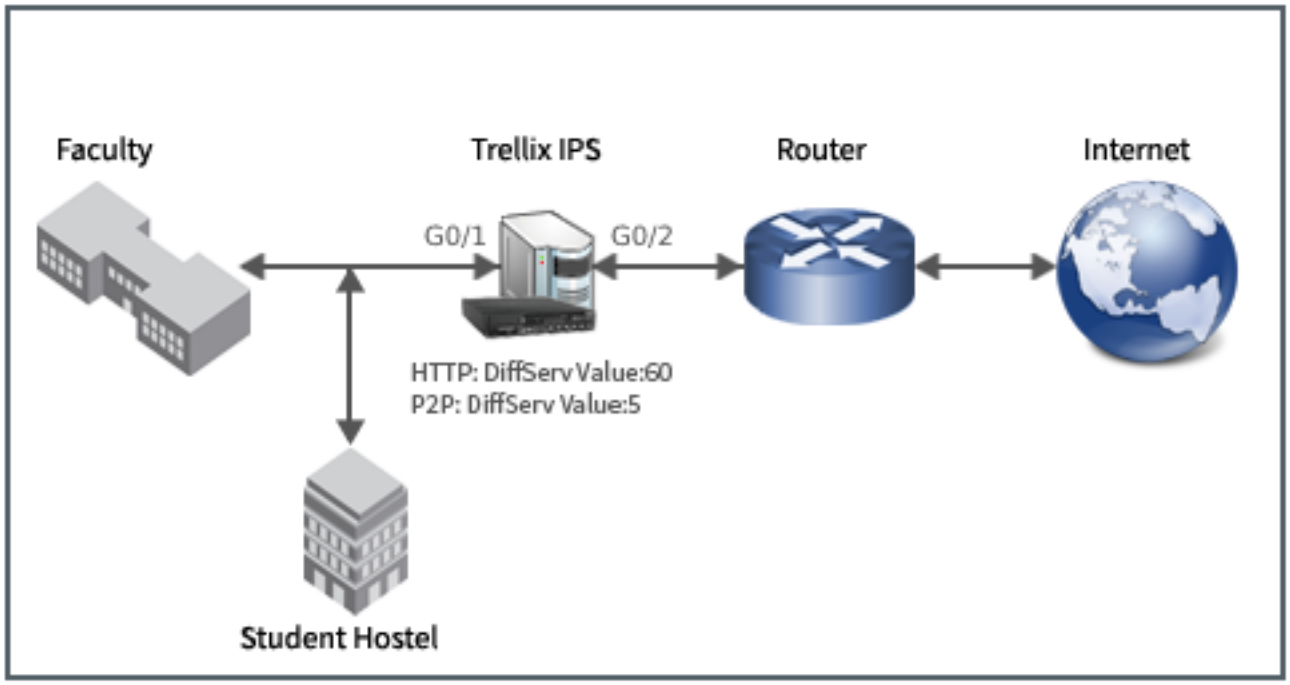
1. Click the **Policy** tab.
2. Select the domain from the **Domain** drop-down list.
3. Go to Intrusion Prevention → **Policy Manager**.
4. In the **Interfaces** tab, double-click the Sensor port to which you would like to assign a QoS policy.

   The **<Device Name/Interface>** panel opens.
5. In the **Quality of Service** section, select the inbound and/or outbound policy from the **Inbound Policy** and/or **Outbound Policy** drop down.
6. Click **Save**.
7. Deploy the configuration changes to the corresponding Sensor.

Network scenario for DiffServ tagging

Consider a network scenario where the internal network of a University is connected to the internet, and Trellix IPS and the router are deployed as shown in the below diagram.

Figure 604. Scenario For DiffServ Tagging



Suppose you want to prioritize the HTTP and P2P traffic coming from the University network to the internet. To prioritize the traffic, you can configure the Sensor for DiffServ or VLAN tagging. The role of the Sensor is just to tag the packets and pass it on to an external network device (here router) for DiffServ or VLAN classification.

Suppose you want to give high priority to the HTTP traffic coming from the University network to the internet. You can configure the Sensor port G0/2 with a DiffServ rule, in which the DiffServ field is set to a value, say 60, for HTTP traffic. When the HTTP traffic from the University network reaches Sensor port G0/2, the Sensor tags the packet headers with the DiffServ field value specified in the configuration (60, in this example). The tagged packets are sent to the router, which is configured to do DiffServ categorization. Now the traffic is prioritized according to the DiffServ priority defined in the router. Note that the Sensor only tags the incoming traffic and passes it on to the external network device (in this case, it is the router) which further performs the DiffServ classification.

Similarly, to provide low priority to the P2P traffic coming from the University network to the internet, you can configure port G0/2 of the Sensor with a DiffServ rule, in which the DiffServ field is set to a value, say 5. When the P2P traffic from the University network reaches Sensor port G0/2, the Sensor tags the packet headers with the DiffServ field value specified in the configuration (5, in this example). The tagged packets then reach the router which performs DiffServ classification and prioritization, based on the rules configured in the router.

How to create Ignore rules for an applied IPS policy

After you specify the security policies to be applied, the Sensor scans the traffic according to these policies and takes the configured action when it finds a matching traffic flow. However, there could be instances where you do not want certain traffic to be treated as an attack by the Sensor even though this traffic might match a specific attack definition. Consider some of this traffic might appear as an attack. You are aware of the purpose of this traffic and you do not want the Sensor to take any response action on this traffic. However, if similar traffic is generated by any other server, you want the Sensor to treat it as an attack and respond accordingly. Trellix IPS provides various options to handle such situations, which are discussed in this chapter.

Configure alert suppression with packet log response

Prerequisite: Make sure the Sensors for which you want to configure alert suppression are active and reachable to the Manager.

You can set a suppression limit for multiple occurrences of a singular attack for a specific source-destination IP address pair that is detected within a limited time frame, as well as set up packet logging for the attacks — this is known as *Exploit throttling*. Exploit throttling limits the number of duplicate alerts that are sent to Manager from a Sensor. Throttling is very effective against repetitive Exploit attacks where a source IP address is spoofed and generates a high number of alerts. In addition, the Sensor saves the alerts and packet logs in first-in first-out (FIFO) buffers in the event it loses communication with Manager, as well as when a Sensor generates alerts faster than it can send to Manager. The Attack Log, in its details, displays this type of alert as **Exploit** with an **Attack Count** of 2 or higher.

NOTE

Alert suppression is unavailable for anomaly-based buffer overflow and shellcode attacks.

In Trellix IPS, an exploit throttle alert is the grouping of multiple instances of the same attack (by Alert ID) from a single source to a single destination detected by the same VIPS (interface or subinterface — if an interface has been segmented into subinterfaces, the interface is no longer the VIPS; the subinterface is). Thus, the equation is: AlertID + VIPS + Source IP + Destination IP + Count = Exploit throttle attack

The **Generate unique suppression summary alerts for up to [*X*] attack, attacker and target combinations** field determines the number of unique Exploit throttle instances to maintain at a given time. For example, if you enter the number 10, then 10 unique Exploit throttle instances can be tracked at a given time. Once 10 is reached, all other cases are kept in a single "wildcard" instance; thus, other unique combinations that occur outside of the 10 uniquely maintained instances are maintained as one instance, and source and destination IP addresses do not appear in the Exploit throttle summary since multiple addresses may be involved. This is due to Sensor memory limits. A throttle entry is removed after the time limit (**The alert suppression window is [*X*] seconds**) has expired.

The **Generate standard alerts for the first [*X*] attack(s) seen during the alert suppression window** identifies the minimum number of alerts that must be detected for a unique suppression instance to be classified as an exploit throttle attack. This number means you *accept* a specific number (*x*) of the same attack. Thus, if you detect *x-1* by the expiration of the interval (**The alert suppression window is [*X*] seconds** field), alerts are sent for each separate occurrence and there is no exploit throttle. If there are *x+1*, the first *x* attacks are sent as individual alerts and the attacks exceeding this count are throttled into one alert that summarizes this persistent attack. By sending a few of the throttled alerts as individuals allows you to view details and packet log information for the first few instances of an attack.

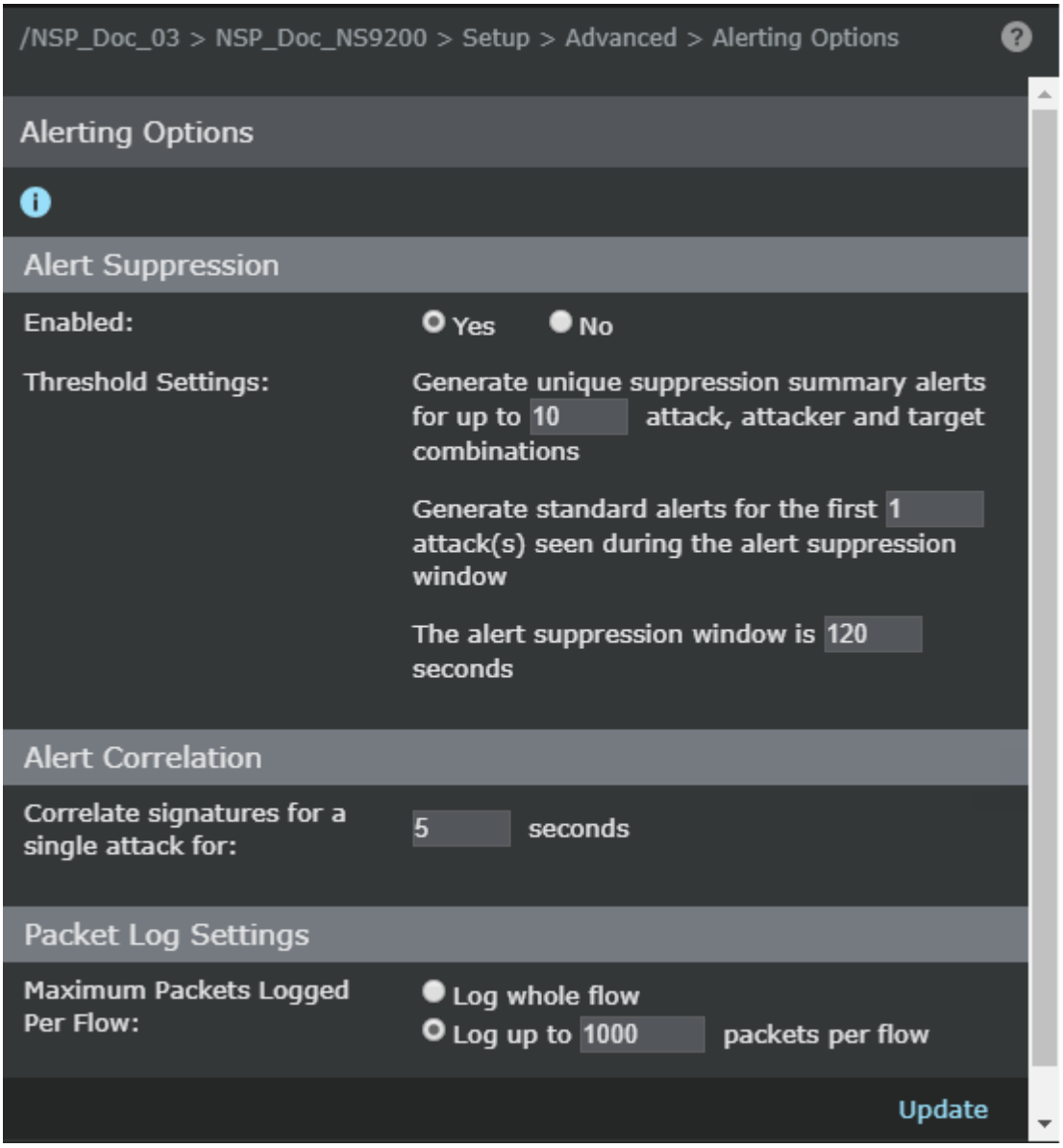
The **The alert suppression window is [*X*] seconds** field is the time span in which you accumulate instances of the same attack. This value acts as a timer; when the timer expires, the current instance is cleared to make room for a new suppression instance.

The **Correlate signatures for a single attack for [*X*] seconds** field notes the amount of time that the Sensor will correlate the signatures used to detect a suppressed attack instance. Many attacks have multiple signatures; thus, the suppression is valid as long as any signature for a suppressed attack has detected a single attack instance. Correlation sends the signature with the lowest Benign Trigger Probability in the suppressed alert record.

Complete the following tasks to enable alert throttling.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Alerting Options**.

Figure 605. IPS Alerting page



6. Select **Yes** for **Enabled** under **Alert Suppression** to turn on alert suppression.

> **NOTE**
>
> Select **No** and click **Update** at any time to disable alert suppression.

7. Type a value within **Generate unique suppression summary alerts for up to [** *X* **] attack, attacker and target combinations**.

   This is the number of unique instances that will maintain counts during the time limit. All other suppression groupings are recorded in a single *wildcard* instance. The default is 10 instances.

8. Type a value within the **Generate standard alerts for the first [*X*] attack(s) seen during the alert suppression window**.

   This number signifies the number of individual alerts for a unique suppression instance that you want to be sent before collecting all of the alerts into one throttle instance. The default is 1 alert. By sending individual alerts before the throttle preserves the ability to generate packet logs for each alert rather than one log for the entire throttle.

9. Type a value within **The alert suppression window is [*X*] seconds**.

   The default is 120 seconds.

10. Type a value within **Correlate signatures for a single attack for** field under **Alert Correlation**.

    The default is 5 seconds. The **Generate unique suppression summary alerts for up to [*X*] attack, attacker and target combinations** is active for this time limit.

11. Select a **Maximum Packets Logged Per Flow** under **Packet Log Settings**.

    Either of the two choices will also contain the 128 bytes previous to the attack. You can do one of the following:

    - **Log Whole Flow** — Logs entire flow from start to finish of transmission.
    - **Log up to*n*packets per flow** — Type the number of packets (from 1000 to 64000) to log within a flow. The logged packets begin with the attack packets. Default is 1000 packets.

    > **NOTE**
    >
    > Even if you select **Log Whole Flow**, the Sensor may not be able to continue logging if it fails.

12. Click **Update**.

    The alerts for exceeding this threshold are called *throttle* alerts. You will see this in the **Alert Details** panel of Attack Log.

13. Deploy configuration changes to the Sensor.

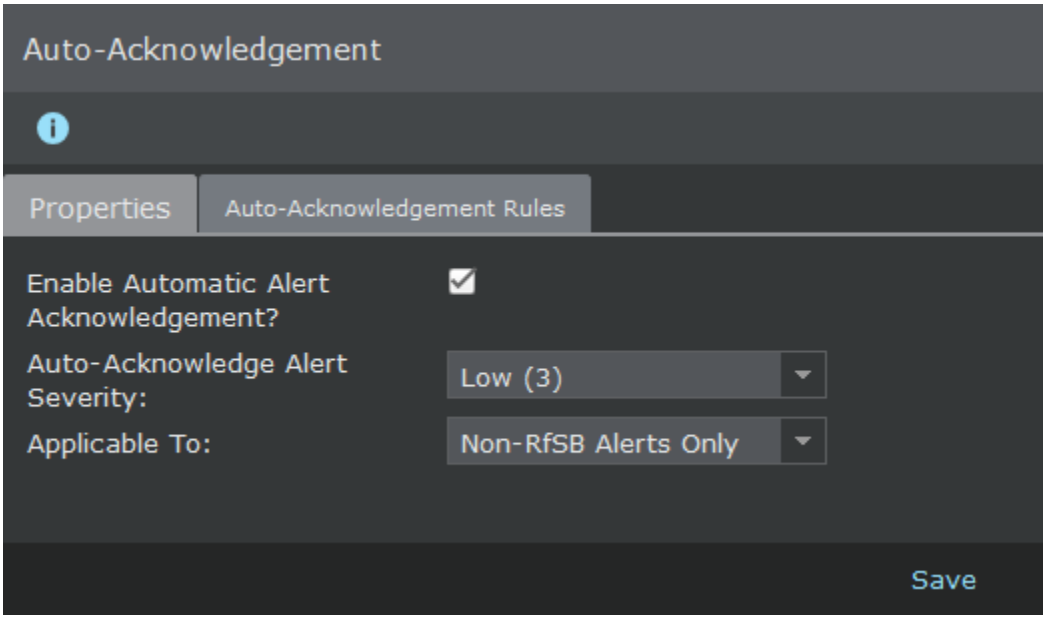
Auto-Acknowledgement of alerts

Using the **Auto-Acknowledgement** feature, you can set up the Manager to automatically acknowledge alerts based on the severity levels of the corresponding attacks. Note that the Sensor plays its usual role here. That is, it detects the attack and sends an alert and the takes the other configured response actions. If you enable this feature, the Manager automatically acknowledges the alerts for the specified attacks. You can also create new acknowledgement rules based on which repeated attacks are automatically acknowledged. This prevents your **Dashboard** from being flooded with information regarding insignificant alerts. The details of the auto-acknowledged attacks do not reflect in the **Dashboard**. You can use the **Attack Log** page to view the acknowledged alerts.

Configure Auto-Acknowledgement based on alert severity

You can set auto-acknowledgement for all alerts or non-RfSB alerts based on their severity levels. This acknowledges the alerts automatically as and when the alerts are generated. Auto-Acknowledgement for alerts is disabled by default. You can view the acknowledged alerts in the **Attack Log** page. The auto-acknowledgement feature is available only at the root admin domain. You cannot set any auto-acknowledgement rules for alerts from the child domains.

Figure 606. Auto-Acknowledge alerts



1. Navigate to Policy → Intrusion Prevention → Exceptions → **Auto-Acknowledgement**.
2. Select the **Enable Automatic Alert Acknowledgement?** checkbox.

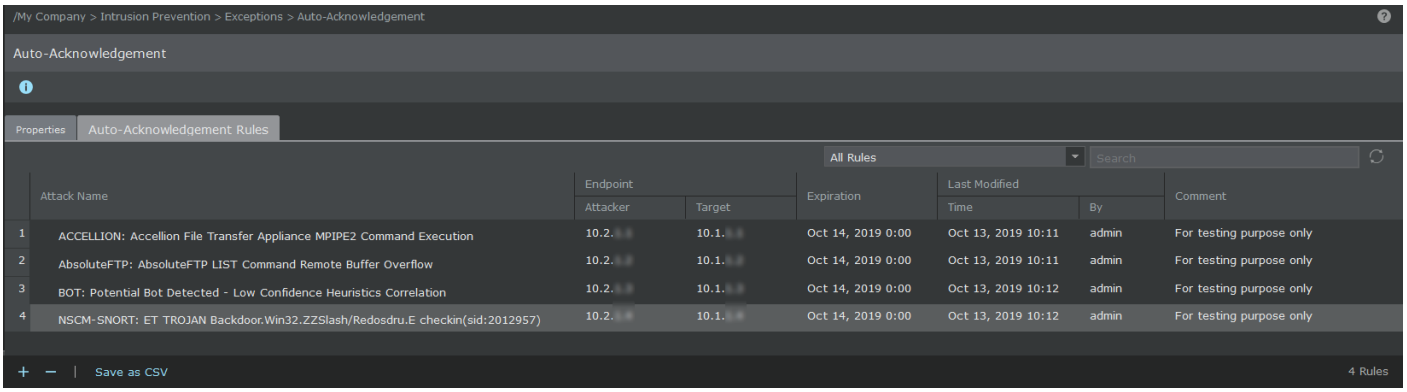
   The **Properties** page is displayed.
3. From the **Auto-Acknowledge Alert Severity**, select the severity level for the attacks.
4. Select the type of alerts to be auto-acknowledged from the **Applicable to** drop-down list.

   You can either set the auto-acknowledgement to non-RfSB alerts only or all the alerts generated which will include the RfSB alerts also.
5. Click **Save** to save your settings.

Configure Auto-Acknowledgement based on rules

You can create auto-acknowledgment rules based on the name, source endpoint, and target endpoint of attacks. You can also define the time period for which the rule could be applicable. The Manager auto-acknowledges those alerts, which match the active rules. The list of auto-acknowledgement rules can be exported.

Figure 607. Auto-Acknowledgement Rules



Use the drop-down on top to filter rules based on the expiration dates. **All Rules** is selected by default. All expired rules are prefixed with the warning symbol which helps differentiate between the active rules and the expired rules. You can use the **Search** field to search for a specific rule. You can also sort the column in ascending or descending order. To hide any column, hover over a column, click the drop-down arrow, and select the columns you want to hide.

1. Navigate to Policy → Intrusion Prevention → Exceptions → Auto-Acknowledgement → **Auto-acknowledgement Rules**.
2. Perform one of the following actions to manage the auto-acknowledgement rules:
   - To create a rule, click the + icon
   - To edit a rule, select the rule you want to edit.

   The **Rule Details** panel opens on the right side.
3. Enter/modify the details for the following fields:

Option	Definition
Attack Name	Enter the name of the attack or select the attack from the list displayed. **NOTE** As you type the name of the attack, a list of attacks are displayed.
Attacker Endpoint	Enter the IP address of the endpoint from where the attack is generated.
Target Endpoint	Enter the IP address of the endpoint to which the attack is targeted.
Expiration	Select the expiration date and time for the rule.
Modified	Shows the last modified user, date, and time at which the rule was modified.
Comment	Optionally enter additional comments.

NOTE

Either the attack name or any one endpoint has to be mentioned while creating a new rule.

4. Click **Save** to save the rule.

Click the icon to close the **Rule Details** panel.

5. To delete an acknowledgement rule, select the rule you want to delete and click the icon.

> **NOTE**
>
> You can select multiple rules and delete.

6. To export the auto-acknowledgement rules, click **Save as CSV**. The list of auto-acknowledgement rules available are exported as a .csv file.

You can also create an auto-acknowledgement rule from the **Attack Log** page. For more information, see *Attack Log* (page 374).

Manage Ignore Rules

Ignore Rules are rules that filter attacks/attack responses in IPv4 or IPv6 traffic, based on source IP address, destination IP address, or both. When Ignore Rules are assigned to an attack definition, that attack is ignored when seen between the source and destination. No alert is generated and none of the configured response action is taken.

In the Manager, you can define Ignore Rules from the **Policy** tab and assign them to domains, Sensors and Sensor interfaces. Ignore Rules assigned at the domain level are associated with all Sensors belonging to that domain. Similarly, Ignore rules assigned at the Sensor level are associated with all ports and interfaces/subinterfaces belonging to that Sensor.

> **NOTE**
>
> When domain-level Ignore rules settings are overridden at the Sensor level, behavior of other resources belonging to that Sensor and using the same rule objects is also affected.

You can define the following types of Ignore Rules in the Manager:

- **IPv4** — IPv4 Ignore Rules without any source/destination port settings
- **IPv6** — IPv6 Ignore Rules without any source/destination port settings
- **TCP/UDP port** — Ignore Rules with only source/destination port settings
- **IPv4 with TCP/UDP port** — IPv4 Ignore Rules with source/destination port settings
- **IPv6 with TCP/UDP port** — IPv6 Ignore Rules source/destination port settings

You can now use rule objects (network objects) to define Ignore Rules at the domain and Sensor levels. This provides a unified way to define various features in the Manager using the rules that are used in the firewall quarantine zones. The rule objects that allow you to define Ignore Rules for the Source or Destination IP address settings are the following:

- **IPv4 Endpoint or IPv6 Endpoint address —** You can create a list of source and destination IPv4 addresses that you want to use in a rule. You can specify up to 10 addresses in a Rule Object.
- **IPv4 Address Range or IPv6 Address Range —** You can create a list of IPv4 or IPv6 address ranges to use in an Ignore rule. In the rule, you can specify an IPv4 or IPv6 address range as the source or destination of traffic. For example, you may want to apply a rule to traffic from IPv4 addresses ranging from 10.1.1.1 to 10.1.1.25. You can specify up to 10 ranges in a Rule Object.

- **IPv4 Network or IPv6 Network —** You can create a list of CIDRs to use in an Ignore rule. In that rule, you can specify a CIDR as the source or destination of traffic. For example, you might want to apply a rule on the traffic targeted for 172.16.225.0/24 network. The three reserved IPv4 ranges according to RFC 1918 and reserved IPv6 address block according to RFC 4193 are provided as default networks. You can specify up to 10 CIDRs in one Rule Object.
- **Network Group (Network Group for Exception Object) —** You can combine one or more Host IP addresses, IP address ranges, or Networks to form a Network Group. For example, you can combine multiple IPv4 addresses or IPv6 ranges to form a Network Group rule object. You can specify up to 10 items in one Network Group Rule Object.

NOTE

The Ignore rules feature is unsupported with X-Forwarded-For (XFF) header parsing feature for HTTP or HTTPS traffic.

To use Ignore Rules, select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Ignore Rules.**

You can perform the following tasks:

- Edit Ignore Rules. This includes adding, cloning, viewing, and deleting rules.
- Manage Ignore Rule assignments.
- Manage Ignore Rules.
- Export Ignore Rules.
- Import Ignore Rules.

How to use the Ignore rules editor?

To manage Ignore Rules, select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Ignore Rules**. The **Ignore Rules** page is displayed.

From this page, you can perform the following tasks:

- Click  to add Ignore Rules
- Click  to copy Ignore Rules
- To view or edit an ignore rule object double-click the row of the rule object
- Click  to delete Ignore Rules
- Click **Save as CSV** to save the Ignore Rules in CSV format.

The list on the **Ignore Rules** page displays the following information:

Field	Description
State	Specifies whether the state of the rule is **Enabled** or **Disabled**
Name	Specifies the name of the ignore rule.
Attack	**Name** — The name of the attack. **Direction** — Displays whether the direction of the attack is **Inbound** or **Outbound**.

Field	Description
Scope	Specifies the resource to which the ignore rule is applied.
Attacker	**Endpoint** — Specifies the attacker endpoint IP address. **Port** — Specifies the attacker port as **TCP**, **UDP**, **TCP or UDP** or **Any**.
Target	**Endpoint** — Specifies the target endpoint IP address. **Port** — Specifies the target port as **TCP**, **UDP**, **TCP or UDP** or **Any**.
Last Updated	**Time** — Specifies the time when the Ignore Rule was last modified. **By** — Displays the user who modified the Ignore rule
Comment	Displays any additional comment specified for the rule.
Search	Type your search criteria in the field to find the ignore rule with the matching elements.

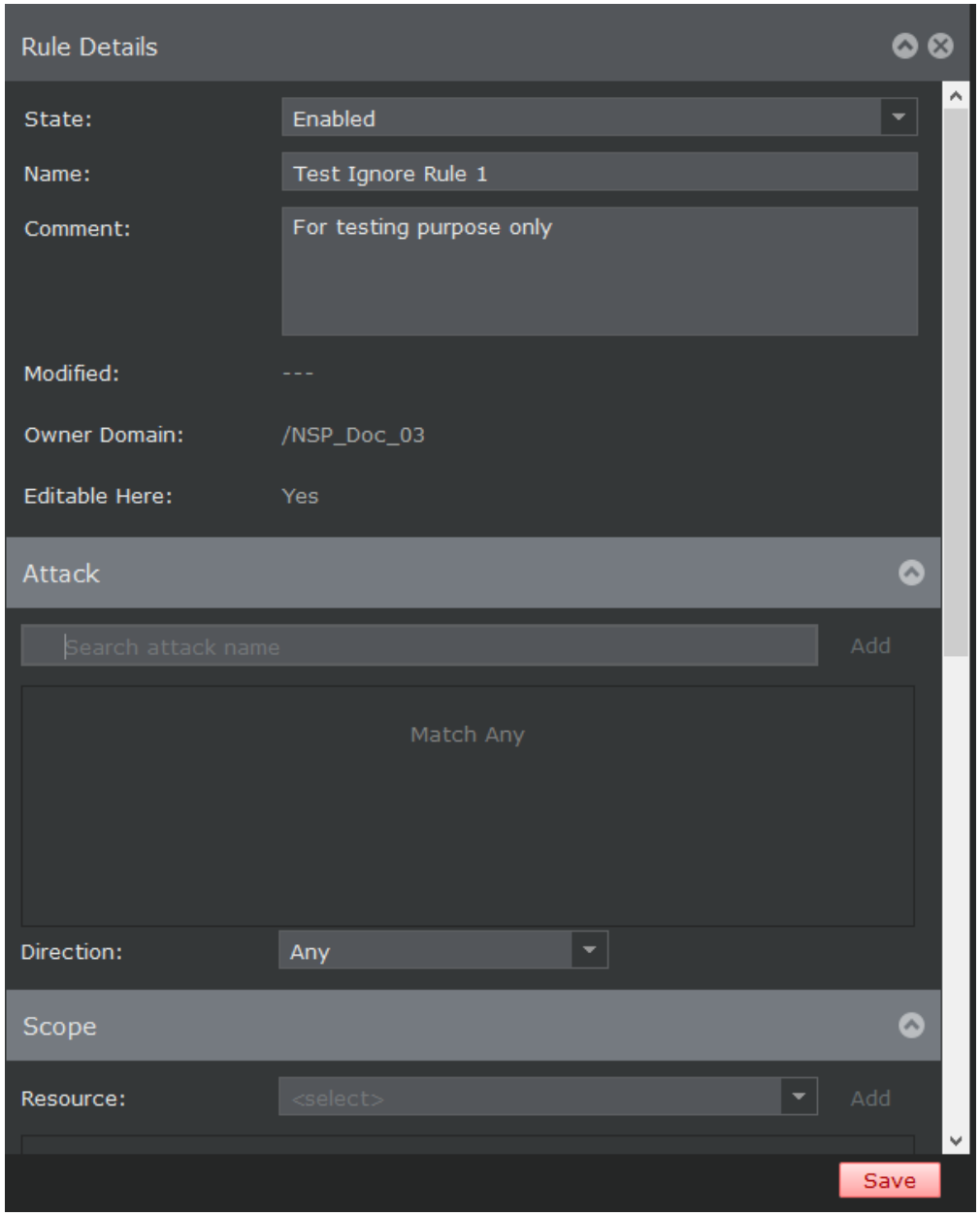
Add Ignore Rules

To add Ignore Rules in the Manager, complete these tasks.

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Ignore Rules**.
2. In the **Ignore Rules** page, click +.

   The **Rule Details** panel appears.

Figure 608. Add an Ignore Rule window



3. Specify your options in the corresponding fields.

Field	Description
State	Select the status of Ignore Rules as **Enabled** or **Disabled** from the drop-down list
Name	Type the name of the Ignore Rule
Comment	Type additional comments if required.
Modified	Name of the user who last modified the rule.

Field	Description
Owner Domain	The name of the admin domain under which the Ignore Rules is added.
Editable here	The status **Yes** indicates that the ignore rule is owned by the current admin domain. The status **No** indicates that the Ignore Rule is not owned by the current admin domain.
Attack	Select the attack to match the criteria. 1. Type the first few letters of the attack name in the **Search attack name** field select the attack from the list. 2. Click the **Add** button to add the attack name to the list. 3. Select the **Direction** from the drop-down list. The options are **Inbound**, **Outbound** and **Any**. Click to remove the attack from the list.
Scope	Select one or more device or interface to match the criteria. 1. Select the device or interface from the drop-down list. 2. Click on the **Add** button to add the device or interface to the list. Click to remove the item from the list.

Field	Description
Attacker	1. Select the rule object from the drop-down list. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in Ignore Rules is 10. 2. Click on the **Add** button to add a rule object to the list. Click  to create a new rule object. The supported network objects are: • **IPv4 Address Range** • **IPv4 Endpoint** • **IPv4 Network** • **IPv6 Address Range** • **IPv6 Endpoint** • **IPv6 Network** • **Network Group (Network Group for Exception Object)** Click  to edit or view a rule object. Click  to remove the rule object from the list. 3. Select the type of port from the **Port** drop-down list. The available options are: • **Any** • **TCP** • **UDP** • **TCP or UDP** 4. Type the port values in the field provided. The supported port values are 1 to 65535. To specify multiple ports used in the same protocol, provide the values separated by commas. Example: 15,25.

Field	Description
Target	Select one or more rule objects. 1. Select the rule object from the drop-down list. **NOTE** The Manager filters the rule objects containing more than 10 entries and lists only those which contain up to 10 entries, since the maximum supported rule object members per rule object in Ignore Rules is 10. 2. Click on the **Add** button to add the rule object to the list. Click  to create a new rule object. The supported network objects are: • **IPv4 Address Range** • **IPv4 Endpoint** • **IPv4 Network** • **IPv6 Address Range** • **IPv6 Endpoint** • **IPv6 Network** • **Network Group for Ignore Rule** Click  to edit or view a rule object. Click  to remove the rule object from the list. 3. Select the type of port from the **Port** drop-down list. The available options are: • **Any** • **TCP** • **UDP** • **TCP or UDP** 4. Type the port values in the field provided. The supported port values are 1 to 65535. To specify multiple ports used in the same protocol, provide the values separated by commas. Example: 15,25.

4. Click **Save** to save the Ignore Rule.

Clone Ignore Rule object

You can clone Ignore Rule. To clone an Ignore Rule.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Exceptions → **Ignore Rules**.

   The Ignore Rules for the selected admin domain are listed.

4. Locate the Ignore Rule that you want to clone.

> **TIP**
>
> You can use the search function to more easily find the Ignore Rule.

5. Select the Ignore Rule and click  .
6. Make the required changes and click **Save**.

View or edit Ignore Rule

To view or modify ignore rule, do the following:

1. In the **Ignore Rules** page, double-click on the row of the ignore rule that you want to modify.

   The **Rule Details** panel is displayed. You can edit the values for the fields.
2. Click **Save** to complete setup of the ignore rule.

Delete Ignore Rule

You can delete an ignore rule from the **Ignore Rules** page. To delete an ignore rule:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Exceptions → **Ignore Rules**.

   Ignore Rules for the selected admin domain are listed.
4. Locate the Ignore Rules that you want to modify.
   - You can use the search function to easily find the Ignore Rule.
   - Make sure the **Editable here** column displays **Yes** for the rule you want to delete. If the **Editable here** column displays **No**, the rule belongs to a parent admin domain.
5. Select the Ignore Rule and click  . Then click **Yes** to confirm deletion.

> **NOTE**
>
> To delete Ignore Rules in bulk, press *Shift* key (for continuous selection) or press *Ctrl* key (for discontinuous selection) and then select the rule objects. The selected items are highlighted. Click and then click **Yes** to confirm deletion.

Import Ignore rules

Between the same versions of the Manager, you can export and import Ignore rules. When you export, the selected Ignore rules are exported into a .xml file. You can then import this .xml file into a Manager to create the Ignore rule contained in that .xml file.

1. Select Intrusion Prevention → Advanced → Policy Import → **Ignore Rules.**
2. Specify the required options to import the ignore rules.

Option	Definition
Append the existing set of rules	When selected, the Manager appends the ignore rules to the existing set of rules.
Import File	Click **Browse** to locate the file to import.
Import	Begins the import process

Export the ignore rules

You can export the ignore rules in CSV format.

1. Select Policy → Intrusion Prevention → Advanced → Policy Export → **Ignore Rules**.

   The **Ignore Rules** page is displayed.

2. Click **Export** to export into an excel sheet.

Management of rule objects

You can use rule objects to create ignore rules. You can use common rule objects across other features in the Manager such as Firewall.

Rule objects, in ignore rules, can be customized to override any settings made at the parent domain level. They can be customized at the admin domain level, child domain level or the Sensor level.

NOTE

The ability to customize a rule object is only available for ignore rules. Firewall, which also uses rule objects, does not support rule object customization.

Icon/Option	Definition
Rule object	Displays the rule objects according to the filter criteria. Click a column heading to sort the table in ascending or descending order. • **Name** — Indicates the name of the rule objects. • **Description** — Indicates the description of the rule object. • **Type** — Indicates the rule object type. • **Owner Domain** — Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain. • **Visibility** — Indicates the visibility settings of settings to the domains, whether it is visible only to the owner domain or to both owner and child domains. • **Editable here** — **Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.

Icon/Option	Definition
Object Type	Filters rule objects in the list. • **Default Objects Only** — Trellix pre-defined these rule objects. For example, the Application and Country are default rule objects. You cannot define these rule objects. • **Custom Objects Only** — You need to define these rule objects. For example, you need to define the Host DNS Name rule object. • **Custom and Default Object** — When selected, it displays both the predefined and user-defined rule objects. For example, IPv4 Network Rule Object has the 3 reserved private networks pre-defined, but you can create your Network rule objects as well.
Rule Object Type	Select the rule object type that you want to view.
Search	Type your search criteria in the field to find rule objects with matching elements. For example, type to list the rule objects containing *google* as part of their names.
 icon	Creates a custom rule object.
 icon	Clones a rule object. You cannot clone default rule objects other than the IPv4 network rule objects.
 icon	Deletes a custom rule object belonging to the current admin domain.
To view or edit a rule object	Double-click the rule object belonging to the current admin domain.

The following table lists the available rule objects and the corresponding icons.

Icon	Rule Object
	IPv4 Endpoint
	IPv6 Endpoint
	IPv4 Address Range
	IPv6 Address Range
	Network Group for ignore rule

Icon	Rule Object
	IPv4 Network
	IPv6 Network

NOTE

IPv6 Address Range and **Network Group for Ignore Rule** are two new types of rule objects that are only applicable to ignore rules.

By default, a Sensor inherits the rule object definitions from the domain that owns the Sensor (when the rule object is not customized at the Sensor level). If there is no customized definition present in this domain, the Sensor inherits the object definition from its parent domains in the hierarchy until a valid definition is found.

You can customize rule object definitions at the child domain level, only if the resources belong to the child domain. Such changes, made at the child domain level, will be visible in the parent admin domain level and can also be modified here.

If you delegate an interface (say G0/1) belonging to a Sensor to a child domain, all the rule objects assigned to that interface (through ignore rules) inherit their definition from the customization at the physical Sensor level. If there is no Sensor level definition, the specific rule object inherits its definition from the admin domain to which the Sensor belongs.

View a rule object

You can view existing rule objects in a selected domain.

For a rule object to be listed, it must meet one of these conditions:

- It is a default rule object.
- It is created at a parent admin domain, but it is set to be visible to the child admin domains.
- The rule object was created at the current admin domain.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

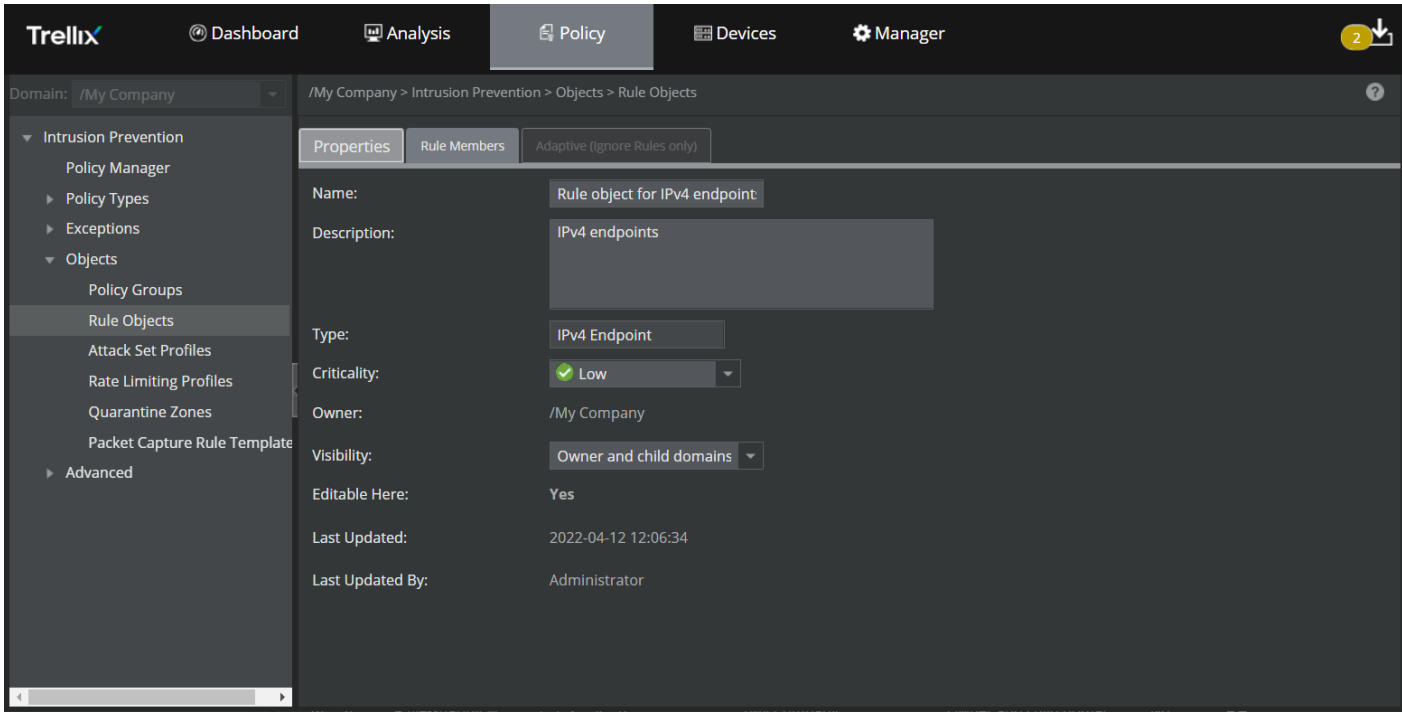
   Rule Objects for the selected admin domain are listed.

   - To locate specific rule objects, enter a string in the **Search** text box. For example, type “google” in the **Search** text box to list the rule objects containing “google” as part of their Names.
   - Select the **Custom Objects Only** or **Default Objects Only** or **Custom and Default Objects** from the drop-down list as required.
   - Select the rule object type in the drop-down list.
   - To view limited details of a rule object, point to the object. To view complete details, select and double-click the rule object.

- The rule object details appear under the **Properties** tab, and the rule members (rule object items) appear under the **Rule Members** tab.

> **NOTE**
>
> An additional tab named **Adaptive (Ignore Rules only)** appears while viewing IPv4 and IPv6 based rule objects.

Figure 609. Viewing Rule Objects

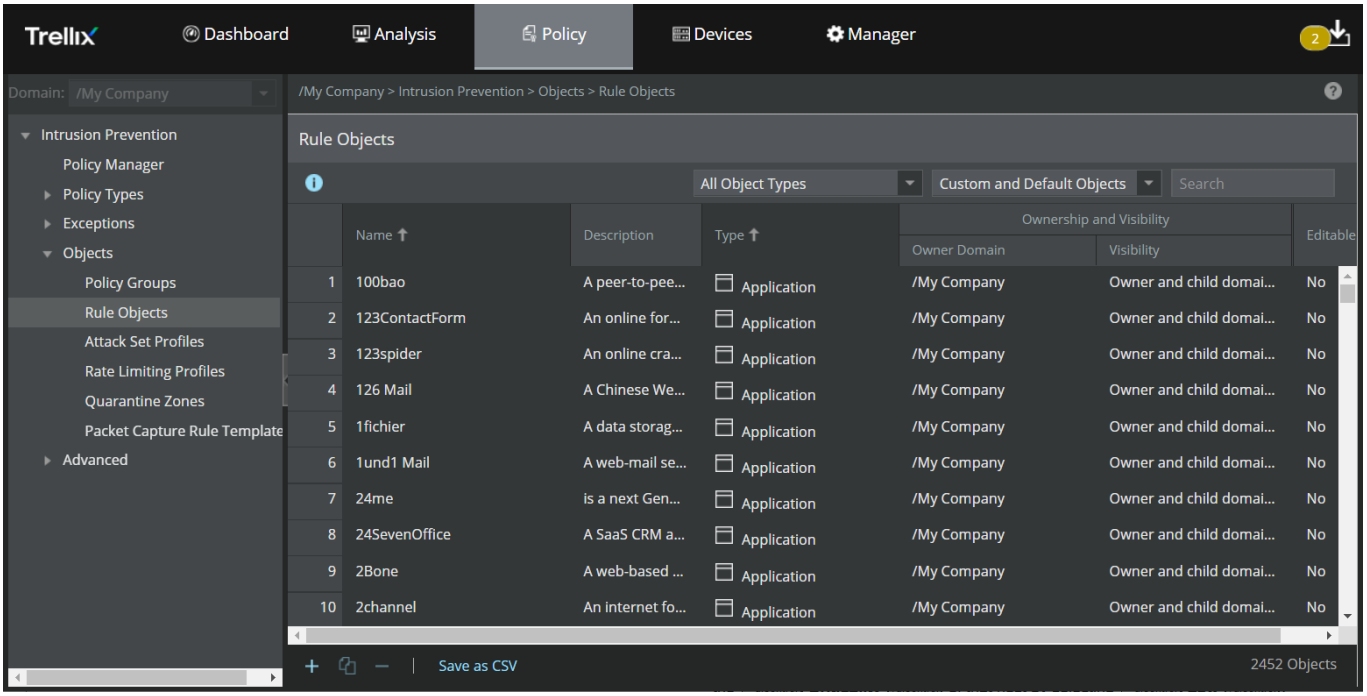


Add a rule object

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Objects → **Rule Objects**.

   Rule objects for the selected admin domain are listed.

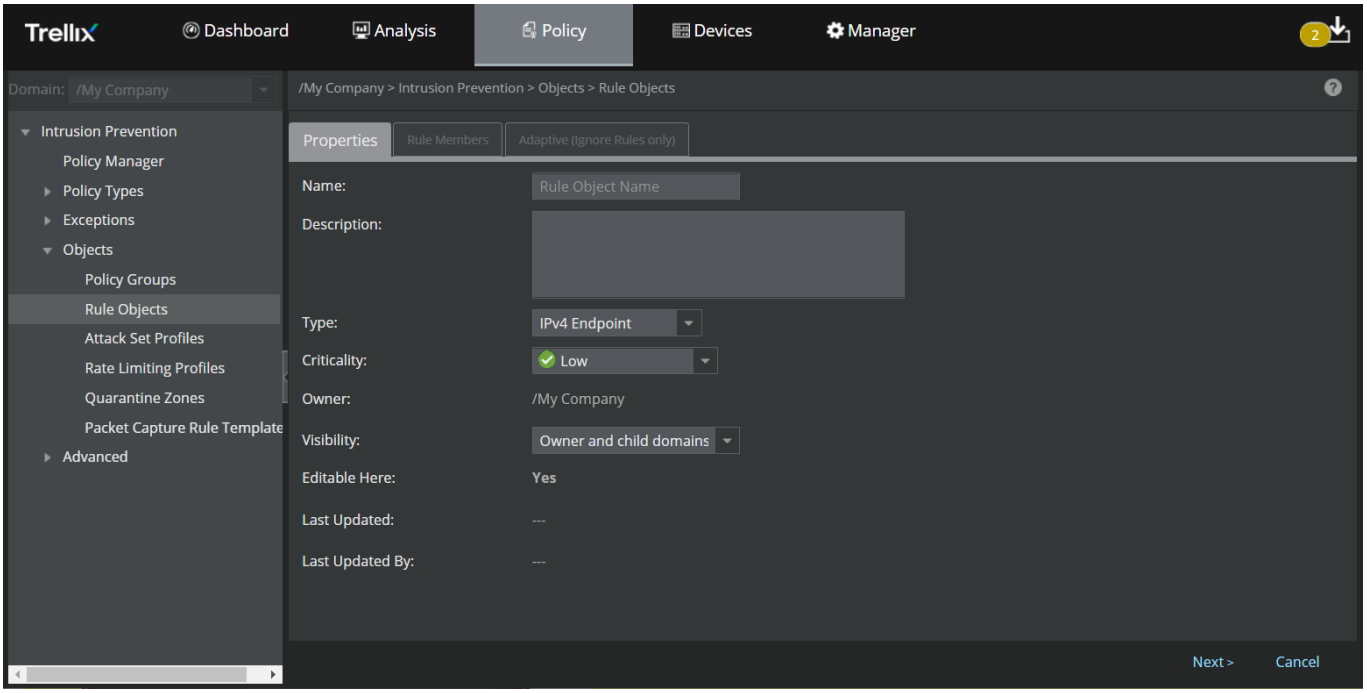
Figure 610. Rule Objects page



2. Click +. This displays two tabs, namely the **Properties** tab and the **Rule Members** tab.

> **NOTE**
>
> An additional tab named **Adaptive (Ignore Rules only)** appears while adding IPv4 and IPv6 based rule objects.

Figure 611. Selecting Criticality for each of your assets

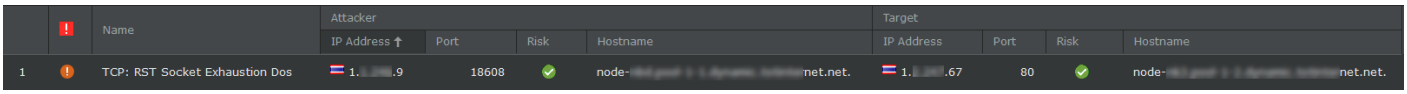


The following table describes the options in the **Properties** tab that are common to all rule objects.

Option	Definition
Name	Enter a unique name to easily identify the rule object.
Description	Enter the description for the rule object.
Type	From the drop-down list, select the type of rule object you want to create. For information on a specific object type, refer to the corresponding sub-section.
Criticality	[Optional] If you have chosen rule object type as IPv4 Endpoint or IPv6 Endpoint, you can specify the **Criticality** of that host by selecting **Low**, **Medium** or **High** from the drop-down list. By default, criticality is **Low**. Determining criticality of a host enables you to categorize all IPv4 Endpoint and IPv6 Endpoint addresses based on their importance to your organization.
Owner	Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain.
Visibility	From the drop-down list, select the option for the visibility level of the rule object. The available options are **Owner and child domains** and **Owner domain only**.
Editable Here	**Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.
Last Updated	Displays the date and time when a rule object was last updated
Last Updated By	Displays the user who modified a rule object

Once you assign criticality to a rule object and an alert involving it is raised, the criticality that you assigned shows up under specific columns in Attack Log. These columns are labeled **Attacker Risk** and **Target Risk**. **Attacker Hostname** and **Target Hostname** displays the names of the rule object.

Figure 612. Display of attacker risk



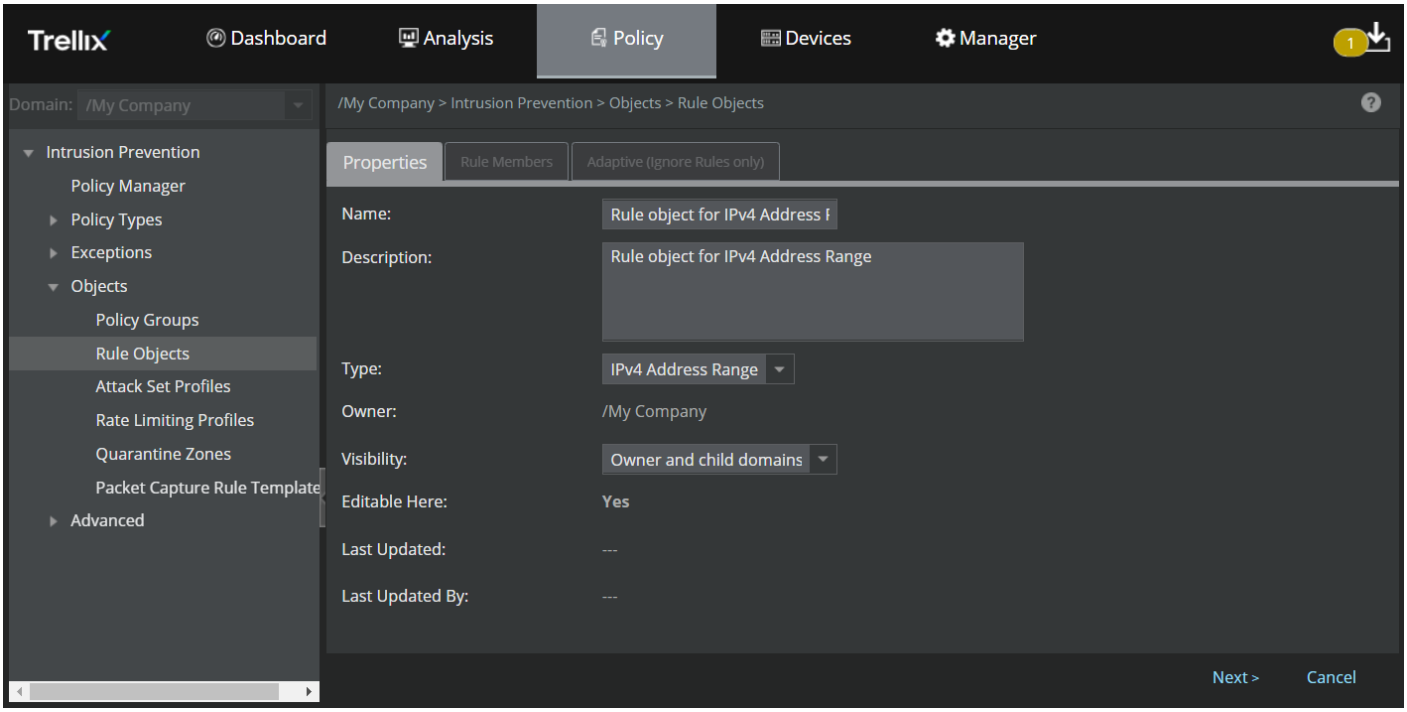
3. Enter the rule object options based on rule object you have selected in the **Type** drop-down list. For information on the subsequent steps to add a rule object, refer to the corresponding sub-sections.

Add an IPv4 or IPv6 Address Range rule object

The steps to add **IPv4 Address Range** and **IPv6 Address Range** rule objects are identical. Follow these steps to add **IPv4 Address Range** or **IPv6 Address Range** rule objects:

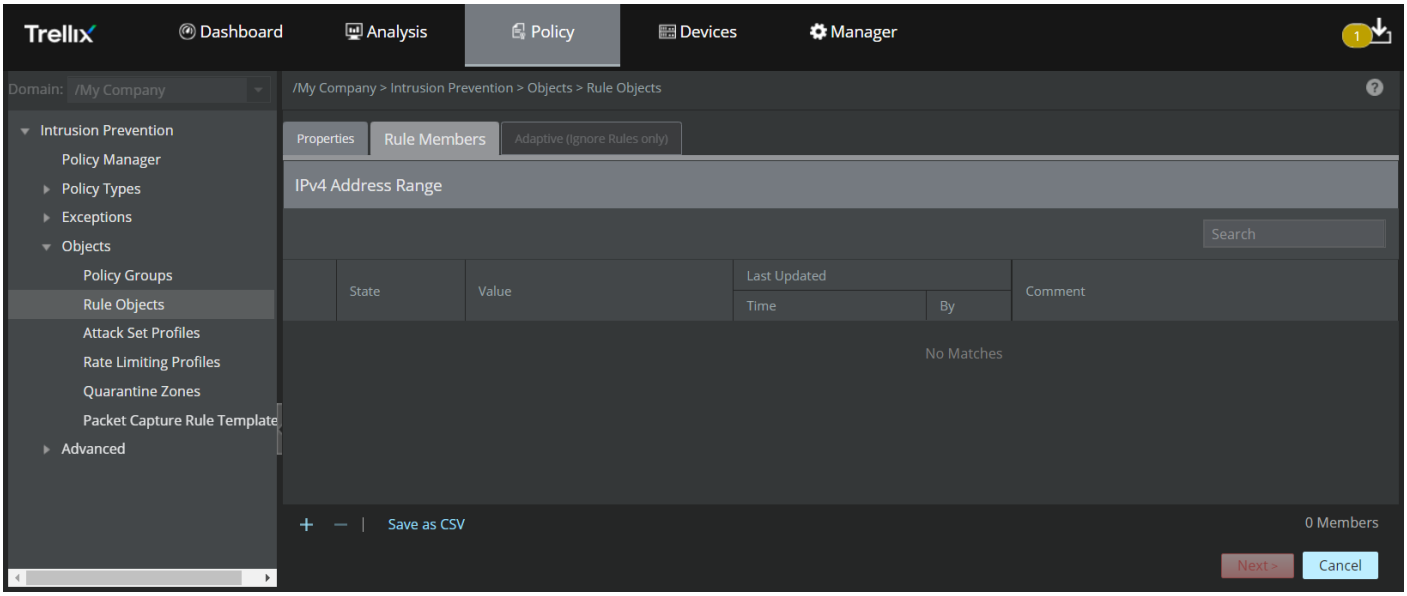
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Address Range** or **IPv6 Address Range** from the rule object **Type** drop-down, click **Next**.

Figure 613. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 614. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 74. Column details in the Rule Members tab - IP Address Range rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 address range based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 address range
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address range.
−	Click this icon to delete single or multiple IPv4 or IPv6 address ranges
Save as CSV	Click this icon to remove a rule object from the list

2. To add an IPv4 or IPv6 address range:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

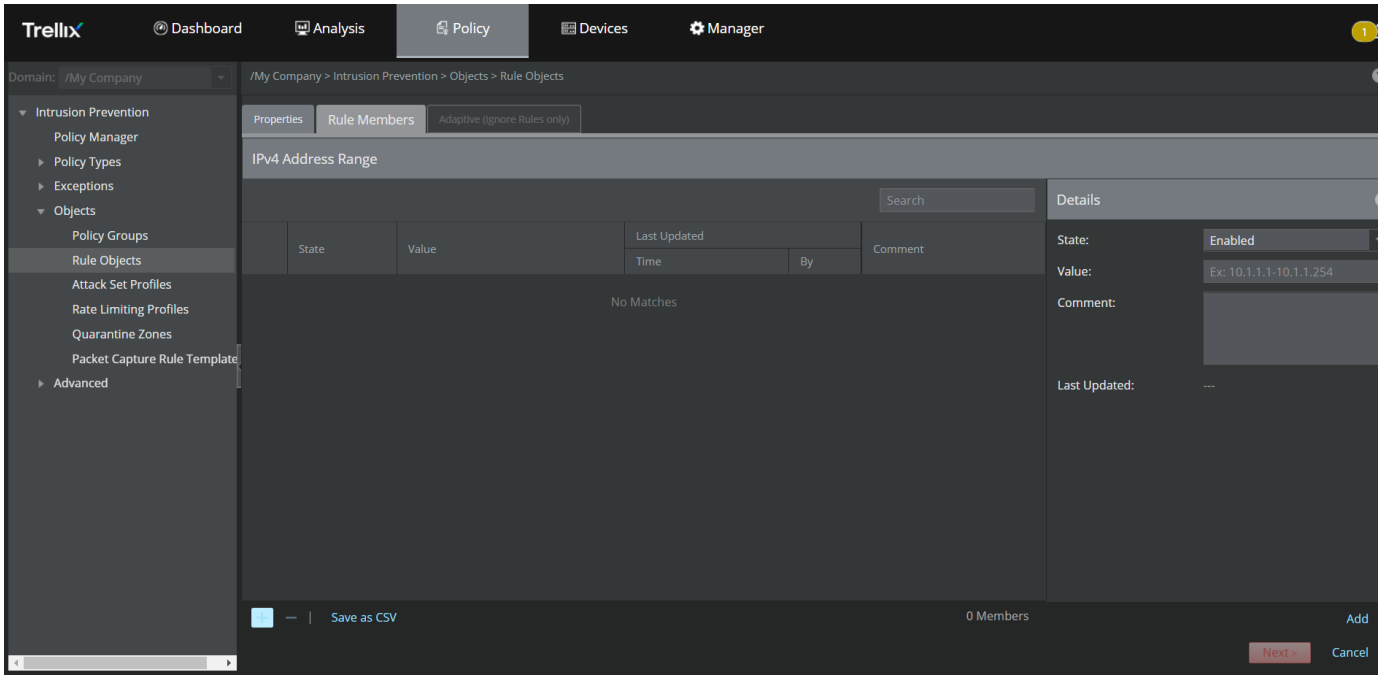
      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Address Range rule object].

Select the **State**, enter a valid IPv4 or IPv6 starting and ending address range in the **Value** field, enter a **Comment** if required and click **Add**.

NOTE

- Make sure to enter a hyphen between the starting and ending range (example: 10.1.1.1-10.1.1.25).
- You can enter up to 20000 IPv4 or 20000 IPv6 address ranges in a single rule object.
- The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
- If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 address ranges in any rule object.

Figure 615. Add individual IP addresses



3. Upon adding all the required IP addresses, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Rule Members** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values.

Option	Definition
Resource to Customize	Select the resource to customize from the drop-down list. **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**.
Add	Click this button to add the IP address range to the **Customizations** list.
Search	Type the search criteria to search for a resource.
	Click this icon to remove an address range from the list.

4. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

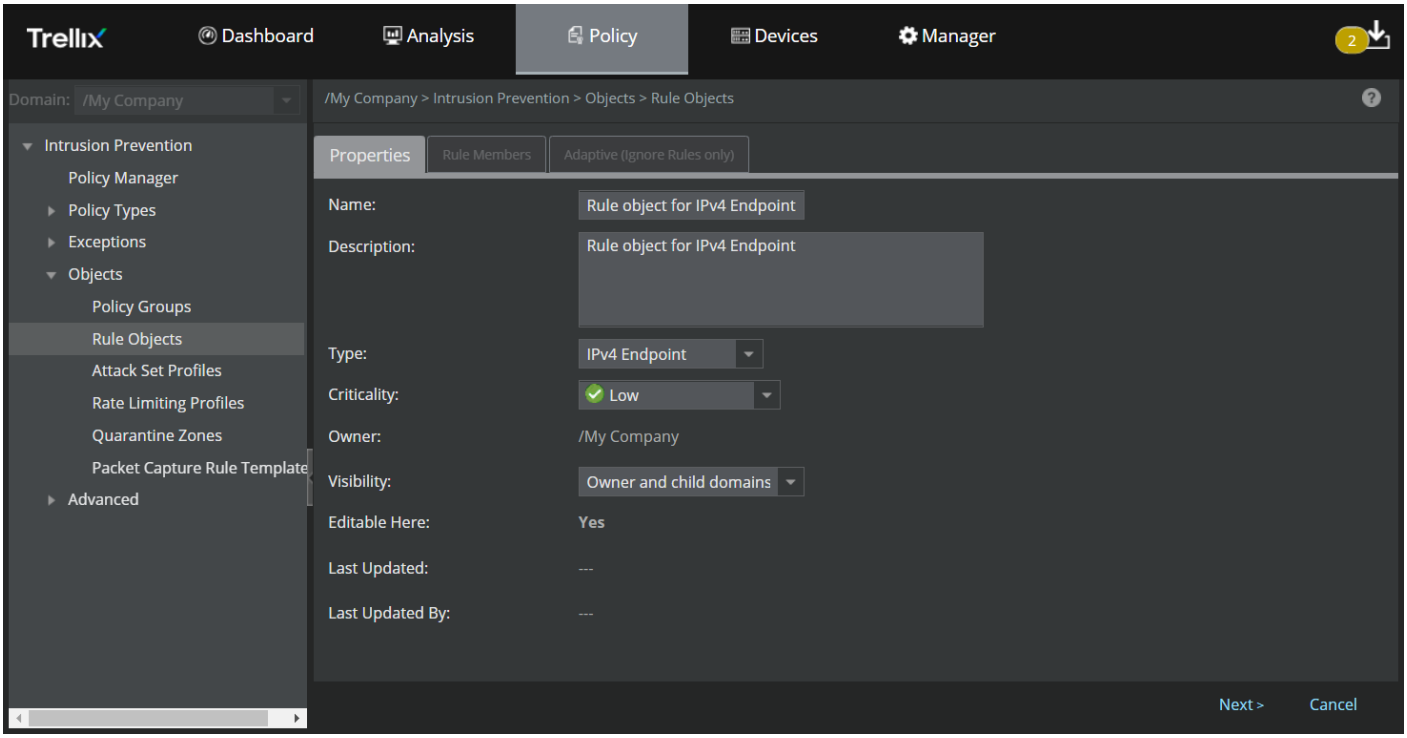
Add IPv4 Endpoint and IPv6 Endpoint rule objects

For quarantine zone access rules, only IPv4 Endpoint rule objects are supported. Also, only one rule member per rule object is applicable for quarantine zone.

The steps to add **IPv4 Endpoint** and **IPv6 Endpoint** rule objects are identical. Follow these steps to add **IPv4 Endpoint** or **IPv6 Endpoint** rule objects:

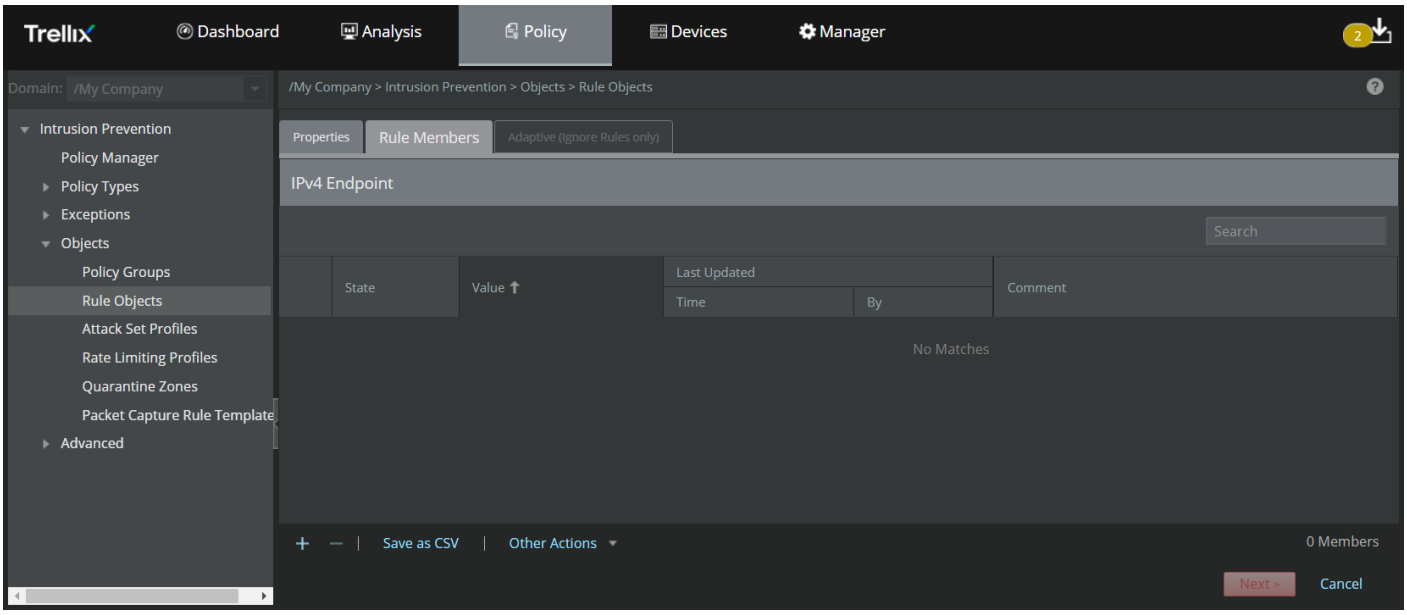
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Endpoint** or **IPv6 Endpoint** from the rule object **Type** drop-down, click **Next**.

Figure 616. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 617. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 75. Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 endpoint based on the rule object type selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 addresses
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address.
−	Click this icon to delete single or multiple IPv4 or IPv6 addresses.
Save as CSV	Click this button to export all the rule members displayed in the grid to a CSV file.
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 addresses • **Export All** — Allows you to export all the IP addresses from the Manager to the local system

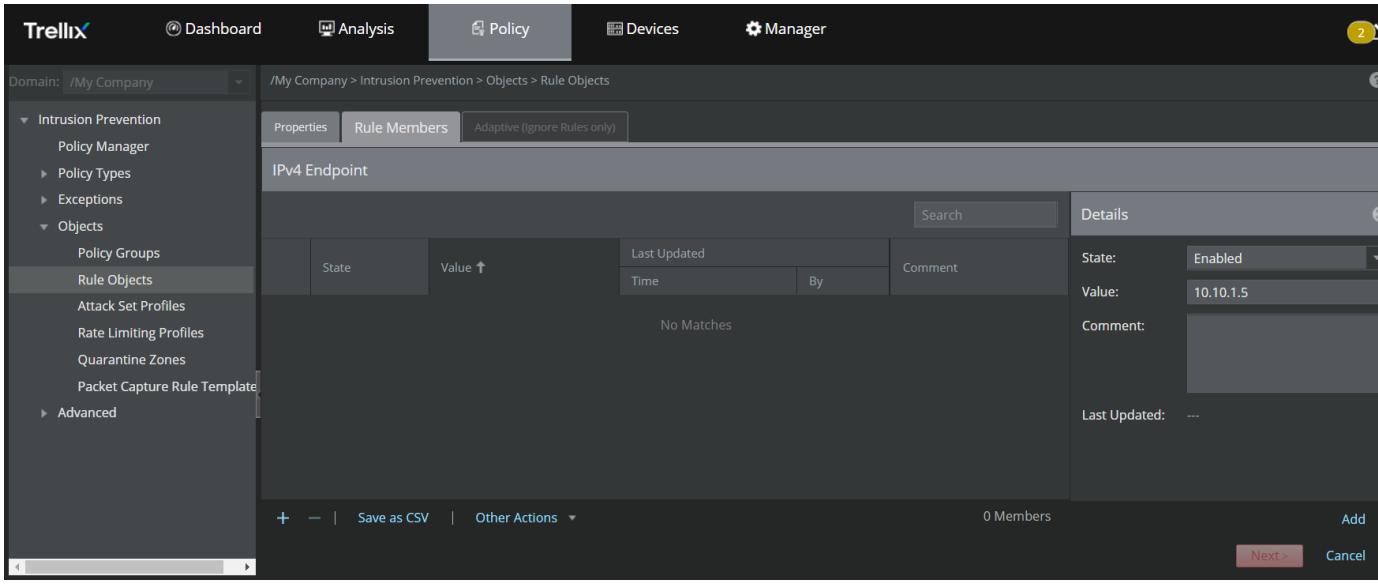
2. There are two ways to add the IP addresses — add individual IP addresses using the + icon or import a list of IP addresses from a CSV file using the Other Actions → **Import** option.
3. To add an individual IPv4 or IPv6 address:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object].

      Select the **State**, enter the IPv4 or IPv6 address in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - Do not specify the CIDR prefix (32) when entering an IPv4 address.
> - You can enter an IPv6 address such as 5507:c0d0:2002:0071:0000:0000:0000:0003. The same address can be represented as 5507:c0d0:2002:0071::0003.
> - You can enter up to 140000 IPv4 or 140000 IPv6 addresses in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 addresses in any rule object.

Figure 618. Add individual IP addresses



   c. Upon adding all the required IP addresses, click **Next**.

      Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

      The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add an IP address to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove an IP address from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of IP addresses from a CSV file using the **Import** option:

a. Click Other Actions → **Import**.

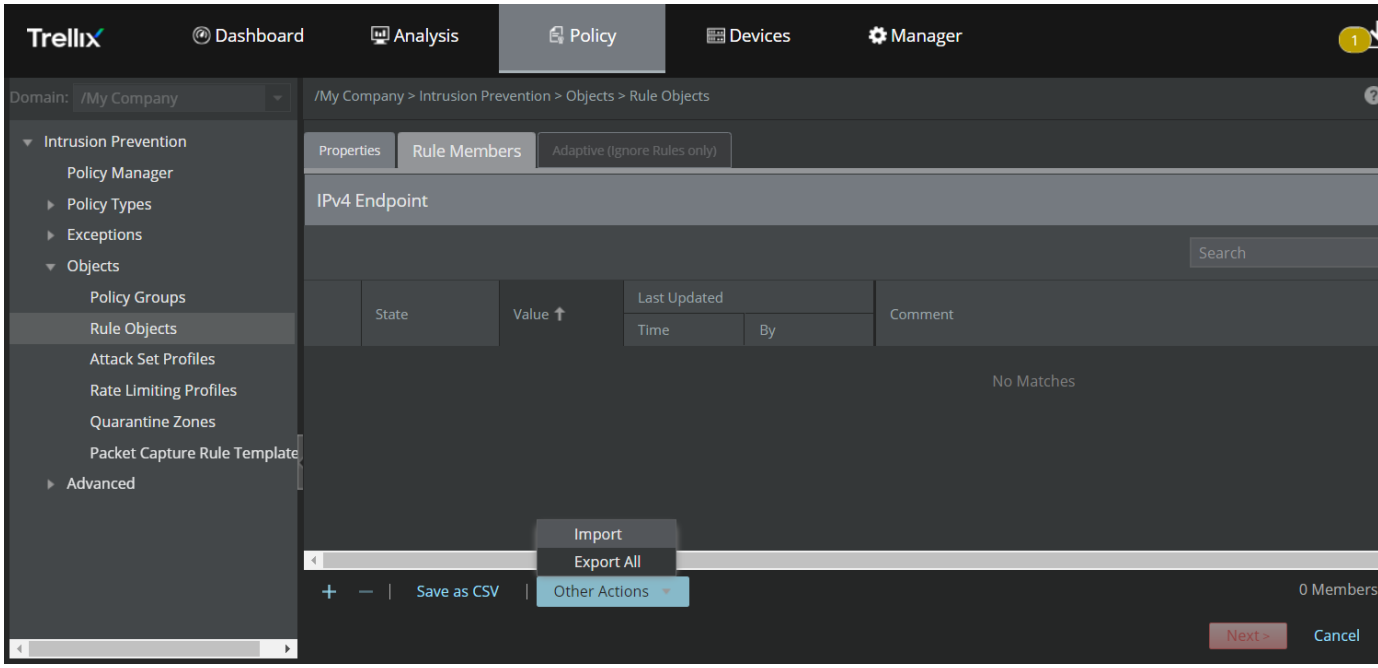
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10 entries.

Figure 619. Import IP addresses from a CSV file

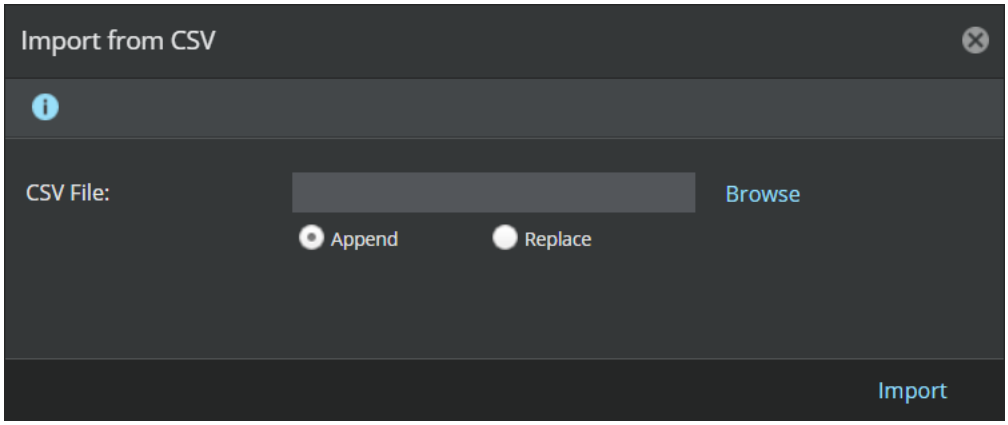


b. **Import from CSV** window appears. Use the **Append** option to add a new list of IP addresses or to append a list of IP addresses to an existing list. Use the **Replace** option to remove the existing list of IP addresses and add a new list from the file being imported.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IP addresses that you plan to import.

Figure 620. Import IP addresses from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 address>,<Comment>

Example file format: 10.10.1.1,textual description

The following is a sample for a CSV file with multiple IPv4 addresses:

Figure 621. CSV file format for IPv4 or IPv6 Endpoints

```
1  1    ..10,textual description
2  1    ..11,
3  1    ..12,
4  1    ..13,
5  1    ..14,
```

The following table describes the details of the IP addresses to be imported in the CSV file format.

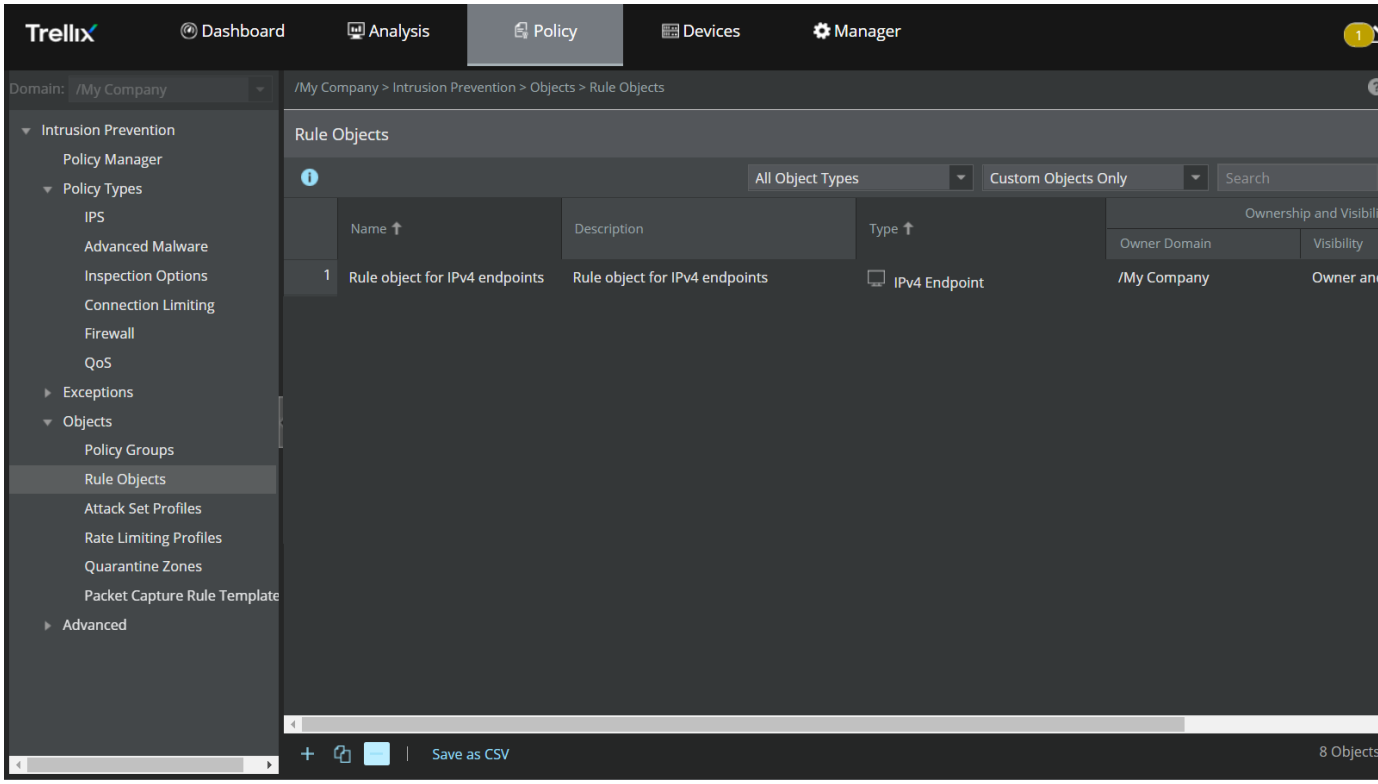
Format	Description
<IPv4 or IPv6 address>	Specifies the IP address to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (,) next to the entry and leave it.

d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

> **NOTE**
>
> The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

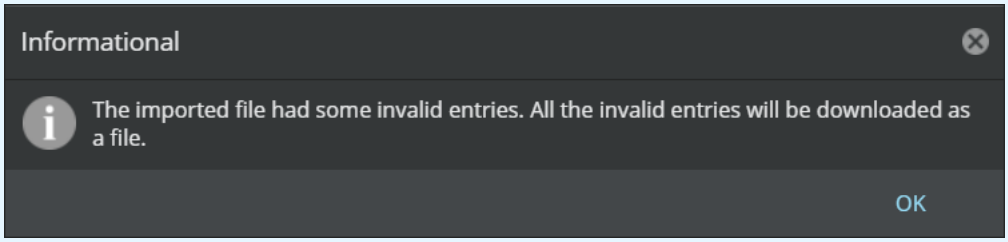
Figure 622. Rule object for IPv4/IPv6 endpoint successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 623. Information dialog-box for invalid entries



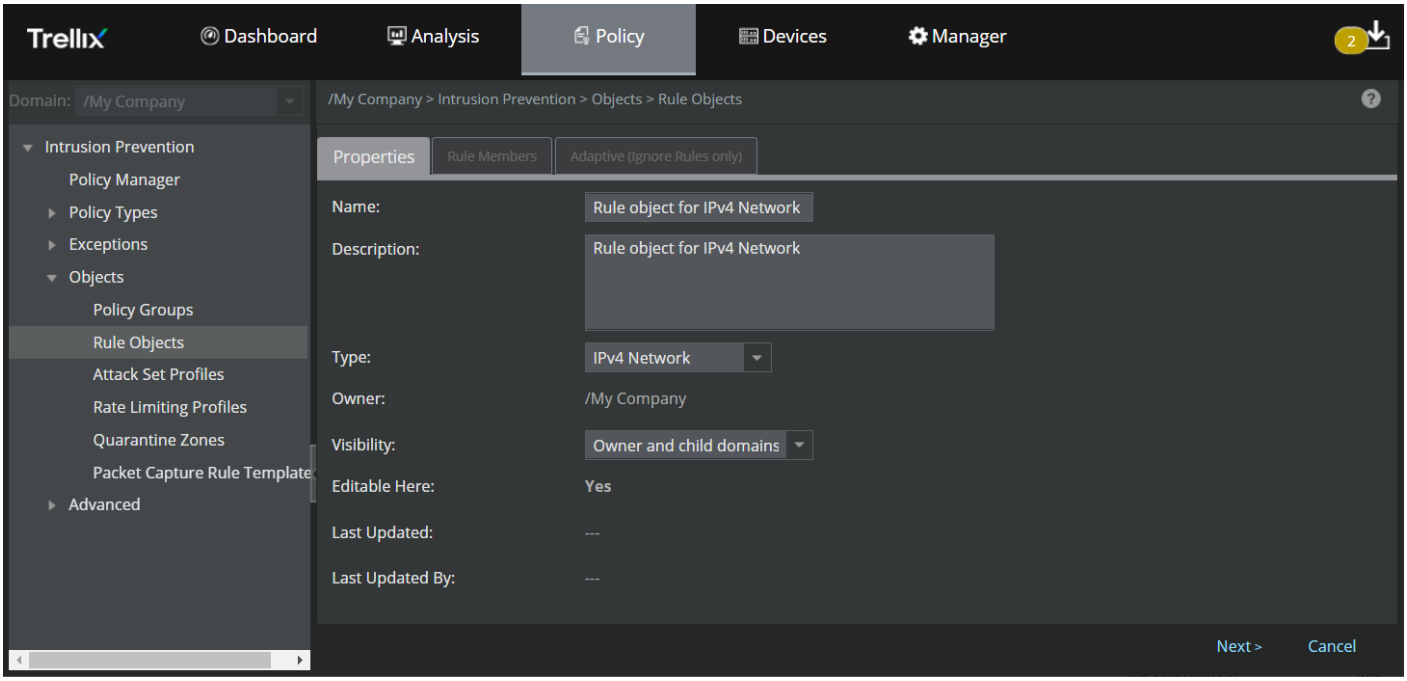
Add IPv4 Network and IPv6 Network rule objects

IPv6 Network is not supported for Quarantine. Also, only one IPv4 Network item per Rule Object is allowed for quarantine zone.

The steps to add **IPv4 Network** and **IPv6 Network** rule objects are identical. Follow these steps to add **IPv4 Network** or **IPv6 Network** rule objects:

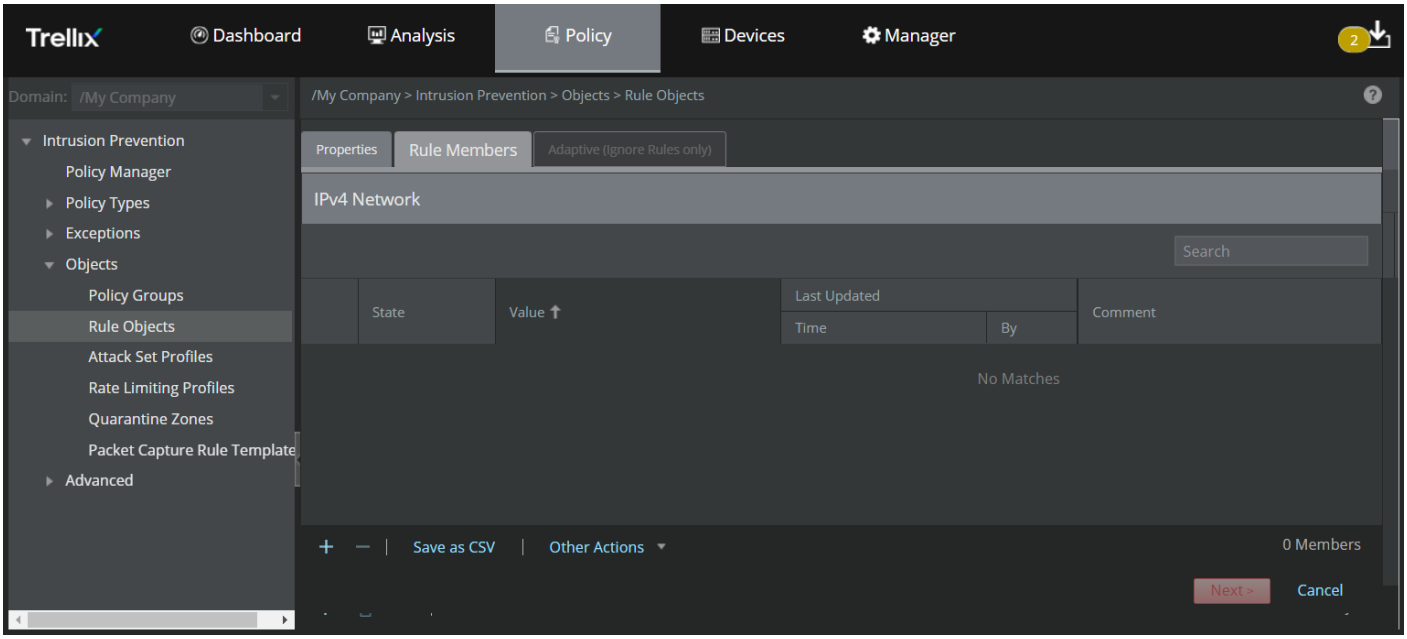
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Network** or **IPv6 Network** from the rule object **Type** drop-down, click **Next**.

Figure 624. Create an IPv4 Network or IPv6 Network rule object



The **Rule Members** tab is displayed.

Figure 625. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 76. Column details in the Rule Members tab - IP Network rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 CIDR block based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 CIDR blocks
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add a valid IPv4 or IPv6 CIDR block. For example, enter 172.16.200.0/24 for IPv4 Network, or 3003:0AB8::/48 for IPv6.
−	Click this icon to delete single or multiple IPv4 or IPv6 CIDR blocks
Save as CSV	Click this icon to remove a rule object from the list

Option	Definition
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 CIDRs • **Export All** — Allows you to export all the CIDRs from the Manager to the local system

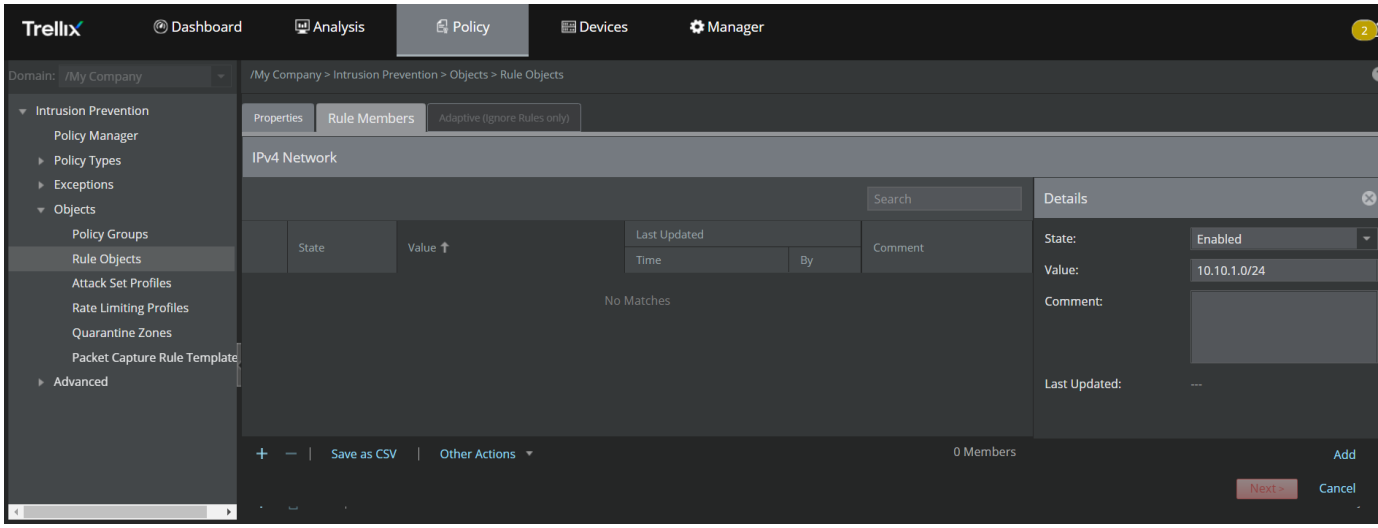
2. There are two ways to add the IP CIDR blocks — add individual IP CIDR block using the + icon or import a list of IP CIDR blocks from a CSV file using the Other Actions → **Import** option.
3. To add an individual IPv4 or IPv6 CIDR block:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Network rule object].

      Select the **State**, enter the IPv4 or IPv6 CIDR block in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - You can enter up to 140000 IPv4 or 140000 IPv6 CIDRs in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 CIDRs in any rule object.

Figure 626. Add individual IP CIDR block



   c. Upon adding all the required IP CIDR blocks, click **Next**.

      Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

      The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add a CIDR block to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove a CIDR block from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of CIDR blocks from a CSV file using the **Import** option:

   a. Click Other Actions → **Import**.

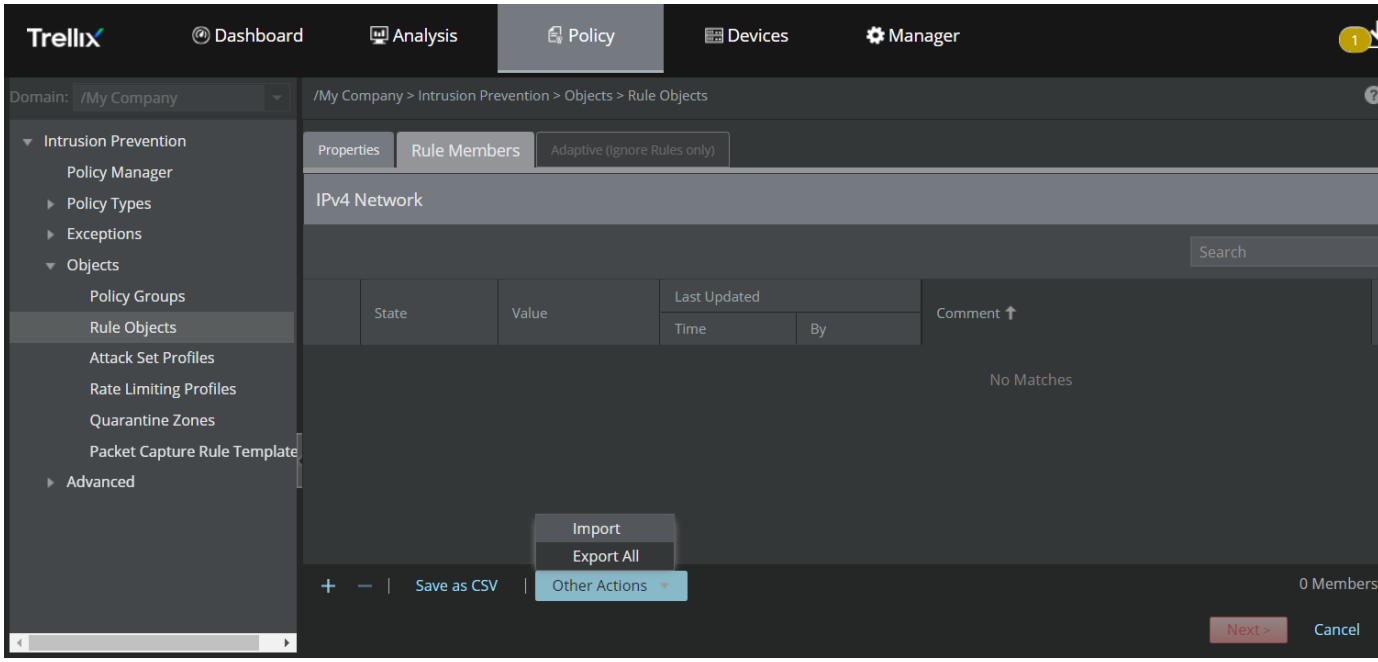
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10.

Figure 627. Import IP CIDRs from a CSV file

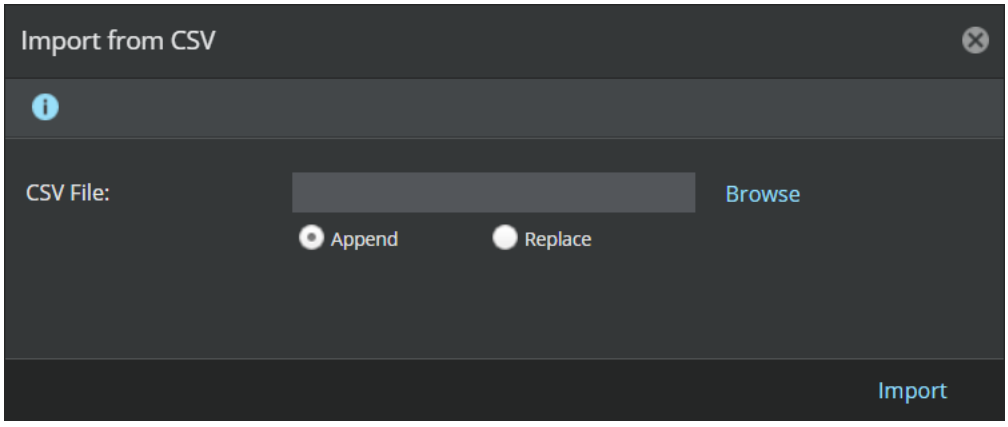


b. **Import from CSV** window appears. Use the **Append** option to add a new list of CIDR blocks or to append a list of CIDR block to an existing list. Use the **Replace** option to replace an existing list of CIDRs with a new list.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IPv4 or IPv6 CIDRs that you plan to import.

Figure 628. Import IP CIDRs from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 CIDR>,<Comment>

Example file format: 10.10.1.0/24,textual description.

The following is a sample for a CSV file with multiple IPv4 CIDRs:

Figure 629. CSV file format for IPv4 or IPv6 Networks

```
134.        .100/7,textual description
134.        .100/8,textual description
134.        .100/9,textual description
134.        .100/10,textual description
134.        .100/11,
134.        .100/12,
```

The following table describes the details of the IP CIDR blocks to be imported in the CSV file format.

Format	Description
<IPv4 or IPv6 CIDR>	Specifies the IPv4 or IPv6 CIDR to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (**,**) next to the entry and leave it.

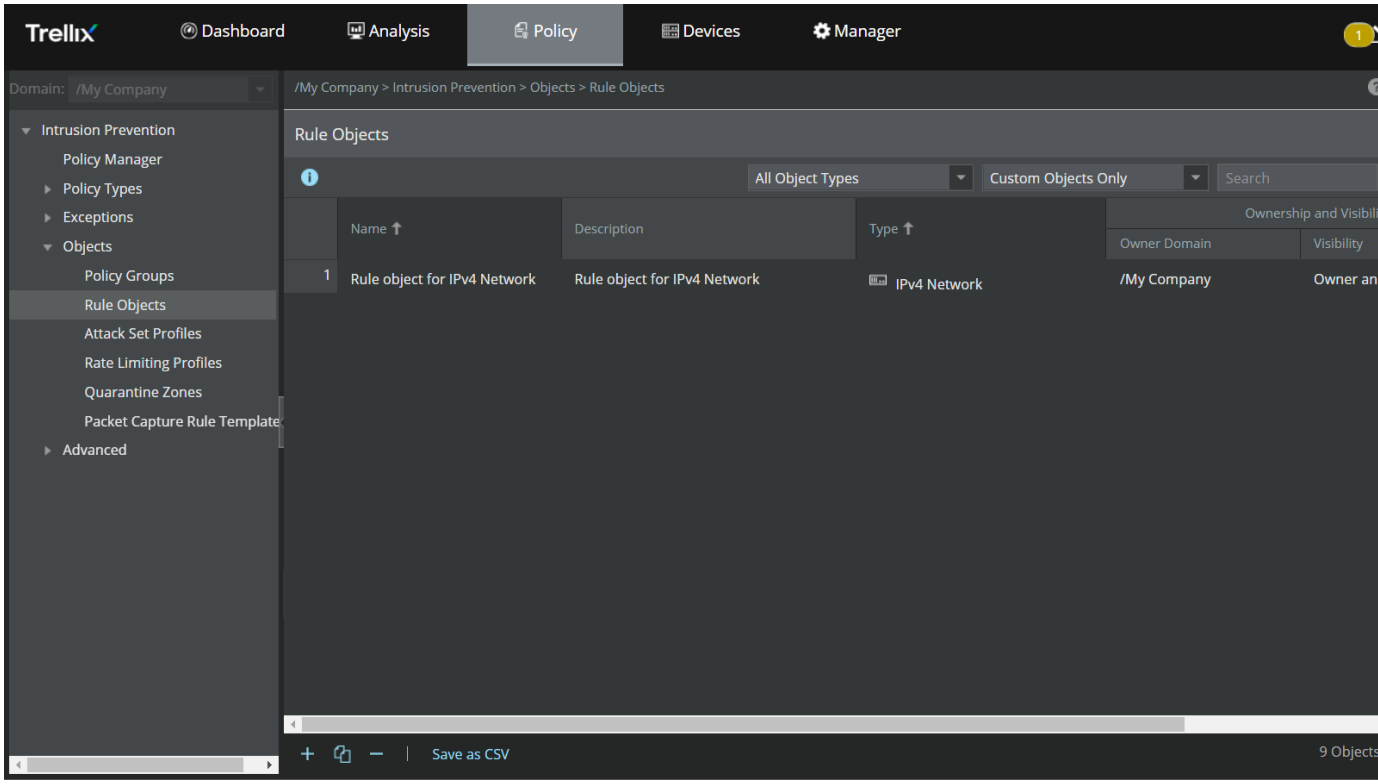
d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

NOTE

The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

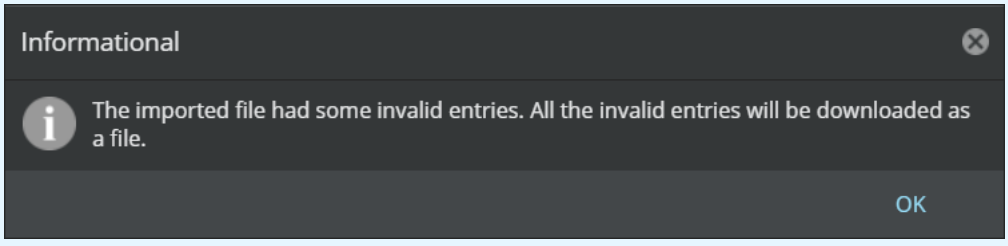
Figure 630. Rule object for IPv4/IPv6 network successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 631. Information dialog-box for invalid entries

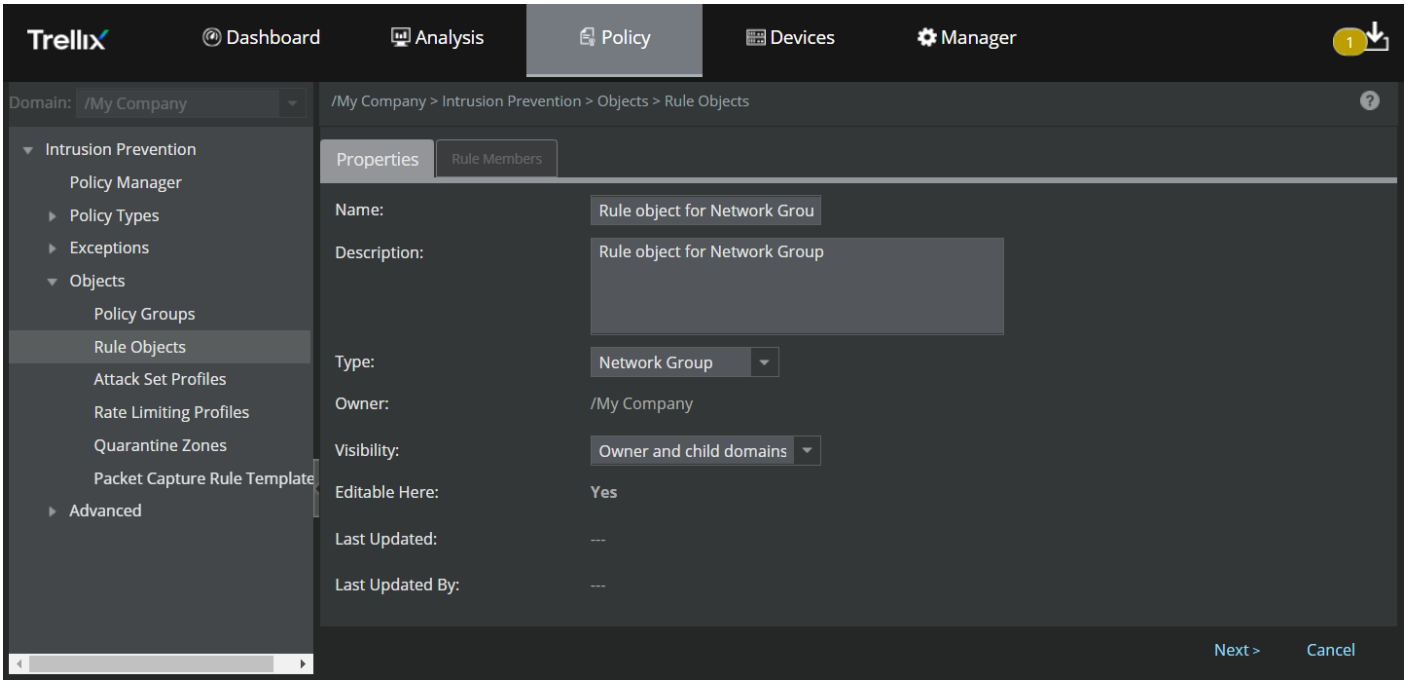


Add a Network Group rule object

Follow these steps to add a **Network Group** rule object:

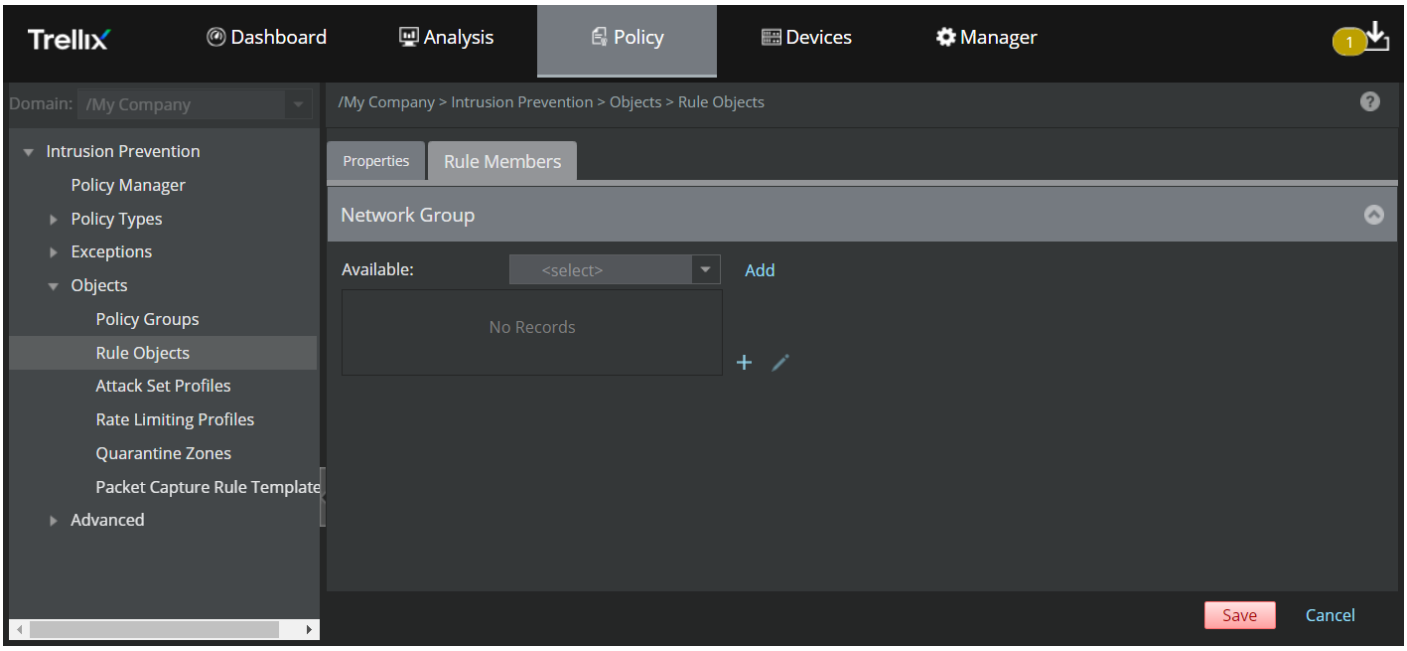
1. Upon specifying the options in the **Properties** tab and selecting **Network Group** from the rule object **Type** drop-down, click **Next**.

Figure 632. Create a Network Group rule object



The **Rule Members** tab is displayed.

Figure 633. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
Application Group	Select a pre-defined **Country** or an existing rule object from the **Available** drop down list
Add	Click this button to move the selected item to the **Rule Member** list
	Click this icon to edit a rule member in the list
	Click this icon to add a new rule object. You can add rule objects of the following type: **Host DNS Name**, **IPv4 Address Range**, **IPv4 Endpoint**, **IPv4 Network**, **IPv6 Address Range**, **IPv6 Endpoint**, **IPv6 Network**.
	Click this icon to remove a rule member from the list

2. Based on the above options, you can choose to add a rule member from the **Available** list or create a new rule object using the  icon and add it to the list.
3. Upon adding the required rule members, not exceeding **10**, click **Save**.

Modify a rule object

You can modify a rule object only at the admin domain where it was created. If required, you can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.

You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

1. Go to Policy → <Admin Domain Name> → Intrusion Prevention → Objects → **Rule Objects.**

   Rule objects for the selected admin domain are listed.
2. Locate the rule object that you want to modify.

   To filter the list, select **Custom Objects Only** and select the corresponding rule object type from the object type drop-down.
3. Make sure the **Editable here** field displays **Yes** for the rule object you want to modify. Then double-click the rule object.

   If the **Editable here** field displays **No**, the rule object belongs to a parent admin domain.
4. Make the required changes and click **Save**.

   If the rule object that you modified is part of an ignore rule that is in use, you must do a configuration update to the Sensor for the changes to take effect.

Clone a rule object

You can clone custom rule objects.

- You cannot clone a default rule object except for Network.
- You can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Go to Policy → <Admin Domain Name> → Intrusion Prevention → Objects → **Rule Objects**. Rule objects for the selected admin domain are listed.
2. Locate the rule object that you want to modify. To filter the list, select **Custom Objects Only** and select the corresponding rule object type from the object type drop-down.
3. Locate the Rule Object that you want to clone.

   TIP

   You can use the search function to more easily find the rule object.

4. Select the rule object and click .
5. Make the required changes and click **Save**.

Delete a rule object

Make sure the rule object is not used in any ignore rule rules or other features.

You can delete a rule object only at the admin domain where it was created.

NOTE

You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

1. In the **Rule Objects** page, locate the rule object that you want to delete.

   To filter the list, select **Custom Objects Only** and select the corresponding rule object type from the object type drop-down.
2. Make sure the **Editable here** field displays **Yes** for the rule object you want to delete. Then select the rule object and click .

   If the **Editable here** field displays **No**, the rule object belongs to a parent admin domain and you will only be able to delete it within that domain.
3. Click **OK** to confirm deletion.

   The rule object is permanently removed from that domain and does not show up in the list.

Assignment of alert

Users with read-write (RW) permission can manipulate the assignment of an alert, including assigning it to oneself, removing current assignment (making it unassigned again) irrespective of who the current assignee is, and assigning the alert to a specific user.

Assign alerts to users

You can assign a new alert to a specific administrative user account.

To assign new alerts to users:

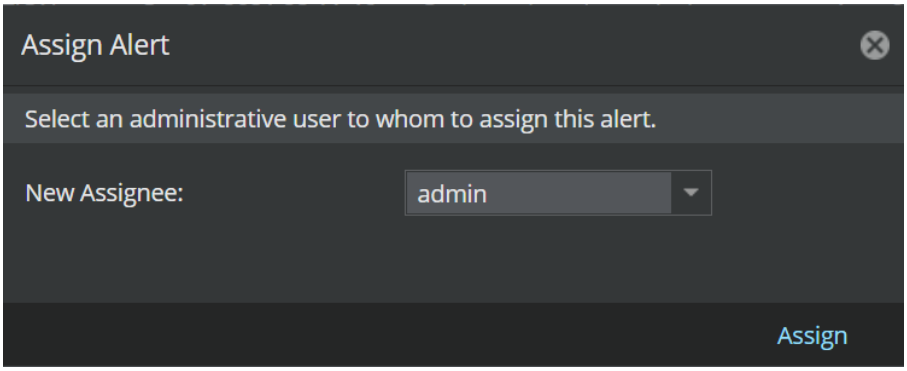
1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert you want to assign.

   By default, a new alert is unassigned.
3. Click **Other Actions**, select **Assign Alert** and either click **Assign to me** or **Assign to Someone Else**.

   If you selected **Assign to me**, the alert is assigned to you. The **Assigned** message flashes once the alert is assigned.

   If you selected **Assign to Someone Else**, the **Assign Alert** pop-up opens. Proceed to step 4.

   Figure 634. Assign alert to someone else

4. Select the user from the **New Assignee** drop-down list.
5. Click **Assign**.

   The **Assigned** message flashes once the alert is assigned to the user.

Remove assignments from alerts

Prerequisites:

- You have the appropriate read/write permissions.
- The alert is in your name.

Steps:

You can remove the alerts that are assigned to you by performing the following steps:

1. In the Attack log, select the alert you want to unassign.
2. Click **Other Actions**, select **Assign Alert** and click **Remove Current Assignment**.

   The **Assignment Removed** message flashes once the assignment is removed.

Ignore rule creation interface

The **Add Ignore Rule** option, available in the Attack Log, gives you the flexibility to eliminate alerts that do not actually pose a threat to your network or those that constitute noise. You can achieve this by creating and assigning ignore rules to different attack types in a single interface. Specifically, these are the three objectives that you can accomplish from a single user-interface:

- Creating and assigning ignore rule objects.
- Disabling an attack definition from the Default Attack Settings (GARE), Baseline Policy, or Light Weight Policy.
- Creating and assigning firewall policies.

Consider the three scenarios below that would necessitate the creation and assignment of ignore rules directly from Attack Log:

- You receive an alert about communication between specific hosts. When you further analyze the alert, you notice that the attack is valid, but not between the specific hosts. In this case, you can create and assign an ignore rule object from Attack Log which ignores the attack taking place between the two hosts for the moment.
- Many employees in your network are using Yahoo! instant messaging and Facebook chat. You are receiving numerous alerts due to this activity in the network. However, your company's corporate policy does not prevent employees from using such applications. Therefore, you can decide to prevent such alerts from appearing by explicitly disabling the attack definition from Attack Log.
- A host that is determined safe, such as a vulnerability scanner, in your network is generating noise which you want to ignore. To do this you can create a stateless ACL directly from the Attack Log to ignore all traffic from that host.

IMPORTANT

This interface will not be available to alerts generated by NTBA.

Create and assign ignore rule objects

1. Select Analysis → <Admin Domain Name> → **Attack Log**.

   The Attack Log page opens.

2. Select an alert to which you want to assign an ignore rule object and click Other Actions → Create Exceptions → **Add Ignore Rule**.

   The **Add Ignore Rule** window opens.

   TIP

   The **Attack**, **Attacker**, **Target** and **Owner Domain** are pre-populated with information about the alert.

3. Enter a **Name** for the ignore rule and comment if required.
4. Select a **Secondary Action** for the alert.

   You can choose to acknowledge all alerts that match the rule or delete them.

5. You can add multiple attacks in the **Attack** section and select the **Direction** for the attacks.

If you want to assign the ignore rule to traffic leaving the network, select **Outbound**. If you want to assign the ignore rule to traffic entering the network, select **Inbound**. However, should you choose to assign the ignore rule to traffic in both directions, select **Any**.

> **TIP**
>
> You can enter the attack name to search the attack or select it from the **Attack** drop-down list and click **Add**.

6. Select the interface to which the rule has to be applied from the **Resource** drop-down list and click **Add**.

   The scope of the ignore rule can be restricted to an interface or a device, or applicable to the admin domain as a whole.

7. Select or enter the **Attacker** IP address from **Endpoint**. You can add multiple **Attacker** IP addresses.

   You can also create a new rule object for the attacker by clicking the *add* icon. Click the *edit* icon to edit the selected IP address.

8. Select the **Port** for the attacker IP address.

   If you selected the port as **TCP**, **UDP**, or **TCP or UDP**, enter the port number.

9. Select the **Target** IP address from **Endpoint** and the **Port** for the IP address.

10. Click **Save** to save the ignore rule.

    You can view the added ignore rule under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Ignore Rules**.

Create and assign firewall policies

A firewall policy or access control list (ACL) is used to control host access by specifying attacker and target. You can create and assign advanced firewall policies using the **Ignore Rules** page.

1. Select Analysis → <Admin Domain Name> → **Attack Log**.

   The Attack Log page opens.

2. Select an alert to which you want to assign an ignore rule object and click Other Actions → Create Exceptions → **Add Ignore Rule**.

   The **Add Ignore Rule** window opens.

> **TIP**
>
> The **Attack**, **Attacker**, **Target** and **Owner Domain** are pre-populated with information about the alert.

3. Enter a **Name** for the ignore rule and comment if required.

4. Select a **Secondary Action** for the alert.

   You can choose to acknowledge all alerts that match the rule or delete them.

5. For an ACL remove the attack. You can remove the attack by clicking the **X** icon.

6. Select the interface to which the rule has to be applied from the **Resource** drop-down list and click **Add**.

   The scope of the ignore rule can be restricted to an interface or a device, or applicable to the admin domain as a whole.

7. Select or enter the **Attacker** IP address from **Endpoint**. You can add multiple **Attacker** IP addresses.

   You can also create a new rule object for the attacker by clicking the *add* icon. Click the *edit* icon to edit the selected IP address.

8. Select the **Port** for the attacker IP address.

   If you selected the port as **TCP**, **UDP**, or **TCP or UDP**, enter the port number.

9. Select the **Target** IP address from **Endpoint** and the **Port** for the IP address.

10. Click **Save** to save the ignore rule.

    You can view the added ignore rule under Policy → <Admin Domain Name> → Intrusion Prevention → Exceptions → **Ignore Rules**.

Disable an attack definition

To disable an attack definition:

1. For instructions up to this step, refer to the section [Create and assign ignore rule objects].
2. Select the source and destination IPs and ports in the corresponding fields.

   To disable an attack definition, select **Any IPv4 address** or **Any IPv6 address** and **Any Port**.

   > **TIP**
   >
   > Since the **Attack Name**, **Direction**, **Source**, **Source Port**, **Destination**, and **Destination Port** are pre-populated with information about the alert, the only remaining steps to disable an attack definition are to choose to ignore a specific attack launched by all hosts, specify the source and destination ports, specify the scope of application of the exception, and click **Save**. Clicking **Save** will disable the attack definition.

3. Select the **Scope** of the exception.

   Notice that the options for the scope of the exception will differ when you make choices as mentioned above. If you choose to disable the exception for a light-weight policy, select **Interface** and specify the exact interface. If you choose to disable the policy for a baseline policy, select **Baseline Policy** and specify the policy. If you choose to disable the exception for the entire domain, select **Global**.

   > **NOTE**
   >
   > The default value will be set to Global, which will mean that the specific attack definition is disabled for the entire admin domain.

4. Select the checkbox to acknowledge or delete the alerts that match the above mentioned settings, if necessary.

   It is not mandatory to select either of the options.

5. Click **Save**.

   You will be prompted to run a configuration update for the changes to take effect.

6. Click **Yes**.

   The **Deploy Pending Changes** window appears. Devices that lie within the purview of the scope of the exception are automatically selected. You can deselect this if you want to update the Sensor configuration later. Trellix recommends completing the Sensor configuration update.

7. Click **Deploy**.

   The device configuration is updated and the attack definition is disabled as configured.

Stateless Scanning Exceptions

The Scanning exceptions feature bypasses the scanning of traffic from a configured VLAN, TCP, or UDP port. The scanning exceptions configurations that are defined can be enabled or disabled at the Sensor level.

NOTE

Scanning exception feature rules are applied to both the Sensors in a fail-over pair. On creating a fail-over pair, the template Sensor rules are copied to the peer Sensor.

Scanning Exceptions feature is supported only in the following Sensor models:

- NS9500
- NS9300
- NS9200
- NS9100
- NS7350
- NS7250
- NS7150
- NS7300
- NS7200
- NS7100
- NS5200
- NS5100
- NS3200
- NS3100

NOTE

NS3500 Sensors do not support Scanning Exception feature.

NOTE

Scanning exceptions rules can be configured on ports running in inline mode. Once set, these rules take precedence over Firewall access rules. Fail-over ports cannot be configured for scanning exceptions.

Firewall access rules and scanning exceptions

Firewall access rules are comparable to scanning exceptions in terms of functionality. Scanning exceptions also enable traffic to bypass the Sensor's inspection. However, firewall access rules provide more features for a more granular control.

If both scanning exceptions and Firewall access rules are configured, the Sensor processes scanning exceptions first. That is, only traffic that is allowed based on scanning exceptions are subjected to the Firewall access rules (stateless or stateful).

Table 77. Comparison of firewall access rules with scanning exceptions

Scanning exceptions	Firewall access rules
The Sensor processes these before the access rules.	The Sensor checks only those packets that did not match the scanning exception rules. If a packet had matched a scanning exception rule, it would have bypassed the Sensor.
These rules allow the matched traffic to pass through the Sensor without inspection for attacks. There is no provision to drop the matched traffic.	The matched traffic can either be dropped or allowed to pass through.
You cannot define the source or destination of the traffic in the rule.	You can apply the rule based on the source and destination of the traffic. You can set any of the following as the criteria for source and destination in case of advanced Firewall policies: • Country to which the source or destination IP address belongs • Host DNS name • Specific IPv4 addresses • Range of IPv4 addresses • Specific network or any network in a group • Windows AD user names or user groups
The criteria to match traffic can be TCP port numbers, UDP port numbers, or VLAN IDs.	Any default or custom Service rule objects except for custom Service rule object where the Protocol Number is 89. You can configure 89, but this traffic cannot be dropped as the Sensor ignores it by default.
No option to specify direction or time.	You can apply the rule in the inbound, outbound, or both directions. In case of advanced Firewall policies, you can specify the time period when the Sensor must enforce a rule.
You define the scanning exceptions at the Sensor level. The TCP- and UDP-based scanning exceptions are applied at the Sensor level. VLAN-based exceptions are applied at the Sensor or port-pair level.	Though Sensor (pre-device) level is what is recommended, you can apply these at the following levels: • Sensor • Interface or subinterface • Port level
Immediately after you define them, the Manager sends the scanning exceptions to the corresponding Sensor. Does not require a configuration update.	Needs a configuration update to take effect.
Supported on NS-series Sensors	Supported on NS-series Sensors models except NS3500.

Scanning exceptions	Firewall access rules
Supported only in inline mode.	Supported in inline, SPAN, and tap mode. However, the response action in SPAN and tap mode do not affect the actual traffic.

For more information on stateless access rules, see the topic Using stateless access rules (page 1309).

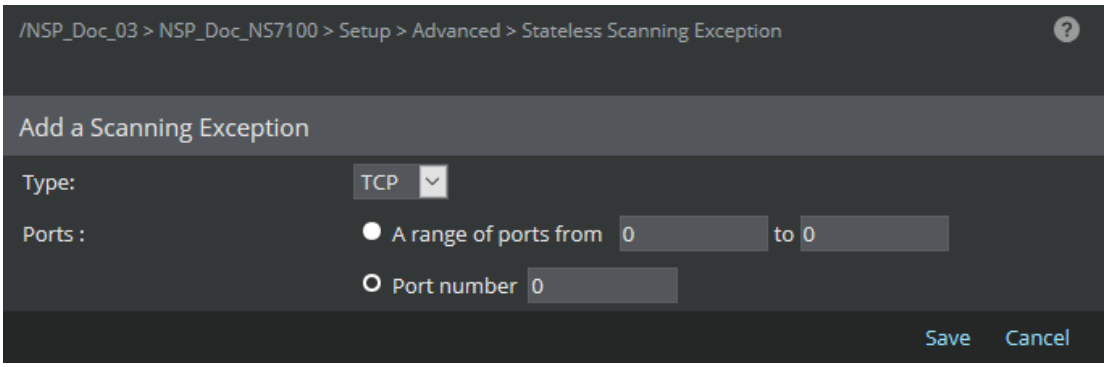
Add a Stateless Scanning Exception

Make sure the Sensor for which you want to create a Stateless Scanning Exception is active and reachable to the Manager over the network.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Stateless Scanning Exception**.
6. Click ➕.

   The **Add a Scanning Exception** page appears.

Figure 635. Add Scanning Exception page



7. In the **Type** field, select the type of port to be set for scanning exception.

   The options are **TCP**, **UDP**, and **VLAN**.
8. Specify the port number or a range of port numbers in the **Ports** field.
   - If you are configuring a range of port numbers for scanning exceptions, select **A Range of Ports from** and type the range of the port numbers in the respective fields.
   - If you select VLAN in the **Type** drop-down list, a new field **Interface** is displayed. You can select the required interface from the drop-down list.
9. Click **Save**.

   After the scanning exception is added, the **Scanning Exceptions** page displays the **Value** (Port number) and the **Resource** (Device name) under the **TCP Rules**, **UDP Rules**, and **VLAN Rules** tables.

Enable the Scanning Exceptions

To enable Scanning Exceptions:

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Stateless Scanning Exception**.

   The **Scanning Exceptions** page appears.
6. Select **Yes** in the **Enable Stateless Scanning Exceptions?** field.

   By default, the selected option is **No**.

   > **NOTE**
   >
   > You should add a scanning exception before enabling it.
7. Click **Save**.

Generate Scanning Exception reports

The Scanning Exceptions report provides a detailed view of the scanning exceptions that are configured on the device's VLAN, TCP, or UDP port. Scanning exceptions information includes the type of exception and the assigned interface.

Steps:

1. Click the **Manager** tab from the Manager Home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Scanning Exceptions**.
3. Select the **Devices**.
4. Select one or more exceptions — VLAN, TCP, and UDP.
5. Select the **Output Format**.
6. Click **Submit**.

Simulated Blocking

Simulated Blocking enables you to put the Sensor in a non-blocking mode whereby exploit attacks are not blocked even if the applied IPS policy is configured to do so. Alerts are still raised based on the configured policy. When Simulated Blocking is enabled, response actions that affect the flow of traffic, such as blocking, sending a TCP reset, and sending an ICMP host unreachable message, are not applied. This feature does not affect the Quarantine actions.

This feature allows an IPS *sanity check* where you get to know the specific attacks that would have hit a blocking rule, that is, which attacks would be blocked during normal operation without actually blocking them (the alerts explicitly mention that blocking has been simulated). You can also use this feature to temporarily disable blocking for troubleshooting.

NOTE

Simulated blocking applies to signature-based attack definitions only. Denial-of-Service and reconnaissance attacks will continue to activate response actions if configured to do so.

Simulated Blocking does not change the behavior of certain features of the Sensor. Further, these features will need to be disabled individually if required. The following list includes all such features:

- DoS blocking
- IP Reputation (formerly TrustedSource)
- Firewall drop action
- Host quarantine
- IP sanity errors checks

You may choose to enable Simulated Blocking and configure the response action in your policy as a TCP Reset or ICMP Unreachable. In such instances, the Sensor does not carry out a designated response action; the **Result** column in the Attack Log displays one of the standard attack results, such as **Attack Failed**, **Attack Successful**, **Attack Blocked**, **Inconclusive**, or **n/a**. These attack result statuses are identical to those that are displayed when Simulated Blocking is disabled.

NOTE

Disable Simulated Blocking before performing an upgrade using the CLI. This allows data in the Manager to synchronize with the Sensor immediately after the upgrade. If not disabled, the first sigfile push will disable this option (by default it is disabled at device level).

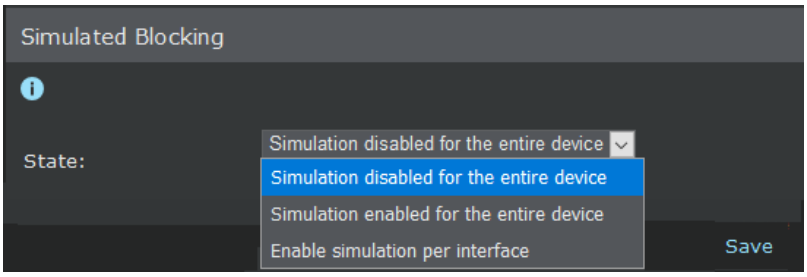
Configure Simulated Blocking at the interface level

You can configure Simulated Blocking at the interface level.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Simulated Blocking**.

   By default, **Simulated Blocking** is disabled for the entire device.

Figure 636. Simulated Blocking dialog



6. Select **Simulated Blocking** for inbound/outbound traffic.

> **NOTE**
>
> Simulated Blocking is not supported separately for the traffic directions. If one is configured (enabled/disabled), the other is also configured similarly.

7. From the **State** drop-down list, make a selection.
   - To enable Simulated Blocking device wide, select **Simulation enabled for the entire device**.
   - To disable Simulated Blocking device wide, select **Simulation disabled for the entire device**.
   - To control Simulated Blocking per VIDS, select **Enable simulation per interface**.
8. Click **Save**.

   The device level settings override the interface level settings, that is, you cannot configure Simulated Blocking at the interface level if it is configured at the device level.

Quarantining hosts

Trellix IPS enables you to quarantine your network hosts when required. For example, some hosts on your network might be compromised and used to attack other hosts in your network and outside. You might have identified hosts that are non-compliant with the security policies of your organization. In such cases, you can use the Quarantine feature of Trellix IPS to isolate the required hosts from the network and force them to remediate before you let them back on your network.

There are two ways to quarantine hosts:

- Configure the Sensor to quarantine hosts automatically when they generate specific attacks.
- Manually quarantine specific hosts that are listed in the Attack Log.

When a Sensor identifies the host that needs to be quarantined, a quarantine rule is created for the source IP address of the host. The host is now in quarantine, meaning it has a restricted access on your network. The compromised hosts are isolated from the network temporarily, thus preventing them from harming other network systems.

> **NOTE**
>
> Quarantine works only when the Sensor monitoring ports are in *inline mode*.

The Quarantine feature is very flexible and easy to implement. You can implement Quarantine with the default settings by just enabling it on the required Sensor monitoring ports or customize it to suit your requirements. Based on how you want to customize Quarantine, you require additional configurations. For example, to enable quarantined hosts to remediate, you must install a remediation portal and provide those details in the Manager. These requirements are discussed in the corresponding sections which contain the steps for customization.

The following are some of the options to customize Quarantine:

- You can restrict the network access of a quarantined host based on the following:
  - The destination IP address that a host wants to access
  - The IP network that a hosts wants to access
  - The network service such as DHCP, FTP, HTTP, SSL and so on.
- If a quarantined host attempts to access a network resource, you can redirect the HTTP traffic from the host to a web page displaying why the host is being quarantined and subsequently redirect it to the remediation portal. In the remediation portal, you can provide the links to the security software to make the host compliant with the security policies of your organization.
- While adding an endpoint to quarantine, you can also configure to redirect the quarantined endpoint to the configured remediation portal. These configurations can be made in the following pages on the **Analysis** tab:
  - **Threat Explorer**
  - **Callback Activity**
  - **High-Risk Endpoints**
  - **Quarantine**
  - **Attack Log**
- You can configure a list of hosts that you want to be excluded from being quarantined. For example, you might want to exclude servers, such as vulnerability scanners from being quarantined.

The state of the host, that is, whether the host is in Quarantine/ Remediation, can be viewed from the **Quarantine** page.

How Quarantine works?

There are two methods to quarantine hosts:

- Configure the Sensor to quarantine hosts automatically when they generate specific attacks.
- Manually quarantine specific hosts that are listed in the Attack Log.

Quarantine configurations — To manually quarantine hosts from Attack Log, you must configure **Quarantine** on the Sensor inline monitoring port that detected the corresponding attack from the host. You can have a different configuration for each port of a port-pair. As part of this configuration, you specify a *Quarantine Zone* for a monitoring port. The Sensor restricts the hosts to be quarantined to this zone. That is, the hosts are isolated in this zone thereby preventing further damage.

NOTE

If you have enabled XFF header parsing for your Sensor, any quarantining of an attacking host is carried out on the original source IP address and not the IP address obtained from the IP header.

For the Sensor to automatically quarantine hosts, two levels of configurations are required. One is the Sensor port configuration as explained above. The second level configuration is enabling Quarantining for the required attacks. Only a sub-set of the attacks are eligible for Quarantining. In the IPS and Reconnaissance policies applied on the Sensor port, locate the eligible attacks and enable Quarantining for the ones that you need.

To implement **Quarantine**, you configure it for the required inline monitoring ports.

IMPORTANT

The Sensor internally maintains data related to your network hosts in a table referred to as the host table. This table also contains data such as the hosts that are quarantined, the duration of the quarantine, and so on. If the Sensor reboots, the quarantine data in the Sensor's host table is cleared. So, hosts that were in quarantine before the reboot will now be out of quarantine.

- You will have to re-quarantine the hosts that you had manually quarantined before the reboot. You manually quarantine hosts from Attack Log.
- For hosts that were quarantined because of attacks, the Sensor will quarantine them again only when it detects those attacks from the hosts.

Quarantine Zones — Quarantine zones contain a ordered set of firewall-type Access Control List (ACL) rules. These rules define what a host can and cannot access when in quarantine. In effect, you use these rules to isolate hosts to only the allowed network resources. For example, you can restrict hosts only to the remediation portal for the duration of the quarantine. These ACL rules are referred to as *Access Rules*.

In each Access Rule, you specify the destination IP address or IP network, the service, and the response action the Sensor should take if the destination and service match. The response action can be to allow or drop the matched traffic.

When a Sensor identifies a host to be quarantined, it applies the quarantine zone specified for the corresponding monitoring port. When the host sends some traffic, the Sensor matches this traffic against the access rules in the quarantine zone in a top-down fashion. If the traffic matches with an Access Rule, it allows or drops the traffic as specified. Like in ACL, the Sensor does not match the remaining rules after the match. If none of the rules match, then the Sensor permits the traffic. You can also configure the Sensor or the Manager to forward the details of matched traffic to a syslog server.

There are some pre-defined quarantine zones available. You cannot directly modify them or delete them. If these quarantine zones do not meet your requirements, you can clone and then modify them. If required, you can also create an entirely new quarantine zone.

Redirection of hosts — When a quarantined user accesses a location, the Sensor can be configured to redirect HTTP traffic and display a message. Further, you can configure the Sensor to send the user to a remediation center. The message can display the reason for quarantine, the duration, the current user details and so on.

Duration of quarantine — You can specify the number of minutes a host needs to be quarantined. Alternatively, you can quarantine a host until you manually release it from the **Quarantine** page. In case of automatic quarantining by the Sensor, you specify the quarantine period when enabling **Quarantine** for a Sensor port. In case of manual quarantining from Attack Log, you specify the duration when you quarantine the host.

Quarantine Exceptions — There can be some hosts that you might want to exclude from automatic or manual quarantine. You can define an allow list of hosts that are to be exempted per monitoring port. These allow lists are referred to as **Quarantine** Exceptions.

High-level steps for configuring Quarantine

This section explains about the requirements and the high-level steps for configuring **Quarantine**.

Requirements for Quarantine

The following are the resources that you would need to implement **Quarantine**. However, recall that these requirements depend on how you want to customize **Quarantine**.

- Trellix IPS involving an NS-series Sensor with the required monitoring ports in inline mode.
- Optionally, you can configure the Sensor to redirect a quarantined host to a remediation portal from where the user can download and apply the required software to make the host compliant with your security policies. These are software such as the virus scanner, DAT files, Microsoft service packs, and so on. To remediate hosts, you need to define an internal web server that contains links to download these software.
- To quarantine a host, a Sensor uses ACL-type rules and restricts the access for the host. When the traffic from a quarantined host matches an ACL rule, you can log the details to a syslog server. By logging the matched traffic, you can know what a host attempted to access when being quarantined. To do this, you need a syslog server.

High-level steps

Note that not all of the following steps are mandatory. Configuration requirement is based on how you want to customize **Quarantine**. For example, the first step of creating Rule Objects is required only if you plan to create a customized quarantine zone or use Rule Objects to create **Quarantine Exceptions**.

1. If you plan to modify the default quarantine zone or create some on your own, you need to define the required Rule Objects in the admin domain. Rule Objects are building blocks with which you define quarantine zone Access Rules. You can also use Rule Objects to create **Quarantine Exceptions**. The procedures to create Rule Objects and their use are the same as in the other Trellix IPS features such as Firewall, QoS, and Exceptions.
2. If you want the details of the traffic that matched a quarantine zone access rule to be forwarded to a syslog server, do the following:
    a. Configure the details of the syslog server at the admin domain.
    b. Enable syslog forwarding on the Sensor.
3. You can configure the Sensor to display the quarantine details when a host attempts to access something outside the quarantine zone. You can choose the default browser message or customize it to suit your requirements.
4. If you have set up a remediation portal, you can configure those details at the domain level.
5. Configure **Quarantine** at the domain level. You can inherit the configuration from the parent domain or customize it. You can also customize specific configurations and retain the parent-domain configuration for the remaining.
6. Configure **Quarantine** for the required inline ports. You can inherit the configuration from the domain or customize it for the port. You can also customize specific configurations and retains the domain-level configuration for the remaining.
7. For automatic quarantining of attacking hosts, enable **Quarantine** for the required attacks in the IPS and Reconnaissance policies applied on the Sensor monitoring port. Also, factor in the direction of the attack and the port when you enable **Quarantine**. Consider that you want to enable **Quarantine** only on the inside port for a particular attack. Then, enable **Quarantine** for the attack in the outbound direction only.
8. View the details of the quarantined hosts in **Attack Log** and **Dashboard**.

Considerations for Quarantine rule creation

Quarantine rule creation exceptions

Review the considerations in this section before you create the rules for **Quarantine**.

Quarantine actions are ignored even if these are enabled at the policy and port level in the following scenarios:

- The host IP has been added or if it is part of the exclusion list that was configured from the Manager. The exclusion list can be configured as an IP CIDR or a specific IP address. If the source IP generating the attack is a part of the quarantine exception list, this indicates that the host is trusted and hence would not get quarantined.
- An ignore rule has been configured, which prevents the alert from being raised for a detected attack. If the ignore rule sorts the alert, the **Quarantine** action is not executed for this attack, and the source IP is not quarantined.

Quarantine access rules and Firewall access rules

Quarantine access rules are configured as part of Quarantine Zones. These rules regulate traffic from a quarantined host. Firewall access rules are configured to regulate traffic in inline mode from all hosts.

Review the following to understand the interaction between **Quarantine** and **Firewall** access rules:

- **Quarantine** drop gets precedence over a **Firewall** permit action.
- **Firewall** drop gets precedence over the **Quarantine** permit action.
- **Firewall** drop over-rides even if the host is in the quarantine exception list.

> **NOTE**
>
> **Quarantine** exception list only indicates that the hosts are excluded from being quarantined, but do not prevent them from being subjected to **Firewall** access rules.

Quarantine with ignore rules and exclusion

- When ignore rule is enabled, no **Quarantine** action occurs, that is, the host is not quarantined.
- If an IP address is a part of the quarantine exception list, the host is not quarantined, but traffic is still subjected to Firewall access rules.

Procedures for configuring Quarantine

The following sub-sections provide the step-by-step information on related to **Quarantine**. They essentially elaborate the high-level steps discussed in the previous section. Again, the required configurations depend on how you want to customize **Quarantine**.

Manage rule objects for Quarantine

You use rule objects to define quarantine zone access rules and quarantine exceptions.

Icon/Option	Definition
Rule object	Displays the rule objects according to the filter criteria. Click a column heading to sort the table in ascending or descending order. • **Name** — Indicates the name of the rule objects. • **Description** — Indicates the description of the rule object. • **Type** — Indicates the rule object type. • **Owner Domain** — Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain. • **Visibility** — Indicates the visibility settings of settings to the domains, whether it is visible only to th owner domain or to both owner and child domains. • **Editable here** — **Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.
Object Type	Filters rule objects in the list. • **Default Objects Only** — Trellix pre-defined these rule objects. For example, the Application and Country are default rule objects. You cannot define these rule objects. • **Custom Objects Only** — You need to define these rule objects. For example, you need to define the Host DNS Name rule object. • **Custom and Default Object** — When selected, it displays both the predefined and user defined rule objects. For example, IPv4 Network Rule Object has the 3 reserved private networks pre-defined, but you can create your Network rule objects as well.
Rule Object Type	Select the rule object type that you want to view.
Search	Type your search criteria in the field to find rule objects with matching elements. For example, type to list the rule objects containing *google* as part of their names.
 icon	Creates a custom rule object.
 icon	Clones a rule object. You cannot clone default rule objects other than the IPv4 network rule objects.
 icon	Deletes a custom rule object belonging to the current admin domain.
To view or edit a rule object	Double-click the rule object belonging to the current admin domain.

Rule objects are mappings to one or more components related to your network traffic. However, for **Quarantine** you can map a rule object only to one component. So, for example, you can specify an IPv4 address as a rule object. Then you can create

a quarantine zone access rule in which you specify this rule object as the destination. Every time you want to refer to this IP address in your quarantine zone access rules or quarantine exceptions, you can use this rule object.

IMPORTANT

In features such as Advanced Firewall policies, you can specify multiple rule objects per component of an access rule. For example, you can specify multiple rule objects as the destination of the traffic. In case of quarantine zone access rule, you can specify only one rule object per component. Also, the rule object that you use in the quarantine zone access rule can have only one item in it. For example, the IPv4 Endpoint rule object that you want to use in quarantine zone access rule can only contain one IPv4 address in it. However, the IPv4 Endpoint rule object for quarantine exception list can contain up to 10 IPv4 addresses.

Rule objects for Quarantine	Relevant for quarantine zone?	Relevant for quarantine exception?
IPv4 Endpoint: Use this rule object to refer to IPv4 addresses in quarantine zone access rules and quarantine exception list.	Yes	Yes
IPv6 Endpoint: Use this rule object to refer to IPv6 addresses in quarantine exception list.	No	Yes
IPv4 Network: Use this rule object to refer to the CIDRs to use in quarantine zone access rules and quarantine exception lists. In a quarantine zone access rule, you can specify a CIDR as the destination of traffic. For example, you might want to apply a rule on the traffic targeted for 172.16.225.0/24 network. Default IPv4 Network rule objects are available for the three reserved IPv4 ranges according to RFC 1918. You can specify up to 10 CIDRs in one rule object for quarantine exception lists.	Yes	Yes

Rule objects for Quarantine	Relevant for quarantine zone?	Relevant for quarantine exception?
Service: To restrict traffic based on the IP protocol, ICMP codes, or the TCP/UDP port numbers, use the Service rule object. You can create Service rule objects or use the default ones. The well-known services on standard TCP and UDP ports, as well as ICMP codes are pre-defined. For example, telnet is predefined as TCP on port 23. Similarly, ICMP codes such as ICMP echo reply and ICMP request are pre-defined. When you create a Service rule object, the options are to specify the protocol number, TCP port, or UDP port. For custom ICMP codes, you need to specify the IP protocol number and the ICMP code in the port field. You can define only one IP protocol specification per rule object. **Notes:** • A Sensor processes the access rules of a quarantine zone in a top-down fashion. So, if you want to drop traffic based on Services, then define those access rules high up in the policy. • For access rules that use Service rule objects, the Sensor factors in any non-standard ports that you have configured for IPS. For example, if you have specified port 2023 as the non-standard port for FTP, and if you have used the FTP Service rule object in a rule, then the Sensor considers FTP on both ports 21 and 2023. • It is not advisable to set permit rules for protocols such as FTP, TFTP, and RPC services that negotiate ports dynamically. For RPC services, you can configure explicit allow and deny rules for RPC as a whole, but not its constituents, such as statd and mountd. • Multimedia protocols such as H.323 and services such as instant messaging and peer-to-peer communication either negotiate the data channel separate from the control channel or negotiate ports that do not follow a standard. However, you can configure access rules to deny these dynamic protocol instances by denying the fixed control port. • An option for denying protocols that use dynamic negotiation is to configure quarantine zone to drop the attacks that are detected in such transmissions. Trellix IPS detects use of and attacks in such programs as Yahoo Messenger, KaZaA, IRC, and so forth.	Yes	No

Notes on IPv4 and IPv6 rule objects

For Firewall and QoS, IPv6 addresses are supported for the following rule objects:

- Host
- Address range
- Network

The default Service rule object for ICMPv6 is also now available.

- You use the above-listed, IPv6-based rule objects to create a Network Group rule object. However, you cannot use a combination of IPv4 and IPv6 based rule objects in one Network Group rule object.

- In a Firewall access rule or QoS rule, you cannot specify an IPv4-based rule object for one field and IPv6-based rule objects for other applicable fields. For example, if you select an IPv6-based rule object in the **Source Address** field, then you cannot specify IPv4-based rule objects for **Destination Address** or **Source User** fields. For this example, you can specify only an IPv6-based rule object or *other* as the value for **Destination Address** and *any* for **Source User**. Recall that User and User Group rule objects are considered as IPv4 based rule objects because Trellix Logon Collector does not collect user information from IPv6 hosts. Similarly, Country and Host DNS Name are also IPv4-based rule objects.

The following table classifies IPv4 and IPv6 rule objects:

Type	Rule objects
IPv4	IPv4 Endpoint, Host DNS Name, IPv4 Address Range, IPv4 Network, User, User Group, Country
IPv6	IPv6 Endpoint, IPv6 Address Range, IPv6 Network

You configure user-based Firewall access rules using the user and user group rule objects. It is important to note the following regarding these rule objects:

- You cannot create, modify, or delete the User or User Group rule objects. The Manager manages these rule objects according to the updates from Trellix Logon Collector.
- You can view these rule objects only n the **Access Rules** tab of the **Firewall** page. You cannot view these rule objects in the **Rule Objects** page.
- The user names verified through Kerberos snooping or the Sensor's Guest Portal are not displayed in the Manager.

View the rule objects

You can view existing rule objects in a selected domain.

For a rule object to be listed, it must meet one of these conditions:

- It is a default rule object.
- It is created at a parent admin domain, but it is set to be visible to the child admin domains.
- The rule object was created at the current admin domain.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

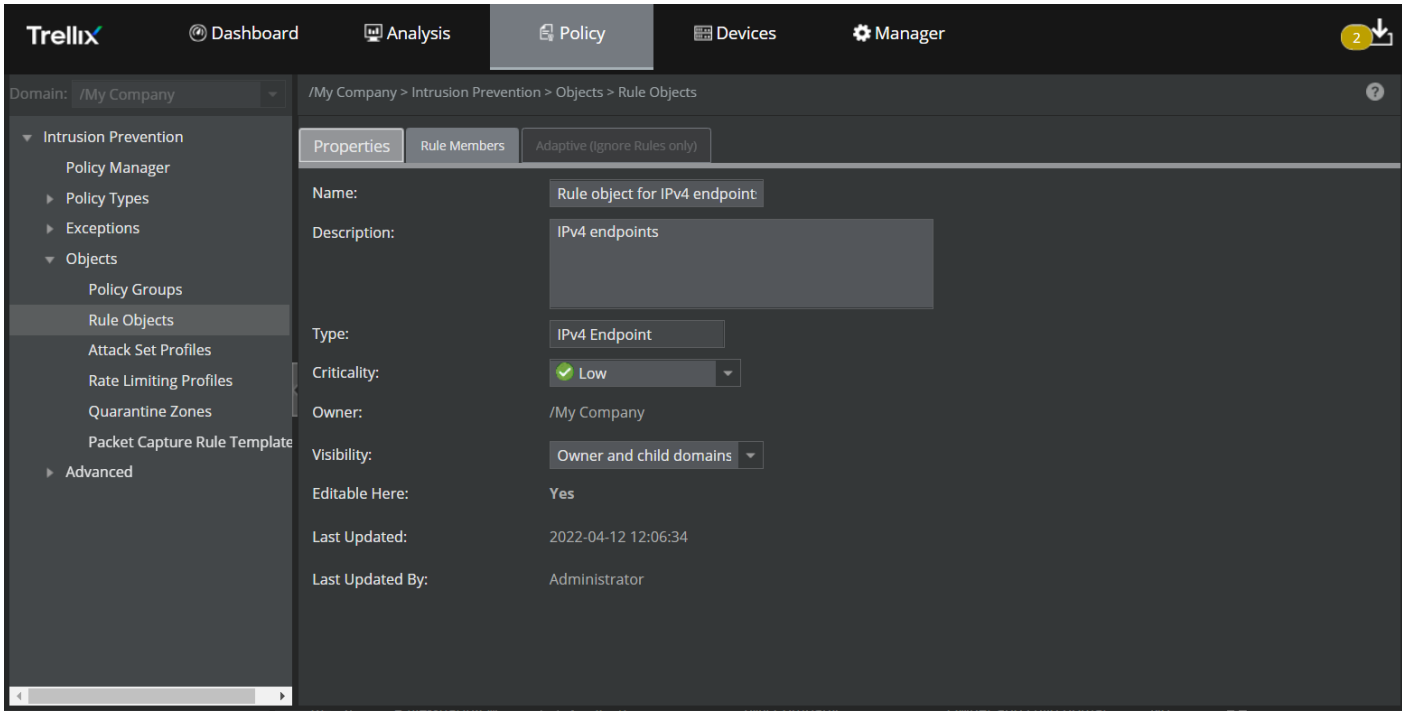
   Rule Objects for the selected admin domain are listed.

   - To locate specific rule objects, enter a string in the **Search** text box. For example, type “google” in the **Search** text box to list the rule objects containing “google” as part of their Names.
   - Select the **Custom Objects Only** or **Default Objects Only** or **Custom and Default Objects** from the drop-down list as required.
   - Select the rule object type in the drop-down list.
   - To view limited details of a rule object, point to the object. To view complete details, select and double-click the rule object.

- The rule object details appear under the **Properties** tab, and the rule members (rule object items) appear under the **Rule Members** tab.

> **NOTE**
>
> An additional tab named **Adaptive (Ignore Rules only)** appears while viewing IPv4 and IPv6 based rule objects.

Figure 637. Viewing Rule Objects



Add a rule object

You can create custom rule objects to use within the Firewall and QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones, and NTBA Communication Rules.

Following table lists the maximum count of rule object items (**Rule Members**) that can be added under each rule object type:

Rule Object type	Rule Members (Maximum count)
Host DNS Name	5000
IPv4 Address Range	20000
IPv4 Endpoint	140000
IPv4 Network	140000
IPv6 Address Range	20000
IPv6 Endpoint	140000

Rule Object type	Rule Members (Maximum count)
IPv6 Network	140000
Application Group, Application on Custom Port, Finite Time Period, Network Group, Network Group for Ignore Rules, Recurring Time Period, Recurring Time Period Group, Service, Service Group, Service Range	10

NOTE

The rule member count specified in the above table is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object.

NOTE

If you are using a Manager running on or before version 10.1.7.55 and a Sensor running on or before 10.1.5.153, the maximum count of rule members you can add under each rule object type is 10.

NOTE

The above rule object count specified for IPv4/IPv6 based rule objects is also applicable for Central Managers. Central Managers running on or before version 10.1.7.55, however, support only 10 rule members per each rule object.

NOTE

If you are using a Central Manager, do not add more than 10 entries in the Central Manager Rule Objects which are associated with QoS policies, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones or Quarantine Exceptions in a Manager.

Steps:

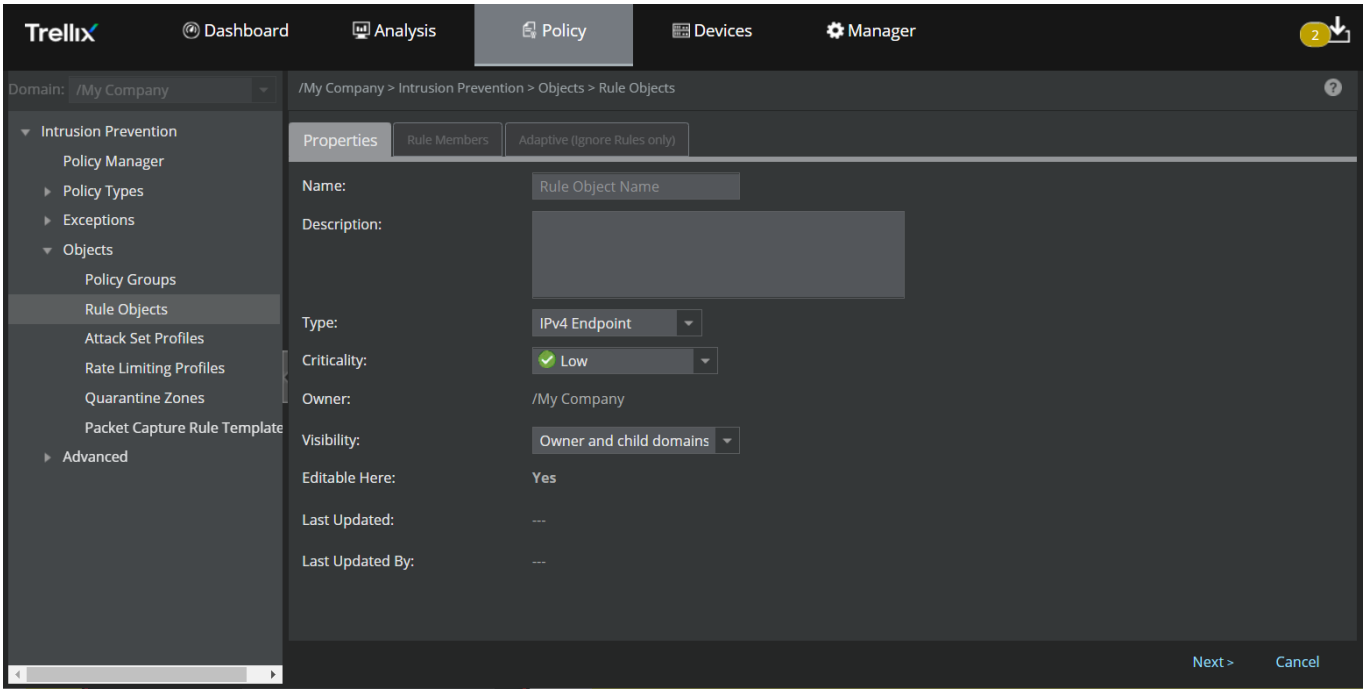
1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.
4. Click . This displays two tabs, namely the **Properties** tab and the **Rule Members** tab.

   NOTE

   An additional **Adaptive (Ignore Rules only)** tab appears while adding IPv4 and IPv6 based rule objects.

Figure 638. Selecting Criticality for each of your assets

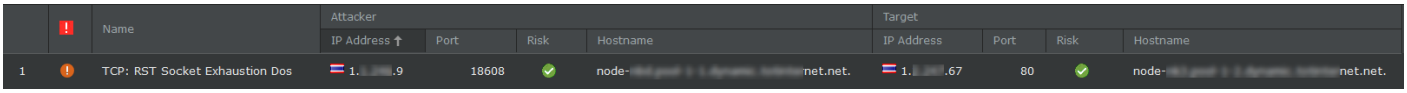


The following table describes the options in the **Properties** tab that are common to all rule objects.

Option	Definition
Name	Enter a unique name to easily identify the rule object.
Description	Enter the description for the rule object.
Type	From the drop-down list, select the type of rule object you want to create. For information on a specific object type, refer to the corresponding sub-section.
Criticality	[Optional] If you have chosen rule object type as IPv4 Endpoint or IPv6 Endpoint, you can specify the **Criticality** of that host by selecting **Low**, **Medium** or **High** from the drop-down list. By default, criticality is **Low**. Determining criticality of a host enables you to categorize all IPv4 Endpoint and IPv6 Endpoint addresses based on their importance to your organization.
Owner	Indicates the admin domain to which a rule object belongs. All the default rule objects belong to the root admin domain.
Visibility	From the drop-down list, select the option for the visibility level of the rule object. The available options are **Owner and child domains** and **Owner domain only**.
Editable Here	**Yes** indicates that the rule object is a custom rule object belonging to the current admin domain. If it is **No**, you cannot edit the rule object because it is a default rule object or a custom rule object defined at a parent admin domain.
Last Updated	Displays the date and time when a rule object was last updated
Last Updated By	Displays the user who modified a rule object

Once you assign criticality to a rule object and an alert involving it is raised, the criticality that you assigned shows up under specific columns in Attack Log. These columns are labeled **Attacker Risk** and **Target Risk**. **Attacker Hostname** and **Target Hostname** displays the names of the rule object.

Figure 639. Display of attacker risk



5. Enter the rule object options based on rule object you have selected in the **Type** drop-down list. For information on the subsequent steps to add a rule object, refer to the corresponding sub-sections.

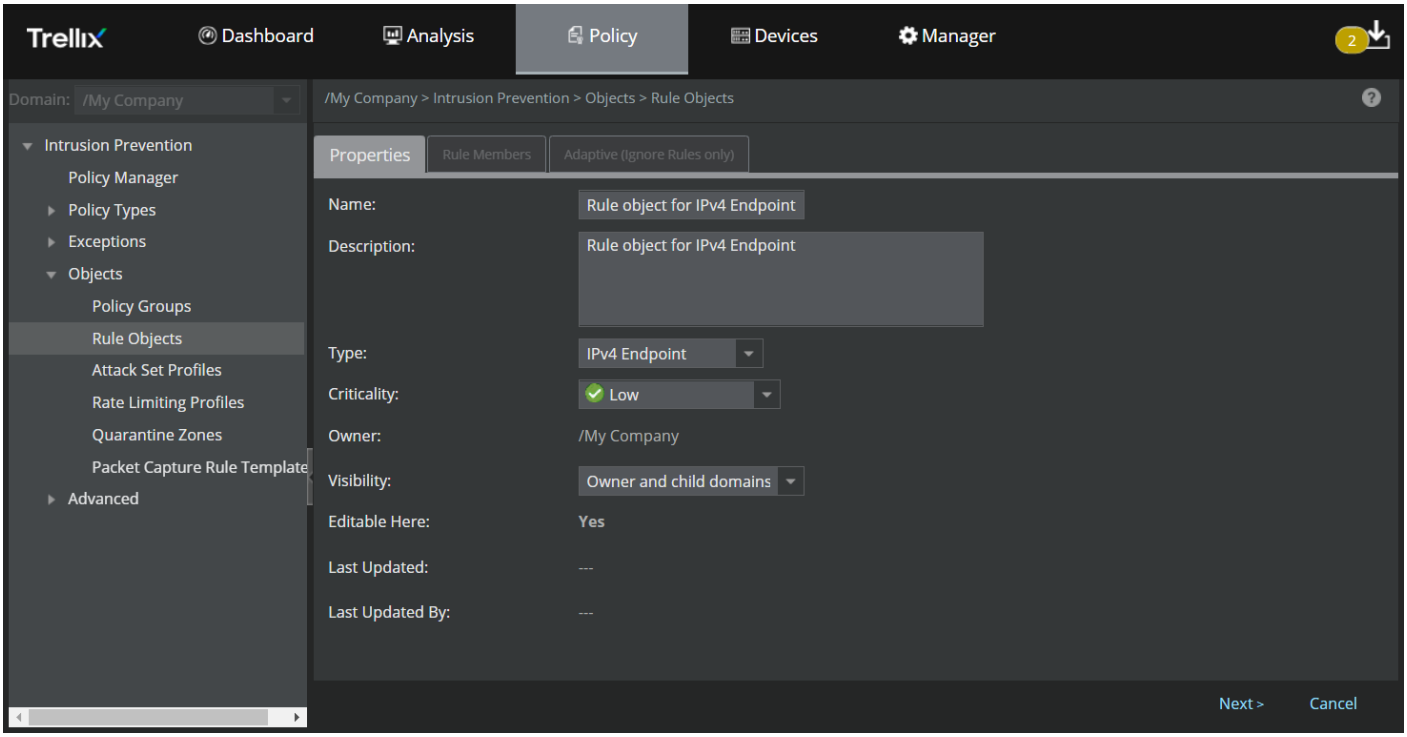
Add IPv4 Endpoint and IPv6 Endpoint rule objects

For quarantine zone access rules, only IPv4 Endpoint rule objects are supported. Also, only one rule member per rule object is applicable for quarantine zone.

The steps to add **IPv4 Endpoint** and **IPv6 Endpoint** rule objects are identical. Follow these steps to add **IPv4 Endpoint** or **IPv6 Endpoint** rule objects:

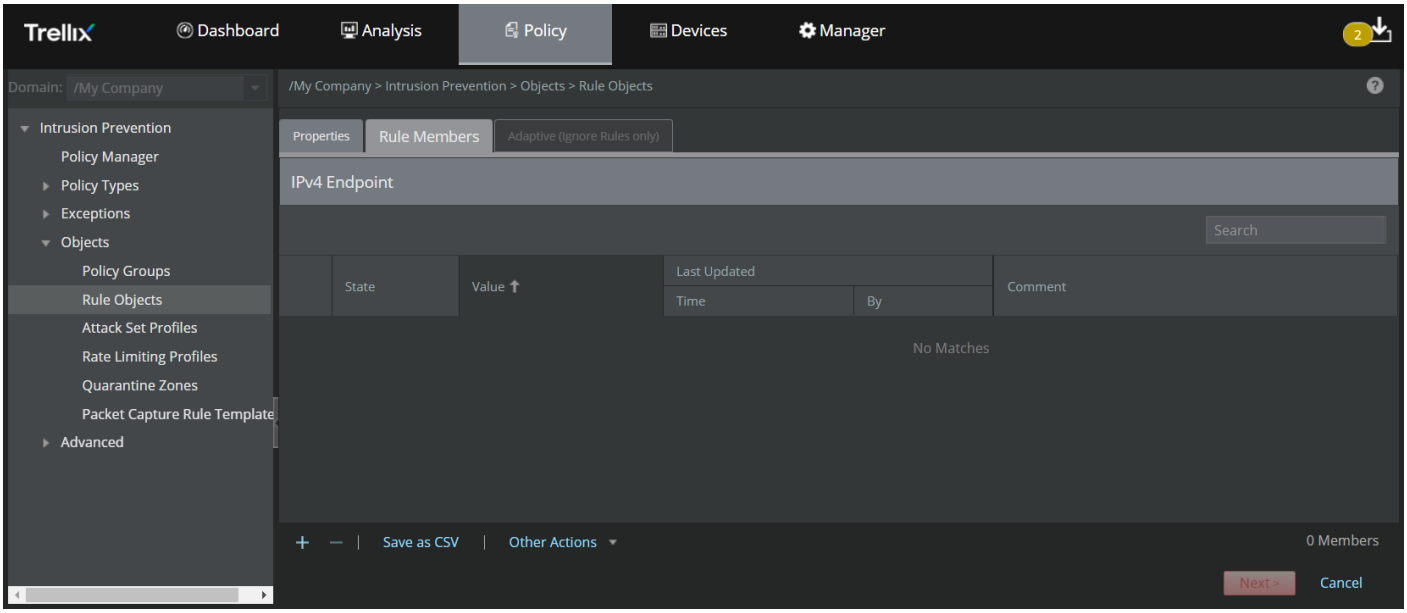
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Endpoint** or **IPv6 Endpoint** from the rule object **Type** drop-down, click **Next**.

Figure 640. Create an IPv4 Endpoint or IPv6 Endpoint rule object



The **Rule Members** tab is displayed.

Figure 641. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 78. Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 endpoint based on the rule object type selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 addresses
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add an IPv4 or IPv6 address.
−	Click this icon to delete single or multiple IPv4 or IPv6 addresses.
Save as CSV	Click this button to export all the rule members displayed in the grid to a CSV file.
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 addresses • **Export All** — Allows you to export all the IP addresses from the Manager to the local system

2. There are two ways to add the IP addresses — add individual IP addresses using the + icon or import a list of IP addresses from a CSV file using the Other Actions → **Import** option.

3. To add an individual IPv4 or IPv6 address:

   a. Click the + icon.

   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

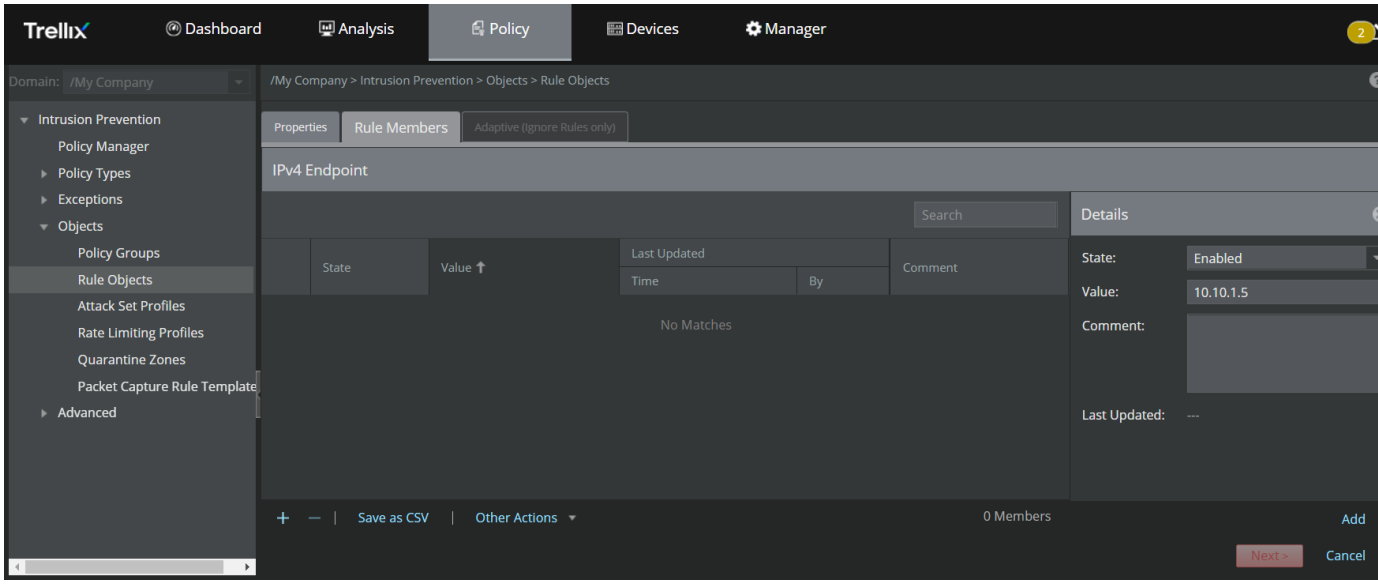
   For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IPv4/IPv6 Endpoint rule object].

   Select the **State**, enter the IPv4 or IPv6 address in the **Value** field, enter a **Comment** if required and click **Add**.

   NOTE

   - Do not specify the CIDR prefix (32) when entering an IPv4 address.
   - You can enter an IPv6 address such as 5507:c0d0:2002:0071:0000:0000:0000:0003. The same address can be represented as 5507:c0d0:2002:0071::0003.
   - You can enter up to 140000 IPv4 or 140000 IPv6 addresses in a single rule object.
   - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
   - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 addresses in any rule object.

   Figure 642. Add individual IP addresses



   c. Upon adding all the required IP addresses, click **Next**.

   Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

   The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add an IP address to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove an IP address from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of IP addresses from a CSV file using the **Import** option:

a. Click Other Actions → **Import**.

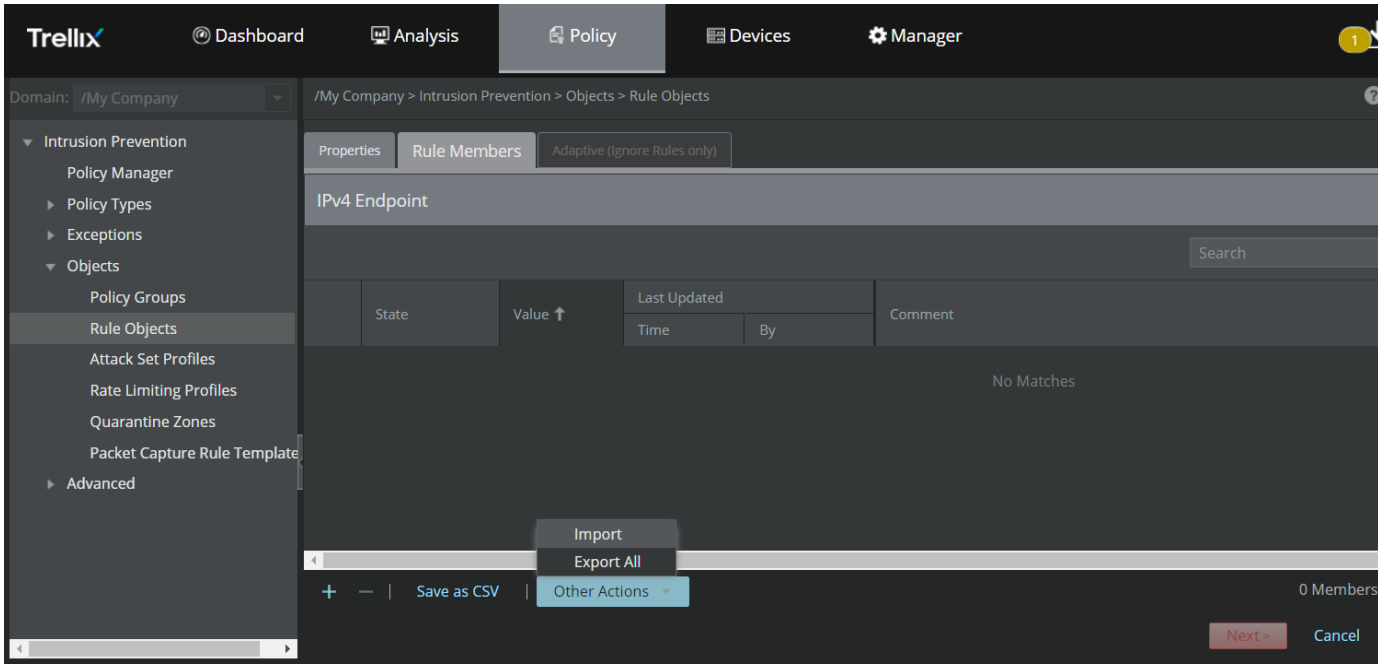
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10 entries.

Figure 643. Import IP addresses from a CSV file

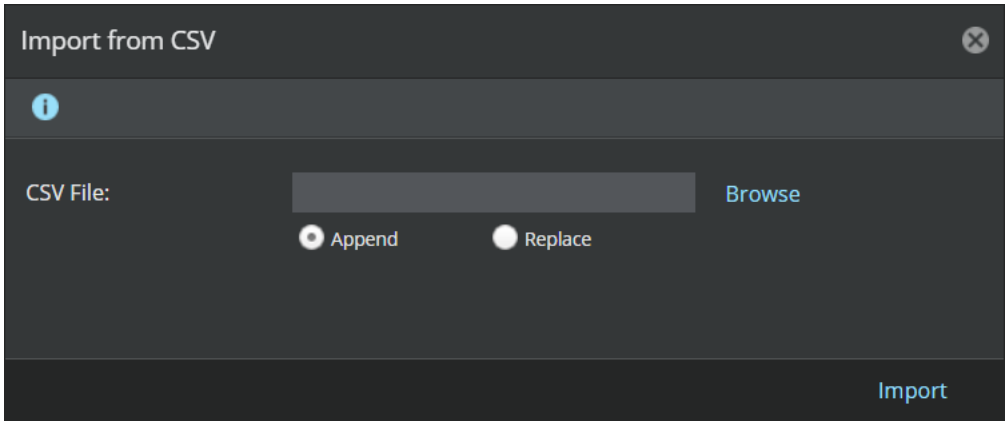


b. **Import from CSV** window appears. Use the **Append** option to add a new list of IP addresses or to append a list of IP addresses to an existing list. Use the **Replace** option to remove the existing list of IP addresses and add a new list from the file being imported.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IP addresses that you plan to import.

Figure 644. Import IP addresses from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 address>,<Comment>

Example file format: 10.10.1.1,textual description

The following is a sample for a CSV file with multiple IPv4 addresses:

Figure 645. CSV file format for IPv4 or IPv6 Endpoints

```
1  1    ..10,textual description
2  1    ..11,
3  1    ..12,
4  1    ..13,
5  1    ..14,
```

The following table describes the details of the IP addresses to be imported in the CSV file format.

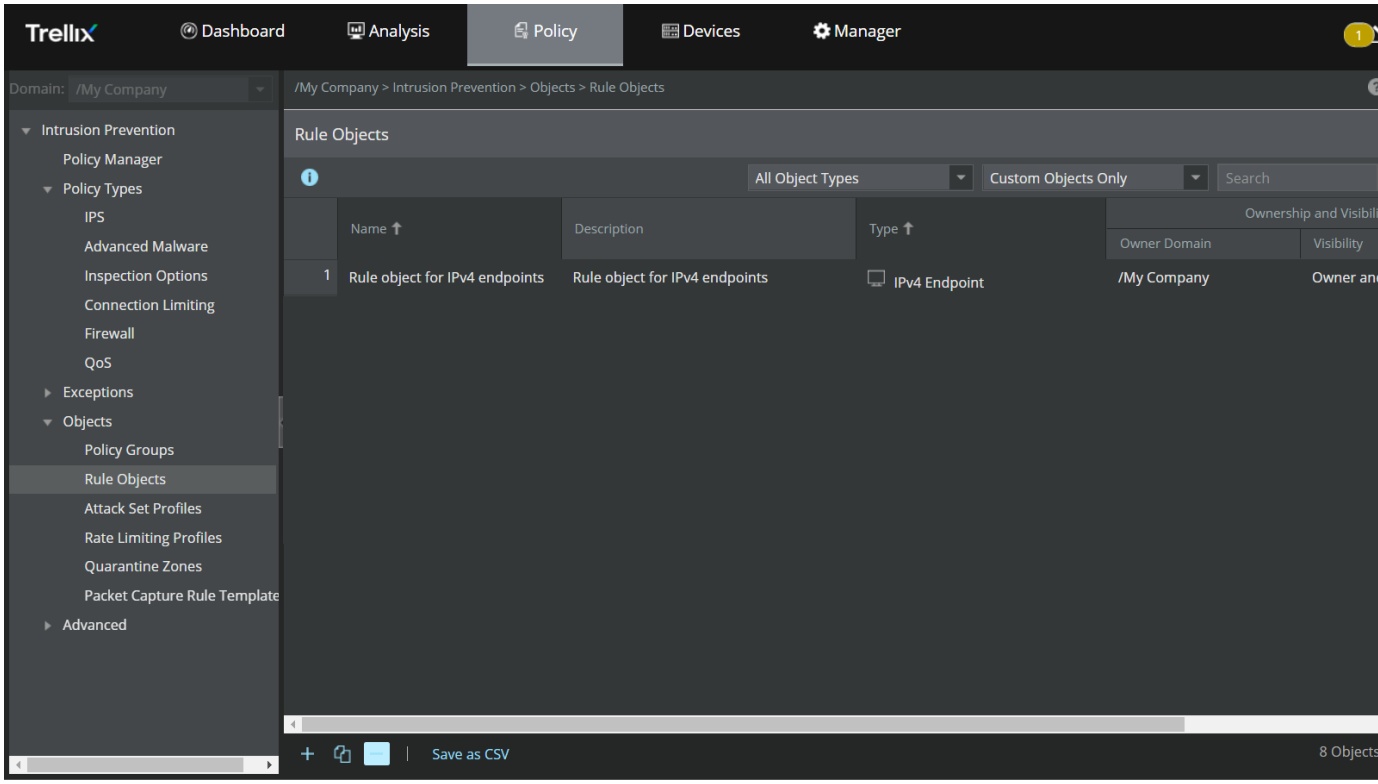
Format	Description
<IPv4 or IPv6 address>	Specifies the IP address to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (,) next to the entry and leave it.

d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

> **NOTE**
>
> The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

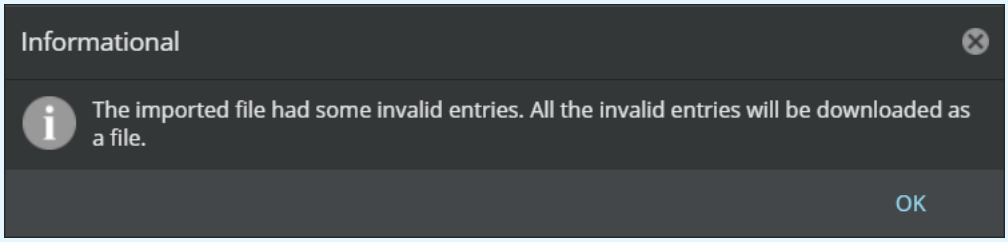
Figure 646. Rule object for IPv4/IPv6 endpoint successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 647. Information dialog-box for invalid entries



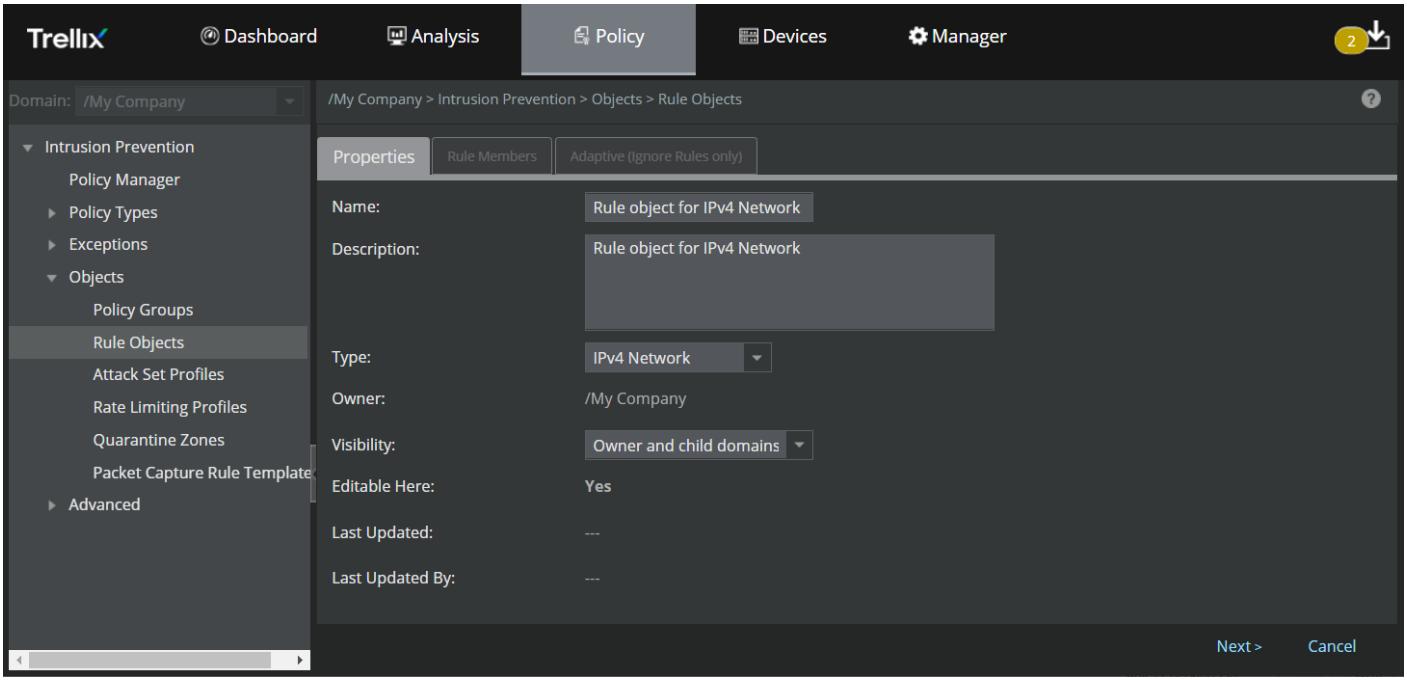
Add IPv4 Network and IPv6 Network rule objects

IPv6 Network is not supported for Quarantine. Also, only one IPv4 Network item per Rule Object is allowed for quarantine zone.

The steps to add **IPv4 Network** and **IPv6 Network** rule objects are identical. Follow these steps to add **IPv4 Network** or **IPv6 Network** rule objects:

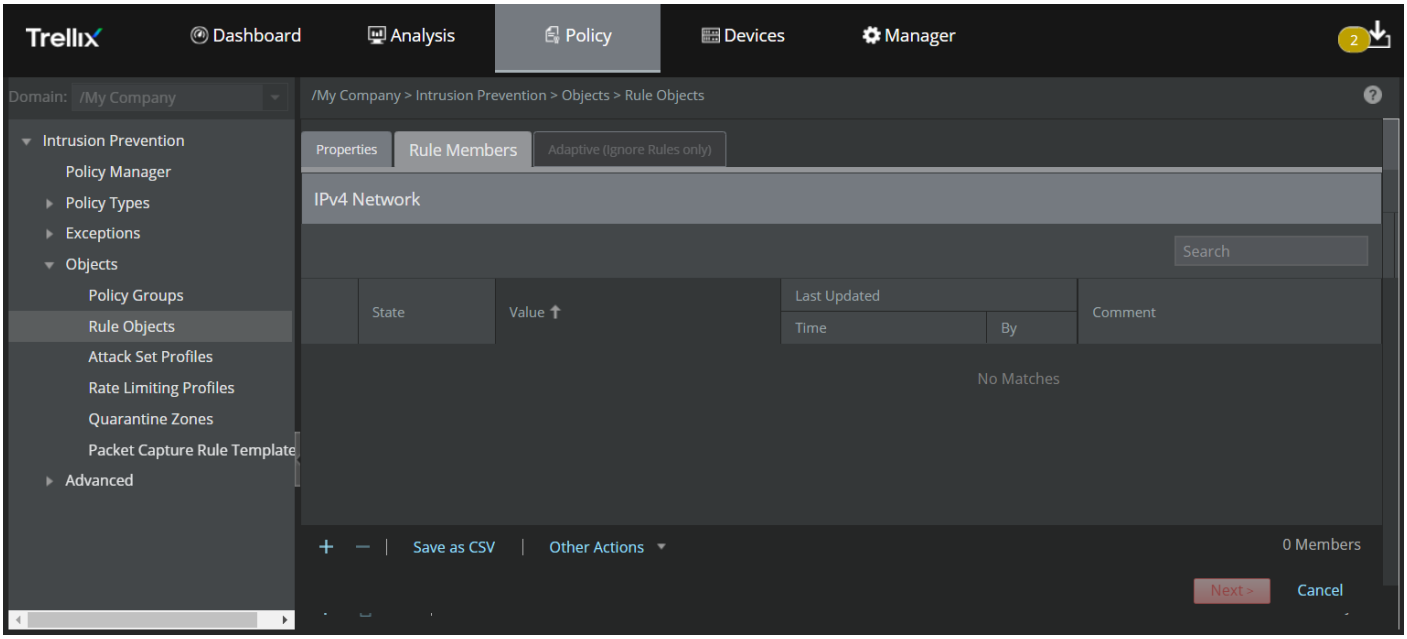
1. Upon specifying the options in the **Properties** tab and selecting **IPv4 Network** or **IPv6 Network** from the rule object **Type** drop-down, click **Next**.

Figure 648. Create an IPv4 Network or IPv6 Network rule object



The **Rule Members** tab is displayed.

Figure 649. Add Rule Members



Following are the details of the columns displayed in the **Rule Members** tab:

Table 79. Column details in the Rule Members tab - IP Network rule object

Column	Description
State	Specifies whether a rule member (in this case, IPv4 or IPv6 CIDR block based on the rule object selected) is **Enabled** or **Disabled**
Value	Displays the IPv4 or IPv6 CIDR blocks
Last Updated	• **Time** — Specifies the time when the rule member was last modified • **By** — Displays the user who modified the rule member
Comment	Displays any additional comment specified for the rule member

You can rearrange/resize the columns to view the details according to your preference.

The following table explains the options in the **Rule Members** tab.

Option	Definition
+	Click this icon to add a valid IPv4 or IPv6 CIDR block. For example, enter 172.16.200.0/24 for IPv4 Network, or 3003:0AB8::/48 for IPv6.
−	Click this icon to delete single or multiple IPv4 or IPv6 CIDR blocks
Save as CSV	Click this icon to remove a rule object from the list

Option	Definition
Other Actions	• **Import** — Allows you to import a file containing a list of IPv4 or IPv6 CIDRs • **Export All** — Allows you to export all the CIDRs from the Manager to the local system

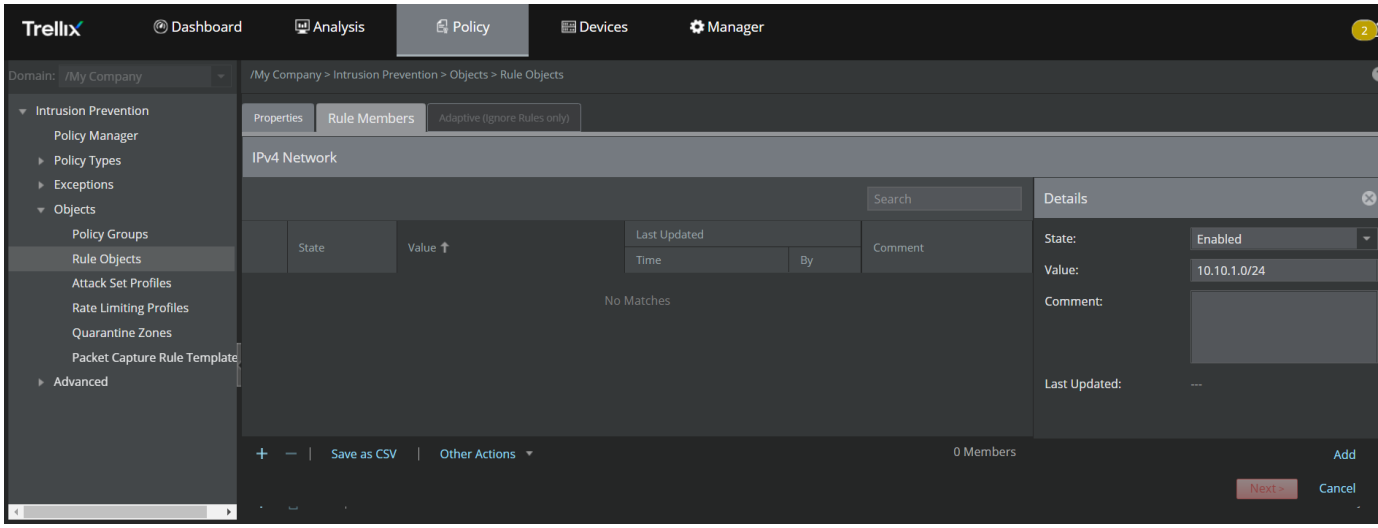
2. There are two ways to add the IP CIDR blocks — add individual IP CIDR block using the + icon or import a list of IP CIDR blocks from a CSV file using the Other Actions → **Import** option.
3. To add an individual IPv4 or IPv6 CIDR block:
   a. Click the + icon.
   b. A **Details** window is displayed on the right-hand side of the **Rule Members** tab.

      For details of the options displayed in the window, refer the table [Column details in the Rule Members tab - IP Network rule object].

      Select the **State**, enter the IPv4 or IPv6 CIDR block in the **Value** field, enter a **Comment** if required and click **Add**.

> **NOTE**
>
> - You can enter up to 140000 IPv4 or 140000 IPv6 CIDRs in a single rule object.
> - The above rule member count is applicable only for Firewall policy. For QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, Quarantine Zones and NTBA Communication Rules, the maximum rule member count applicable for each rule object type is 10. For Quarantine Zones, only one rule member should be assigned per rule object. So, you need to add rule members to a rule object accordingly.
> - If the Manager is on or before version 10.1.7.55 and the Sensor is on or before 10.1.5.153, you can add a maximum of 10 IPv4/IPv6 CIDRs in any rule object.

Figure 650. Add individual IP CIDR block



   c. Upon adding all the required IP CIDR blocks, click **Next**.

      Adaptive (Ignore Rules only) tab is displayed. This is an optional tab.

      The following table explains the options in the **Adaptive (Ignore Rules only)** tab.

Option	Definition
Customization	Select **Disabled** to disable customization or select **Use custom values per resource** to customize values
Resource to Customize	Select the resource to customize from the drop-down list **NOTE** This option is displayed only if you select the customization option as **Use custom values per resource**
Add	Click this button to add a CIDR block to the **Customizations** list
Search	Type the search criteria to search for a resource
	Click this icon to remove a CIDR block from the list

d. Based on the above options, make any configuration changes if required, and click **Save**. The rule object will be created.

4. To import a list of CIDR blocks from a CSV file using the **Import** option:

   a. Click Other Actions → **Import**.

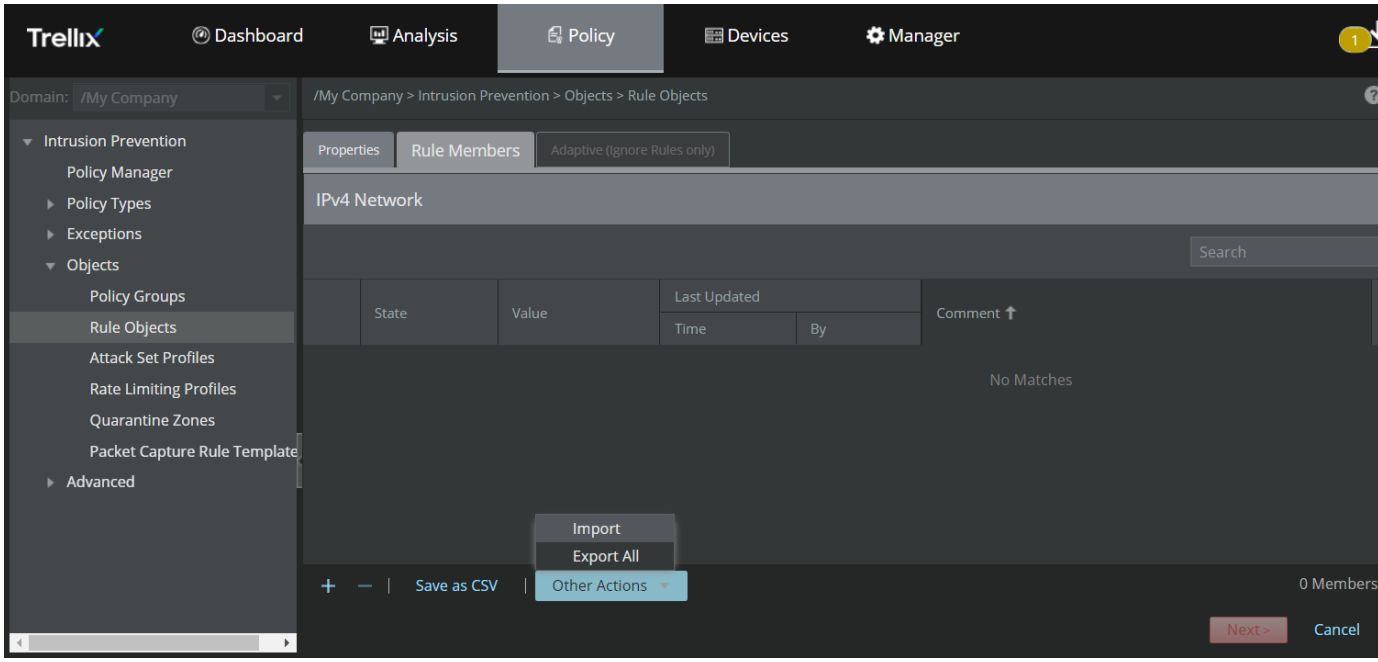
NOTE

You cannot import the file while adding individual entries. In case you plan to import a file along with the individual entries, add the entries first, save the rule object and re-open the rule object to import the file. Make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 140000.

NOTE

If you are assigning the rule object to QoS policy, Ignore Rules, Outbound SSL Decryption Exclusions, and NTBA Communication Rules, make sure that total rule member count (sum of CSV file entries and individual entries) does not exceed 10.

Figure 651. Import IP CIDRs from a CSV file

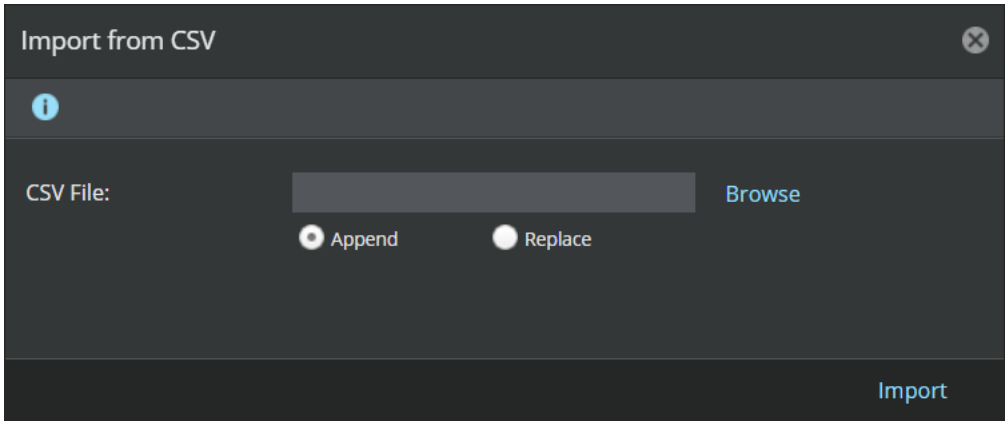


b. **Import from CSV** window appears. Use the **Append** option to add a new list of CIDR blocks or to append a list of CIDR block to an existing list. Use the **Replace** option to replace an existing list of CIDRs with a new list.

> **NOTE**
>
> If any duplicate entries exist while appending, the Manager replaces the existing entries with the entries being imported.

c. Click **Browse** to locate the CSV file that contains the list of IPv4 or IPv6 CIDRs that you plan to import.

Figure 652. Import IP CIDRs from a CSV file



The file to be imported should be in the following CSV format: <IPv4 or IPv6 CIDR>,<Comment>

Example file format: 10.10.1.0/24,textual description.

The following is a sample for a CSV file with multiple IPv4 CIDRs:

Figure 653. CSV file format for IPv4 or IPv6 Networks

```
134.        .100/7,textual description
134.        .100/8,textual description
134.        .100/9,textual description
134.        .100/10,textual description
134.        .100/11,
134.        .100/12,
```

The following table describes the details of the IP CIDR blocks to be imported in the CSV file format.

Format	Description
<IPv4 or IPv6 CIDR>	Specifies the IPv4 or IPv6 CIDR to be imported
<Comment>	Specifies the description of the IP address to be imported. If you do not want to specify a comment for an entry, add comma (**,**) next to the entry and leave it.

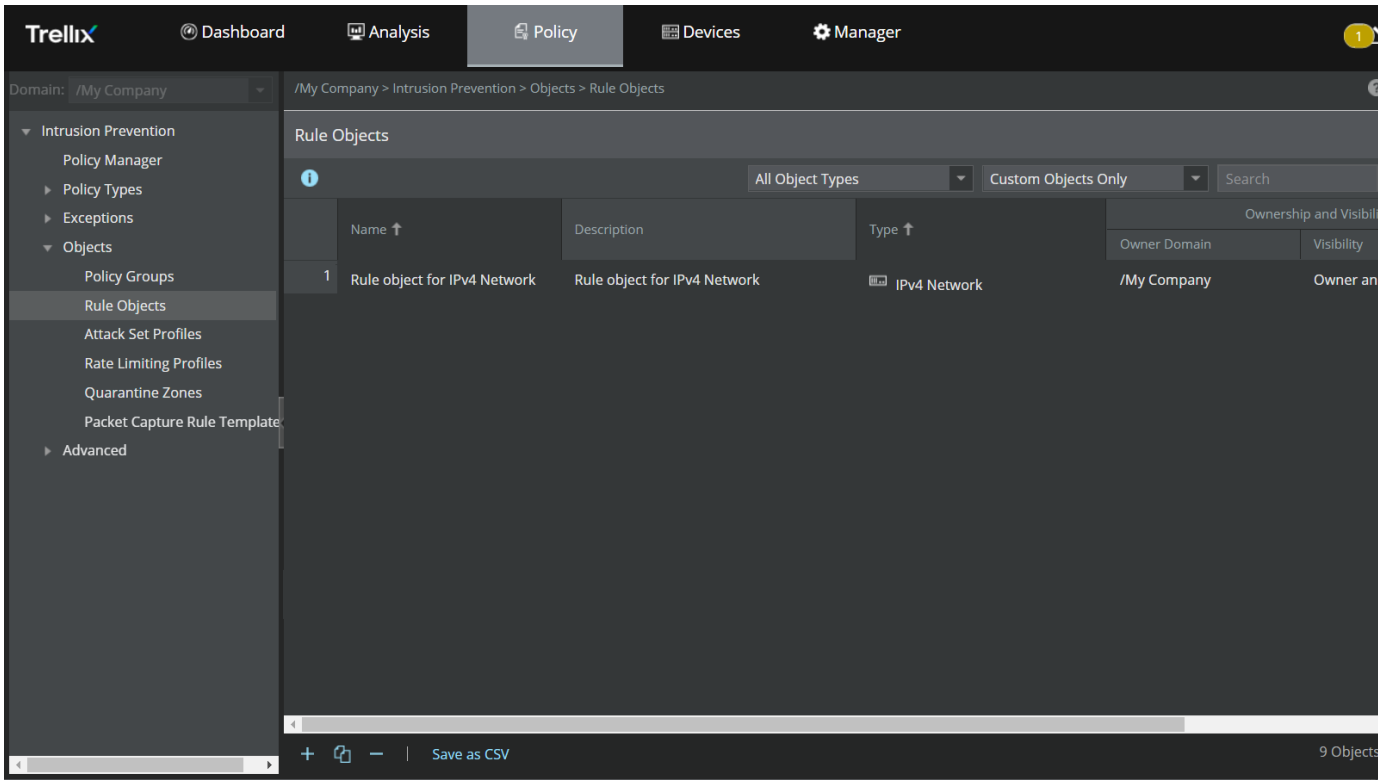
d. Click **Import** upon selecting the CSV file.

e. All the entries in the CSV file will be imported and the rule object will be saved automatically.

NOTE

The **State** of the rule members will be set to **Enabled** by default. You may change the state of a rule member by accessing the rule object.

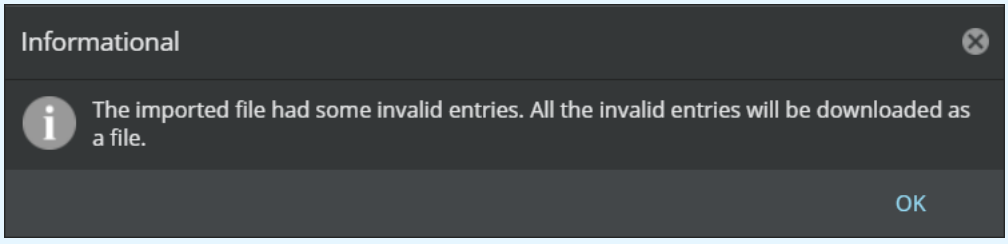
Figure 654. Rule object for IPv4/IPv6 network successfully created



NOTE

If there are any invalid entries in the CSV file, the Manager displays an **Informational** dialog-box stating about the invalid entries. All such entries will also be collected to a CSV file. This file will either download onto the local machine automatically or require you to choose a download location, based on your web browser's download settings. Upon downloading the file, click **OK** to close the **Informational** dialog-box. In this case, the rule object will be created upon closing the dialog-box.

Figure 655. Information dialog-box for invalid entries

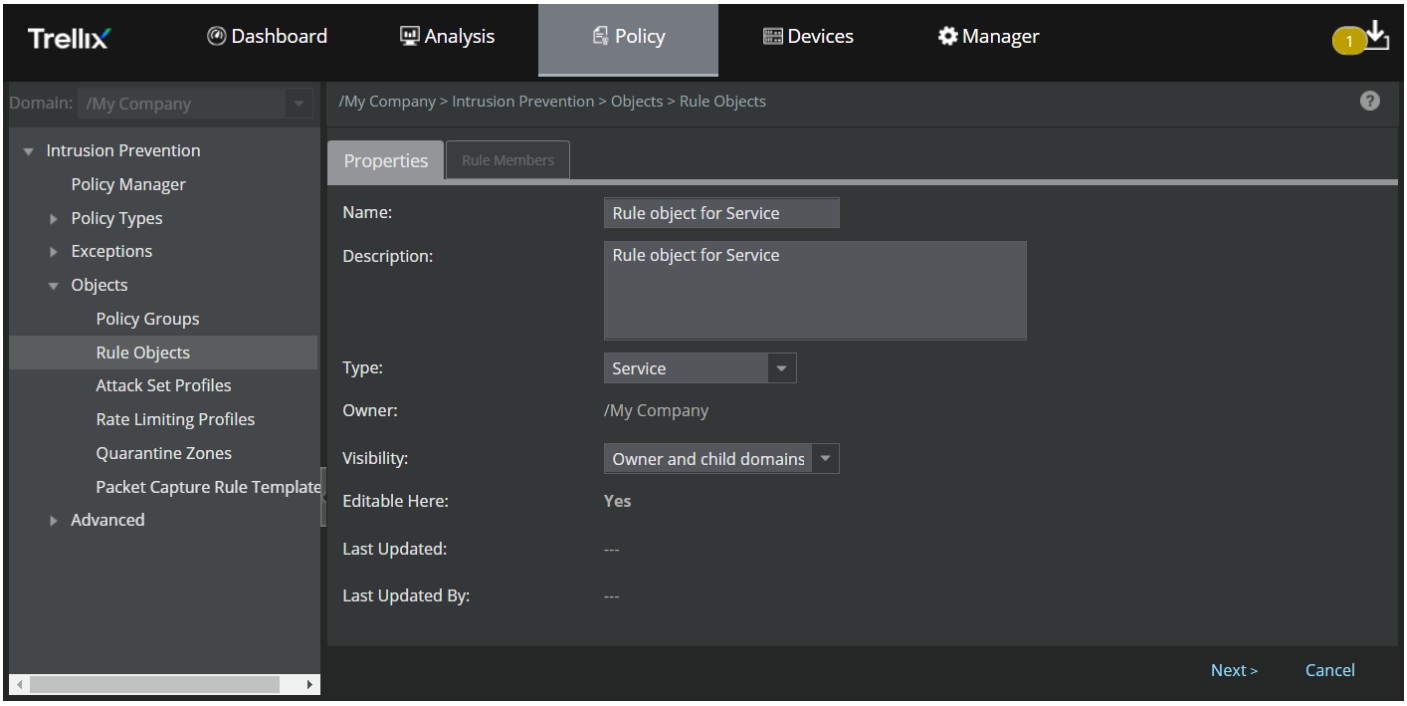


Add a Service rule object

Follow these steps to add **Service** rule object:

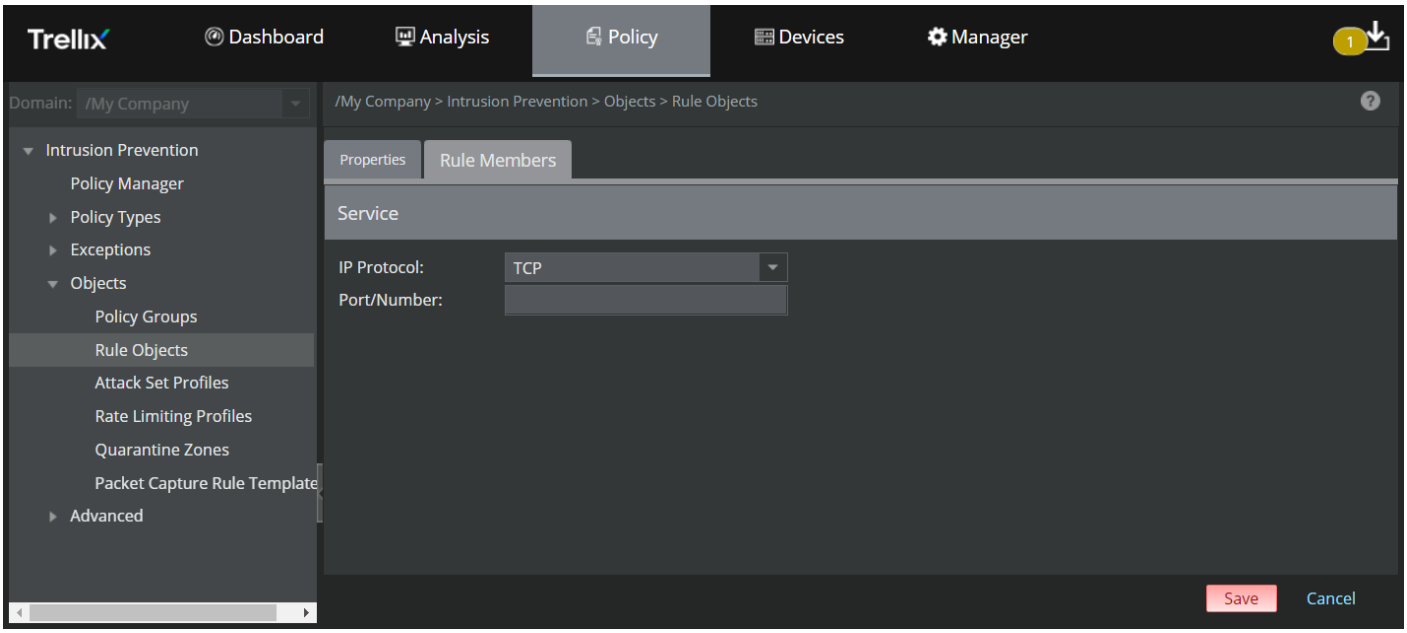
1. Upon specifying the options in the **Properties** tab and selecting **Service** from the rule object **Type** drop-down, click **Next**.

Figure 656. Create a Recurring Time Period rule object



The **Rule Members** tab is displayed.

Figure 657. Add Rule Members



The following table explains the options in the **Rule Members** tab.

Option	Definition
IP Protocol	Select the required protocol from the drop-down list. The options are **TCP**, **UDP** and **Protocol Number**.
Port/Number	If you select **TCP** or **UDP** as the **IP Protocol**, you can optionally enter a port number between from 1 to 65534. Alternatively, you can specify a protocol number between from 0 to 255.

2. Based on the above options, you can select the **IP Protocol** and specify a **Port/Number**.
3. Click **Save**.

Clone a rule object

You can clone custom rule objects.

- You cannot clone a default rule object except for Network.
- You can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

Steps:

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule objects for the selected admin domain are listed.
4. Locate the Rule Object that you want to clone.

   TIP

   You can use the search function to more easily find the rule object.
5. Select the rule object and click .
6. Make the required changes and click **Save**.

Modify a custom rule object

You can modify custom rule objects.

- You cannot modify or delete a default rule object.
- You can modify or delete a custom rule object only at the admin domain where it was created. If required, you can clone a custom rule object that was created at a parent admin domain and then modify it as required in the current admin domain.

- You cannot clone a default rule object except for Network. You cannot edit or delete any default rule object. You can edit or delete custom rule objects only at the admin domain where they were created.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

   Rule Objects for the selected admin domain are listed.
4. Locate the rule object that you want to modify.
   - You can use the search function to easily find the rule object.
   - Make sure the **Editable here** column displays **Yes** for the rule object you want to modify. If the **Editable** column displays **No**, the rule object belongs to a parent admin domain.
5. Double-click the rule object.
6. Make the required changes and click **Save**.

NOTE

If the rule object that you modified is part of a policy that is in use, you must do a configuration update to the Sensor for the changes to take effect.

Delete a custom rule object

Delete a custom rule object that you no longer use. You can delete a custom rule object only at the admin domain where it was created.

- You cannot delete a default rule object.
- You cannot delete a rule object that is used in a Firewall policy, QoS policy or, in a group rule object.
- You can delete a rule object only at the admin domain where it was created.

NOTE

Options differ depending on the rule object type you select. For information on a specific object type, refer to the corresponding sub-section.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Rule Objects**.

Rule objects for the selected admin domain are listed.

4. Locate the Rule Object that you want to modify.
   - You can use the search function to easily find the rule object.
   - Make sure the **Editable here** column displays **Yes** for the rule object you want to delete. If the **Editable here** column displays **No**, the rule object belongs to a parent admin domain.
5. Select the rule object and click −. Then click **Yes** to confirm deletion.

> **NOTE**
>
> To delete rule objects in bulk, press **Shift** key (for continuous selection) or press **Ctrl** key (for discontinuous selection) and then select the rule objects. The selected items are highlighted. Click − and then click **Yes** to confirm deletion.

Forward quarantine zone access rule matches to a syslog server

For all traffic that matched a quarantine zone access rule, the Sensor can forward the details to a syslog server. You can use these details for analysis and reporting purposes. For example, you can view the details of hosts that attempted to access a critical network when in quarantine. You can also log the packets that matched the quarantine zone access rules.

To forward the matched details to a syslog server, you must complete the following:

- If you want the Sensor to send the logged details directly to the syslog server, ensure that the configured syslog server is accessible to the Sensor's management port.

  > **NOTE**
  >
  > Only NS-series Sensors can directly send logs to a syslog server.

  Alternatively, if you want the Sensor to send the details through the Manager, then the Manager must be able to communicate to the syslog server. In this case, the Sensor forwards the logs to the Manager, which formats and converts them to syslog messages and sends them to the configured syslog server. You can then view the log from a third-party syslog application.
- Enable syslog forwarding for **Quarantine** at the admin domain level.

  > **NOTE**
  >
  > For syslog forwarding, the admin domains have the option to include the logs from the corresponding child domains.
- Enable syslog forwarding for **Quarantine** at the Sensor level. When you enable at the Sensor level, you can specify the conditions for logging. For example, you can specify whether to log permitted traffic or denied traffic. You can also specify if traffic should be logged only if specified in the quarantine zone access rule.

At both the domain and Sensor levels, the process of configuring the syslog server details is similar between Firewall Policies, and Quarantine. However, the configuration for Firewall Policies is different from Quarantine. That is, even if you are using the same syslog server for all these features, you must configure them separately for Firewall Policies and Quarantine. You can also configure different syslog servers for Firewall Policies and Quarantine.

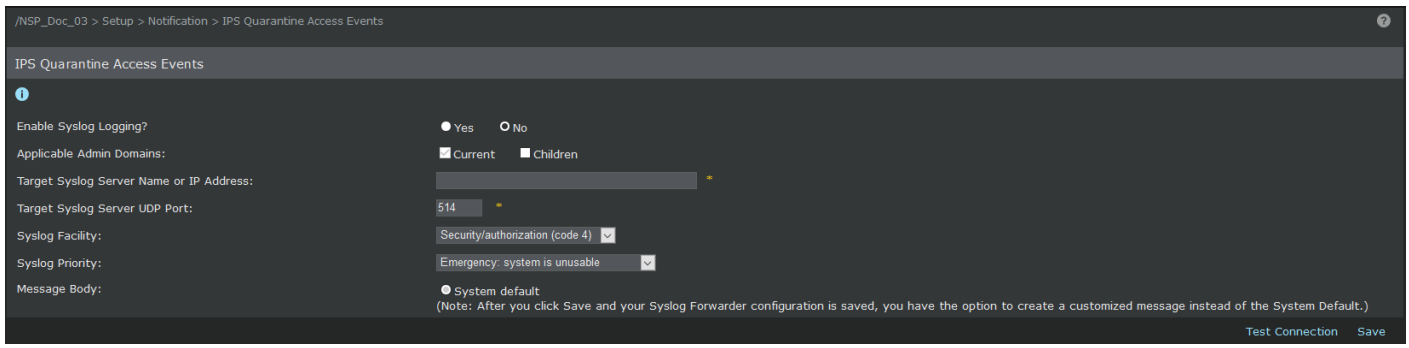
Enable syslog forwarding for Quarantine for the domain

You can inherit the syslog details from the parent domain or configure specifically for the current domain. This applies to all the Sensors in the domain only with respect to **Quarantine**. You can also choose to apply it to a child domain.

Steps:

1. To access the **Syslog** page, do the following.
   a. Click the **Manager** tab.
   b. From the **Domain** drop-down list, select the domain you want to work in.
   c. Select Setup → Notification → **IPS Quarantine Access Events**.
2. Specify the domain-level syslog details in the corresponding fields.

Figure 658. Syslog server details for Quarantine



Option	Definition
Enable Syslog Logging?	If you select **Yes,** the details of the traffic that matched a quarantine zone access rule is forwarded to a syslog server. You can also configure the details now and enable it at a later time.
Applicable Admin Domains	• **Current** — The syslog configuration applies only to the current domain. This is always enabled for the current domain. • **Children** —The syslog configuration applies to child domains as well. You can also modify this syslog configuration at a child domain if required.
Target Syslog Server Name or IP Address	Enter the syslog server name or its IP (IPv4 or IPv6) address. If you specify the syslog server name: • The Manager uses the DNS servers configured in its TCP/IP properties. • If you choose the Sensor to forward the logs to a syslog, then the Sensor uses the DNS servers that you configured in the **Name Resolution** page for the Sensor.
Target Syslog Server UDP Port	Enter the communication port number on the target server which is authorized to receive syslog messages. The standard port for syslog, which is 514, is pre-filled in the field. If you are using a non-standard port, then replace 514 with that number.

Option	Definition
Syslog Facility	Lists the syslog prioritization values. By default, the syslog messages forwarded to a syslog server are of **Security/authorization <prioritization value>**.
Syslog Priority	Lists the syslog priority values. By default, the syslog messages forwarded to a syslog server are of **Debug** severity.
Message Body	Optionally, customize the default syslog message. There are two types: • **System Default** — The default message is a quick summary for easy recognition. • **Customized** — You can customize the message after you successfully save the syslog configuration details. Click **Test Connection** to view the option to edit the default message.
Test Connection	Checks if the Manager is able to send syslogs to the syslog server. Check your syslog server if it has received the test message from the Manager. If not, check the syslog server name or IP address that you had provided. Ping the syslog server from the Manager server to see if the Manager is able to reach the syslog server. **NOTE** You can use the test connection feature, even if you have set **Enable Syslog Logging?** to no.
Save	Saves the syslog configuration changes in the Manager database. Once you click **Save**, you will be able to customize the message format sent to the syslog server. **NOTE** If you have modified the syslog configuration, then do a configuration update of the Sensors for the changed settings to take effect.

Customize the syslog forwarder message

Prerequisite: You must have saved the syslog server details successfully in the **Syslog** page.

Steps:

1. To access the **Syslog** page from the **Manager** tab, do the following.
   a. Click the **Manager** tab.
   b. From the **Domain** drop-down list, select the domain you want to work in.
   c. Select Setup → Notification → **IPS Quarantine Access Events**.

Option	Definition
Enable Syslog Logging?	Select **Yes** to enable syslog and **No** to disable syslog.

Option	Definition
Applicable Admin Domains	**Current** — Refers the admin domain currently selected. This is enabled by default. **Children** — Refers the child admin domains of the current domain.
Target Syslog Server Name or IP Address	The IP address or name of the syslog server which becomes the destination of the alert notifications sent by all devices. **NOTE** The length of server name has been increased to support up to 255 characters from 40 characters.
Target Syslog Server UDP Port	Port on the target syslog server that is authorized to receive syslog messages. The default protocol for syslog forwarding from Sensors is UDP. Therefore, this port must not be altered.
Syslog Facility	Standard syslog prioritization value. The choices are as follows: • **Security/authorization (code 4)** • **Security/authorization (code 10)** • **Log audit (note 1)** • **Log alert (note 1)** • **Clock daemon (note 2)** • **Local user 0 (local0)** • **Local user 1 (local1)** • **Local user 2 (local2)** • **Local user 3 (local3)** • **Local user 4 (local4)** • **Local user 5 (local5)** • **Local user 6 (local6)** • **Local user 7 (local7)**

Option	Definition
Syslog Priority	You can map each severity (Informational, Low, Medium, or High) to one of these standard syslog severities: • **Emergency** – System is unusable • **Alert** – Action must be taken immediately • **Critical** – Critical conditions • **Error** – Error conditions • **Warning** – Warning conditions • **Notice** – Normal but significant condition • **Informational** – Informational messages • **Debug** – Debug-level messages
Message Body	**System default** — The default message is a quick summary of an event. **Customized** — Personalized message of an event.

2. Click **Test Connection** in the **Syslog** page.
3. Click **Edit** in the **Message Body** field in the **Syslog** page.

   The **Customize Syslog Forwarder Message** page displays.
4. Customize the format for the syslog forwarder message.

Option	Definition
Message	Form the message by typing in the required text and by clicking on the parameters provided below this field. **IMPORTANT** For Syslog information to appear correctly, ensure that you use the dollar-sign ($) delimiter immediately before and after each element. Example: $SENSOR_NAME$
Save	Saves the message you created. Displays the **Syslog** page when you click.
Cancel	Cancels the changes you made to the message.
Reset to System Default	After you customize the syslog message, the **Reset to System Default** button appears in the **Customize Syslog Forwarder Message** page. Click this button to revert to the system default message.

5. Click **Save** in the **Syslog** page.

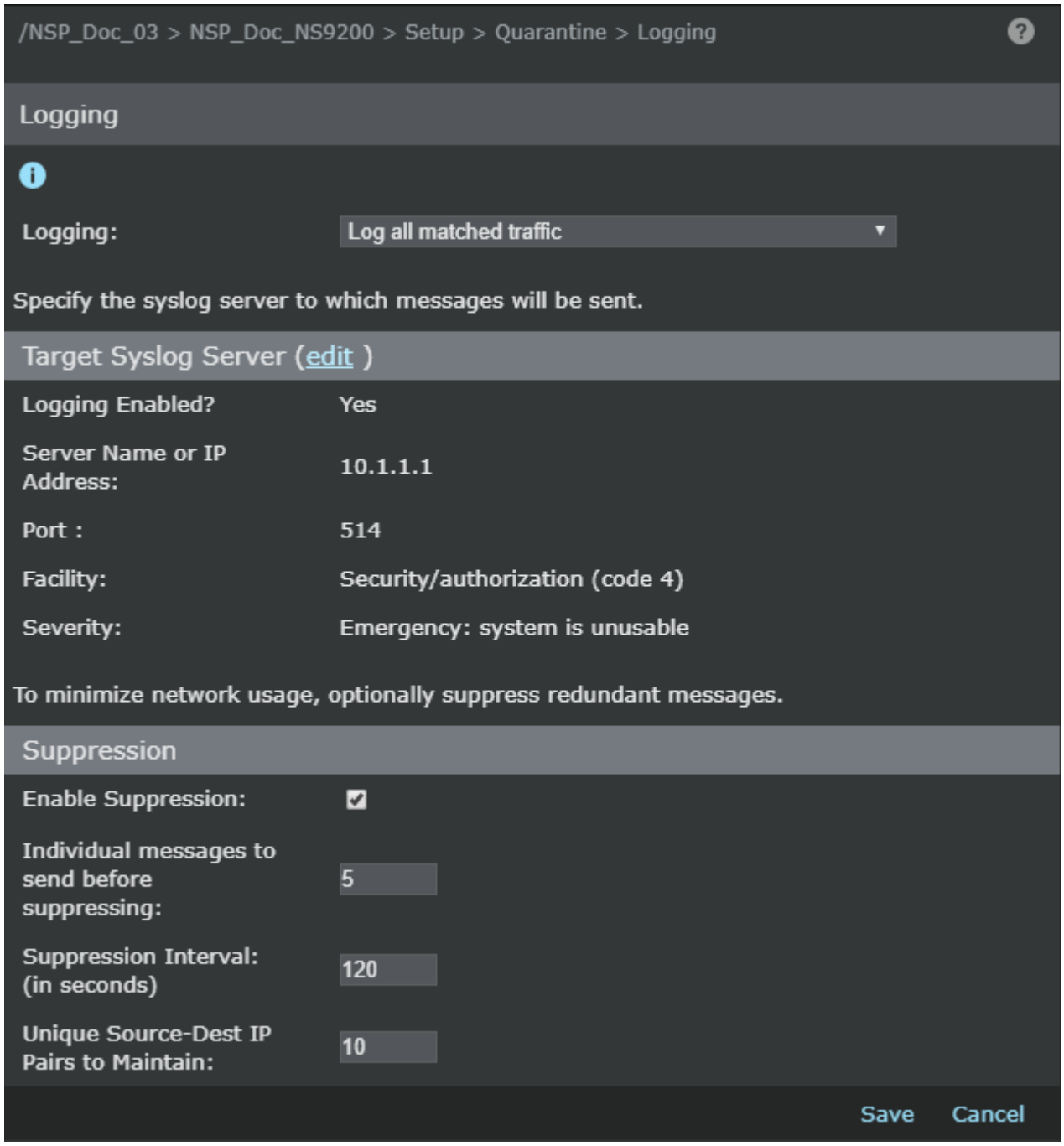
Enable syslog forwarding for Quarantine for a Sensor

The following are the steps to enable syslog forwarding for a Sensor.

1. Click the **Devices** tab.

2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Quarantine → **Logging**.

Figure 659. Enabling syslog forwarding for a Sensor



6. Specify the Sensor-level syslog details in the corresponding fields.

Option	Definition
Logging	Sets the condition when the Manager or the Sensor should send the log message to the syslog server. The options are: • **Disabled on this device** — This disables logging on the device. This option overrides the setting on the individual access rules. The remaining options in the **Logging** page are not displayed if you choose this option. • **Log all matched traffic** — Logs all traffic that matched a rule regardless of whether it was dropped/denied or permitted. This option overrides the setting on the individual access rules. • **Log all dropped/denied traffic** — Logs all traffic that was either dropped or denied according to an access rule. This option overrides the setting on the individual access rules. • **Log all permitted traffic** — Logs all traffic that was permitted according to an access rule. This option overrides the setting on the individual access rules. • **Log traffic only if the matched rule is configured to log** — Logs only if you had configured logging for the corresponding access rule.
Target Syslog Server	Displays the syslog server details that you have configured at the corresponding admin domain. Click **Edit** to go to the **Syslog** page and modify the required details.
Enable Suppression	Option to suppress redundant messages. Only if you select it, the remaining fields in the **Suppression** table are displayed. Suppressing log entries causes the Sensor to send initial log entries representing the first instance of an event (the number of which is configurable), and then suppress further instances of the same event for a configurable number of seconds. This is a useful tool in keeping the log file size under control.
Individual messages to send before suppressing	Indicates the number of messages to be sent within the seconds specified in the **Suppression Interval** field for suppression to begin.
Suppression Interval (in seconds)	Time span in which you accumulate instances of the same rule match. This value acts as a timer; when the timer expires, the current instance is cleared to make room for a new suppression instance.
Unique Source-Dest IP Pairs to Maintain	Determines the number of unique suppression instances to maintain at a given time. For example, if you enter the number 10, then 10 unique instances can be tracked at a given time. Once 10 is reached, all other cases are kept in a single "wildcard" instance; thus, other unique combinations that occur outside of the 10 uniquely maintained instances are maintained as one instance, and source and destination IP do not appear in the summary since multiple addresses may be involved. An entry is removed after the time limit (Suppression interval) expires.
Save	Saves the configuration in the Manager database. **NOTE** Do a configuration update to the applicable Sensors for the configuration to take effect.

Option	Definition
Cancel	Reverts to the last saved configuration.

Manage Quarantine Zones

When you configure **Quarantine** at the admin domain and Sensor port level, you need to specify the **Quarantine Zone** which must be used to quarantine hosts. At the Sensor port level, you can retain the **Quarantine Zone** configured at the admin domain or override it with a different **Quarantine Zone**. To enable you to quickly configure **Quarantine**, some pre-defined **Quarantine Zone** are provided. If these do not meet your requirements, you can clone them and edit them. If not, create **Quarantine Zone** according to your requirement.

Notes:

- You cannot edit or delete the pre-defined **Quarantine Zone**.
- The pre-defined **Quarantine Zone** belongs to the root admin domain and is visible to all the child admin domains.
- Syslog forwarding is not enabled for the access rules of the pre-defined **Quarantine Zone**.
- You cannot edit or delete a **Quarantine Zone** defined at a parent domain.
- You cannot delete a **Quarantine Zone** if it is applied to a domain or Sensor port.
- A configuration update of the Sensors is required for the changes to a **Quarantine Zone** to take effect.
- You can create or edit rule objects even when creating an access rule. However, for the sake of explanation, this section assumes that you have created the required rule objects prior to creating the access rules.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Intrusion Prevention → Objects → **Quarantine Zones**.

Option	Definition
Name	Displays the name of the **Quarantine Zone**
Description	Displays the description of the **Quarantine Zone**
Ownership and Visibility	
Owner Domain	Indicates the admin domain to which a **Quarantine Zone** belongs. All the default **Quarantine Zones** belong to the root admin domain.
Visibility	Indicates the visibility level of the domain
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Last Updated	
Time	Displays the time when the **Quarantine Zone** was last modified
By	Displays the user who modified the **Quarantine Zone**
New	Creates a **Quarantine Zone**
Copy	Clones a **Quarantine Zone**

Option	Definition
Edit	Displays the details of a **Quarantine Zone**. You can also edit a **Quarantine Zone** belonging to the current admin domain.
Delete	Deletes a custom **Quarantine Zone** belonging to the current admin domain

You can sort the list in ascending or descending order based on any of the columns by clicking on the column heading. You can also view the **Columns** option to enable or disable the display of the columns by selecting or deselecting the relevant check-boxes.

4. To create a **Quarantine Zone**, click **New**.
5. Specify the details on the **Properties** tab.

Option	Definition
Name	Enter a unique name to easily identify the **Quarantine Zone**.
Description	Describe the **Quarantine Zone** for other users to identify its purpose.
Owner	Displays the admin domain to which a **Quarantine Zone** belongs
Visibility	When selected, makes the **Quarantine Zone** available to the corresponding child admin domains. However, the **Quarantine Zone** cannot be edited or deleted from the child admin domains.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain.
Statistics	
Lasted Updated	Displays the timestamp when the **Quarantine Zone** was last modified
Last Updated By	Displays the user who last modified the **Quarantine Zone**
Rules	Displays the number of access rules currently defined in the **Quarantine Zone**
Next	Saves the changes made on the **Properties** tab and displays the **Access Rules** tab
Cancel	Reverts to the last saved configuration

6. On the **Access Rules** tab, click the appropriate button to insert a new rule.

Option	Definition
	Inserts a new rule above the currently selected rule
	Inserts a new rule below the currently selected rule
	Clones the currently selected rule
	Deletes the currently selected rule
	Moves the currently selected rule one row up

Option	Definition
	Moves the currently selected rule one row down

7. Double-click on each column of the access rule and specify your choices.

Option	Definition
State	Displays whether an access rule is enabled or disabled. Sensor does not apply disabled rules. This option might help you during troubleshooting.
Description	Optionally enter additional information about the rule. This might help you to easily understand the logs forwarded to the syslog server.
Destination	Select the IPv4 Endpoint or the IPv4 Network rule object. Click  to create a new rule object. Click  to edit or view a rule object.
Service	Restricts traffic based on the IP protocol, ICMP codes, or the TCP/UDP port numbers. Click  to create a new rule object. Click  to edit or view a rule object.
Response	Specify if the Sensor should allow or block traffic that matches the rule. Select **Drop** to discard the traffic or click or select **Permit** to pass the traffic. Consider that you want to log the matched traffic details only for specific access rules. Then, select **Log to Syslog?** for those rules. **NOTE** Ensure that in the **Logging** page of the Sensor, the **Log traffic only if the matched rule is configured to log** option is selected for the **Logging** field. The **Log to Syslog?** option has no impact if you select any other option for the **Logging** field in the **Logging** page.
OK	Saves the **Quarantine Zone** access rules in the Manager database. The **Quarantine Zone** is listed in the **Quarantine Zones** list.
Save	Saves all the **Quarantine Zone** access rules
Cancel	Reverts to the last saved configuration

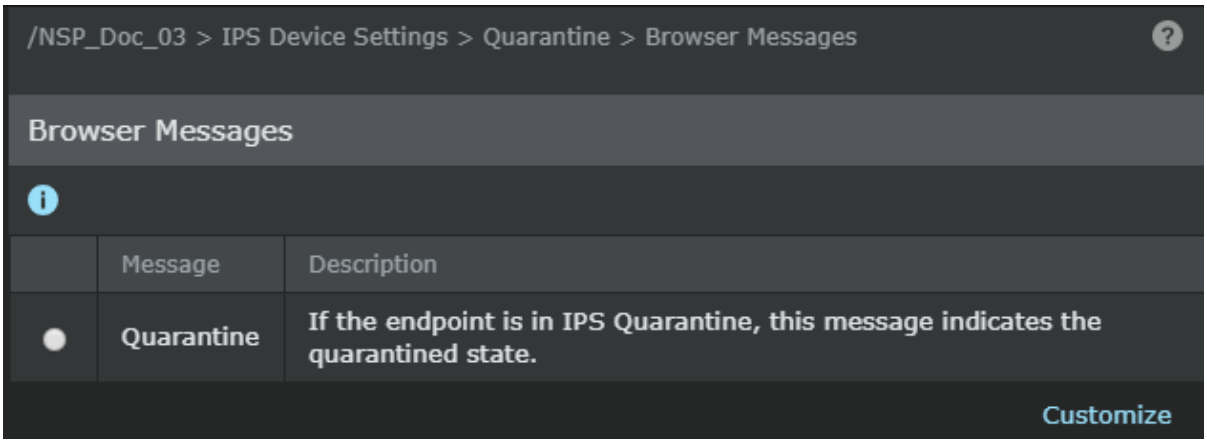
Following the steps above, you can **Copy**, **Edit** or **Delete** the custom **Quarantine Zone**.

Customize Quarantine browser message

When the quarantined host tries to access network resources outside its assigned **Quarantine Zone**, a **Quarantine** browser message is displayed to the host. Manager provides a built-in **Quarantine** browser message, which can be customized according to your requirements.

1. Click the **Devices** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Global → IPS Device Settings → Quarantine → **Browser Messages**.

Figure 660. Customize Quarantine browser message



4. To edit and customize the built-in browser message select **Quarantine** and then click **Customize**.
5. In the **Customize Browser Message** page, edit the default content according to your requirement.

Option	Definition
Message Text	Displays the current format for the message.

Option	Definition
Content-Specific Variables	Click the following to insert the corresponding variable in the **Message Text** field. • **Health Level** — Indicates whether the host is in good health based on its compliance with your organization's security policies. For example, a host is in good health if it has the required security applications and patches as mandated by your policies. • **Host Name** — Indicates the name of the quarantined host. • **IP Address** — Indicates the IP address of the quarantined host. • **MAC Address** — Indicates the IP address of the quarantined host. • **Network Access Zone** — Indicates the name of the network access zone to which the host is restricted to for the quarantine period. • **Sensor Name** — The Sensor that is quarantining the host. • **User Name** — The user logged on to the host at the time of quarantine. • **Attack ID** — The Trellix-assigned universally unique hexadecimal value of the attack that caused the host to be quarantined. • **Attack Name** — Trellix-assigned named to the attack that caused the host to be quarantined. • **Quarantine Time** — The start time of the quarantine. • **Duration** — The time period for which the host is quarantined.
Save	Saves the changes made to the browser message.
Reset	Reverts to the default browser message. If you click this button, even the saved customizations are lost.
View	Click to view how the browser message appears for the user. The remediation portal IP is displayed if you have configured those details in the Manager already.
Cancel	Click to revert to the last saved version of the browser message.

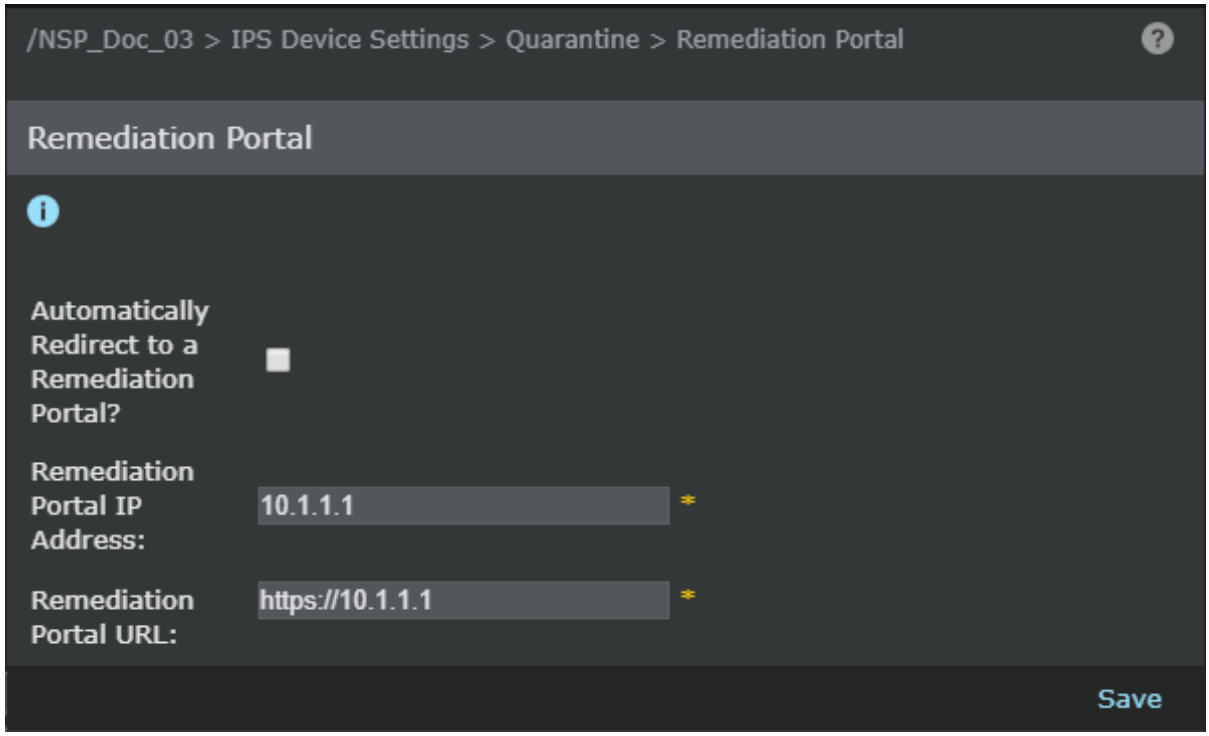
Specify the Remediation portal details

You can configure a web portal in your internal network that contains links to download security software. You can then configure the details of this portal in Trellix IPS. When a Sensor detects HTTP traffic from a quarantined host, it redirects the host to this portal.

With respect to **Quarantine**, the Sensor redirects HTTP traffic from a quarantined host throughout the quarantine duration even if the user has already installed all the software available through the remediation portal.

1. Click the **Devices** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Select Global → IPS Device Settings → Quarantine → **Remediation Portal**.

Figure 661. Remediation portal settings



4. Specify the **Remediation Portal** settings.

Option	Definition
Automatically Redirect to a Remediation Portal?	When selected, Sensor redirects a quarantined host to the remediation portal when it detects HTTP traffic from the host.
Remediation Portal IP Address	Enter the IPv4 address of the server hosting the remediation portal.
Remediation Portal URL	Type the entire path to the remediation portal including the IP address of the server.
Save	Saves the remediation portal configuration. This configuration applies to all the Sensors in the admin domain. **NOTE** Do a configuration update of the Sensors for the changes to take effect.

Quarantine settings for an admin domain

You can configure and enable **Quarantine** globally for an admin domain. Then for the corresponding member Sensors and child domains, you can inherit these settings or modify them selectively.

When you enable **Quarantine**, you can specify the following:

- Whether to inherit the **Quarantine** configuration from the parent domain
- Whether to make these settings visible to the child domains downstream
- Whether the Sensor needs to display the browser message
- The **Quarantine Zone** to be applied and the duration of the quarantine
- Hosts to be excluded from **Quarantine**

Enable Quarantine for an admin domain

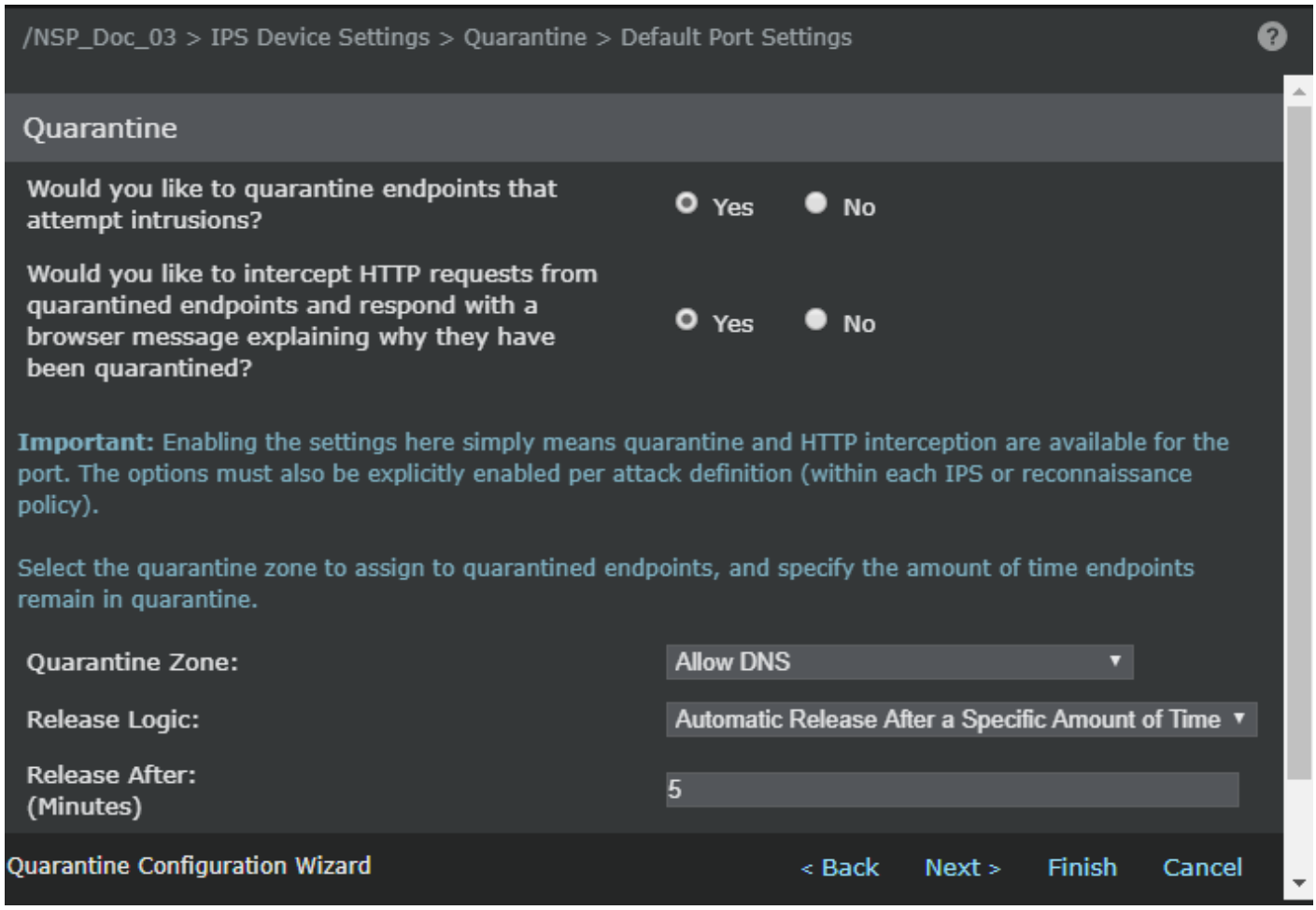
Use the **Quarantine Configuration Wizard** to configure the default **Quarantine** settings for an admin domain. That is, these settings are available for the child domains as well as the Sensors managed by the admin domain. Then, you can inherit or customize these settings at the child-domain level and Sensor level.

1. Click the **Devices** tab.
2. From the **Domain** drop-down list, select the domain you want to work in.
3. Click the **Global** tab.
4. Select IPS Device Settings → Quarantine → **Default Port Settings**.

   The **Quarantine Configuration Wizard** opens.
5. Configure Quarantine at the admin-domain level using the **Quarantine Configuration Wizard**.

> **NOTE**
>
> Throughout this wizard, click **Next** to proceed to the next page. Click **Cancel** to exit the wizard without saving the changes.

Figure 662. Quarantine settings using the wizard



Option	Definition
Inherit From Parent Domain	When selected, the settings from the parent domain are applied. Click **Finish** and no further configuration is required. However, in the parent domain, you must have selected **Visible to Child Admin Domains**. To use a different configuration for this domain, deselect **Inherit From Parent Domain**. **NOTE** This is not applicable to the root admin domain.
Visible to Child Admin Domain	When selected, a child domain is able to use the same **Quarantine** settings.
Would you like to quarantine endpoints that attempt intrusions?	When selected, enables the **Quarantine** feature for this admin domain.

Option	Definition
Would you like to intercept HTTP requests from quarantined endpoints and respond with a browser message explaining why they have been quarantined?	Enables redirection to the **Quarantine** browser message and subsequently to the **Remediation Portal**.
Quarantine Zone	Lists the quarantine zones that are available for the admin domain.
Release Logic	• **Automatic Release After a Specific Amount of Time** — The Sensor automatically releases the host from quarantine after the time period you specify in the **Release After** field. • **Keep in Quarantine Until Explicit Released** — The Sensor quarantines the host until you manually release it.
Release After	Enter the quarantine time period (between 5 and 60 minutes), if you had selected **Automatic Release After a Specific Amount of Time** in the **Release Logic** field.

Quarantine Exceptions	Displays the details of the hosts and networks for which you do not want to quarantine.
	NOTE
	At the Sensor level, you can inherit this list and append more entries or configure a different quarantine exception list for that Sensor.
	• **New** — Adds a new record to the quarantine exception list.
	  • **Type** — Select based on how you plan to create the quarantine exception record. You can choose to enter the IPv4/IPv6 address of the host to be excluded, IPv4 network to be excluded, or select a IPv4 Endpoint, IPv4 Endpoint or IPv4 Network rule object.
	  • **Value** — Based on your selection in the **Type** field, enter the IP address, network, or choose the rule object.
	  • **Description** — Optionally, enter any notes regarding the quarantine exception record.
	• **Edit** — Select a record in the quarantine exception table and click this button to make changes to the **Value** and **Description** fields of that record.
	• **Delete** — Select a record in the quarantine exceptions table and click this button to delete it from the Manager database.
	• **Import** — If you have too many entries, then you can import them from a .csv file.

Option	Definition
Finish	Saves the **Quarantine** configuration to the Manager database and exits the wizard. **NOTE** You must do a configuration update to the Sensors for these changes to take effect.

Quarantine settings at Sensor level

For **Quarantine** to work, you must configure **Quarantine** on the Sensor inline monitoring port that detected the corresponding attack from the host. You can have a different configuration for each port of a port-pair. Similar to admin domain, you use the **Quarantine Configuration Wizard** at the Sensor level as well. You can inherit the domain settings or customize the settings selectively for a Sensor.

View the Quarantine configuration summary for a Sensor

Before you enable or modify **Quarantine** settings, you can view the summary of the current **Quarantine** for the Sensor.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Quarantine → **Summary.**

   You can view the following details in the **Summary** page:

   - Whether syslog forwarding is enabled for the Sensor and the suppression details.

     NOTE
     Click **Logging** to open the syslog **Logging** page for the Sensor.

   - The **Quarantine** status for each inline Sensor monitoring port. If you enable **Quarantine** domain level, then it is enabled by default for all the inline ports. Similarly, if you disable it at the domain level, it is disabled for all the ports. However, you can enable or disable **Quarantine** for an inline port regardless of the configuration at the domain level.

Enable Quarantine for an inline monitoring port

Make sure the Sensor is up and you have deployed the required monitoring ports in inline mode.

Use the **Quarantine Configuration Wizard** to enable and configure **Quarantine** for specific Sensor monitoring ports.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.

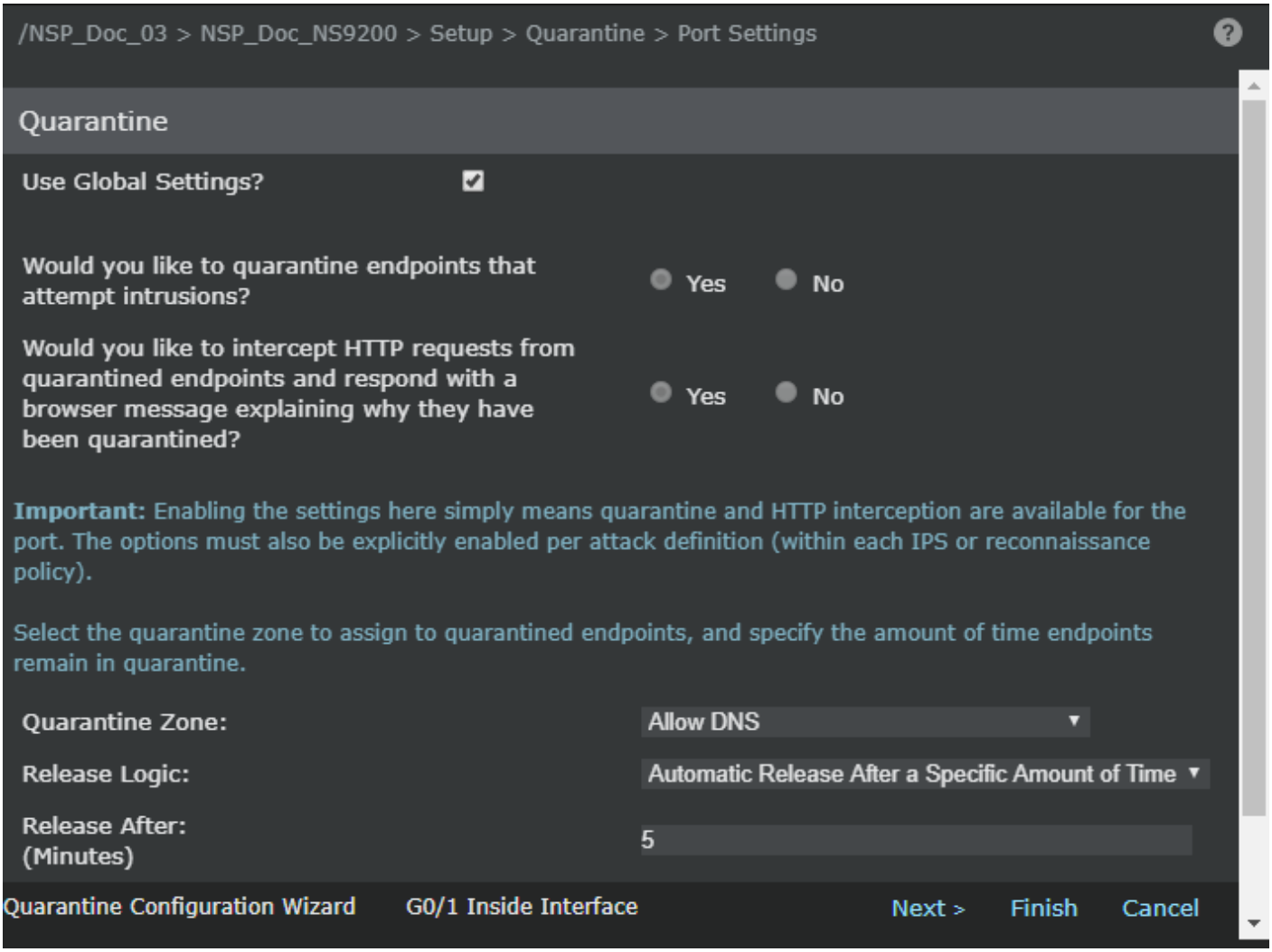
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Quarantine → **Port Settings**.
6. From the **Port** drop-down list, select the Sensor monitoring port for which you want to configure **Quarantine**.

   The current **Quarantine** configuration for the port are displayed.
7. Click **Run Configuration Wizard**.

   This button is available only if the Sensor is up.
8. Configure **Quarantine** for the selected Sensor monitoring port using the **Quarantine Configuration Wizard**.

> **NOTE**
>
> Throughout this wizard, click **Next** to proceed to the next page. Click **Cancel** to exit the wizard without saving the changes.

Figure 663. Quarantine Configuration Wizard for monitoring ports

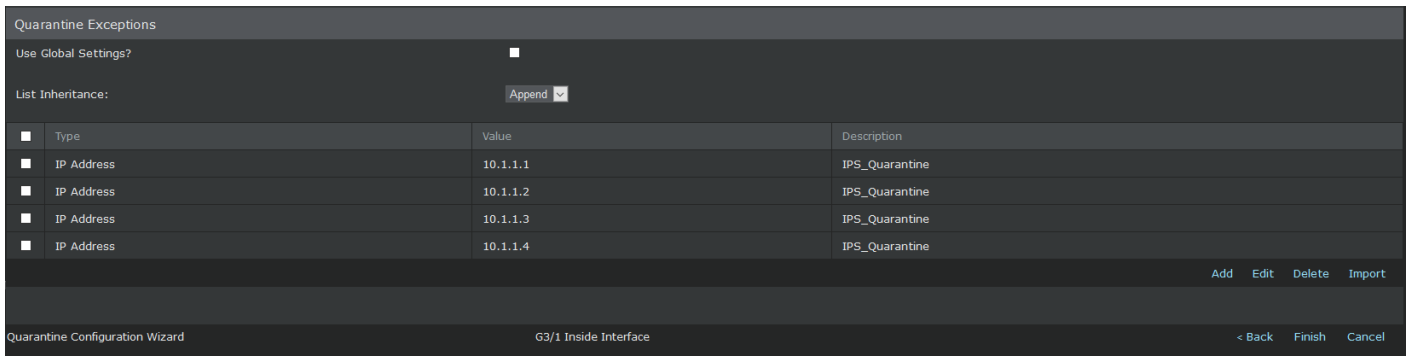


Option	Definition
Use Global Settings	When selected, the **Quarantine** configuration from the admin domain is applied to this Sensor port. You can proceed to the next page in the wizard. However, you must have enabled **Quarantine** at the domain level. To modify the **Quarantine** settings for the Sensor port, deselect **Use Global Settings**.
Would you like to quarantine endpoints that attempt intrusions?	When selected, enables the **Quarantine** feature for the selected port.
Would you like to intercept HTTP requests from quarantined endpoints and respond with a browser message explaining why they have been quarantined?	For the selected port, enables redirection to the **Quarantine** browser message and subsequently to the **Remediation Portal**.
Quarantine Zone	Lists the Quarantine Zones that are available for the port.
Release Logic	• **Automatic Release After a Specific Amount of Time** — The Sensor automatically releases the host from quarantine after the time period you specify in the **Release After** field. • **Keep in Quarantine Until Explicit Released** — The Sensor quarantines the host until you manually release it.
Release After	Enter the quarantine time period (between 5 and 60 minutes), if you had selected **Automatic Release After a Specific Amount of Time** in the **Release Logic** field.

Option	Definition

Quarantine Exceptions	Displays the details of the hosts and networks for which you do not want to quarantine.
	• **Use Global Settings** — When selected, the quarantine exceptions list from the admin domain is applied to the Sensor port. However, you must have enabled **Quarantine** with a quarantine exceptions list at the domain level. To customize the list for the Sensor port, deselect **Use Global Settings**.You can inherit the list of quarantine exceptions from the admin domain.
	• **List Inheritance: Append** — When selected, the quarantine exceptions list from the admin domain is displayed and you can add more entries to it.
	• **List Inheritance: Override** — Select to configure a separate quarantine exceptions list for the port.
	• **New** — Adds a new record to the quarantine exceptions list.
	  • **Type** — Select based on how you plan to create the quarantine exceptions record. You can choose to enter the IPv4/IPv6 address of the host to be excluded, IPv4 network to be excluded, or select a IPv4 Endpoint, IPv6 Endpoint or IPv4 Network rule object.
	  • **Value** — Based on your selection in the **Type** field, enter the IP address, network, or choose the rule object.
	  • **Description** — Optionally, enter any notes regarding the quarantine exceptions record.
	• **Edit** — Select a record in the quarantine exceptions table and click this button to make changes to the **Value** and **Description** fields of that record.
	• **Delete** — Select a record in the quarantine exceptions table and click this button to delete it from the Manager database.
	• **Import** — If you have too many entries, then you can import them from a .csv file.

Finish	Saves the **Quarantine** configuration to the Manager database and exits the wizard. **NOTE** You must do a configuration update to the Sensors for these changes to take effect.



Quarantine configuration in the policies

For a Sensor to automatically quarantine hosts that generate attacks, you need to enable **Quarantine** settings in the corresponding attack definitions. By default the **Quarantine** feature is disabled for all attacks. Regardless of whether you have enabled **Quarantine** in an attack, you can manually quarantine a host from the Attack Log.

You can enable **Quarantine** for attacks in the IPS and Reconnaissance policies. This applies to attacks from the Trellix Signature Set as well Custom Attack Definitions.

For ease of use, the Manager provides you various options to enable **Quarantine** for attacks:

- Open multiple IPS or Reconnaissance policies. Then enable **Quarantine** for a specific attack or multiple attacks in these policies.
- At the root admin domain, use the **Master Attack Repository** page to enable **Quarantine** for one or multiple attacks across IPS and Reconnaissance Policies.

Regarding attacks from the Signature Set, there are some for which **Quarantine** might not be relevant. Even if you enable **Quarantine** for such attacks, the Sensor does not quarantine hosts that generate these.

You can enable **Quarantine** for attacks from the Central Manager. Similar to other policy customization done at the Central Manager, it applies to the corresponding Central Manager policies used in all the Managers.

Enable Quarantine in attack definitions

Based on whether you are using the **Master Attack Repository** page or the policy editors, you have completed the steps provided in the previous sections.

1. On the **Attack Definitions** tab, double-click on the row of the attack that you want to configure and update the settings. The attack details are displayed on the right panel displaying the settings under the **Settings** tab.
2. Configure the settings for the attack definitions in the **Quarantine** field, under **Sensor Actions**.

   The following are the available Quarantine options:

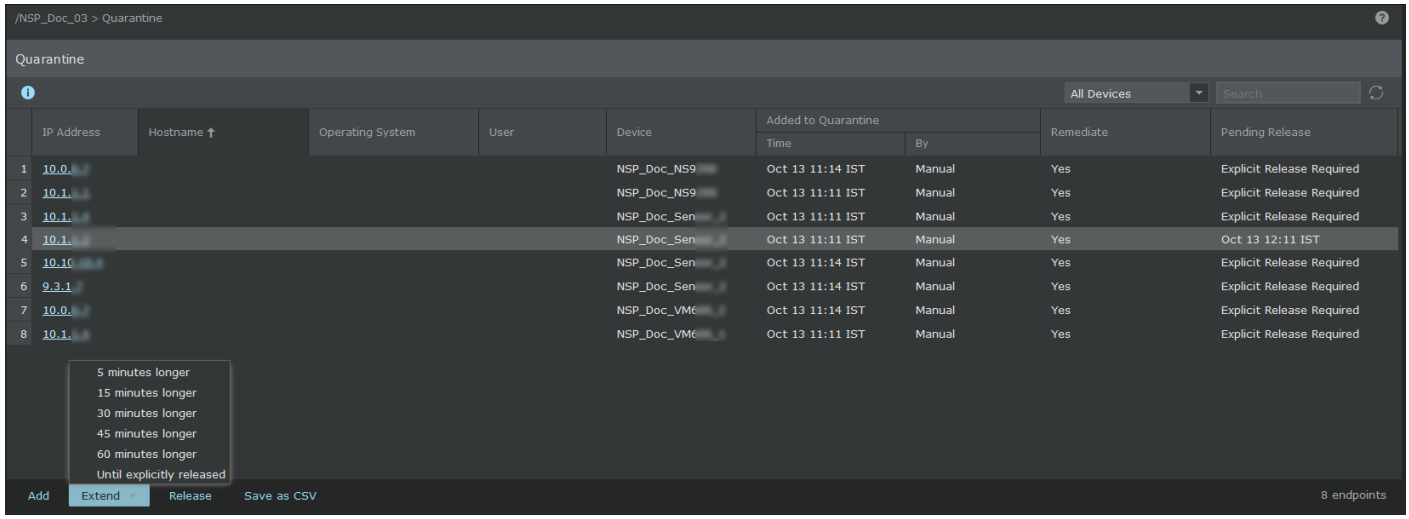
   - **Inherit (Disabled)**
   - **Quarantine Attacker**
   - **Quarantine and Remediate**
   - **Attacker**
   - **Disabled**
3. Click **Update** and then **Save** in the **Attack Definitions** window.
4. If the modified policy is applied to a Sensor, you need to update the Sensor configuration, for the changes to be effective.

Manage endpoints to quarantine

You can manually quarantine endpoints and also view endpoints in quarantine.

1. In the Manager, click the **Analysis** tab and select the domain from the **Domain** drop-down list.
2. Select Quarantine. The **Quarantine** page is displayed.

Figure 664. Quarantine page

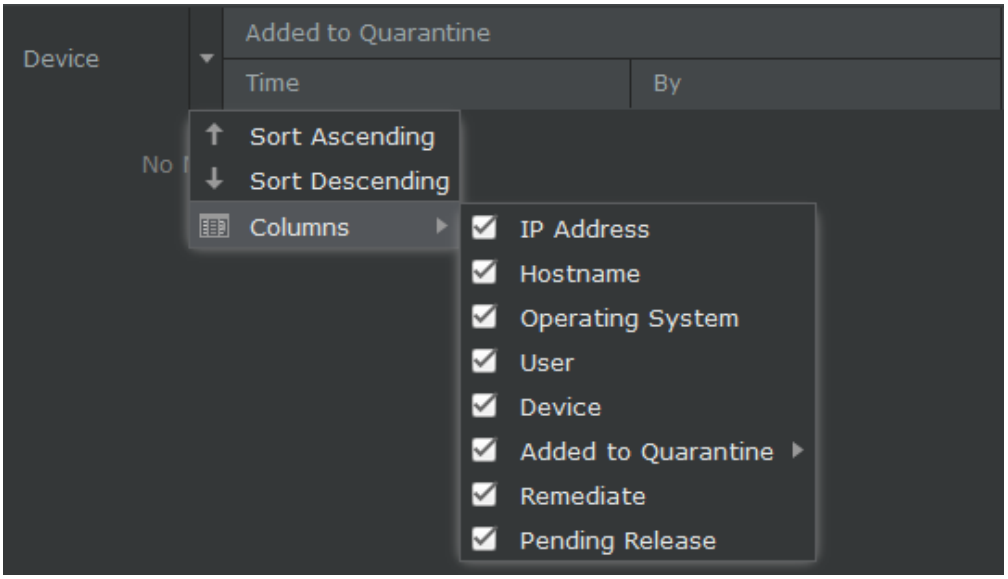


The **Quarantine** page displays the following details:

Option	Definition
IP Address	Displays the IP address of the quarantined endpoint.
Hostname	Displays the name of the quarantined host.
Operating System	Displays the operating system of the quarantined host.
User	Displays the user name of the quarantined host.
Device	Displays the Sensor on which the endpoint is quarantined.
Added	Specifies the time when the endpoint was first added to quarantine and the name of the attack or administrative user triggering the quarantine. Click the hyper link to view the attack description in the attack encyclopedia.
Remediate	Specifies if the quarantined host is redirected to the remediation portal or not (displays **Yes** or **No**). **NOTE** Remediation is applicable only to IPv4 address.
Pending Release	Specifies the time when the endpoint is scheduled to be released from quarantine.
Add	Click here to add a new IP address to be quarantined on a Sensor.
Extend	Click here to extend the quarantine time of an IP address.
Release	Click here to release an IP address from quarantine on a Sensor.
Save as CSV	Saves all the quarantined host list in .csv format.

You can filter the display of columns by clicking a column header and then select or unselect the checkbox for the list of columns you want to view in the **Quarantine** page.

Figure 665. Filter options



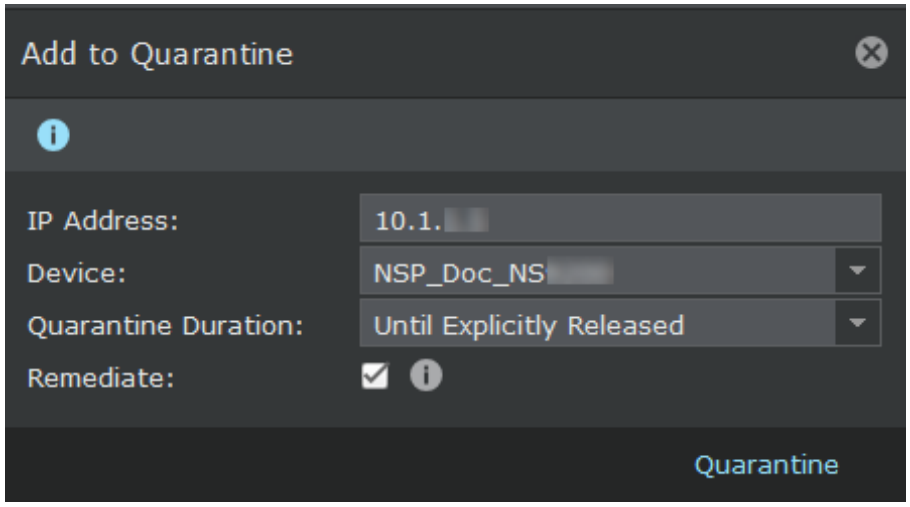
Click a column header and select the option to sort based on ascending or descending order. The options are **Sort Ascending** and **Sort Descending**. The column based on which the list is sorted is indicated in the column header by an up arrow icon for ascending order and down arrow icon for descending order.

Add endpoints to quarantine

You can quarantine endpoints to block all the traffic originating from the specified IP address seen on the selected device for the selected time. While adding an endpoint to quarantine, you can also re-direct the quarantined endpoint to the configured remediation portal.

1. Click the **Analysis** tab and select the domain from the **Domain** drop-down list.
2. Select Quarantine. The **Quarantine** page is displayed.
3. Click **Add**. The **Add to Quarantine** pop-up is displayed.

Figure 666. Add to Quarantine



4. Update the following fields:

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal**. Remediation cannot be configured for IPv6 address. The checkbox and the information icon for remediation is not displayed if you enter an IPv6 address in the **IP Address** field.

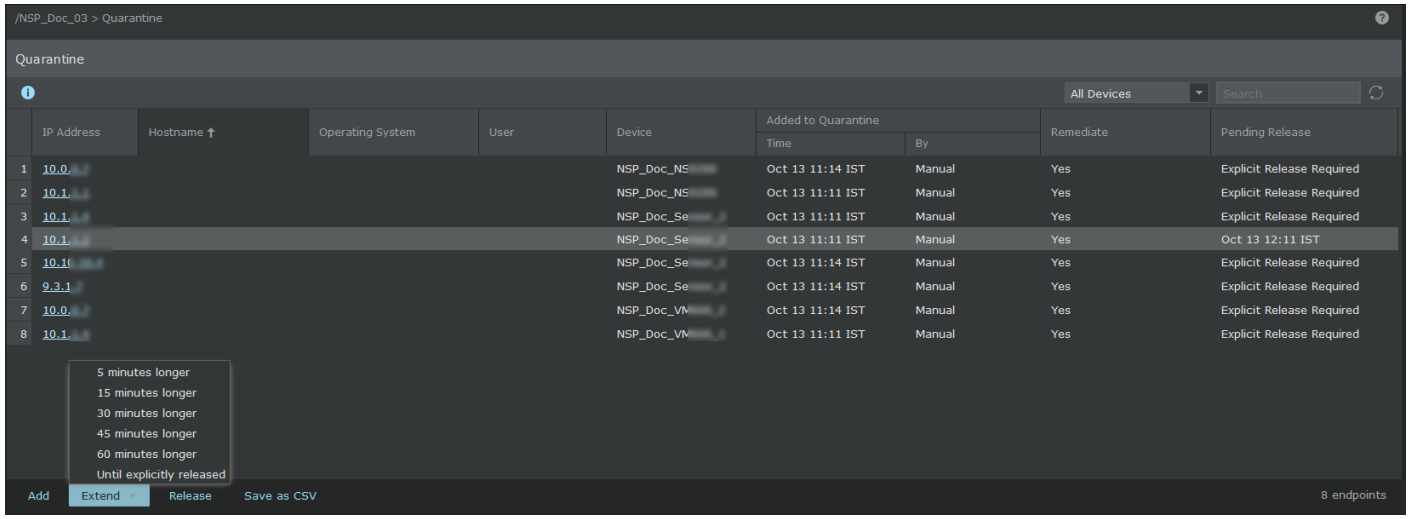
5. Click **Quarantine**. The endpoint is added and displayed in the **Quarantine** page.

Extend quarantine

You can extend the quarantine duration for an endpoint.

1. On the **Quarantine** page, select the row of the endpoint to which you want to extend the quarantine.

Figure 667. Quarantine page



2. Click the **Extend** button and select any of the following options:

Option	Definition
5 minutes longer	Extends the quarantine to 5 minutes.
15 minutes longer	Extends the quarantine to 15 minutes.
30 minutes longer	Extends the quarantine to 30 minutes.
45 minutes longer	Extends the quarantine to 45 minutes.
60 minutes longer	Extends the quarantine to 60 minutes.
Until explicitly released	Extends the quarantine for an indefinite period until you explicitly release the quarantine.

3. Confirm the change in a window message that prompts you to confirm the extension of quarantine.

Release quarantine

You can release the quarantine of the selected endpoint from the **Quarantine** page.

1. On the **Quarantine** page, select the row of the endpoint to which you want to release the quarantine.
2. Click **Release**. A confirmation window message to release the endpoint from quarantine is displayed.
3. Confirm the release of endpoint from quarantine. The endpoint is removed from the **Quarantine** page.

Manually quarantine hosts from Attack Log

From the Attack Log, you can manually quarantine hosts. To quarantine hosts from Attack Log, you must enable **Quarantine** on the corresponding inline monitoring ports. **Quarantine** from Attack Log has no relation to enabling it in the attack definitions. You can also add IP addresses to quarantine from the **Quarantine** page.

NOTE

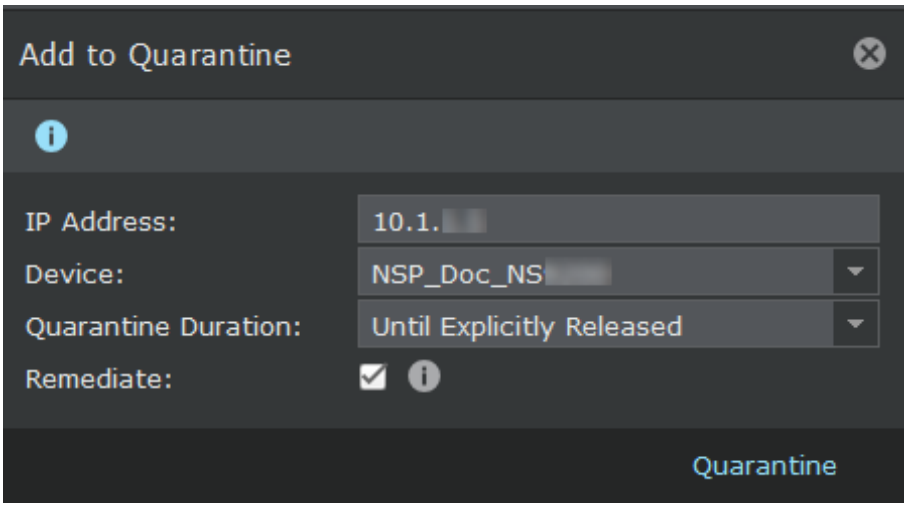
If the source IP is behind a proxy server, the proxy server IP is quarantined. Consequently, all traffic through the proxy server gets quarantined.

Add endpoints to quarantine from Attack Log page

You can quarantine endpoints from the list of alerts displayed in the **Attack Log** page.

1. Navigate to Analysis → <Admin Domain Name> → **Attack Log**.
2. Select the alert whose IP has to be quarantined.
3. Click **Other Actions**, and select **Quarantine Endpoint**. Click the endpoint IP address you want to quarantine.

Figure 668. Add to Quarantine



The **Add to Quarantine** pop-up opens.

4. Update the following fields:

Option	Definition
IP Address	Enter the IP address of the endpoint.
Device	Select the specific device of the endpoint whose traffic originating from the IP address you want to block.
Quarantine Duration	Select the quarantine duration from the drop-down list.
Remediate	Select the checkbox to redirect the configured endpoint to the configured remediation portal. **NOTE** You can configure the remediation portal settings in Devices → Global → IPS Device Settings → Quarantine → **Remediation Portal**.

5. Click **Quarantine**.

View Quarantine options in the Endpoints page

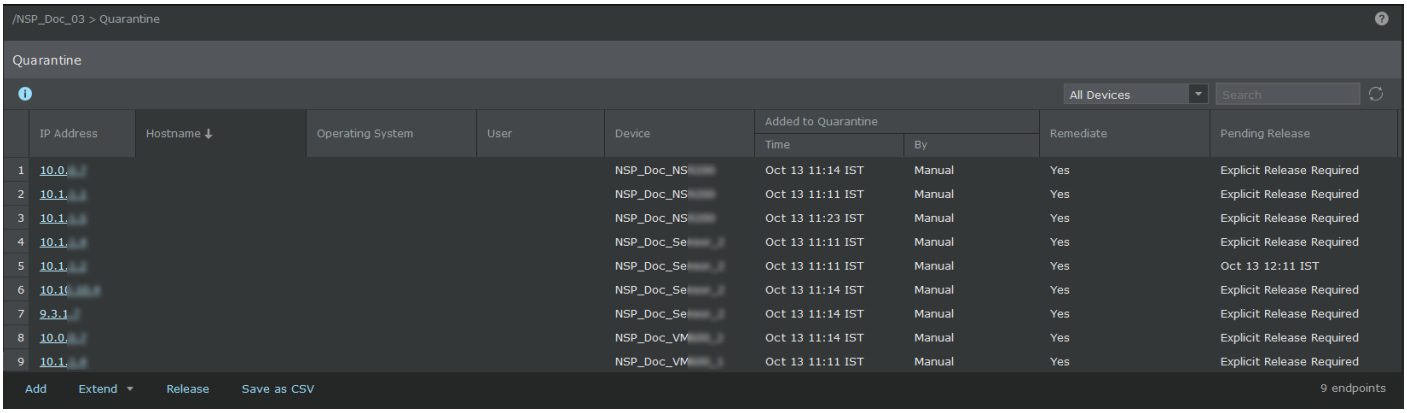
The **Quarantine** page on the **Analysis** tab gives two options for **Quarantine**:

- **Extend**
- **Release**

To select the above options for a quarantined endpoint, do the following:

1. On the **Analysis** tab, select the **Domain** and then the **Quarantine** page.
2. Click **Add** to add an IP address to quarantine.

Figure 669. Quarantine settings

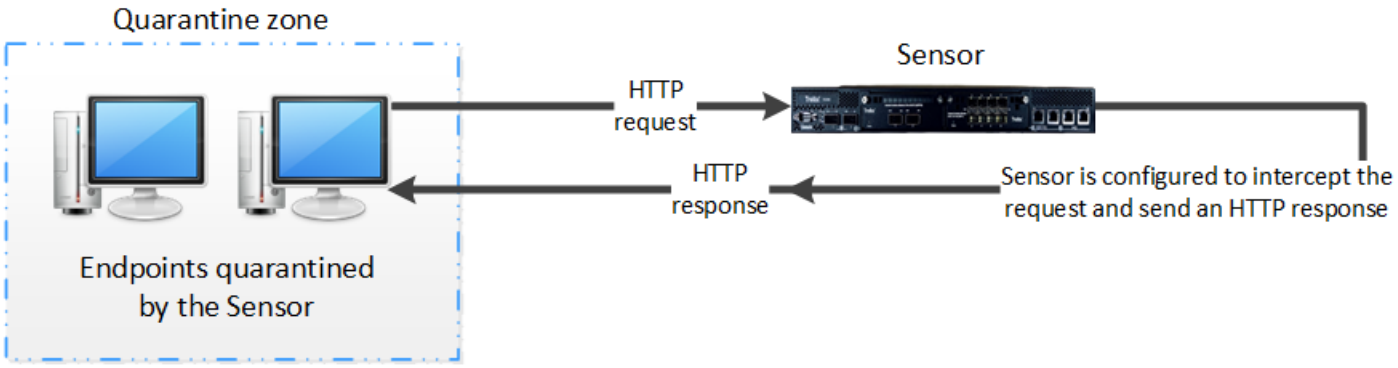


The options are displayed for **Quarantine**:

- **Add** — Add the endpoint from which the alert originated
- **Extend** — Extends the quarantine duration for an endpoint.
- **Release** — Removes the endpoint from **Quarantine**. When you select this option, a message is displayed to confirm if you want to release the endpoint from **Quarantine**. Select the required option.

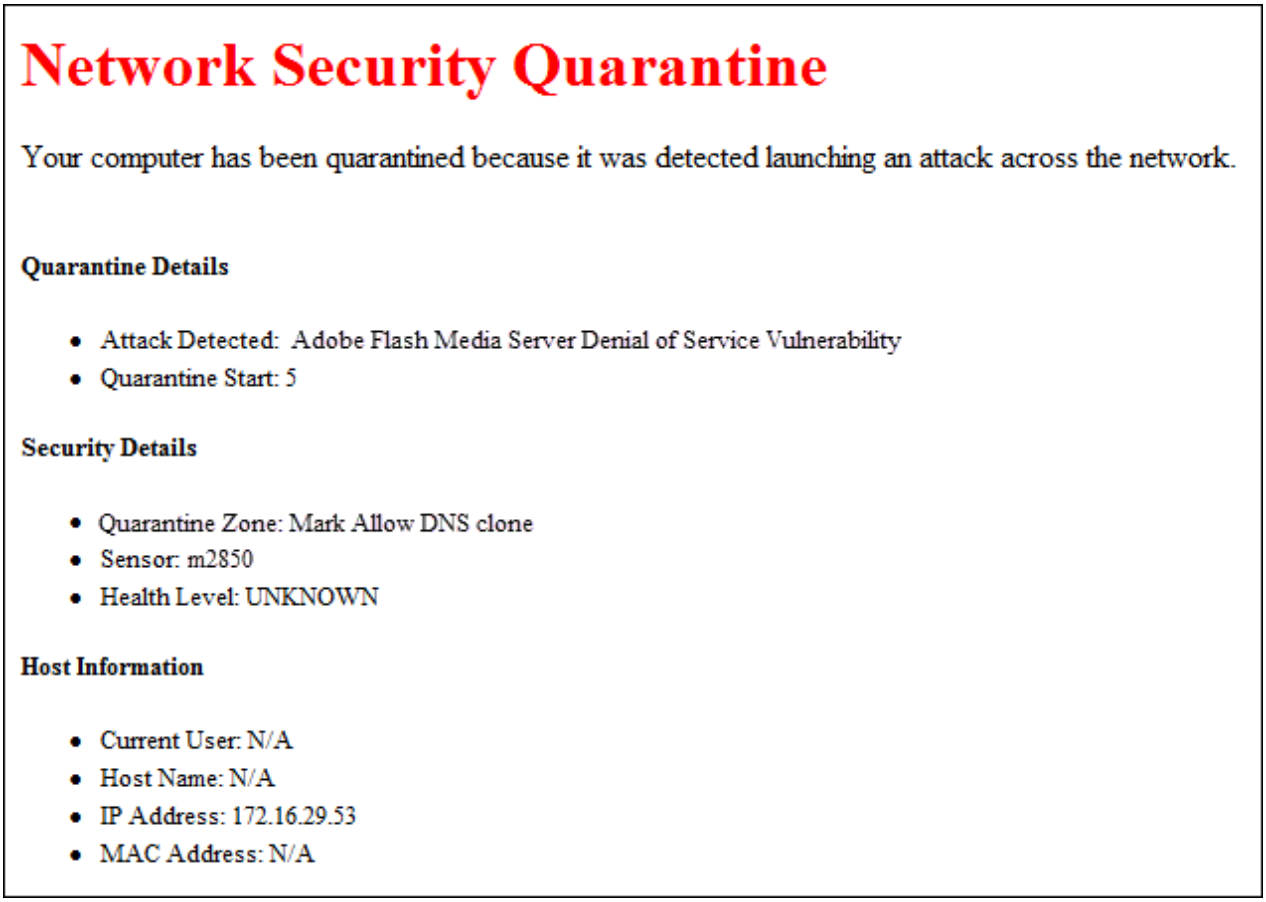
Browser redirect

Figure 670. Browser redirect



When a user attempts to browse to a location outside the **Quarantine Zone**, the Sensor can be configured to intercept the HTTP request and respond with a browser message explaining the reason for quarantine and its duration. Consider the illustration presented.

Figure 671. Browser redirect message sent by the Sensor to the quarantined endpoint



Network Security Quarantine

Your computer has been quarantined because it was detected launching an attack across the network.

Quarantine Details

- Attack Detected: Adobe Flash Media Server Denial of Service Vulnerability
- Quarantine Start: 5

Security Details

- Quarantine Zone: Mark Allow DNS clone
- Sensor: m2850
- Health Level: UNKNOWN

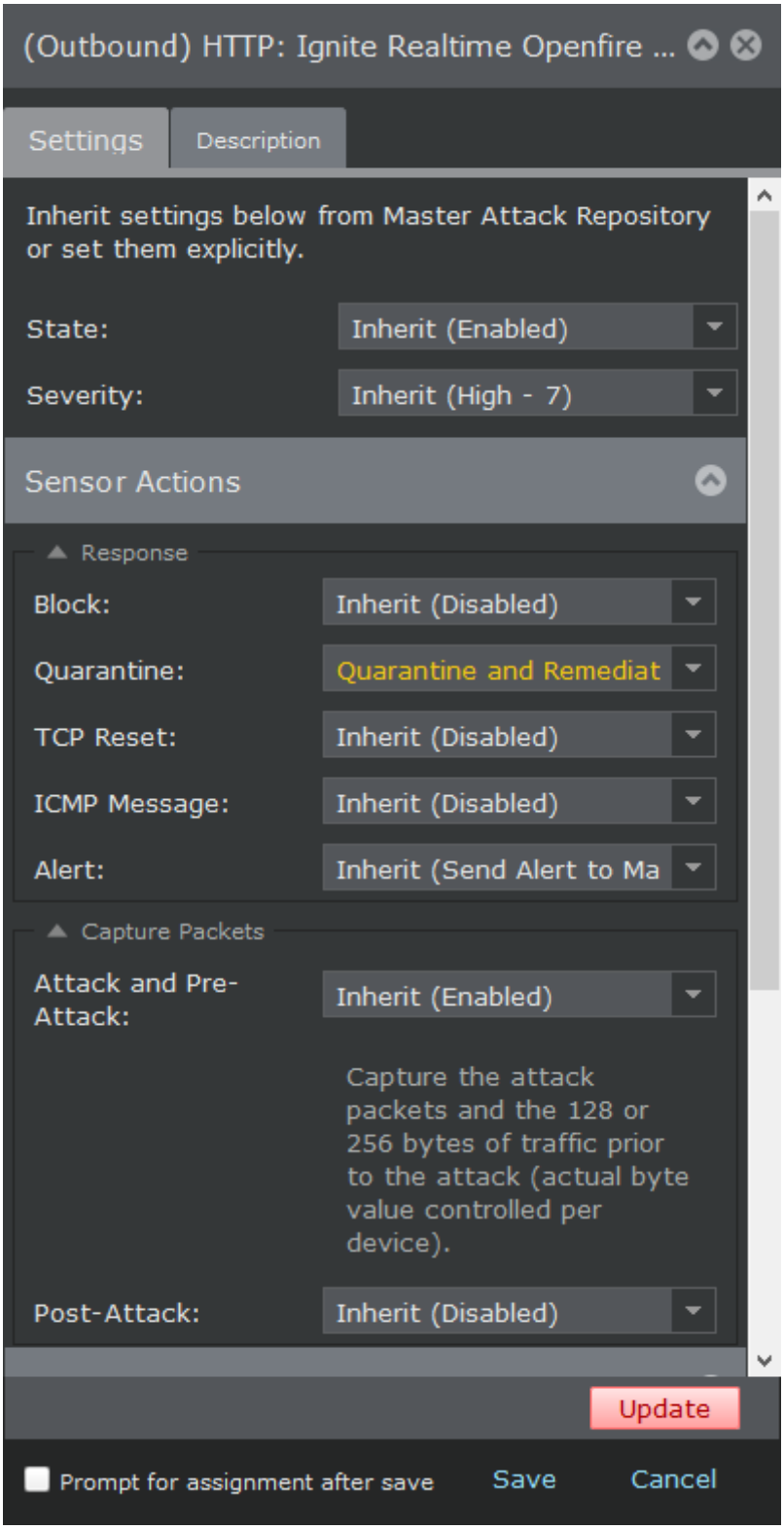
Host Information

- Current User: N/A
- Host Name: N/A
- IP Address: 172.16.29.53
- MAC Address: N/A

Marco's endpoint was quarantined by the Sensor when the Sensor detected the endpoint launching an attack. Now, when he attempts to browse to a business critical finance portal which lies outside the designated **Quarantine Zone**, he receives a notification from the browser stating that his endpoint has been quarantined. What actually happened here was the administrator of Marco's network had configured the Sensor to:

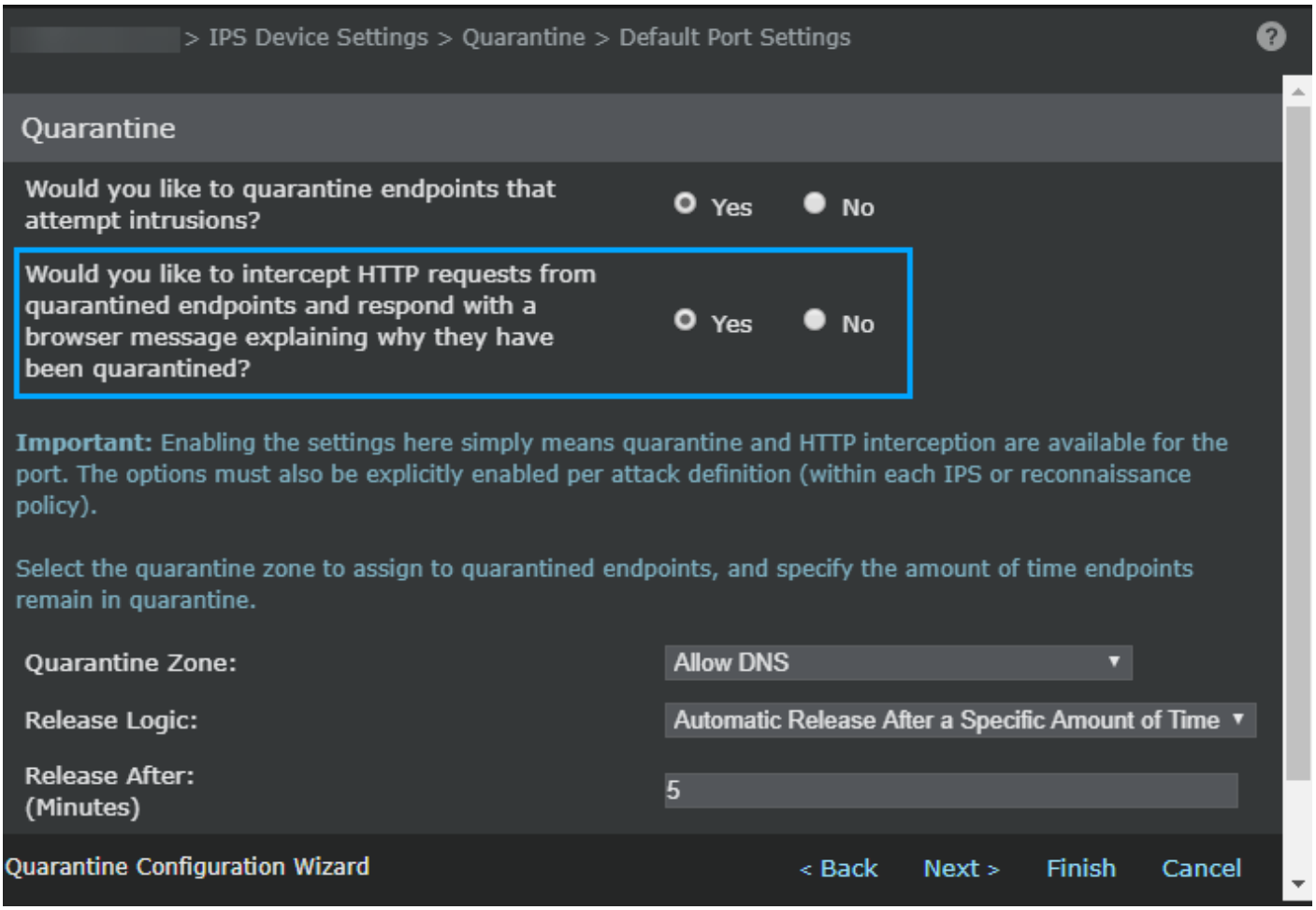
- Quarantine an endpoint if it attempted to launch an attack.
- Respond with a browser message which stated the reason for quarantine if the quarantined endpoint user attempted to access a URL outside the **Quarantine Zone**.

Figure 672. Configuration of Quarantine based on attack



Marco's administrator had firstly enabled quarantine for all the hosts which are generating a specific attack by quarantining the attacker IP. The next thing the administrator did to ensure every quarantined endpoint that generated this attack receives an HTTP response was to select the **Quarantine and Remediate Attacker** option in **Quarantine** drop-down in the **Attack Definitions** page for the policy.

Figure 673. Settings in the Quarantine page for the admin domain



The administrator had then configured the Sensor in the **Default Port Settings** page in the Manager. In order to quarantine any violating endpoints, the administrator enables **Would you like to quarantine endpoints that attempt intrusions?**. And once an endpoint has been quarantined, in order to respond with a browser message, the administrator enables **Would you like to intercept HTTP requests from quarantined endpoints and respond with a browser message explaining why they have been quarantined?**.

Similar configurations of this feature can be done from the following locations in the Manager:

- Quarantine for an admin domain (page 1472)
- Quarantine for a Sensor (page 1476)
- Quarantine configuration in the policies (page 1480)

Inspection of special traffic types

You can configure Trellix IPS to inspect some traffic types that are different from the regular traffic that you see on a network.

IPS on double VLAN tagged traffic

Double VLAN tagging provides access to the infrastructure of Internet service providers (ISPs) in Metropolitan Area Networks (MANs). It allows the service provider to provide certain services, such as Internet access on specific VLANs for specific customers, and yet allow the service provider to provide other types of services for their other customers on other VLANs. VLAN double tagging enables service providers to use a single VLAN to support customers who have multiple VLANs.

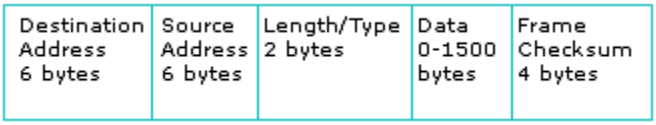
Suppose an enterprise has multiple VLANs across multiple customer sites in a metropolitan area. The enterprise has a higher bandwidth requirement and needs more physical links for communicating with the different VLANs. In such a scenario, double VLAN tagging can be used as a solution.

Here, the enterprise can use ISPs in a public MAN to carry traffic between different customer sites. To identify the Ethernet frames/packets from different customers in the MAN, each frame needs to carry a customer identification tag. That is, a single identification label is needed to identify the VLAN traffic from a customer. With double tagging, another tag/identifier is added to the packets from the VLANs that belong to the same user.

How VLAN tagging works?

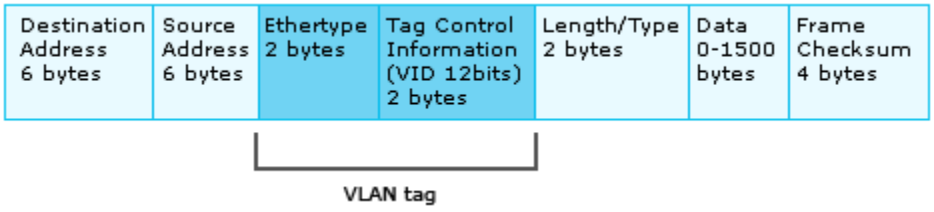
The original Ethernet frame without tagging is shown below.

Figure 674. Original Ethernet frame without tagging



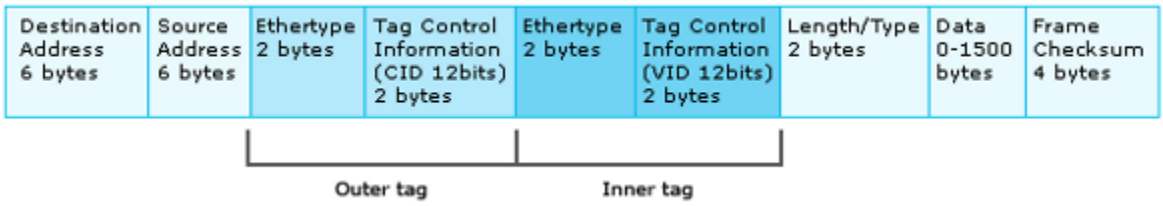
In regular VLAN tagging, a tag/identifier is used to identify the traffic from VLANs.

Figure 675. Regular tagging



In double VLAN tagging, when the frame enters the ISP network, a second VLAN tag is inserted into the frame. This tag is specific to the customer, and identifies the traffic from all the VLANs from that customer. This second tag is also known as the outer VLAN tag or Customer Identification tag (CID). The original VLAN tag is called the inner VLAN tag or VLAN identifier tag (VID).

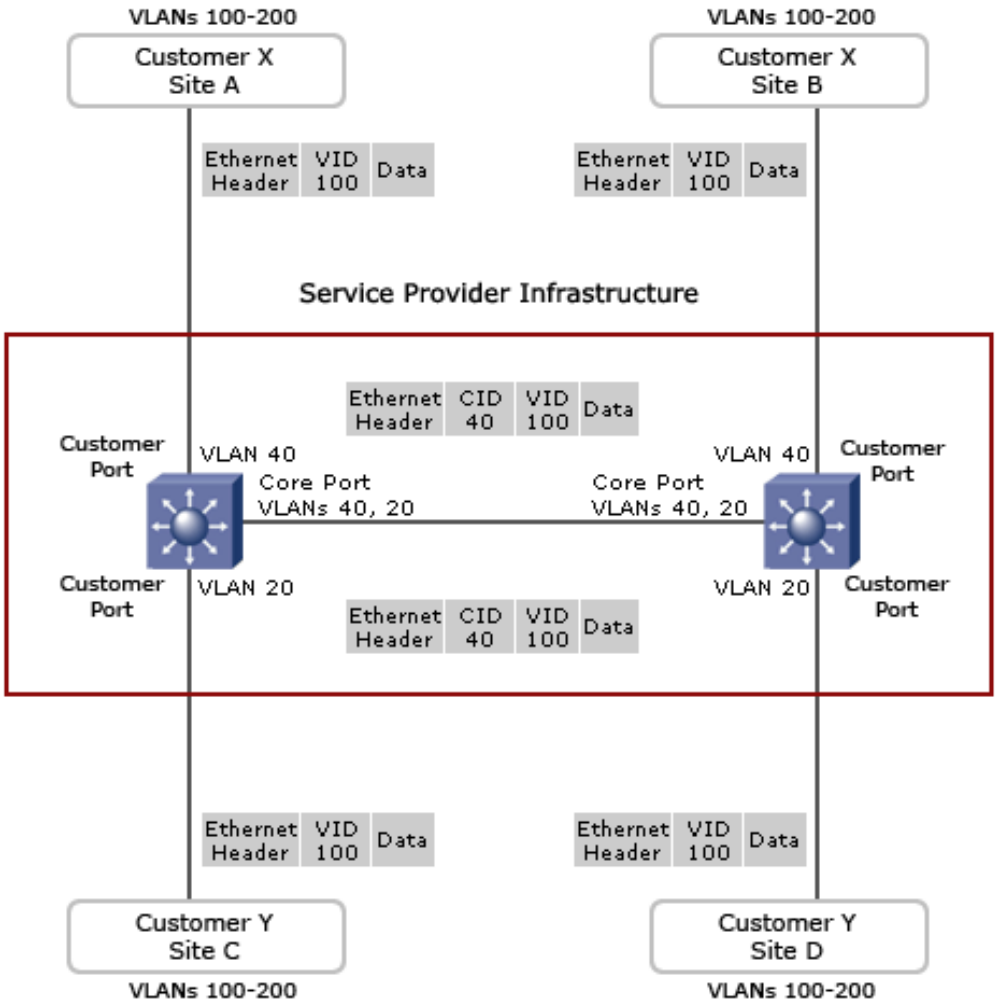
Figure 676. Double VLAN tagging



Scenario for double VLAN tagging

Consider this scenario for double VLAN tagging.

Figure 677. Scenario for double VLAN tagging



Packets entering the customer port of the service provider switch are VLAN tagged packets with original VLAN identifiers (VID) from the customer network. When the VLAN tagged packets exit the core port of the switch into the service provider network,

an additional CID or outer VLAN tag is added on top of the inner VLAN tag. Within the service provider infrastructure, the VID is ignored and bridging is based on the value of the CID. When the double tagged packets enter another core port of the service provider switch, the CID tag is removed and the packets are transmitted to the appropriate customer ports associated with the CID. Therefore, when the packets exit the customer port, the original VLAN tags are preserved.

How Trellix IPS handles double VLAN tagged traffic?

Sensors by default inspect double VLAN tagged traffic for attacks. There is no additional configuration required for inspecting double VLAN tagged traffic.

For double VLAN tagged frames, Trellix IPS uses the VLAN ID in the outer tag (CID). A Sensor uses the outer VLAN tag for identifying the VLAN subinterface the traffic belongs to. For such traffic, only the outer VLAN tag is displayed in the alerts, dashboard, reports and so on.

NOTE

Trellix IPS supports attack detection for double VLAN tagged frames having Ethernet type as 0x8100 in the outer VLAN tag. Frames having outer VLAN tag with other possible Ethernet type values (0x9100 and 0x9200) will be forwarded without parsing for attack detection.

NS-series Sensor models can inspect double VLAN tagged traffic for attacks.

Tunneled traffic

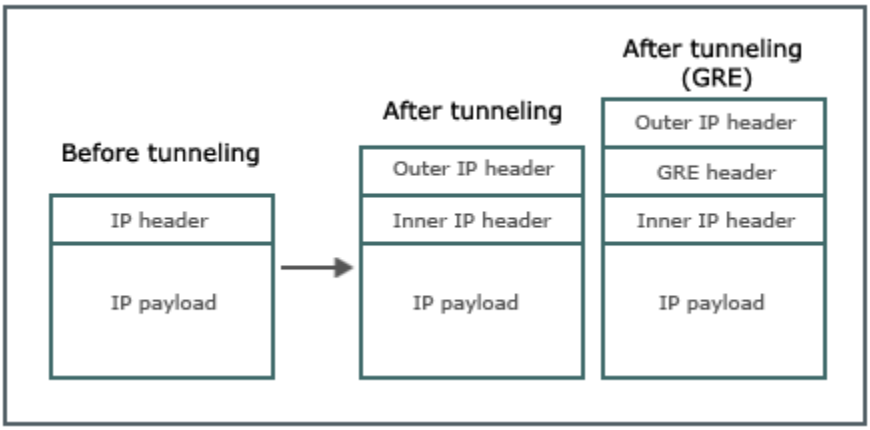
IPv6 packets can pass through IPv4 networks when they are encapsulated in an IPv4 packet. By a similar way, IPv4 packets can also pass through IPv6 networks. This method of encapsulating a packet within another packet of a different protocol to enable the packet to pass through incompatible networks is called as tunneling.

NS-series Sensors support 4 types of tunneled traffic. That is, these 4 types are parsed for attacks:

- IPv6 in IPv4
- IPv6 in IPv6
- IPv4 in IPv6
- IPv4 in IPv4

Multi-level tunneled traffic is not supported. That is, the packets are allowed to pass through but are not parsed for attacks.

Figure 678. Generic diagram of a tunneled packet



Note that an outer IP header is inserted after tunneling, and it contains the tunnel (that is, intermediate) source and destination IP addresses. In case of Generic Routing Encapsulation (GRE) tunneled traffic, an additional GRE header is inserted. The inner header contains the actual source and destination IP addresses.

The following are some key points regarding how the Sensors handle tunneled traffic:

- The Sensor follows the traffic according to the inner header to detect attacks. Therefore, the alerts, dashboards, reports and so on display the details from the inner header. Also, the exception objects are applied on the inner header.
- In case of CIDR subinterfaces, the Sensor uses only the IPv4 header to determine to which CIDR the traffic belongs to. In case of IPv4 in IPv6, it is determined based on the inner IPv4 header. In case of IPv4 in IPv4, it is based on the outer IPv4 header.
- If you have configured Firewall, note that Firewall access rules are applied only to the outer header. Also, the destination IP protocol number should be set to 4 or 41 for tunneled traffic and 47 for GRE tunneled traffic in the Firewall access rules.
- TCP resets to the source or destination host at the time of detection include the outer header as well as the inner header. TCP reset from an alert through SNMP is not supported for tunneled traffic. Reset unfinished three-way handshake option does not work for tunneled traffic.
- Only IPv4 traffic is parsed for DoS attacks. For tunneled traffic, Sensors use the inner IP header to detect DoS attacks. Therefore, DoS attack detection for tunneled traffic is applicable only if the inner IP header is an IPv4 header.
- All NS-series Sensor models can parse GRE tunneled traffic:

  The other Sensors simply allow the GRE tunneled traffic to pass through.
- Only GRE version 0 is supported.
- GRE traffic with sequence number options is just forwarded without being parsed.
- GRE traffic with routing headers is just forwarded without being parsed.
- For Sensors in fail-over mode, you need to enable tunneling on both the member Sensors for GRE tunneled traffic to be parsed.

> **NOTE**
>
> Tunneling is disabled by default.

The following CLI command is available for tunneling:

- **`show parsetunneledtraffic status:`** To know the current tunneling configuration status of a Sensor.

For details, see the [CLI commands] section.

Jumbo frame parsing

Jumbo frames are Ethernet frames, which carry larger payloads per packet than the standard Ethernet frame. They are designed to enhance network throughput and improve CPU utilization for large file transfers, by enabling more efficient payloads per packet. For example, a jumbo frame size packet can carry more than 1500 bytes of payload in an Ethernet frame.

Trellix IPS parses jumbo frames in attack detections. Sensors support jumbo frame parsing in the inline, tap, and SPAN modes.

The following Sensor models support jumbo frame parsing of up to 9,216 bytes (9 KB) of IP payload:

- IPS-VM600 and IPS-VM5000 on ESXi and KVM
- NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, and NS3600

> **NOTE**
>
> 1 Gigabit Sensor ports will inline forward jumbo frames that are greater than 9KB (9216 bytes) of IP payload and up to 9724 bytes. Frames with IP payload greater than 9724 bytes will be dropped on a 1 Gigabit port. However, 10 Gigabit Sensor ports will inline forward jumbo frames greater than 9KB (9216 bytes)of IP payload and up to 16KB (16384 bytes). Frames with IP payload greater than 16KB will be dropped on a 10 Gigabit port.

Jumbo frame parsing is not supported on NS3500, NS3200, and NS3100 Sensors.

Sensor functions with jumbo frame support

Review this section to know how some of the features work with respect to jumbo frames.

IPS attack detection — The Sensor detects all attack types (Reconnaissance, DoS, Exploit, HTTP response-based attacks etc) in jumbo frames for both IPv4 and IPv6 traffic. Attacks are also detected in fragmented and non-fragmented jumbo frames with VLAN, double VLAN and MPLS header. The Sensor detects attacks in fragmented jumbo frames up to 9216 bytes (9KB) in the IPv4/IPv6 traffic.

The IPS Sensor interface type can be of any type such as dedicated, VLAN, and so on.

Note that the Sensor also detects attacks in jumbo frames targeted to the non-standard ports.

According to the configured attack response actions, the Sensor responds or blocks the packets. Alerts are raised in the Attack Log as with the standard Ethernet frames.

Trellix Custom Attack detection — The Sensor detects custom attacks in jumbo frames and alerts are raised in the Attack Log.

IP Spoofing detection — The Sensor drops IP spoofed packet received in a jumbo frame.

Fail-open and fail-close modes — The Sensor supports fail-open and fail-closed modes for jumbo frames.

Traffic management — If the jumbo frames are of size less than 9,216 bytes, the Sensor implements the QoS policies for DiffServ tagging and VLAN 802.1p tagging.

Syn cookie handling — When SYN cookie is enabled on the Sensor in conjunction with jumbo frame parsing, you may experience TCP segmentation for application with payloads greater than the Sensor-advertised MSS, resulting in non-jumbo frames even if the network path supports jumbo frames. This will result in performance degradation since the endpoints exchange non-jumbo frames in spite of the network path supporting jumbo frames.

Firewall policies — When jumbo frame parsing is enabled in the Sensor, Firewall access rules are applied as configured for jumbo frames of size up to 9216 bytes (9KB).

Snort Custom Attack detection — When jumbo frame parsing and Snort are enabled, the Sensor detects Snort attacks (if any) in the jumbo frames. Attacks are also detected in fragmented jumbo frames where the Snort signature falls in more than one fragment.

GRE tunneled traffic — When the tunnel configuration and jumbo frame parsing are enabled, the Sensor performs IPS detection on the GRE-tunneled traffic received as jumbo frames.

Jumbo frame parsing is also supported with quarantine, port clustering, fail-over, layer 2 mode, malware analysis, and Sensor performance monitoring.

Enable jumbo frame parsing

For the Sensor to inspect jumbo frames for attacks and other supported IPS features, you must enable jumbo frame parsing at the Sensor level.

> **NOTE**
> Jumbo frame traffic with SSL encryption will not be decrypted even if SSL decryption is enabled.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **IP Settings**.

Figure 679. Common IP Parameters dialog

6. In the **Common IP Parameters** section of the **IP Settings** page, select **Enabled** from the **Jumbo Frame Parsing** drop-down list and click **Update** to update the Sensor of the configuration change.
7. Reboot the Sensor for the changes to be effective.

> **NOTE**
> For Sensors in a HA pair, jumbo parsing must be enabled on each member Sensor of the HA pair.

IPS for mobile networks

Usage of phones has increased by many folds in the past decade. Industry analysts claim that there are around 4 billion mobile phones in use worldwide for 7 billion people, apart from the millions of tablets. Networks are under a constant threat as more and more people use mobile phones. A small vulnerability in the network could expose all the phones connected to different attacks. The user of the phone may sometimes not even be aware of the attack. With the widespread use of internet on the phone, mobile networks face the same threats as computers. This section talks about different ways in which Trellix Intrusion Prevention System enables you to protect mobile networks from malware attacks.

Parsing of GTP Tunneled traffic

Trellix Intrusion Prevention System provides comprehensive protection against various malware attacks for mobiles. The GTP (GPRS Tunneling Protocol) parsing provided in the Sensors scans network traffic and when attacks are detected, raises alerts in the Manager. Based on the attack detected on the mobile networks and based on the policies configured for that particular type of attack, the Sensor will initiate necessary actions.

NOTE

Parsing of GTP tunneled traffic works on NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3200, and NS3100 Sensors only.

Terminologies

Before starting to understand how Trellix IPS works in conjunction with GTP, following are few terminologies which will help understand the feature better:

- **General Packet Radio Service (GPRS)** — This is packet-oriented mobile data service which uses either second generation (2G) or third generation (3G) cellular communication to transmit data on the system's GSM, UMTS and LTE networks.
- **Global System for Mobile communication (GSM)** — This is a standard used to describe protocols for 2G and 3G cellular networks used by mobile phones.
- **Universal Mobile Telecommunications System (UMTS)** — This is a GSM based standard for the third generation mobile cellular network that includes authentication of users through SIM cards.
- **Long-Term Evolution (LTE)** — This is a standard for high speed data for mobiles and data terminals based on wireless communication.
- **Gateway GPRS Support Nodes (GGSN)** — The GGSN is used for internetworking between the GPRS and external packet switched networks.
- **Serving GPRS Support Nodes (SGSN)** — The SGSN is responsible for delivery of data packets to and from the mobile stations within the mapped geographical service area.
- **GTP user data tunneling (GTP-U)** — This is an IP based tunneling protocol used by GTP for carrying user data between the SGSN and GGSN.
- **GTP Control (GTP-C)** — This is used within the GPRS core network for signaling between GGSN and SGSN.
- **GTP version 1 (GTPV1)** — GTP uses the sub-protocols, GTP-C and GTP-U for communication. GTPV1 uses only UDP for communication. It uses port 2152 for communication and transmitting data.
- **Gn** — This is an IP based interface between SGSNs, other SGSNs and internal GGSNs (in the same geographical location, when not in roaming).

- **Gp** — This is an IP based interface between internal SGSN and external GGSN (when the network is in roaming).
- **Gi** — This is an IP based interface between the GGSN and Public Data Network (PDN) directly to the internet or through a WAP gateway.
- **Internet Protocol Security (IPsec)** — This is a protocol used for securing and authenticating each IP packet during communication.
- **Layer 2 Tunneling Protocol (L2TP)** — This is a tunneling protocol to support virtual private networks.
- **Point-to-Point Protocol (PPP)** — This is a data link protocol used to establish direct connection in physical networks.

Types of attacks possible

Attacks can be in the form of systematic overloading of the network with a small amount of traffic using the signaling overload. The network is choked with unwanted traffic in the form of bots, worms, DoS. Even a systematic low bandwidth of <256 Kbps of unwanted scan traffic can cause signaling overload and cause service disruption.

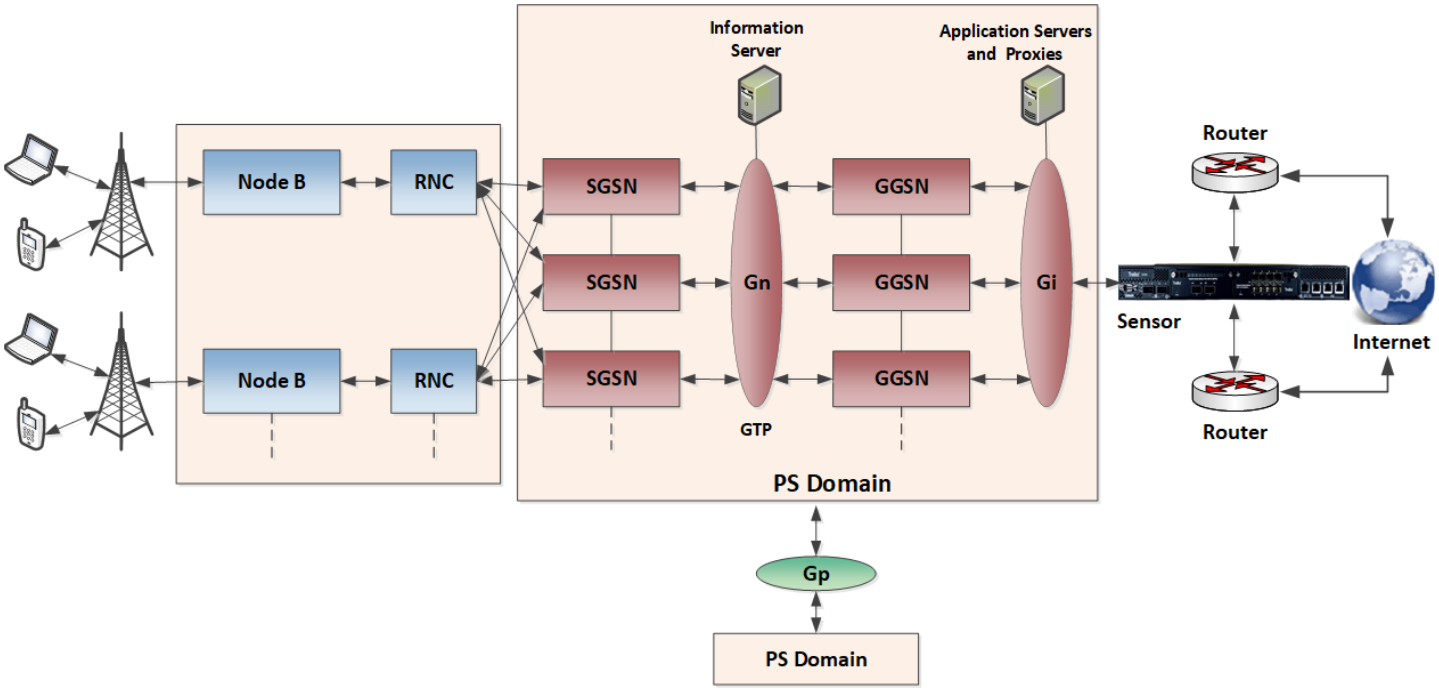
Following are some of the types of attacks against which Trellix IPS provides protection:

- Sending unsolicited traffic from one mobile to other mobiles.
- Paging attack where the network bandwidth is clogged with concentrated flash crowds due to low bandwidth which is similar to a DoS attack.
- Attacks that are based on dedicated channel (DCH) assignment
- Most of the third generation networks inherit known problems from the parent technologies like different forms of TCP/IP vulnerabilities.
- Interception and impersonation attacks steal the information that is transmitted over the cellular network by breaking the confidentiality or integrity. This is due to lack or weak authentication and encryption mechanisms for GSM/UMTS.
- Sending unsolicited traffic from the internet towards a large group of mobile connections results in battery depletion and overbilling attacks.
- Security weaknesses in the IP Multimedia Subsystem (IMS) results in bringing down an entire network by loading a single component in the signaling path, with a low bandwidth traffic.
- SMS flooding attack is typically by loading signaling channels on which SMS are transmitted.

GTP Decoding

When the IPS Sensor is deployed in a mobile network it parses all the traffic flowing in the network. When it detects any malicious traffic, the Sensor raises alerts accordingly. The Sensor also looks for vulnerabilities in the mobile network, which could lead to an attacks in the future.

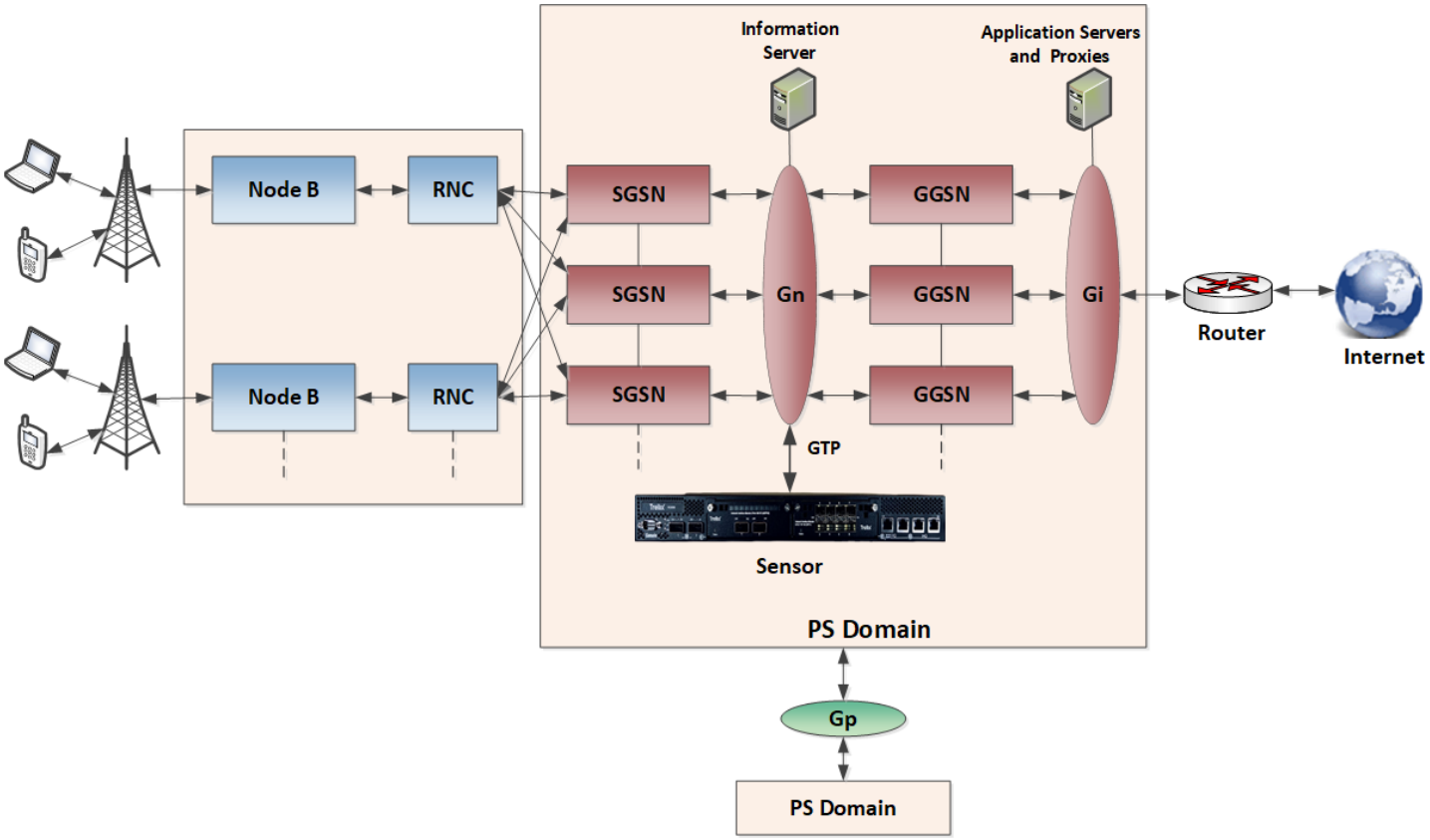
Figure 680. IPS inspection of mobile network without GTP decoding



During GTP parsing, the Sensor is deployed either in inline or SPAN/TAP mode. The Sensor is deployed on the Gn/Gp interface to detect handset-to-handset malicious communication, internal or external attacks. The Sensor parses the traffic between SGSNs and GGSNs for any attack and also inspects the IP payload. The Sensor only parses the GTP-U traffic and drops the GTP-C traffic. The Sensor inspects the UDP header for the underlying protocol and the subscriber IPv4 or IPv6 traffic. Other subscriber traffic such as the IPSec, L2TP, PPP are bypassed and not inspected for attacks. IP datagrams transmitted from the internet can sometimes be fragmented. The Sensor defragments these datagrams for any malicious traffic. The Sensor is capable of handling high rate data of GTP traffic, upto 8Gbps because of the internal load balancing design.

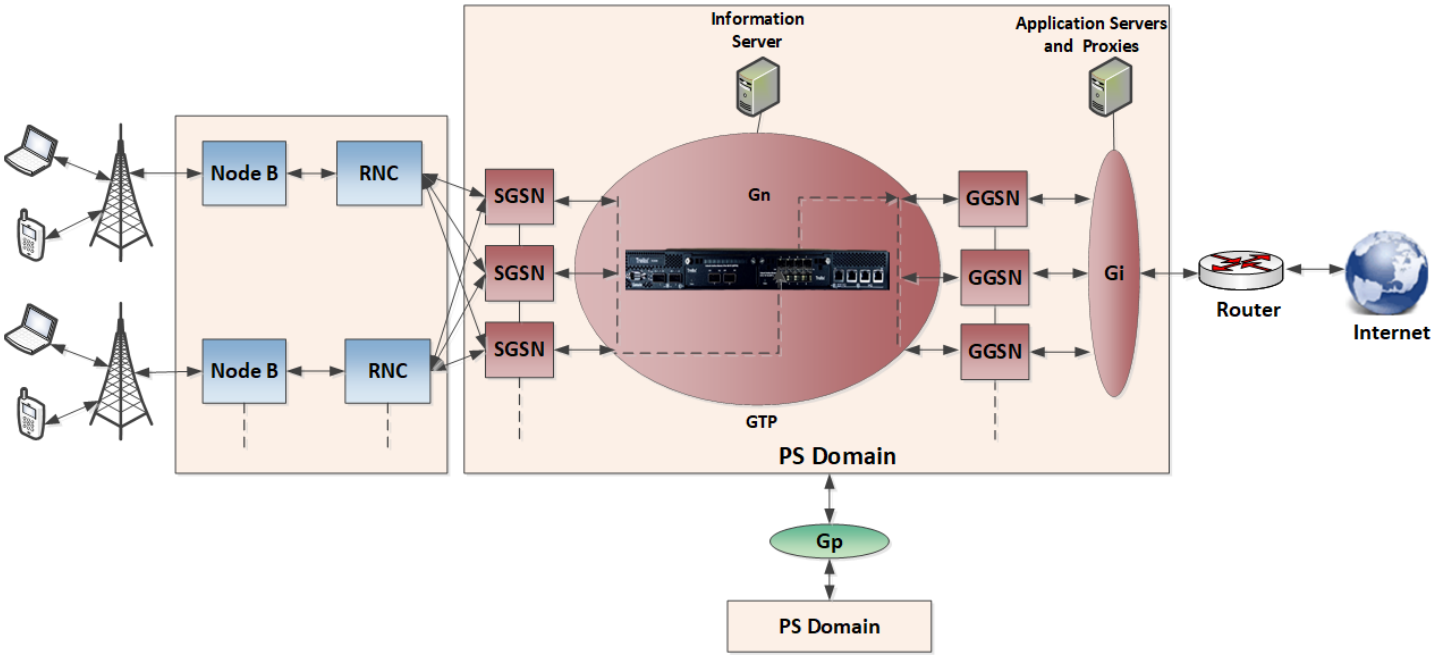
The Sensor has ports connected to a SGSN's Gn interface in either inline or SPAN/TAP modes and parses the GTP tunneled traffic. Any request from a mobile is first sent to the nearest tower which then connects to the Radio Network Controller (RNC). The RNC then encrypts the data packets before sending it to the nearest SGSN. The data packets are then transmitted to other SGSN or GGSN via the Gn interface or to other GGSNs via the Gp interface. The Sensor placed between the SGSN and the GGSN, that is connected to the Gn interface, inspects the packets for vulnerability or malicious contents before forwarding the packets.

Figure 681. GTP parsing by the Sensor in SPAN mode



In the inline mode, after the data packets are processed, the Gi interface forwards the packets to the internet to gather the requested information. The requested information packets are then forwarded back to the mobile. The Sensor deployment in inline mode is illustrated below:

Figure 682. GTP parsing by the Sensor in inline mode



Subscriber information from RADIUS regarding data usage is submitted to the Sensor together with the attacks seen on GTP-U traffic. The information extracted by RADIUS Accounting helps retrieve subscriber information as a part of the alerts/events.

Enable mobile malware detection

Following are the steps to enable mobile malware detection:

1. The GTP feature is disabled on the Sensor by default. You can enable the GTP feature on the Sensor by using the these steps:
   - Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **Advanced Device Settings** and select **Inspect Tunneled Traffic** and click **Save**. This enables parsing of traffic for all supported tunneling protocols including GTP for malware detection. By default, this checkbox is deselected.

     NOTE

     At an admin domain level, configure this for multiple Sensors by navigating to Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings** and select **Inspect Tunneled Traffic** and click **Save**.

   - Check the status of tunneled traffic with this CLI command:

     Syntax:

     `show parsetunneledtraffic status`

     Displays the status of the current tunneling configuration of the Sensor.
2. Enable GTI File Reputation under Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **Advanced Malware** and click +.
   - To create a new policy and enable the GTI File Reputation for the required file type, navigate to Policy → <Admin Domain Name> → Intrusion Prevention → **Policy Manager**.

3. Configure the DNS Server under Devices → <Admin Domain Name> → Global → Common Device Settings → **Name Resolution**.

   For more information, see section Configure the DNS server details (page 1280), chapter [Configure Firewall Policies].

4. Set the policy to Default Prevention under Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.

   NOTE

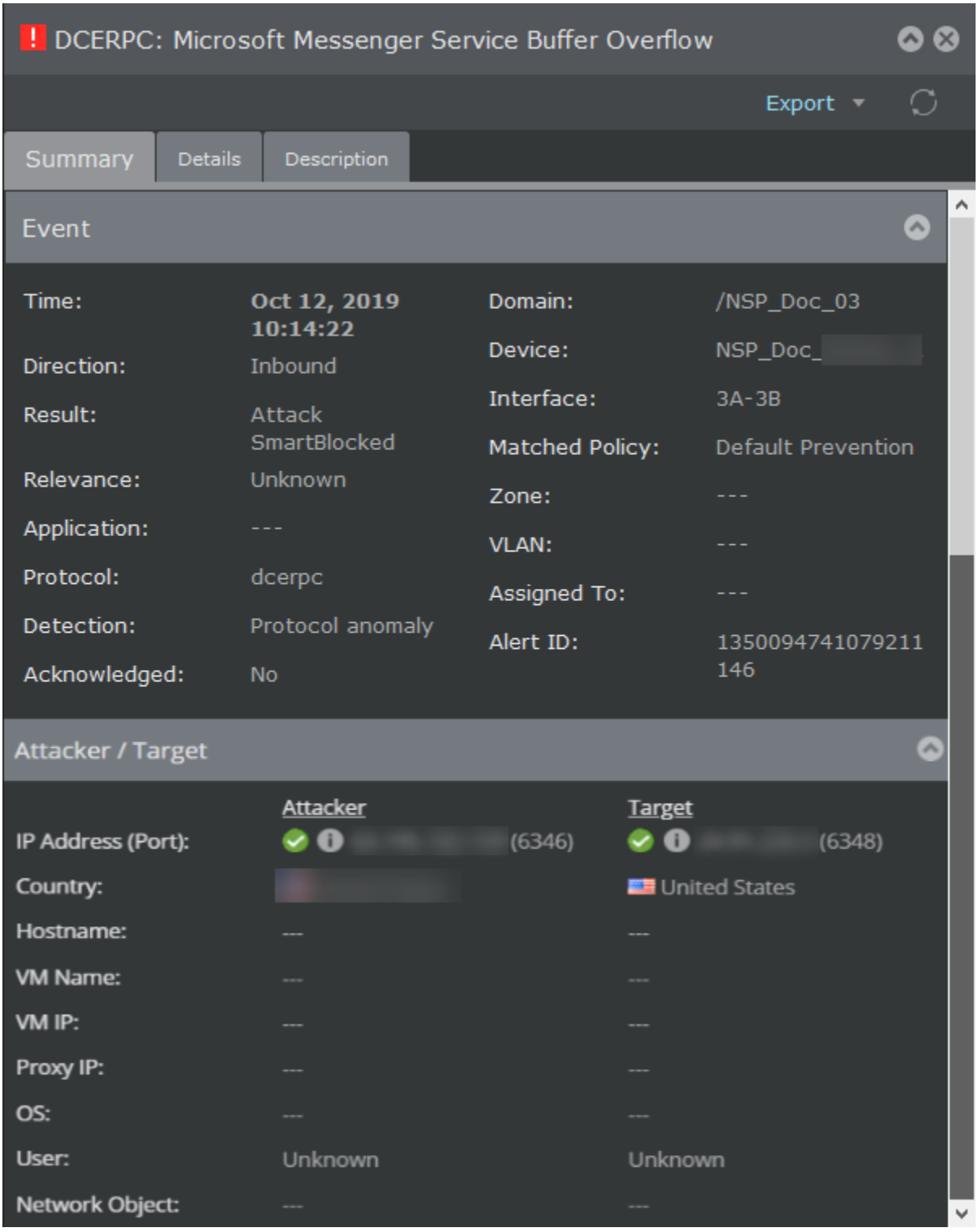
   The Default Prevention policy is set by default. In case it is not set, then navigate to the above mentioned path to set it.

5. You can set and view the following policy details configured in the Manager:
   - Reconnaissance attack details
   - Callback Detector details
   - Network Forensics details
   - Packet Capture details
   - Customizing scan attack details

   Trellix IPS generates alerts and events, which help keep track of the malware, bots, worms detected.

You can view the attacker and target IP addresses from where the attack was generated when GTP feature is enabled. The alerts can be viewed in Attack Log which also displays the details of the attack.

Figure 683. The inner attacker and target IP address as displayed in the alert



Monitoring subscriber and RADIUS accounting traffic

Trellix Intrusion Prevention System enables you to monitor traffic in a mobile network. IPS for mobile networks is supported for NS-series models.

Sensors deployed in mobile networks monitor subscriber traffic and RADIUS accounting traffic that goes out of GGSN to Internet gateway and RADIUS servers. Each mobile device in the network has an IP address. When IPS inspection is enabled using the **`set mnsconfig`** command, the Sensor parses RADIUS accounting exchanged between GGSN and the RADIUS server and forms an association of IP addresses and subscriber mobile identity details like phone number, IMSI number, and APN. The Sensor also associates the attacks that are detected on the internet traffic with the mobile subscriber identity data and includes them in alerts sent to the Manager.

Due to the use of fixed source and destination ports in all RADIUS packets that are exchanged over UDP by the GGSN/RADIUS server, there is a possibility that the Sensor could miss parsing RADIUS accounting traffic at high data rates. This situation can be avoided by using the **`set mnsconfig radiusLB`** CLI command.

When the mobile security feature is enabled, Sensors can detect application download on Android (.apk file) and work with Trellix GTI File Reputation to detect/block malware.

You can monitor subscriber and RADIUS accounting traffic using the following CLI commands:

- **`set mnsconfig on/ off`**: Enables capturing and tagging of mobile subscriber data in the alerts sent to the Manager. This feature is disabled by default. Mobile entries are not persisted across a Sensor reboot.
- **`set mnsconfig radiusLB on/ off`**: Enables/ disables RADIUS traffic load balancing
- **`show mnsconfig`**: Displays the status of mobile network security (enabled or disabled)

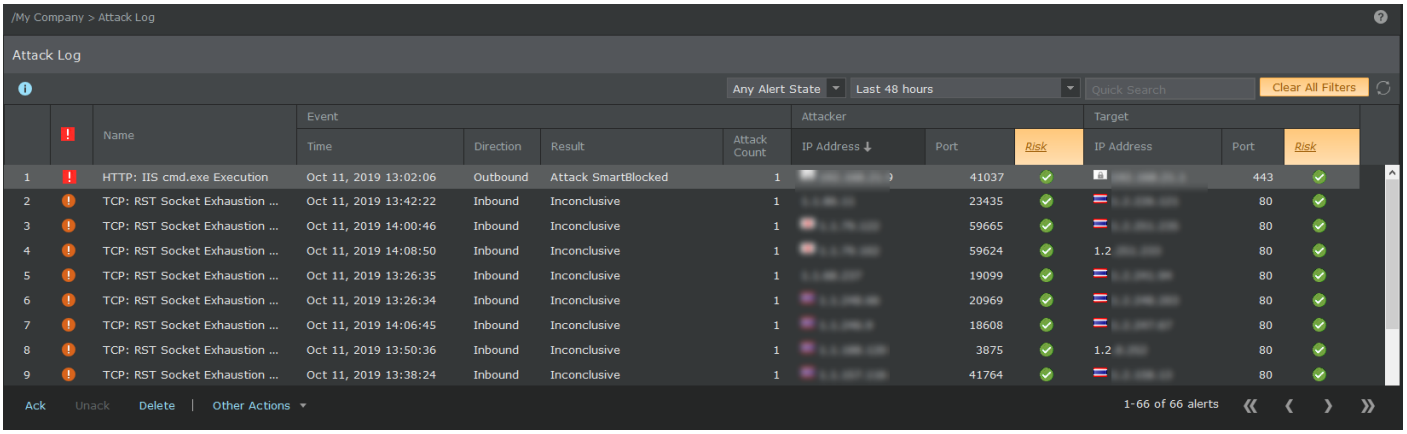
For more information on the CLI commands, see the [CLI commands] section.

View mobile alerts in Attack Log

The Attack Log displays the following new fields for mobile alerts:

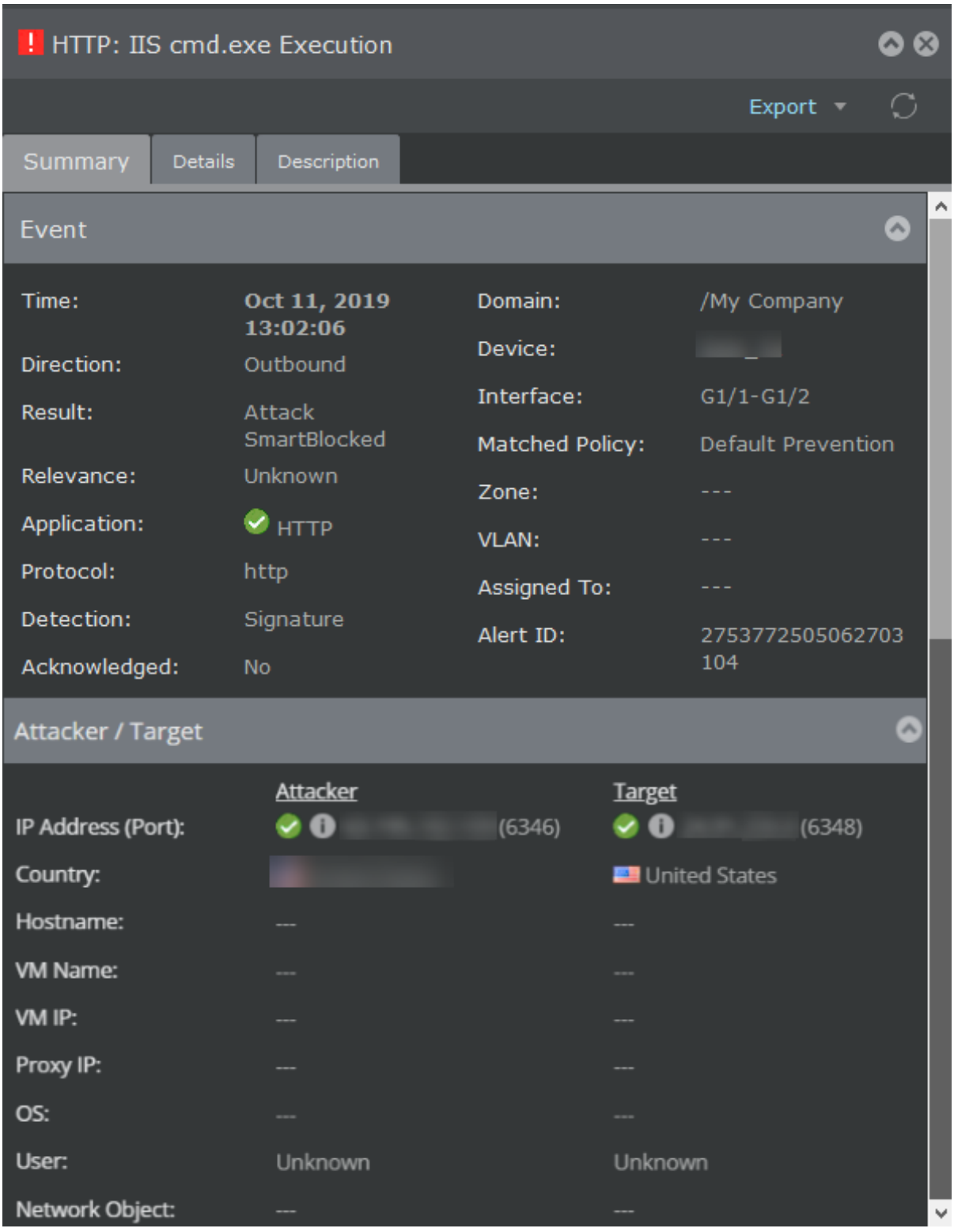
- Attacker Phone Number — attacker mobile phone number
- Attacker IMSI — attacker International Mobile Subscriber Identity (IMSI)
- Attacker APN — attacker Access Point Name (APN)
- Target Phone Number — target mobile phone number
- Target IMSI — target International Mobile Subscriber Identity (IMSI)
- Target APN — target Access Point Name (APN)

Figure 684. Mobile alerts



You can view mobile related alerts, when the IPS for mobile networks is enabled and the attack is to/from a mobile phone.

Figure 685. Alert details



Troubleshooting support

The following debug commands are supported:

- mobileDbg delete

  Clears the mobile entries: IP, Phone, IMSI and APN.

  Syntax:

  `moblieDbg delete`

- mobileDbg print

  Displays the mobile entries: IP, Phone, IMSI and APN.

  Syntax:

  `moblieDbg print`

Advanced Traffic Inspection

In recent times, the design of the network protocols (mechanism to send and receive data to end applications) has exposed vulnerabilities that allow data to bypass information security devices to deliver an exploit or attack to target networks. The network traffic uses encoding or encryption techniques to evade detection. Trellix IPS provides a mechanism to perform advanced inspection on such traffic. Using **Advanced Traffic Inspection**, the following traffic segments are decoded/reassembled:

- The SMTP protocol specification does not address the transfer of binary data, so binary data is encoded to that end. Base64/Quoted-printable encoded PDF files in SMTP traffic can now be inspected to detect threats or anomalies.
- The HTTP response traffic might contain chunked payloads. Such payload chunks can be reassembled, facilitating the detection of any threats or anomalies.
- The HTTP response traffic might contain encoded PDF files. Such encoded files in the HTTP response traffic can be inspected to detect any threats or anomalies.
- MS RPC/SMB traffic can be fragmented, segmented, or both. Such data can be reassembled to detect any threats or anomalies.

NOTE

When Advanced Traffic Inspection is enabled in a deployment with 90 percent good traffic and 10 percent traffic that uses evasions, the Sensor throughput could drop by approximately 5 percent.

Configure Advanced Traffic Inspection at the interface or sub-interface level

Advanced Traffic Inspection is disabled by default and inspects traffic per VIDS. You can enable it in the **Policy Manager** page of an interface or subinterface.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to inspect traffic for.
3. Navigate to Intrusion Prevention → **Policy Manager**.
4. On the **Interface** tab, double-click the interface to enable the advanced traffic inspection.

The **<Device Name/Interface>** panel opens.

5. In the **Inspection Options** section, select the policy from the **Policy** drop down list.

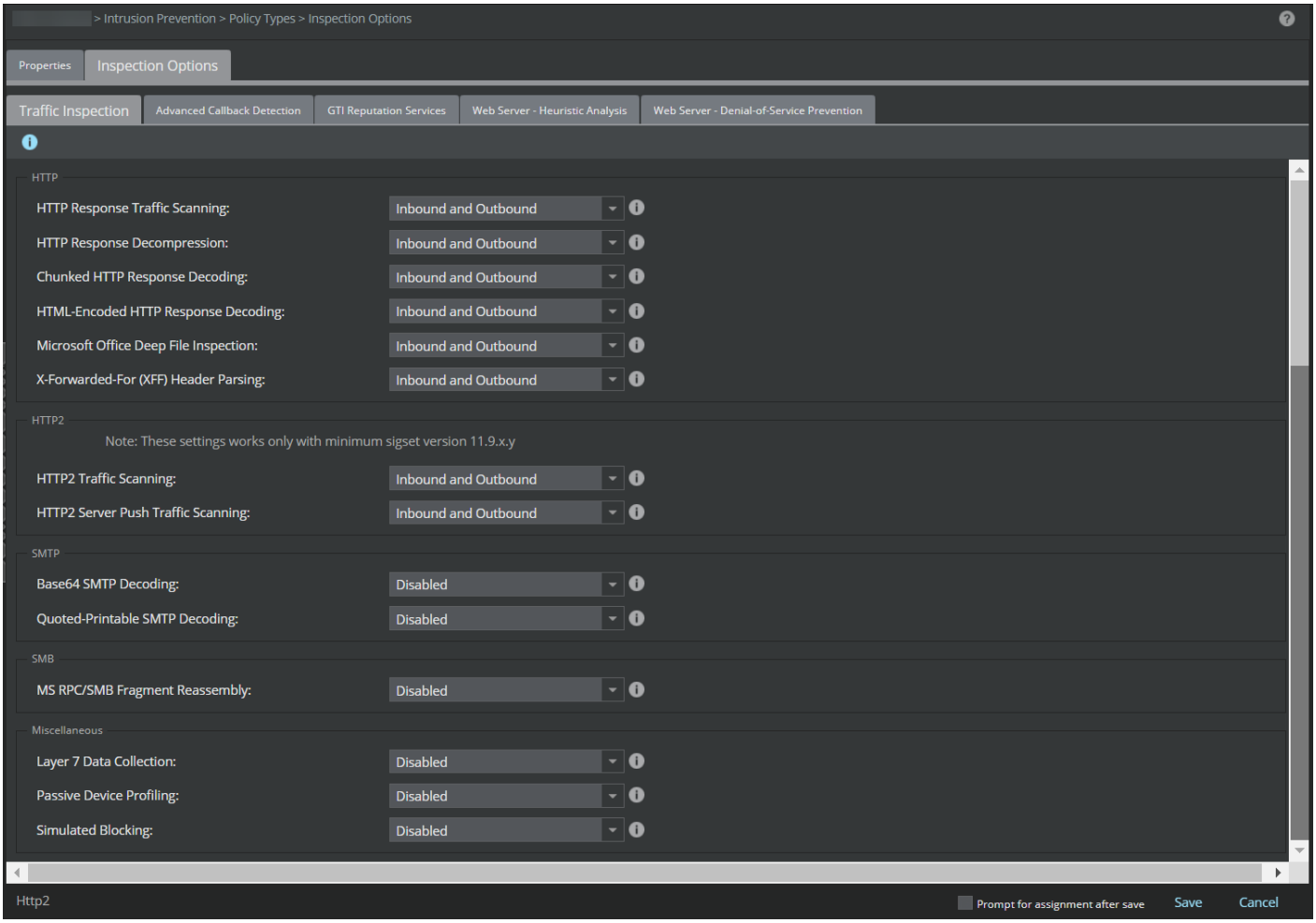
   To create a new policy, click the + icon or double-click on the policy to edit an already assigned policy.

   If you are creating a new policy proceed to step 6. If you are editing an existing policy proceed to step 7.

6. The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and click **Next**.

   The **Inspection Options** page opens.

Figure 686. Configure Advanced Traffic Inspection



7. In the **Traffic Inspection** tab, under **HTTP**, enable **HTTP Response Traffic Scanning** in the required direction to enable **Chunked HTTP Response Decoding**, **HTML-Encoded HTTP Response Decoding**, **HTTP2 Traffic Scanning** and **HTTP2 Server Push Traffic Scanning**.
8. Under **SMTP**, enable **Base64 SMTP Decoding** and **Quoted-Printable SMTP Decoding** in the required direction.
9. Under **SMB**, enable **MS RPC/SMB Fragment Reassembly** in the required direction.

NOTE

The options that explicitly mention HTTP response traffic require HTTP Response Scanning to be enabled in that same direction. These options are disabled if the HTTP response traffic is disabled.

Option	Definition
Chunked HTTP Response Decoding	Chunked transfer encoding is a data transfer mechanism of HTTP. The web server breaks the HTTP response content into chunks. Chunked transfer encoding uses the HTTP response header in place of the content-length header, which the protocol would otherwise require. Chunked transfer encoding supports sending dynamically generated content to clients without having to buffer it. Such payload chunks can evade network inspection devices.
HTML-Encoded HTTP Response Decoding	HTTP response traffic can be sent using HTML encoding, and attackers can use this encoding mechanism to evade detection of malicious payload. Enable this for the Sensor to decode such traffic for inspection. Some of the encoding techniques used are: • Deflate — This compression technique is used mainly to compress data in PDF file formats. PDF documents support using “deflate” encoding in parts of the document. • HTML encoding — The HTML response data is encoded using the "&#" encoding technique. The encoding can be in decimal or hexadecimal format. • Base64 — Base64 encoding is used to encode binary data that is to be stored and transferred over media that are designed to deal with textual data. This encoding technique ensures that the data remains intact without modification during transport.
Base64 SMTP Decoding	Select to inspect Base64 encoded traffic over SMTP.
Quoted-Printable SMTP Decoding	The SMTP protocol specification uses MIME content transfer encoding to transport binary data. Since SMTP protocol can handle only 7-bit ASCII data, each 3-byte group of binary data is converted to 6-bit number and replaced with an ASCII character. Quoted-printable and Base64 are the two basic MIME content transfer encodings. Quoted-printable encoding uses printable ASCII characters, such as alphanumeric and the equals sign (=), to transmit 8-bit data over a 7-bit data path. Quoted-printable encoding technique maps arbitrary bytes into sequences of ASCII characters.
MS RPC/SMB Fragment Reassembly	SMB is a network file sharing protocol. MS-RPC provides a framework for interprocess communication mechanism to exchange data between two processes residing on the same machine or on two remote machines accessible over a network. MS-RPC's transport layer could be TCP, UDP, HTTP, or SMB. SMB protocol supports segmentation of its data. Also, MS-RPC protocol supports fragmentation of its payload. Since MS-RPC can be carried within SMB protocol data, either fragmentation or segmentation or a combination of both can be used to evade any network packet inspection device.
Save	Saves your configuration in the Manager database

Click **Save** in the **Inspection Options** page.

10. To save the configuration changes, click **Save** in the **<Device Name/Interface>** panel.

11. Perform a configuration update for the Sensor.

Layer 7 data collection

Trellix IPS supports collecting Layer 7 data for all major protocols such as HTTP, FTP, and SMTP. In case of SMTP, it could be the sender's address, recipient's address, and attachment name. This information is needed for forensic analysis.

L7 data collection is enabled by default. The percentage of maximum number of concurrent flows with Layer 7 data varies by Sensor model.

The default value is set to 20% for NS9300, NS9200, NS9100, NS7350, NS7300, NS7250, NS7200, NS7150, NS7100, NS5200, NS5100, NS3500, NS3200, NS3100 Sensors, and Virtual IPS Sensors.

The default value is set to 100% for NS9500, NS7600, NS7500, and NS3600 Sensors.

NOTE

In case of an upgrade, the previous default value i.e., 20% or configured custom value is retained.

Enable Layer 7 Data Collection for an interface or subinterface

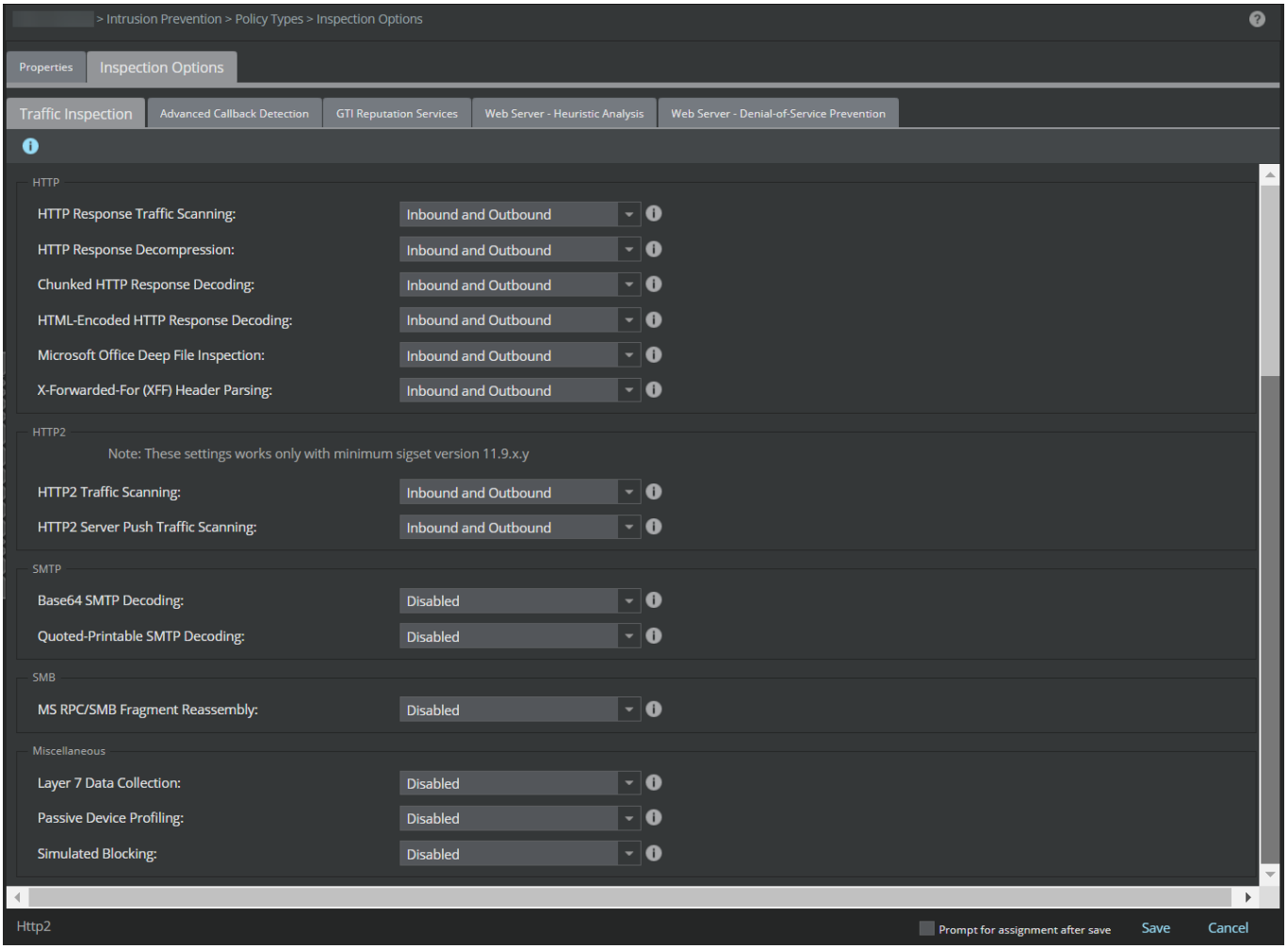
You can enable Layer 7 Data Collection per interface or sub-interface. To optimize Sensor performance, you can also specify the protocols and the fields that are to be exported.

1. Click the **Policy** tab.
2. From the **Domain** drop-down list, select the domain you want to inspect traffic.
3. Navigate to Intrusion Prevention → **Policy Manager**.
4. On the **Interface** tab, double-click the interface to enable the advanced traffic inspection.

   The **<Device name/Interface>** panel opens.
5. In the **Inspection Options** section, select the policy from the **Policy** drop down list.

   To create a new policy, click the + icon or double-click on the policy to edit an already assigned policy.
6. The **Properties** page opens. Enter the **Name** and **Description**. Select the **Visibility** and click **Next**.

   The **Inspection Options** page opens.



7. On the **Traffic Inspection** tab, under **Miscellaneous**, enable **Layer 7 Data Collection** in the required direction.
8. Click **Save** in the **Inspection Options** page.
9. To save the configuration changes, click **Save** in the **<Device name/Interface>** panel.

   You can manage layer 7 data collection options in the following path:

   a. Click the **Devices** tab.

   b. Select the domain from the **Domain** drop-down list.

   c. In the left pane, click the **Devices** tab.

   d. Select the device from the **Device** drop-down list.

   e. Navigate to Setup → Advanced → **L7 Data Collection**.

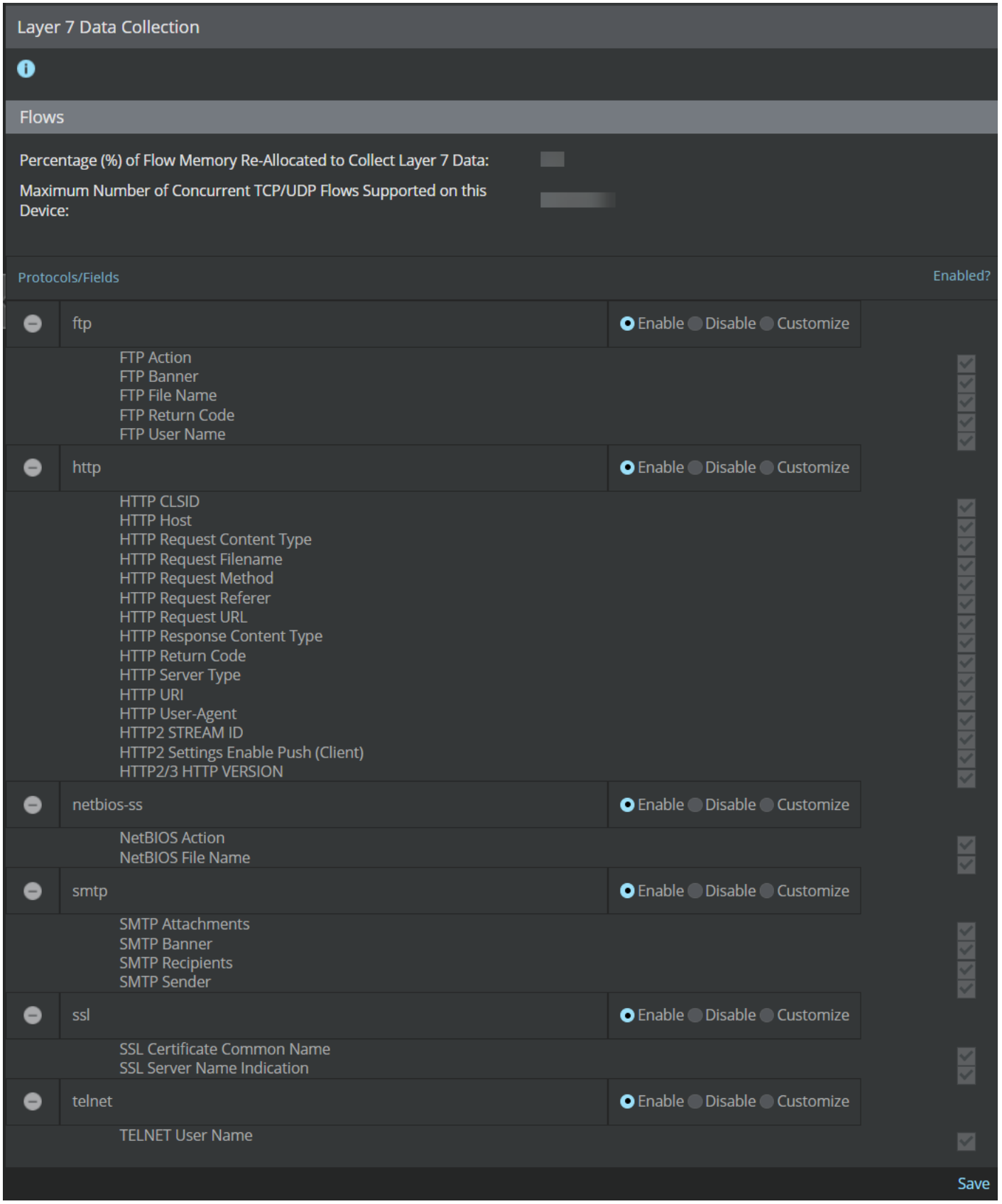
      The **Layer 7 Data Collection** page displays.

   f. Modify the required Layer 7 Data Collection options.

IMPORTANT

Enabling Layer 7 Data Collection is per interface or sub-interface. However, the Layer 7 Data Collection options are device wide. That is, these changes are applied to all the interfaces and sub-interfaces of the corresponding device. Also, you must reboot the device for the changes to take effect. You can do a hitless or a full reboot.

For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.


Layer 7 Data Collection
Flows
Percentage (%) of Flow Memory Re-Allocated to Collect Layer 7 Data:
Maximum Number of Concurrent TCP/UDP Flows Supported on this Device:
Protocols/Fields
Enabled?
ftp
Enable Disable Customize
FTP Action
FTP Banner
FTP File Name
FTP Return Code
FTP User Name
http
Enable Disable Customize
HTTP CLSID
HTTP Host
HTTP Request Content Type
HTTP Request Filename
HTTP Request Method
HTTP Request Referer
HTTP Request URL
HTTP Response Content Type
HTTP Return Code
HTTP Server Type
HTTP URI
HTTP User-Agent
HTTP2 STREAM ID
HTTP2 Settings Enable Push (Client)
HTTP2/3 HTTP VERSION
netbios-ss
Enable Disable Customize
NetBIOS Action
NetBIOS File Name
smtp
Enable Disable Customize
SMTP Attachments
SMTP Banner
SMTP Recipients
SMTP Sender
ssl
Enable Disable Customize
SSL Certificate Common Name
SSL Server Name Indication
telnet
Enable Disable Customize
TELNET User Name
Save

Option	Definition
Percentage (%) of Flow Memory Re-Allocated to Collect Layer 7 Data	The percentage of the maximum number of concurrent flows that capture Layer 7 data. The default value is 20%. **NOTE** For NS7500 and NS9500 Sensors above 10.1.5.116, the default value is set to 100%. For example, an NS7500 Sensor with 7.5Gbps throughput supports around 10,000,000 concurrent flows. So if you enable Layer 7 Data Collection with a value set to 30%, up to around 3,000,000 flows can capture Layer 7 data. Currently, if there are 5,000,000 flows passing through the Sensor, then only the first 3,000,000 flows are examined for Layer 7 data capture. You can click **Edit** to modify the percentage of flows that capture Layer 7 data. However, this will change the number of concurrent flows supported by the Sensor.
Maximum Number of Concurrent TCP/UDP Flows Supported on this Device	The maximum number of concurrent TCP/UDP flows supported by the Sensor. This capacity differs based on the Sensor model. Refer to [Trellix Intrusion Prevention System Product Guide] for the value for each model.
Protocols/ Fields	To optimize Sensor performance, you can choose to enable it for certain fields of the required protocols.
ftp	Select **Enable**, **Disable**, or **Customize** to personalize your settings for the FTP protocol. Click to view the corresponding fields. The following options are available: • FTP Action • FTP Banner • FTP File Name • FTP Return Code • FTP User Name To disable a specific field, you must first select **Customize**.

Option	Definition
http	Select **Enable**, **Disable**, or **Customize** to personalize your settings for the HTTP protocol. Click  to view the corresponding fields. The following options are available: • HTTP CLSID • HTTP Host • HTTP Request Content Type • HTTP Request Filename • HTTP Request Method • HTTP Request Referrer • HTTP Request URL • HTTP Response Content Type • HTTP Return Code • HTTP Server Type • HTTP URI • HTTP User-Agent • HTTP2 STREAM ID • HTTP2 Settings Enable Push (Client) • HTTP2/3 HTTP VERSION To disable a specific field, you must first select **Customize**.
netbios-ss	Select **Enable**, **Disable**, or **Customize** to personalize your settings for the NetBIOS protocol. Click  to view the corresponding fields. The following options are available: • NetBIOS Action • NetBIOS File Name To disable a specific field, you must first select **Customize**.
smtp	Select **Enable**, **Disable**, or **Customize** to personalize your settings for the SMTP protocol. Click  to view the corresponding fields. The following options are available: • SMTP Attachments • SMTP Banner • SMTP Recipients • SMTP Sender To disable a specific field, you must first select **Customize**.

Option	Definition
telnet	Select **Enable**, **Disable**, or **Customize** to personalize your settings for the TELNET protocol. Click  to view the corresponding fields. The following option is available: • TELNET User Name To disable, you must first select **Customize**.
Save	Applies the changes across the Sensor. You must do a hitless or full reboot for the changes to take effect. **NOTE** For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.

CLI command for Layer 7 Data Collection

To know the status of Layer 7 Data Collection, run **`show l7 status`** in the debug mode. For more information, refer to the [CLI commands] section.

Sensor performance with Layer 7 Data Collection

Turning on the Layer 7 Data Collection feature reduces Sensor performance.

- HTTP Response Scanning setting
- Proportion of HTTP traffic to other protocols
- Relative number of HTTP requests and responses in each direction
- Size of a response page sent to the client by the sites or applications that are typically accessed

The following table provides the performance details in a test environment.

- The test environment used 5 HTTP 1.1 get page requests per TCP connection with a 10 K response, each sent in one direction.
- When Advanced Traffic Inspection is enabled, in a deployment with 90 percent of traffic without evasions and 10 percent of traffic with evasions, the overall Sensor throughput would further drop by an additional five percent approximately. For example, if you get 1 Gbps throughput with Layer 7 Data Collection enabled, you would see 950 Mbps if Advanced Traffic Inspection is also enabled.

NS-series Sensor performance with Layer 7 Data Collection

NOTE

Since the default value of L7 data collection is set to 20% of all traffic, the number of flows decreases by approximately 15%.

Table 80. NS9500 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS9500 stack - 100 Gbps throughput	Disabled	Disabled	100 Gbps
		Enabled for outbound direction	100 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	100 Gbps
		Enabled for outbound direction	100 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	100 Gbps
		Enabled for outbound direction	100 Gbps
NS9500 stack - 60 Gbps throughput	Disabled	Disabled	60 Gbps
		Enabled for outbound direction	60 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	60 Gbps
		Enabled for outbound direction	60 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	60 Gbps
		Enabled for outbound direction	60 Gbps
NS9500 stack - 40 Gbps throughput	Disabled	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
NS9500 standalone - 30 Gbps throughput	Disabled	Disabled	30 Gbps
		Enabled for outbound direction	30 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	30 Gbps
		Enabled for outbound direction	30 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	30 Gbps
		Enabled for outbound direction	30 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS9500 standalone - 20 Gbps throughput	Disabled	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
NS9500 standalone - 10 Gbps throughput	Disabled	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps

Table 81. NS9x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS9300	Disabled	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
NS9200	Disabled	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
NS9100	Disabled	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
	Percentage of flows that capture L7 data: 5	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps

Table 82. NS7600 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7600 - 15 Gbps throughput	Disabled	Disabled	15 Gbps
		Enabled for outbound direction	15 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	15 Gbps
		Enabled for outbound direction	15 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	15 Gbps
		Enabled for outbound direction	15 Gbps
NS7600 - 10 Gbps throughput	Disabled	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
NS7600 - 5 Gbps throughput	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps

Table 83. NS7500 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7500 - 7.5 Gbps throughput	Disabled	Disabled	7.5 Gbps
		Enabled for outbound direction	7.5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	7.5 Gbps
		Enabled for outbound direction	7.5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	7.5 Gbps
		Enabled for outbound direction	7.5 Gbps
NS7500 - 5 Gbps throughput	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS7500 - 3 Gbps throughput	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps

Table 84. NS7x50 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7350	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS7250	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
NS7150	Disabled	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps

Table 85. NS7x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7300	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS7200	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
NS7100	Disabled	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1.5 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
		Enabled for outbound direction	1.5 Gbps

Table 86. NS5x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS5200	Disabled	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
NS5100	Disabled	Disabled	600 Mbps
		Enabled for outbound direction	600 Mbps
	Percentage of flows that capture L7 data: 5	Disabled	600 Mbps
		Enabled for outbound direction	600 Mbps
	Percentage of flows that capture L7 data: 100	Disabled	600 Mbps
		Enabled for outbound direction	600 Mbps

Table 87. NS3600 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS3600 - 5 Gbps throughput	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS3600 - 3 Gbps throughput	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
NS3600 - 1 Gbps throughput	Disabled	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps

Table 88. NS3500 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS3500	Disabled	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 5	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 100	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps

Table 89. NS3x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS3200/NS3100	Disabled	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 5	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 100	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps

Virtual IPS Sensor performance with Layer 7 Data Collection

Table 90. Sensor performance details with respect to Layer 7 Data Collection

Sensor model (on ESXi/KVM)	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
IPS-VM600	Disabled	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 20	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
IPS-VM5000	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 20	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps

Exporting Layer 7 data to NTBA appliances

If you have deployed NTBA appliances, you can configure IPS Sensors to export Layer 7 data through NetFlow records to NTBA appliances.

Configure the monitoring ports to export L7 data

If you have at least one NTBA appliance added to the Manager, you can configure the required Sensor monitoring ports to export Layer 7 data to NTBA appliances.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → NTBA Integration → **Exporting.**

   Refer to [McAfee Network Threat Behavior Analysis Product Guide] for information on the **Exporting** page.

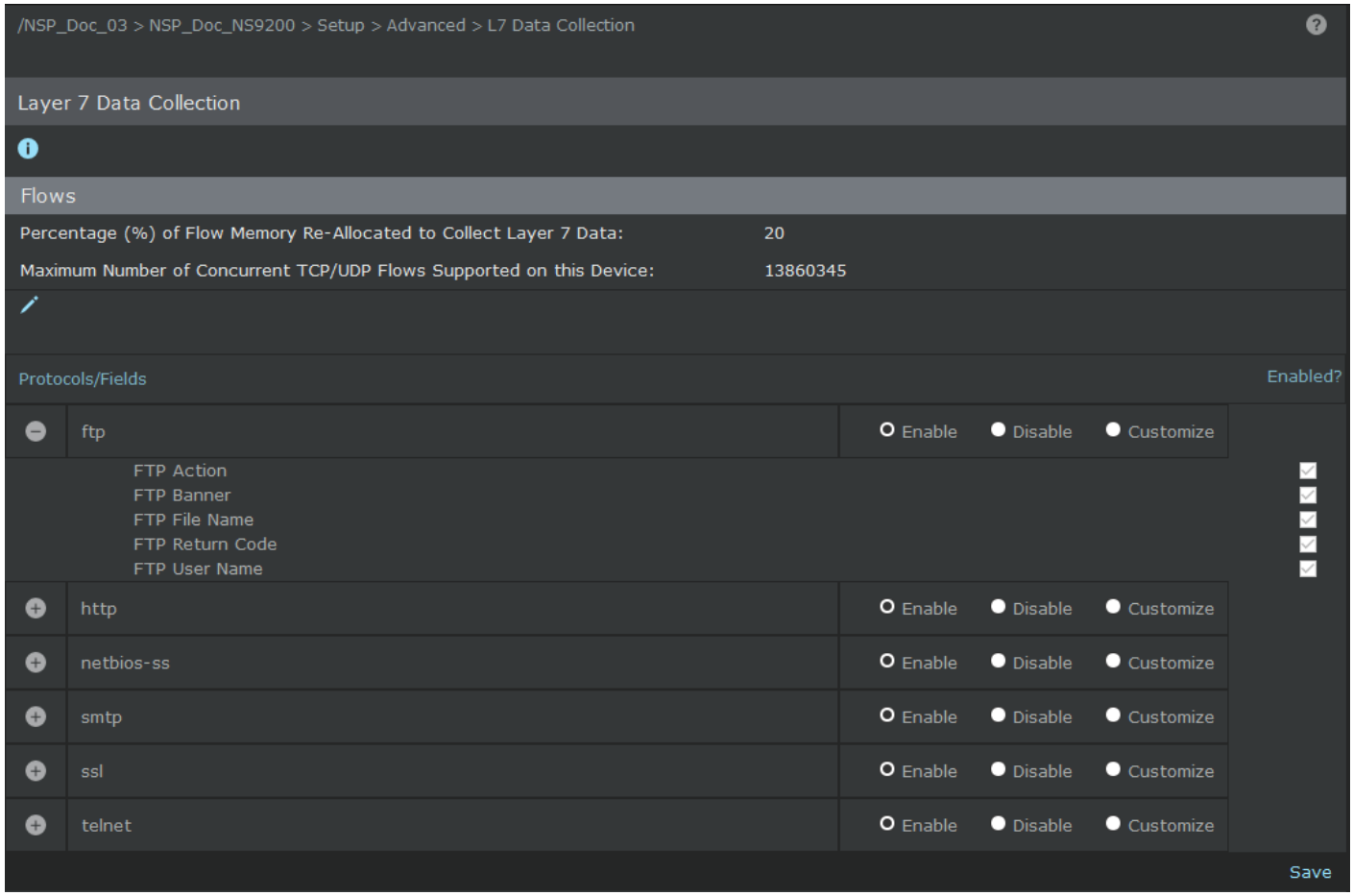
   In addition to enabling monitoring ports to export Layer 7 data, you must enable Layer 7 data collection on at least one interface or subinterface that corresponds to the monitoring ports configured to export that data.

Define the Layer 7 data to be exported

You can specify the Layer 7 data to be exported to NTBA appliances. This setting applies to the entire Sensor.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. In the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → NTBA Integration → **L7 Data Collection.**

Figure 687. Define the L7 Data to be exported



Refer to [McAfee Network Threat Behavior Analysis Product Guide] for information on the **L7 Data Collection** page.

IP Reputation

The Sensor integrates with Trellix GTI server to obtain real-time reputation ratings for IP addresses. The ratings obtained from IP Reputation for an IP address are used to drop or quarantine traffic from the host based on the configuration. The reputation score indicates the risk level.

When IP Reputation is enabled, the Sensor uses the reputation of the source host as an additional factor for blocking, which in turn enhances SmartBlocking.

NOTE

Reputation is determined using a combination of IP address and port. The same IP address might therefore have a different reputation depending on the port currently in use.

Refer to [Trellix Intrusion Prevention System Integration Guide] for more details.

Configure Endpoint Reputation for an admin domain

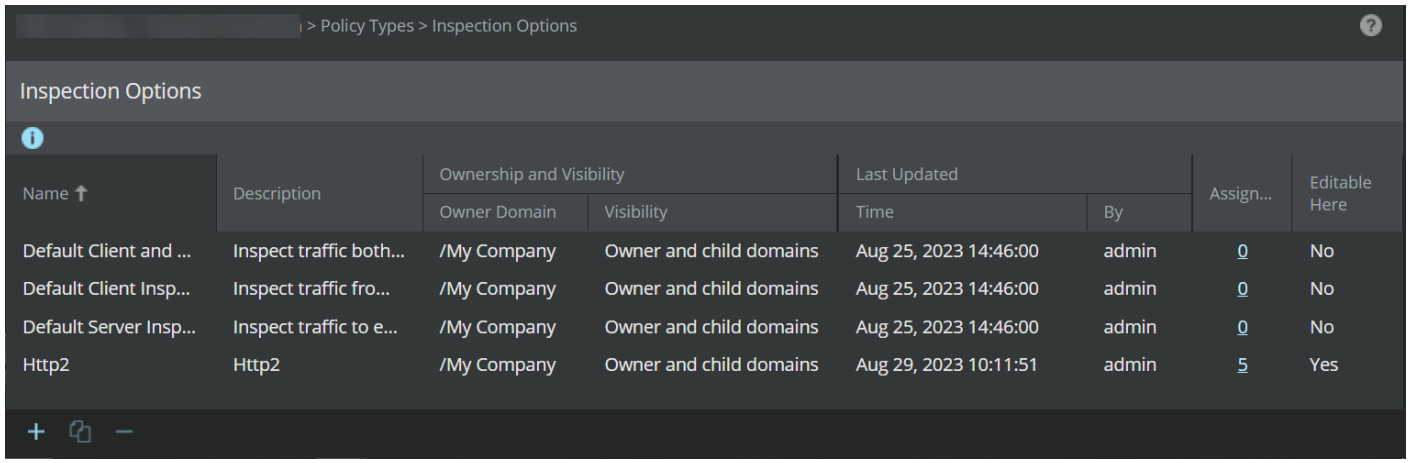
Prerequisite: If the Manager is not integrated with Trellix GTI Lookup, you can see the following message: **Please enable sending of Alert Data Details on the Participation page to make integration with GTI Lookup available**. Select Integration → **Global Threat Intelligence** to enable the integration.

If you configure Endpoint Reputation at an admin domain, you can inherit these settings for the interfaces of the Sensors in this domain. You can also customize these settings for specific interfaces.

Steps:

1. In the Manager, go to Policy → <Admin_Domain_Name> → Intrusion Prevention → Policy Types → **Inspection Options**.

   The **Inspection Options** page is displayed.



2. Double-click a policy for which you want to configure Endpoint Reputation.

   To add a new policy, click +. Using either action, a page with the policy details appears with the **Properties** tab selected.

3. Update the following fields as applicable:

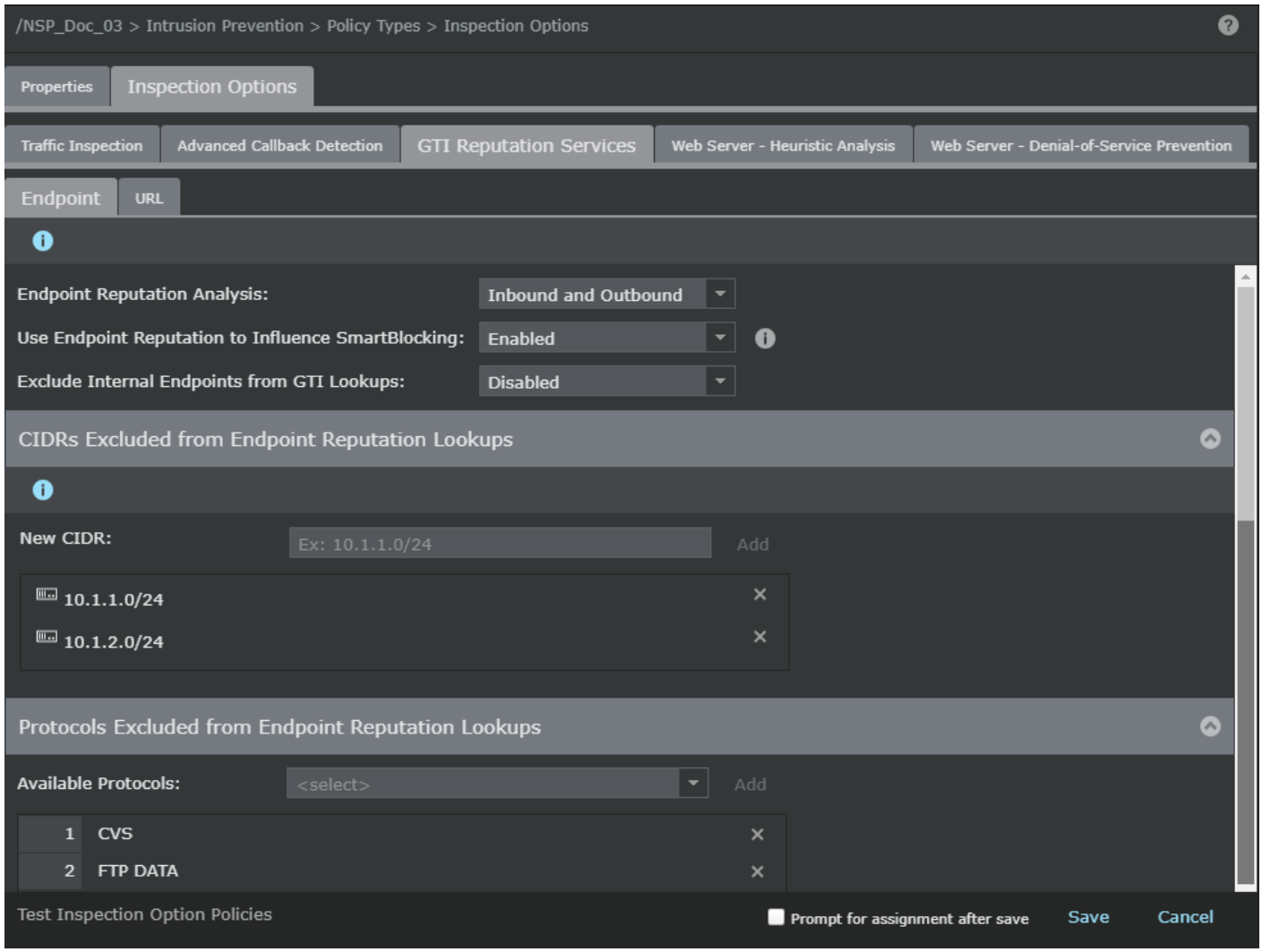
Option	Definition
Name	Enter a unique name to easily identify the policy.
Description	Optionally describe the policy for other users to identify its purpose.
Owner Domain	Displays the admin domain to which the policy belongs

Option	Definition
Visibility	When selected, makes the policy available to the corresponding child admin domains. However, the policy cannot be edited or deleted from the child admin domains. From the drop-down list, select the option for the visibility level of the rule object. Available options are **Owner and child domains** and **Owner domain only**.
Editable here	The status **Yes** indicates that the policy is owned by the current admin domain. This field is uneditable.
Statistics	
Lasted Updated	Displays the time stamp when the policy was last modified. This field is uneditable.
Last Updated By	Displays the user who last modified the policy. This field is uneditable.
Assignments	Indicates the number of inline ports to which the policy is assigned
Prompt for assignment after save	If you deselect this option you can save the policy now and assign it to the Sensor resources as explained in the following section. If you select this option, the **Assignments** window opens automatically when you save the policy and you can assign the policy to the required Sensor resources.
Cancel	Reverts to the last saved configuration

4. Click **Next**.

   The screen shifts to the **Inspection Options** tab. By default, the **Traffic Inspection** tab is selected.

5. Click the **GTI Reputation Services** tab. Endpoint Reputation Analysis is used to influence SmartBlocking decisions, create connection limiting rules, or to take action when a connection to or from a high-risk endpoint is seen on your network.



On the **Endpoint** tab, configure the following fields:

Option	Definition
Endpoint Reputation Analysis	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**
Use Endpoint Reputation to Influence SmartBlocking	Select **Enabled** to enable endpoint reputation to Influence SmartBlocking. Select **Disabled** to disable the option.
Exclude Internal Endpoints from GTI Lookups	Select **Enabled** to exclude internal endpoints from Trellix GTI Lookups. Select **Disabled** to disable the option.
CIDRs Excluded from Endpoint Reputation Lookups	

Option	Definition
New CIDR	Enter the new CIDR and click **Add** to add to the CIDR list to be excluded. Click ✕ to remove the CIDR from the list. **NOTE** The CIDR exclusion list is shared by **Advanced Callback Detection** and **Endpoint Reputation Analysis** .
Protocols Excluded from Endpoint Reputation Lookups	In the drop-down list, select the protocol to be excluded from Trellix GTI Lookups and click **Add**. The selected protocol is displayed in the field below. Click ✕ to remove the protocol from the list.
Prompt for assignment after save	When selected, you are automatically prompted to select the Sensor resources to which you want to assign the policy.

6. Click **Save** to confirm your settings.

   Clicking **Cancel** reverts to the last saved configuration.

Configure Endpoint Reputation for an interface

Prerequisite: You must enable Endpoint Reputation at the interface level for the Sensor to perform IP address lookups. At the interface level, you can inherit the settings from the admin domain or customize it for the interface.

Steps:

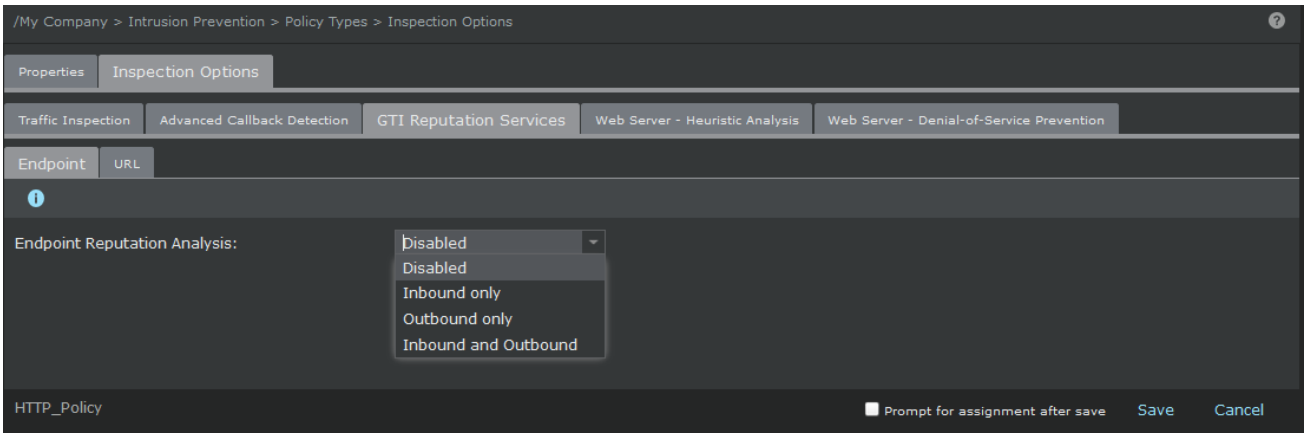
1. In the Manager, select Policy → <Admin Domain Name> → Intrusion Prevention → **Policy Manager**.
2. Double-click the interface for which you want to configure Endpoint Reputation.

   A **<Device Name/Interface>** panel appears for the selected interface.
3. In the **Inspection Options** section of the **<Device Name/Interface>** panel, select the Endpoint Reputation policy you want from the **Policy** drop down list.

   To create a new policy, click the + icon or double click on the policy to edit an already assigned policy.
4. Click the + icon.

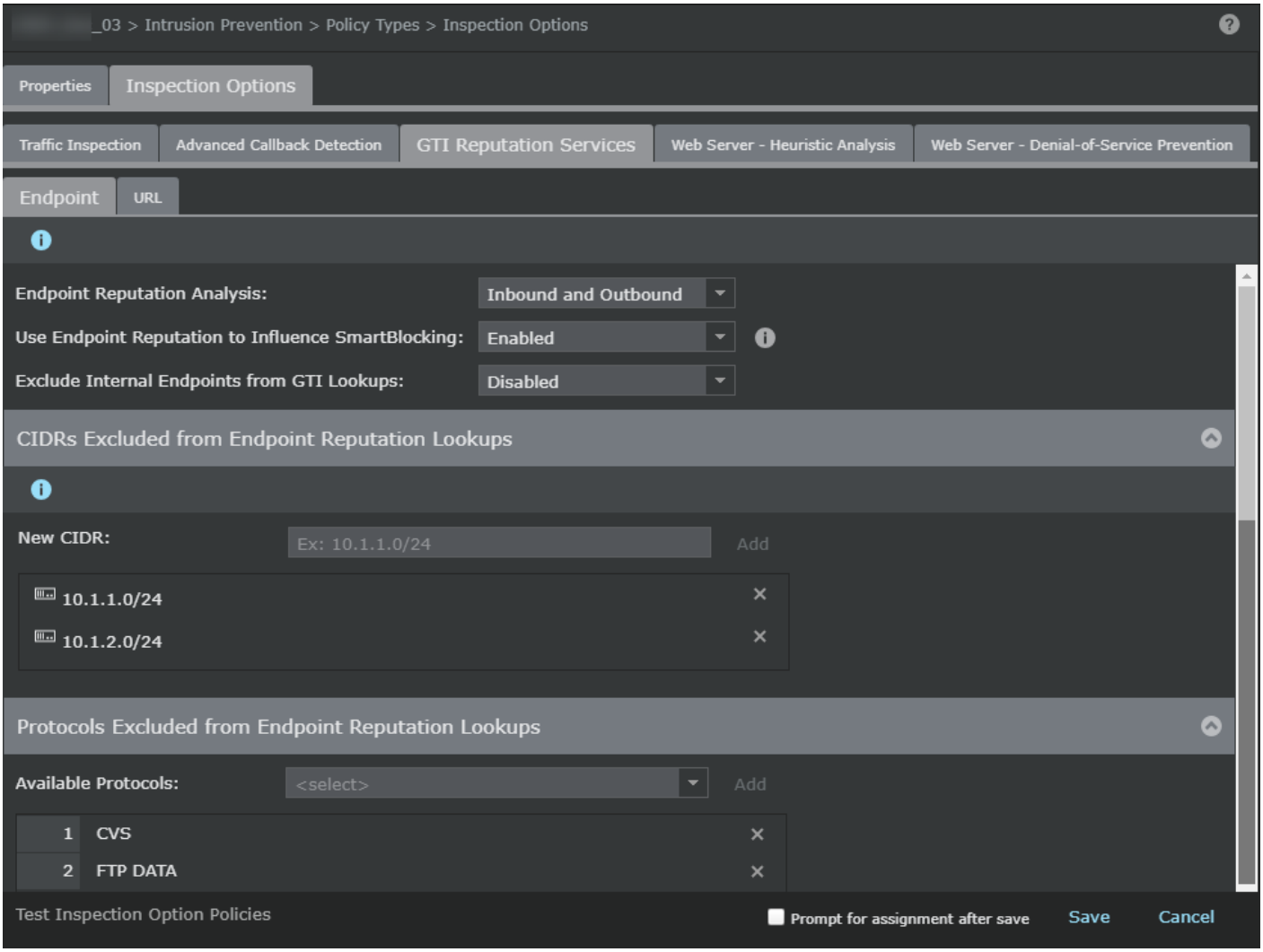
   The **Properties** tab for a new policy appears.
5. Enter the **Name** and **Description**, select the **Visibility**, and click **Next**.

   The page shifts to open the **Inspection Options** tab.
6. Click the **GTI Reputation Services** tab and the **Endpoint** sub-tab opens.
7. Enable **Endpoint Reputation Analysis** in the required direction.



If the outbound connection is enabled, the reputation of the destination IP address is identified. If the inbound direction is enabled, the reputation of the source IP address is identified.

8. Specify the Endpoint Reputation options in the corresponding fields.



Option	Definition
Endpoint Reputation Analysis	Select any of the following options: • **Disabled** • **Inbound only** • **Outbound only** • **Inbound and Outbound**
Use Endpoint Reputation to Influence SmartBlocking	Enable to enhance the blocking of an attack by a high-risk host.
Exclude Internal Endpoints from GTI Lookups	Enable to exclude all the internal hosts from Reputation Lookups based on their IP addresses.
CIDRs Excluded from Endpoint Reputation Lookups	List of IPv4 networks that are excluded from Reputation Lookup. • **New CIDR** — Click to add an IPv4 network. After you enter the network address and the CIDR notation, click **Add**. • Delete — Hover over the network you want to delete and click the "x" icon to delete the network. **NOTE** For the IP addresses specified the exclusion list, the entire flow is marked as exclusion list irrespective of the direction of the flow.
Protocols Excluded from Endpoint Reputation Lookups	Create the exclusion list for Reputation Lookup based on protocols. When a protocol is added, the Sensor does not perform Reputation Lookup with respect to the corresponding flow. • **Available Protocols** — Select the protocol to be excluded from the drop down list and click **Add**. • Delete — Hover over the protocol you want to delete and click the "x" icon to delete the protocol.
Save	Saves the Endpoint Reputation Lookup configuration.
Cancel	Cancels the configuration process and exits the page.

9. Click **Save** in the **<Device Name/Interface>** panel to save the configuration changes.
10. Do a configuration update for the corresponding Sensor.

Using a Sensor to capture data packets

Capture of data packets

Trellix IPS supports capturing data packets on ingress traffic in your network. When captured, these data packets can be used to perform forensics analysis that help in identifying network security threats. Analysis of the captured data packets can help you monitor whether the data communication and network usage of your production environment complies with the outlined policies of your organization. The captured data packets can also be used for troubleshooting Sensor issues. Data packets can be captured in the port mode or file mode.

In the port mode, you can configure a port of your Sensor to capture data packets. The captured packets are forwarded to an external device (for example, a Sniffer) via a monitoring port configured in span mode.

When a port is designated for capturing packets, it cannot be used for IPS inspection. Note that the packet copy between the Sensor and the external device must happen over a direct link between these two devices, that is, without a switch in between.

The packet capture in Trellix IPS can also be used to forward selected traffic to Trellix Data Loss Prevention and/or third-party devices.

Figure 688. Packet Capture — Sending packet copy to Trellix DLP

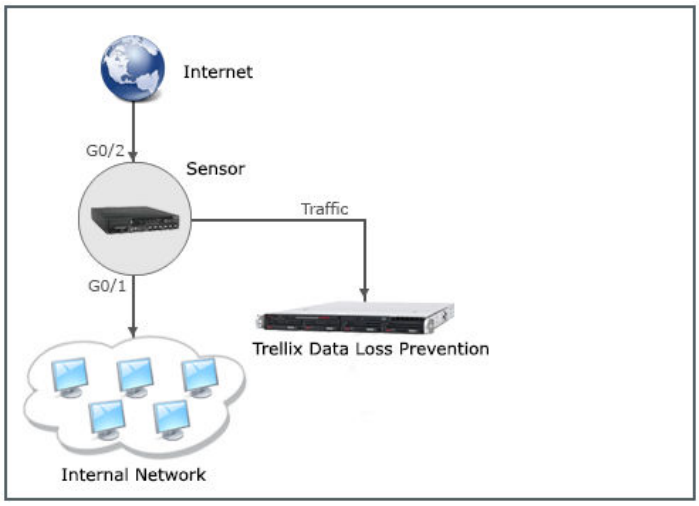
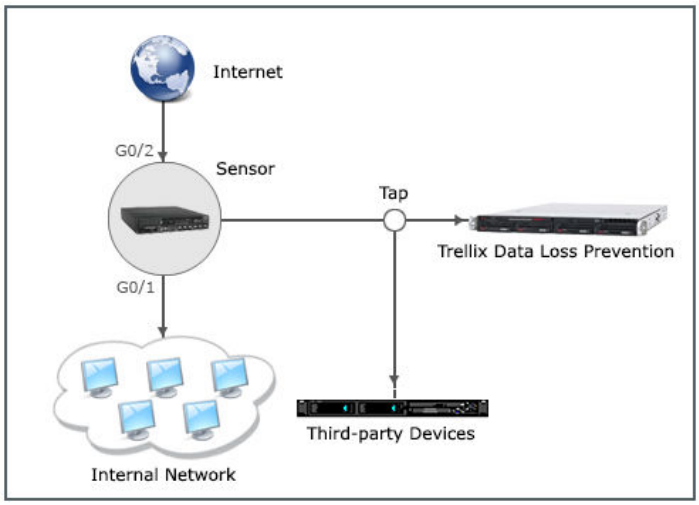


Figure 689. Packet Capture — Sending packet copy using a TAP



In the file mode, the captured files are sent to the Manager or an SCP server. The maximum file size can be configured to the maximum value of Sensor-defined limits. The SCP server should be running and reachable from the Sensor. The Sensor can store only one captured file. If you have not uploaded the file and start the capture session again, the file will be overwritten. Once the packet capturing session is complete the Sensor uploads the file to the Manager. If the Sensor reboots while packet capturing is in progress, then you need to upload the file again.

NOTE

Packet capturing from the Manager is supported on NS-Series and Virtual IPS Sensors. In case of a failover setup, each Sensor captures data packets separately.

The packet capture configurations are done using packet capture rules which are applied to a Sensor. You can define packet capture rule templates, which allow you to apply the same capture rules across multiple devices. With templates, you define capture rules at the device level and then insert them into the configuration of as many Sensors as required.

Packet capture might not occur when:

- The Sensor is in layer 2.
- Scanning Exceptions is enabled on the Sensor.
- When tunneling is disabled, the Sensor can capture tunneled traffic only when the **Capture Rule** for **Protocol** is set to **All**. Any other rule will not capture tunneled traffic.

NOTE

From the Manager, capturing of jumbo packet frames is not supported in port mode. In the file mode, jumbo packet frames are truncated to a maximum size 1526 bytes or the configured snap length.

When the application protocol filter rules are configured and the Sensor receives fragmented traffic matching these filter rules, the Sensor captures only the first fragmented packet of the flow and not the subsequent ones. This is because the port information is present in the first fragment alone.

Trellix recommends that you ensure that the capture traffic volume is less than the capacity of the configured capture port of the Sensor. Otherwise, this can affect the Sensor performance.

Configure packet capture settings in port mode

To configure the packet capture settings:

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → **Capture Now**.

   The **Capture Now** page appears.

2. From the **Send Captured Packets To** drop-down list, select **Monitoring (SPAN) Port**.

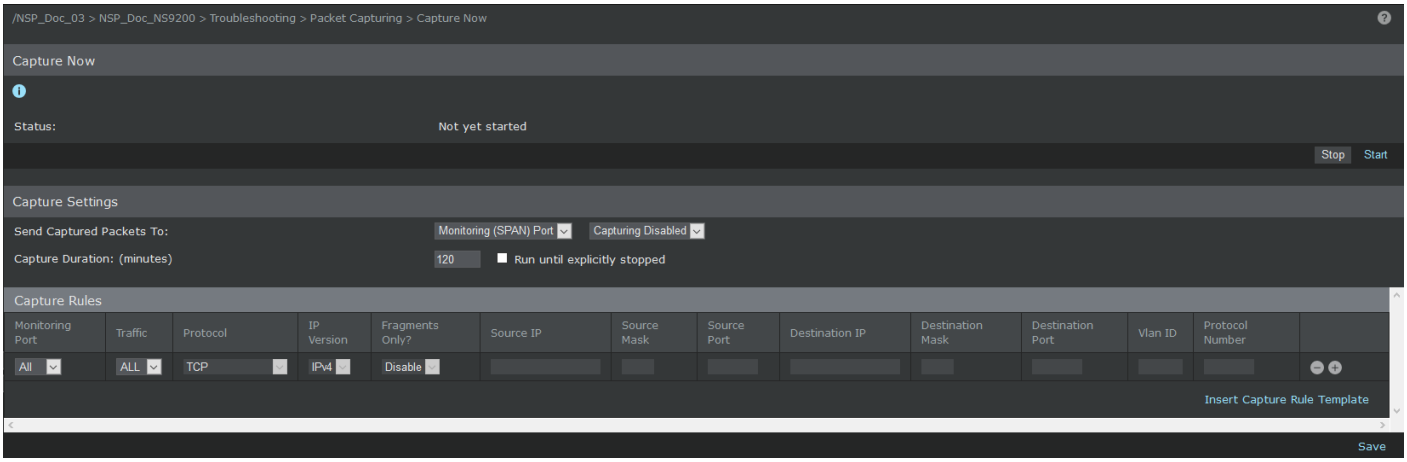
   NOTE

   Configure packet capture settings in span port is not supported on a stack of NS9500 Sensors.

3. Type the **Capture Duration** in minutes.

> **NOTE**
>
> Select the **Run until explicitly stopped** option to keep capturing for an indefinite period till you stop the capture.

Figure 690. Configure SPAN port for packet capture



4. Configure the **Capture Rules**.
5. Click **Save** to save the capture settings.

> **NOTE**
>
> After saving the capture settings, you can observe the timestamp using the **Status** field in the **Capture Now** window; note that the status is available only after you start a packet capture session.

6. Click **Start**.

> **NOTE**
>
> The monitoring port should be configured in the Filter Rule before starting the capture.

The **Status** displays the total number of packets that are captured.

7. To stop the packet capture session, before the configured duration, click **Stop**.
8. Click **Cancel**. The Sensor stops the capture and deletes the captured file.

> **NOTE**
>
> If file upload has started then it cannot be canceled.

Configure packet capture settings in file mode

The packet capture operation can be performed in the file mode to either send the captured files to the Manager or to an SCP server. The maximum file size is a requirement for capturing data in this mode. The maximum file size is based on the following Sensor defined limits:

Sensor	Maximum capture size
NS9500 stack - 100 Gbps throughput	100 MB
NS9500 stack - 60 Gbps throughput	100 MB
NS9500 stack - 40 Gbps throughput	100 MB
NS9500 standalone - 30 Gbps throughput	100 MB
NS9500 standalone - 20 Gbps throughput	100 MB
NS9500 standalone - 10 Gbps throughput	100 MB
NS9300, NS9200, NS9100	100 MB
NS7600 - 15 Gbps throughput	100 MB
NS7600 - 10 Gbps throughput	100 MB
NS7600 - 5 Gbps throughput	100 MB
NS7500 - 7.5 Gbps throughput	100 MB
NS7500 - 5 Gbps throughput	100 MB
NS7500 - 3Gbps throughput	100 MB
NS7350, NS7250, NS7150	100 MB
NS7300, NS7200, NS7100	100 MB
NS5200, NS5100	58 MB
NS3600 - 5 Gbps throughput	100 MB
NS3600 - 3 Gbps throughput	100 MB
NS3600 - 1 Gbps throughput	100 MB
NS3500	40 MB
NS3200, NS3100	40 MB
IPS-VM5000	58 MB
IPS-VM600	58 MB

Send the captured file to the Manager

To start the capture and send the captured file to the Manager:

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → **Capture Now**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Packet Capturing → **Capture Now**.
2. From the **Send Captured Packets To** drop-down list, select **The Manager**.
3. Type the maximum file size to be captured in the **Maximum Capture Size (MB)** field.

NOTE

The maximum file size can be configured up to the maximum value of Sensor defined limits.

4. Configure the **Capture Rules**.

NOTE

If you are configuring for a Sensor from a stack of NS9500 Sensors, you cannot configure rules at an interface level. You have to configure to **All** interface.

5. Click **Save** to save the capture settings.
6. Click **Start**.

   When the maximum file size is reached, the Sensor uploads the captured file to the Manager.
7. To stop the packet capture session, before the configured maximum file size, click **Stop**. The Sensor pushes the captured file to the Manager.
8. Click **Cancel**. The Sensor stops the capture and deletes the captured file.

NOTE

If file upload has started then it cannot be canceled.

Send the captured file to an SCP server

To capture and send the files to the SCP server:

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → **Capture Now**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Packet Capturing → **Capture Now**.
2. From the **Send Captured Packets To** drop-down list, select **An SCP Server**.
3. Enter the SCP Server credentials, **SCP Server IP**, **SCP Server User Name** and **SCP Server Password**.
4. Type the maximum file size in the **Maximum Capture Size (MB)** field.

NOTE

The maximum file size can be configured up to the maximum value of Sensor defined limits.

5. Click **Test Connection**.

   The **Test Connection** operation establishes a connection between the Sensor and the SCP server, and creates a test file. This is to verify whether the server is reachable and the files can be written.

NOTE

The **Test Connection** operation can fail due to MACs and Ciphers mismatch between the Sensor and SCP server.

6. Configure the **Capture Rules**.

NOTE

If you are configuring for a Sensor from a stack of NS9500 Sensors, you cannot configure rules at an interface level. You have to configure to **All** interface.

7. Click **Save** to save the capture settings.
8. Click **Start**.

   When the maximum file size is reached, the Sensor uploads the captured file to the Manager.
9. To stop the packet capture session, before the configured maximum file size, click **Stop**. The Sensor sends the captured file to the SCP server.
10. Click **Cancel**. The Sensor stops the capture and deletes the captured file.

NOTE

If file upload has started, then it cannot be canceled.

Configure and manage packet capture rules

You can filter the rule for capturing packets and apply it as a packet capture profile.

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → **Capture Now**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Packet Capturing → **Capture Now**.
2. Under **Capture Rules**, the following list of capture rules is displayed.

Option	Definitions
Monitoring port	The monitoring ports on which the rule is applied: The options are: **All** and **<Interface depending on the Sensors>**. **NOTE** Some options may not be displayed, depending on the configured Sensor model. **NOTE** If you are configuring for a Sensor from a stack of NS9500 Sensors, you cannot configure rules at an interface level. You have to configure to **All** interface.
Traffic	The traffic for which the capture rule is to be filtered. The options are: **ALL**, **ARP** and **IP**.
Protocol	Type of protocols to be filtered. The options are: **TCP**, **UDP**, **ICMP**, and **Protocol Number**.
IP Version	Type of IP Setting. The options are **IPv4** and **IPv6**
Fragments Only?	Captures only the fragmented traffic. By default this option is disabled.
Source IP	Source IP address of the packet
Source Mask	Source IP mask
Source Port	Source port number of the packet. This option will be enabled only if you select the protocol type as **TCP** or **UDP**.
Destination IP	Destination IP address of the packet
Destination Mask	Destination IP mask
Destination Port	Destination port number of the packet. This option will be enabled only if you select the protocol type as **TCP** or **UDP**
Vlan ID	VLAN ID of the packet to be captured. This option will be disabled if you select the protocol type as **ALL** or **ARP**. **NOTE** Only the outer VLAN ID will be inspected in case of double VLAN tagged traffic
Protocol Number	The protocol number. This can be specified only if the option **Protocol Number** is selected under **Protocol**.

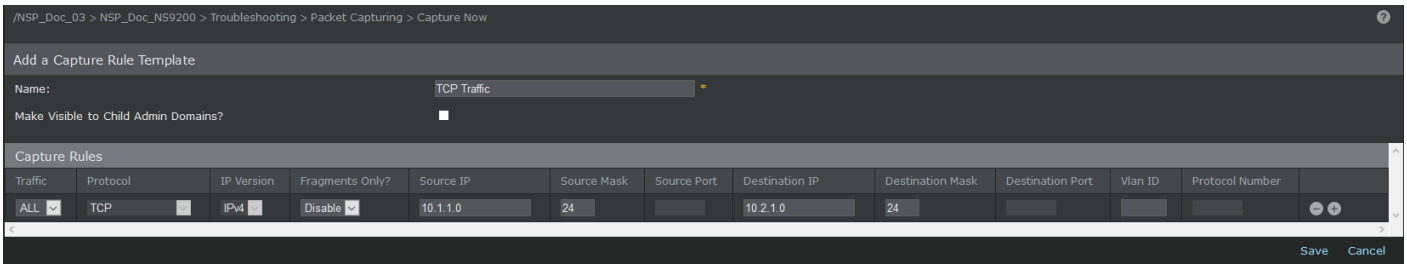
- When a packet capture session is in progress, you cannot configure/push a new packet capture profile. To apply a new profile, the packet capture session needs to be stopped.

- You can add/remove the rows by clicking **-** or **+** signs on the right-hand side of the **Capture Rules** field.

3. The Capture Rule Template can be defined at the admin level to be applied across multiple Sensors or at a Sensor level.
   - To create a packet capture rule template at an admin-domain level, select Policy → <Admin Domain Name> → Intrusion Prevention → Objects → Packet Capture Rule Templates → **New**.
   - To create a packet capture rule template at a standalone Sensor level, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → Capture Now → Insert Capture Rule Template → **New**.
   - To create a packet capture rule template at a Sensor in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Packet Capturing → Capture Now → Insert Capture Rule Template → **New**.

   The **Add a Capture Rule Template** page opens.

Figure 691. Add a Capture Rule Template window



4. Type the **Name** of the capture rule.
5. Select the **Make Visible to Child Admin Domains?** option to make the rule visible to the child admin domain.
6. Click **Save** to save the capture rule.
7. The capture rules can be modified. Once a rule is modified, click **Save**.
8. To delete a capture rule, click − against the rule. Click **Save**.

> **NOTE**
>
> A modification of the template rule does not affect the rule of the Sensor on which it has been applied.

Capture packets from Sensor CLI

You can capture incoming and outgoing packets in NS9500, NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3200, NS3100, and Virtual IPS Sensors from the Sensor CLI. The following CLI commands are available in the Sensors that allow you to capture packets:

> **NOTE**
>
> Capturing of jumbo packet frames from the Sensor CLI is not supported in both port mode and file mode.

NOTE

The CLI commands mentioned are applicable only when packet capture is configured in file mode.

- **`pktcapture intfport`**
- **`pktcapture intfport-pair`**
- **`pktcapture stack-node`**
- **`pktcapturefile`** (Discard or upload captured packets to the Manager or SCP server based on the configuration.)

To capture packets continuously, the following CLI commands are available:

- **`pktcapture-circular intfport`**
- **`pktcapture-circular intfport-pair`**
- **`pktcapture-circular stack-node`**

To debug various integration or connectivity issues on the management port, the CLI command **`pktcapture mgmt`** is available.

NOTE

The packet capture feature is mainly for troubleshooting purposes. Trellix recommends you enable it for a limited period with appropriate supervision.

NOTE

Trellix recommends that you ensure appropriate filters are applied when enabling packet capture. Otherwise, this can affect the Sensor performance.

These CLI commands allow you to capture packets from the Sensor CLI on an ad-hoc basis. The commands use the configuration in the Manager to determine if the captured packets should be sent to the Manager or to an SCP server. If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using these commands.

NOTE

If the Manager is in the process of capturing packets and at the same time you run this command from the Sensor CLI, the Sensor will display a message that a packet capture process is already running. Similarly, if you have started packet capture from the CLI, the Manager displays the packet capture **Status** as **Running**. In the Manager, you cannot stop a packet capture session that is started in the CLI and vice-versa. As a best practice, you should start and stop a packet capture session from the same place; either from the CLI or from the Manager.

For more information on the CLI commands, see IPS CLI Commands - Normal Mode (page 1877) .

View packet capture status

The Manager gets periodic updates from the Sensor regarding the packet capture status.

For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → **Capture Now**.

For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Packet Capturing → **Capture Now**.

The **Capture Now** window is displayed.

The status of the packet capture session is displayed.

Manage captured files

To manage the captured files in the Manager:

1. For a standalone Sensor, select Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → Packet Capturing → **PCAP Files**.

   For Sensors in a stack, select Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → Packet Capturing → **PCAP Files**.

   The list of the captured files is stored in the Manager in a specific filename format.
2. Select a specific file and click **Open/Export**.

   You can view the file or save it at the wanted location.
3. To delete the selected file, click  .

IP spoofing detection

The Anti-Spoofing feature enables the detection of packets that either originate from sources external to your network (inbound) which use your internal addresses as the source IP addresses, or originate from your internal network (outbound) which use IP addresses not defined in your customized list of *good* addresses.

> **NOTE**
>
> In these sections, the term *IP spoofing detection* refers to the detection of IP-spoofed attacks, whereas the term *Anti -Spoofing* refers to the feature in Trellix IPS that detects these attacks.

You can apply IP address spoofing detection to any inline interface that has been previously segmented by CIDR-based addressing. A Sensor maintains a table of CIDR-based addresses it protects. Then, for example, if it detects a packet that originated from outside your network but contains an identified internal address, it just drops the packet.

Any port pair in inline mode that has been segmented by CIDR addressing is eligible for IP spoofing detection. This includes any CIDR-segmented subinterfaces of an eligible port pair. For example, port pair G0/1-G0/2 protects the 192.16.1.0/24 and 192.16.2.0/24 networks in inline mode. You create the subinterface *Payroll-Server* to protect host 192.16.1.1/32. When you enable IP spoofing detection for G0/1-G0/2, all three addresses are checked for IP spoofing attacks.

Enable IP address spoofing detection

Prerequisite: Make sure that for the port-pairs for which you need to enable Anti-spoofing feature, their **Mode** is set to inline and their **Interface Type** is set to CIDR.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Anti-Spoofing**.

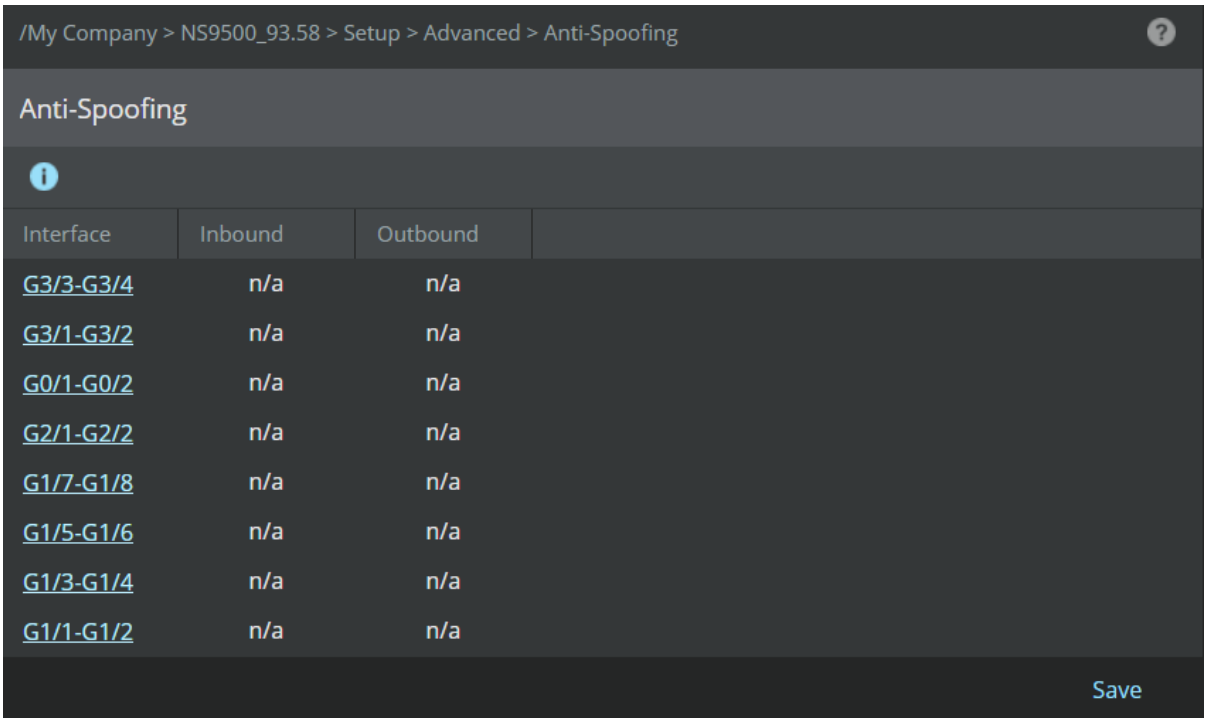
   The **Anti-Spoofing** page displays. Note that the tabs relate to the interfaces on the Sensor.
6. For the required port-pairs, enable **Anti-Spoofing** in the required directions - inbound, outbound, or both.

   You can only enable IP spoofing detection for port-pairs in inline mode with CIDR interface types. CIDR entries must be previously configured for IP spoofing detection to function properly. You can enable Anti-spoofing at the interface level; you cannot enable it for specific CIDR subinterfaces.

   NOTE

   You can click an interface name to view the CIDRs configured for that interface.

Figure 692. Configuring Anti-spoofing



7. Click **Save** to enable IP spoofing detection.

   Once you click **Save**, the configuration is sent through SNMP to the Sensor; thus, you do not have to update the configuration changes to the Sensor.

NOTE

When you enable Anti-spoofing, a Sensor drops any IP-spoofed packets but raises no alert. You can view a list of dropped packets by clicking on the **Dropped Packets** tab in Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Traffic Statistics**. Once in the tab, select the port for which you want to see the list and count of dropped packets.

Alternatively, you can use the **`show inlinepktdropstat`** Sensor CLI command to view the number of IP-spoofed packets dropped by a Sensor. For information on using this CLI, refer to the [CLI commands] section.

Enable layer 2 settings

Enabling the **Layer 2 Settings** action provides permission for the device to go into [layer 2 pass-through mode], or [fail-open mode], when there are multiple occurrences of critical device faults in a specified period of time. This feature provides another measure for preventing a bottleneck at the device when deployed in High Availability networks.

NOTE

The **Layer 2 Settings** mode is on (enabled) by default.

By default, if the device experiences a critical operating error, such as a suspended task or "hung" processor, it reboots. If a device continues to experience critical errors, a reboot is initiated for every critical error. If the device is not closely monitored, the constant rebooting can create a bottleneck at the device. Also, in the case of External Tap and SPAN or Hub monitoring modes, passing traffic is not being inspected.

The **Layer 2 Pass-Through** mode enables you to set a threshold on the number of critical failures within a configured period of time that the device can experience before being forced into fail-open mode. For example, you configure **Layer 2 Pass-Through** mode to enable if there are three critical faults in any 10-minute period. At minutes one, three, and seven, faults occur; the Layer 2 Pass-Through Mode is enabled. Here is another scenario: at minutes one, four, eleven, and thirteen, faults occur. In this case, the last three faults occurred within 10 minutes of each other, thus the device enters Layer 2 Pass-Through mode.

Device reboot may take a few minutes to complete. This downtime is not counted against the Layer 2 duration; only device uptime is counted.

NOTE

The **Layer 2 Pass-Through** mode is off (not enabled) by default. This option enables fail-open operation for critical faults between Layer 3 and Layer 7 only; failures at Layer 1 and Layer 2 continue to cause a reboot of the device.

NOTE

The Manager provides the capability to allow Layer 2 bypassing to a Sensor directly from the Manager interface, rather than having to do it from the CLI. The modes **Assert** and **Deassert** could now be set from the Manager interface. For more details on enabling the modes, refer to *Enable Layer 2 Modes* (page 1545).

The following occurs when Layer 2 Pass-Through Mode is activated:

- Processing of traffic on all monitoring ports of the affected device ceases.
- The device sends a fault message to the Manager indicating that it is now in Layer 2 Pass-Through mode.

Steps:

1. For a standalone Sensor, click Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Layer 2 Bypass**.

   For Sensors in a stack, Click Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Layer 2 Bypass**.
2. Select **Yes** to enable **Layer 2 Pass-Through Monitoring**.
3. Enter a **Trigger After** value.

   The threshold determines the number of critical failures within the **Occurring Within** time before switching to pass-through mode.
4. Enter an **Occurring Within** time.

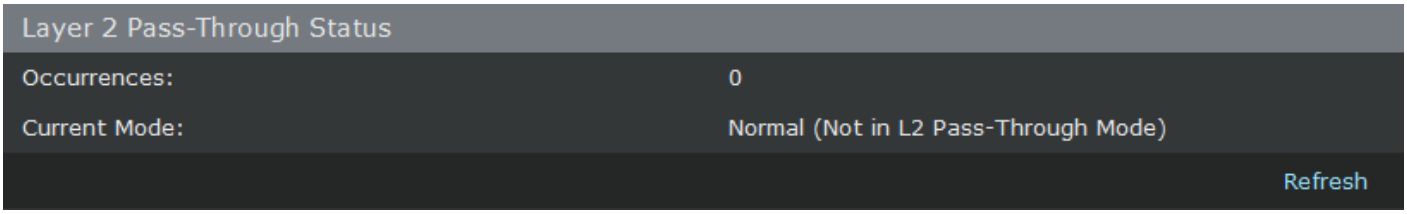
   This time represents the number of minutes within which the **Trigger After** value must be met to switch into pass-through mode.

Figure 693. Layer 2 Settings window

5. Select yes to enable **ARP Spoofing** on the device.
6. Click **Save**.

   Once applied, you can view the number of critical faults and current mode in the **Layer 2 Pass-Through Status** dialog at the bottom of the screen.

Figure 694. Layer 2 Pass-Through Status dialog



Note the following status fields:

- **Occurrences**: current number of threshold-breaching events.
- **Current Mode**: current mode of the device. **Normal** means that Layer 2 pass-through mode is not enabled in the device. **L2 Pass-Through Mode** means pass-through mode is enabled.

Enable Layer 2 Modes

The Manager provides the capability to allow Layer 2 bypassing to a Sensor directly from the Manager interface, rather than having to do it from the CLI. This allows you to set **Assert** and **Deassert** modes from the Manager interface.

To view the steps on enabling the **Layer 2 Assert Mode**, see the section *Enable Layer 2 Assert Mode* (page 1545).

To view the steps on enabling the **Layer 2 Deassert Mode**, see the section *Enable Layer 2 Deassert Mode* (page 1547).

Enable Layer 2 Assert Mode

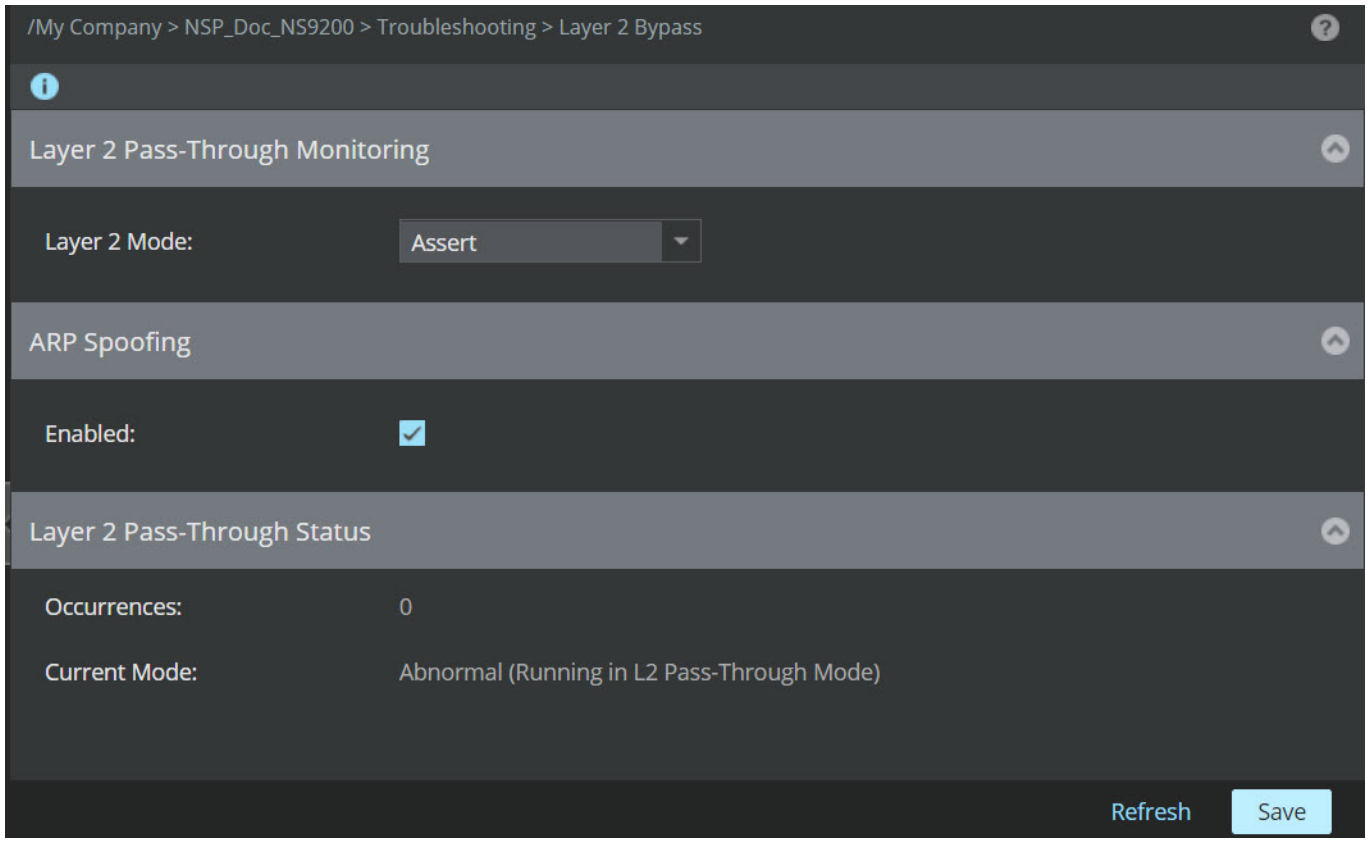
The changes made on the Manager interface are also reflected on Sensor CLI. To view the status on the Sensor, enter **`status`** command.

Steps:

1. To enable the **Assert** mode, click Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Layer 2 Bypass**.
2. In the **Layer 2 Pass-Through Monitoring** section, select **Assert** in the drop-down list against **Layer 2 Mode**.
3. Check **ARP Spoofing** to enable it on the device.
4. Click **Save**.

   Once applied, you can view the number of critical faults and current mode in the **Layer 2 Pass-Through Status** dialog at the bottom of the screen.

Figure 695. Layer 2 Settings window



Note the following status fields:

- **Occurrences**: Displays the current number of threshold-breaching events
- **Current Mode**: Displays the current mode of the device. **Abnormal** means that Layer 2 pass-through mode is enabled in the device. **L2 Pass-Through Mode** means pass-through mode is enabled.

NOTE

To view the status of **Assert** mode for Sensors in a stack, Click Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Layer 2 Bypass**

NOTE

- The Manager interface does not allow you to move to **ON/OFF** mode once the layer 2 mode is set to **Assert**, then only **Deassert** is allowed.
- If you set the mode to **'Assert'**, it gets applied to all the Member Sensors for a stack / HA.
- The Layer 2 modes **Assert/Dessert** could only be set from Manager interface for Sensor versions 10.1.5.107 and above. For others, it is recommended to set these modes through CLI commands.

Enable Layer 2 Deassert Mode

The changes made on the Manager interface are also reflected on Sensor CLI. To view the status on the Sensor, enter **`status`** command.

Steps:

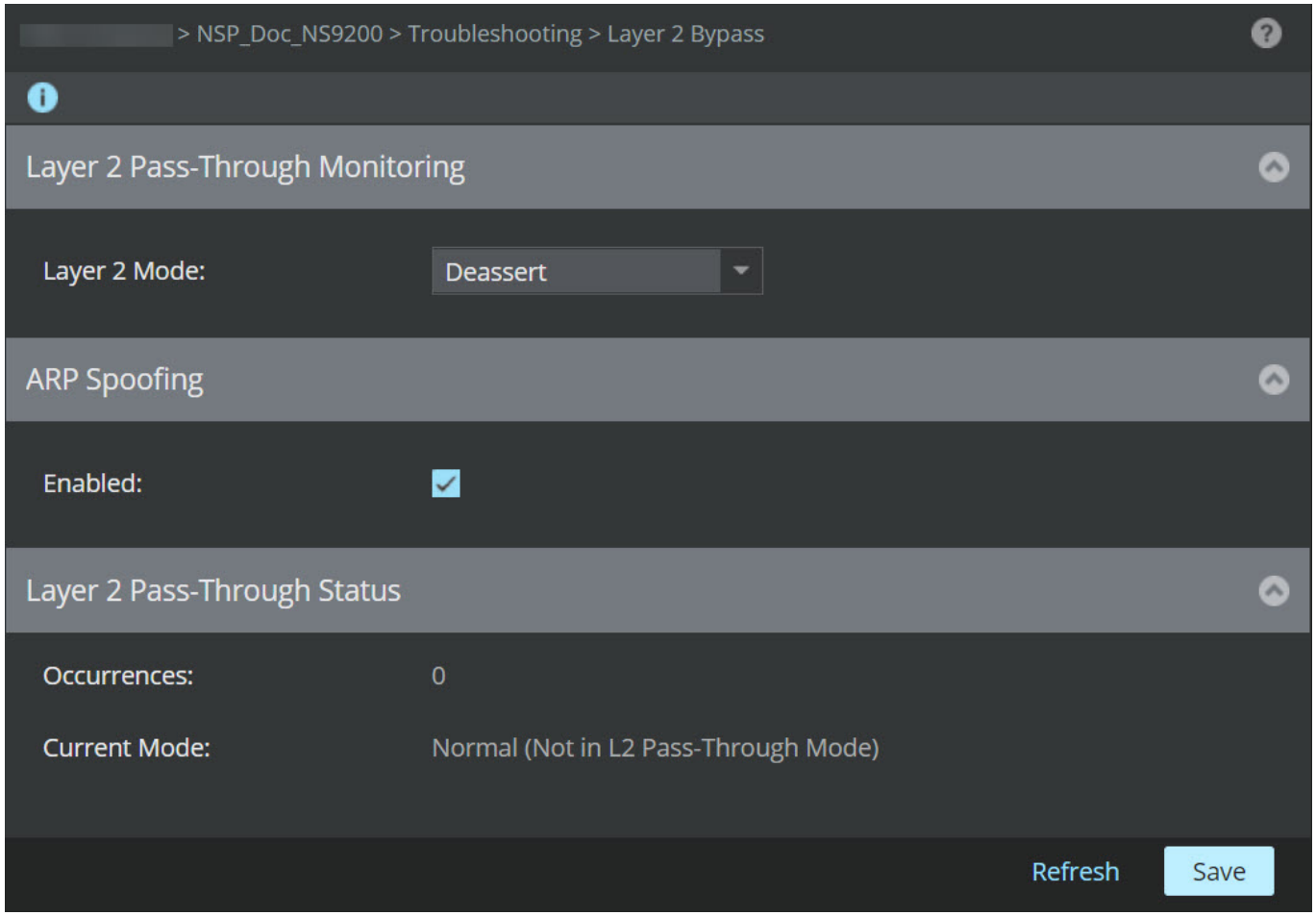
1. To enable the **Deassert** mode, click Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Layer 2 Bypass**.
2. In the **Layer 2 Pass-Through Monitoring** section, select **Deassert** in the drop-down list against **Layer 2 Mode**.

   > **NOTE**
   >
   > The **Deassert** mode is displayed only if layer 2 mode is previously set to **Assert** mode.

3. Check **ARP Spoofing** to enable it on the device.
4. Click **Save**.

   Once applied, you can view the number of critical faults and current mode in the **Layer 2 Pass-Through Status** dialog at the bottom of the screen.

Figure 696. Layer 2 Settings window



Note the following status fields:

- **Occurrences**: Displays the current number of threshold-breaching events
- **Current Mode**: Displays the current mode of the device. **Normal** means that layer 2 pass-through mode is not enabled in the device. **L2 Pass-Through Mode** means pass-through mode is enabled.

NOTE

To view the status of **Deassert** mode for Sensors in a stack, Click Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Layer 2 Bypass**

NOTE

The Manager interface does not allow you to move to **Deassert** mode when the layer 2 mode is set to **ON/OFF**.

Layer 2 mode on drops at Switch/NIC ports

Layer 2 drops feature monitors drops at various points that impact the customer traffic. It provides the capability for Sensor to enter into Layer 2 mode upon detecting heavy drops at the switch/NIC ports and prevent network outage.

To prevent any adverse impact on monitoring Layer 2 drops, Trellix recommends to factor in either of the following considerations:

- Avoid enabling Layer 2 drops and packet capture at the same time on Sensor appliance.
- Ensure sufficient filters are added to limit the packets captured such that it does not cause drops in the NIC when both the features are enabled.

You can configure the settings for Layer 2 mode on drops with **`set l2OnDrops (enable|disable|sensitivity-level)`** from Sensor CLI. After configuring the required settings, **`show l2OnDropsConfig`** can be used to view the status of Layer 2 mode.

The following table describes the various configuration settings available for Layer 2 mode on drops:

Parameter	Description
`enable`	Puts the Sensor to Layer 2 mode when high drops are seen.
`disable`	Disables Layer 2 mode on drops.
`sensitivity-level`	Configures the sensitivity level for Layer 2 mode on drops.

The Sensor monitors these drops periodically. If number of drops exceeds the drop count threshold value in consecutive occurrences and the configured sensitivity level is met, then the Sensor is put in to Layer 2 mode.

The following table consists of actual Drop Count Threshold and Number of Consecutive Occurrences for various Sensitivity Levels:

Sensitivity Level	Drop Count Threshold	Number of Consecutive Occurrences
Low	50000	5

Sensitivity Level	Drop Count Threshold	Number of Consecutive Occurrences
Medium	30000	4
High	10000	3

NOTE

- Layer 2 on drops is applicable only to NS-series Sensors.
- The Layer 2 mode must be **'ON'** to configure **`set l2OnDrops (enable|disable|sensitivity-level)`**.
- If you want to restore the Sensor automatically to normal state, you have to configure **`latency-monitor restore-inline`**.

It must be considered that too many drops due to packet capture can influence Layer 2 drops action depending on the configuration.

NOTE

Packet capture feature is a debugging tool that is provided to help you with troubleshooting problems, auditing, to gain insights, and to use the incoming NIC.

Detection of ARP spoofing

ARP (Address Resolution Protocol) Spoofing detection is accomplished by mapping a table of IP address to corresponding MAC addresses. The detection of multiple ARP reply packets with a different sender MAC address than its mapped IP results in an alert. Check Attack Log for ARP spoofing-related alerts.

In ARP spoofing, the MAC address of a spoofed ARP packet is the real MAC address of the host attempting the spoofing.

Sometimes misconfiguration (two different machines are using the same IP address) and occasionally system malfunction (host or switch) may result in such ARP spoofing packets.

The following CLI commands are also provided to assist with the ARP Spoofing detection feature:

- **`arp delete`** removes a single MAC/IP address association from the database.
- **`arp dump`** puts the contents of the current MAC/IP address mapping table in the database to the Sensor.dbg file, where it can be used by Technical Support for debugging purposes.
- **`arp flush`** deletes the contents of the MAC/IP addresses mapping table.
- **`arp spoof enable`** enables ARP spoofing detection. (This is akin to enabling it within the Manager interface.)
- **`arp spoof disable`** disables ARP spoofing detection.(This is akin to disabling it within the Manager interface.)
- **`show arp spoof status`** displays whether the ARP spoofing feature is currently enabled or disabled.

Detection of ARP Spoofing results in the triggering of ARP Spoofing alerts. These alerts display in the Attack Log component of Manager. Their names are prefixed with "ARP:" (for example, "ARP: ARP Spoofing with Different MAC Addresses").

Exit layer 2 pass-through mode

To return a device that is in Layer 2 Pass-Through Mode to normal operation, do the following:

1. For a standalone Sensor, click Devices → <Admin Domain Name> → Devices → <Device_Name> → Troubleshooting → **Layer 2 Bypass**.

   For Sensors in a stack, click Devices → <Admin Domain Name> → Devices → <Device_Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Layer 2 Bypass**.
2. Select **No** for the **Enabled** field.
3. Click **Save**.
4. Reboot the device.

Configure IP Settings

You can use Trellix IPS to parse IPv4 and IPv6 traffic for attacks. You can customize the IPv4 and IPv6 parameter checks for a Sensor using the **IP Settings** page. IP parameters are effective only when the configured Sensor is deployed in inline mode.

> **NOTE**
>
> Trellix IPS does not prevent DoS attacks involving IPv6 traffic.

NS-series Sensors can parse IPv6 packets.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **IP Settings.**
6. To edit a parameter, specify a new value and click **Update** for that parameter.

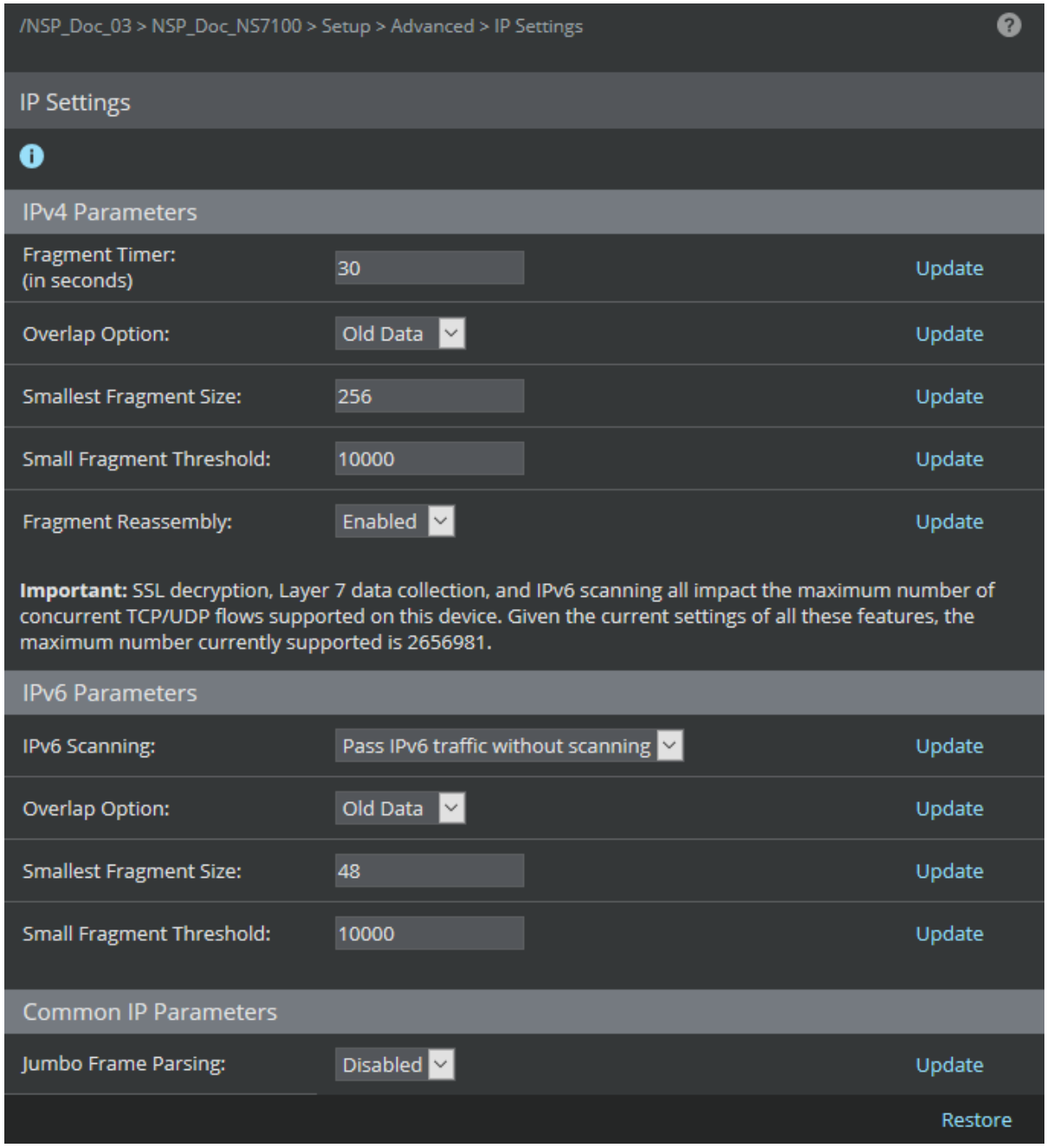
   > **NOTE**
   >
   > You must reboot the Sensor for the changes to take effect.

   To restore the default values, scroll down to the bottom of the page and click **Restore**.

   > **CAUTION**
   >
   > To prevent system errors, Trellix recommends that only users with detailed knowledge of IP configure these settings.

   - Trellix IPS can handle tunneled traffic.

- The communication between your Manager server, client, and Sensors can only be in IPv4.



Option	Definition
IPv4 Parameters	
Fragment Timer (in seconds)	Time to wait for all fragments of an IPv4 or IPv6 flow to be received or the transmission is dropped. The default value is 30 seconds.

Option	Definition
Overlap Option	Fragmented IPv4 packets might overlap, thus you need to select which data to process first - the newer data or the older data. By default, new data is processed first. • **Old Data** — Common for Windows and Solaris systems • **New Data**
Smallest Fragment Size	Smallest allowable size for an IPv4 fragment to be seen as "normal." All IPv4 fragments under this size are counted toward the IPv4 **Small Fragment Threshold**. The default size is 256. You can modify this to a value which is a multiple of 8 and is between 8 and 1480. You can enter a value between 8 and 1480 in multiples of 8.
Small Fragment Threshold	The number of IPv4 fragments under the IPv4 **Smallest Fragment Size** allowed in 60 seconds. If this threshold is exceeded, an alert is sent. The default is 10000. You can modify this to a value between 100 and 100,000.
Fragment Reassembly	When enabled, fragmented IPv4 traffic is held and reassembled to allow inspection. Disabling this option may help if you are experiencing dropouts in traffic, since partial fragments may timeout and be dropped while held. By default, fragment reassembly is enabled.
IPv6 Parameters	For IPv6 traffic, system events are generated for the following: • Reserved address where source or destination address is all zeros or 15 zeros then 1. • Final fragment with zero offset where next header = 44, fragment offset =0, and fragment header M = 0. You can view system events. For more information, see [Trellix Intrusion Prevention System Product Guide].
IPv6 Scanning	Specify how the Sensor should process IPv6 traffic. • **Drop all IPv6 traffic (inline only)** — The Sensor drops IPv6 traffic in the inline mode. • **Pass IPv6 traffic without scanning** — The Sensor passes IPv6 packets but does not scan them for attacks. • **Scan IPv6 traffic for attacks** — The Sensor scans IPv6 traffic for attacks. If you select **Scan IPv6 traffic for attacks** or if you had selected this earlier and you are selecting a different option now, then you need to reboot the Sensor for the change to take effect. By default, IPv6 packets are not parsed but allowed to pass. You can check the IPv6 status of a Sensor using the **`status`** command from Sensor CLI.

Option	Definition
Overlap Option	Fragmented IPv6 packets may overlap, thus you need to select which data to process first: the newer data or the older data. • **Old Data** — Common for Windows and Solaris systems • **New Data** • **Drop** — The Sensor drops any overlapping fragments. By default, older data is processed first.
Smallest Fragment Size	Smallest allowable size for an IPv6 fragment to be seen as "normal." All IPv6 fragments under this size are counted toward the IPv6 **Small Fragment Threshold**. The default size is 48. You can modify this to a value which is a multiple of 8 and is between 40 and 1280.
Small Fragment Threshold	The number of IPv6 fragments under the IPv6 **Smallest Fragment Size** allowed in 60 seconds. If this threshold is exceeded, an alert is sent. The default is 10,000. You can modify this to a value between 100 and 100,000.
Common IP Parameters	
Jumbo Frame Parsing	When enabled, Trellix IPS allows jumbo frame parsing of up to 9,216 bytes of IP payload for the following Sensor models: • NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150,NS7300, NS7200, NS7100, NS5200, NS5100, and NS3600 • IPS-VM5000 and IPS-VM600 on ESXi and KVM By default, jumbo frame parsing is disabled. After enabling this setting, update the configurations on the Sensor, and reboot the Sensor for the changes to be effective. **NOTE** Jumbo frame parsing is not supported on NS3500, NS3200, and NS3100 Sensors.

Configure Protocol Settings

You can customize the protocol parameters for a Sensor using the **Protocol Settings** page.

1. Click the **Devices** tab.
2. Select the domain from the **Domain** drop-down list.
3. On the left pane, click the **Devices** tab.
4. Select the device from the **Device** drop-down list.
5. Select Setup → Advanced → **Protocol Settings.**
6. To edit a parameter, type or select a new value and click **Update** for that parameter.

To restore the default values, scroll down to the bottom of the page and click **Restore**.

> **CAUTION**
>
> To prevent system errors, Trellix recommends that only users with detailed knowledge of TCP configure these settings.

Option	Definition
TCP	
TCB Inactivity Timer	If a TCB (Transmission Control Block) does not receive any packets before this timer expires, the TCB is marked inactive. TCBs are limited, therefore inactive TCBs can be allocated to new session (or connections).
TCP Segment Timer	Time to wait for the out of order segments to become ordered before dropping them.
TCP 2MSL Timer	Time to wait for a connection control block to be freed before it is torn down. The maximum segment lifetime (MSL) is the amount of time that a packet can be in transit on the network.
Cold Start Time	When Sensor is first turned on, it does not have any flow information. Set the Cold Start Time to specify a window of time for the Sensor to allow packets without established control blocks to pass through.
Cold Start Ack Scan Alert Discard Interval	After a cold start, the Sensor will not alert for Ack Sweeps or Ack Scans until this interval (timer) expires.
Cold Start Drop Action	When starting a Sensor for the first time, you can decide to allow (forward) or drop all packets that do not have a flow control block recognized by the Sensor. • **Forward Flows** • **Drop Flows**

Option	Definition

TCP Flow Violation	• **Permit** — For out-of-order packets, the Sensor holds packets up to (TCP Segment Timer) seconds for re-assembly before performing inspection. If re-assembly fails because some packets are still missing, the Sensor simply forwards the traffic. When the TCP state is not established, the Sensor allows the packets to pass through.
	• **Deny** — For out-of-order packets, the Sensor holds packets up to (TCP Segment Timer) seconds for re-assembly before performing inspection. If re-assembly fails because some packets are still missing, the Sensor drops the traffic. When the TCP state is not established, the Sensor drops the traffic.
	• **Permit out-of-order** — The Sensor allows out-of-order packets to continue to transmit without processing. When the TCP state is not established, the Sensor allows the packets to pass through.
	• **Deny no TCB** (Deny if State Not Established) — For out-of-order packets, the Sensor holds packets up to (TCP Segment Timer) seconds for re-assembly before performing inspection. If re-assembly fails because some packets are still missing, the Sensor simply forwards the traffic. When the TCP state is not established, the Sensor drops the traffic.
	• **Stateless Inspection** — The Sensor detects attacks without requiring a valid TCP state. This option should be used only when Sensors are placed in a network where the Sensors do not see all packets of a TCP flow like in an asymmetric network configuration. Stateless Inspection can only be implemented in IPv4 packets.
	When Stateless Inspection is enabled:
	  • Firewall and syn cookie protection cannot be enabled.
	  • HTTP redirection to the Remediation Portal may or may not work depending on your network deployment scenario for example, in a setup where SYN+ACK packets cannot be sent from the Sensor to the client.

Normalization On/Off Option	Sensor performs TCP/IP/ICMP options checking to normalize the traffic.
TCP Overlap Option	TCP segments may overlap, thus you need to select which data to process: the newer data or the older data. • **New Data** — Common for Linux, Solaris, HP_UX, and FreeBSD systems • **Old Data** — Common for Windows systems

Option	Definition
SYN Cookie	SYN cookies are used to counter SYN flood attacks. With SYN cookies enabled, whenever a new connection request arrives at a server, the server sends back a SYN+ACK with an Initial Sequence Number (ISN) uniquely generated using the information present in the incoming SYN packet and a secret key. If the connection request is from a legitimate host, the server gets back an ACK from the host. • **Disabled** — Disable SYN cookies. • **Inbound Only** — Use SYN cookies for inbound traffic only. • **Outbound Only** — Use SYN cookies for outbound traffic only. • **Both Inbound and Outbound** — Use SYN cookies for inbound and outbound traffic. **CAUTION** • SYN cookie feature is not enabled by default. • Do not enable SYN cookies when passing MPLS traffic through a Sensor. • Sensors using SYN cookie settings must be in inline mode. If you don't have any ports in inline mode, configure at least one port to be inline. • A Sensor will only see a packet once on any interface. However, if a Sensor is monitoring an interface containing VLAN-tagged traffic, a separate subinterface must be configured for each VLAN to ensure a packet is not seen more than once.
Inbound Threshold Value	The number of incomplete SYNs beyond which SYN cookies have to be enabled for an incoming connection.
Outbound Threshold Value	The number of incomplete SYNs beyond which SYN cookies have to be enabled for an outgoing connection.
Reset unfinished 3 way handshake connection	When enabled, automatically sends a TCP RST to the source when the TCP SYN timer has expired for a connection. • **Disabled** • **Set for all traffic** • **Set for DoS attack traffic only**
UDP	
Supported UDP Flows	Number of UDP transmissions allowed per Sensor. This varies for each Sensor model. The default number of UDP transmissions that is supported is displayed, which you can change. See the NS-series Sensor capacity by model number (page 2321) for the default and maximum number of supported UDP flows for each Sensor model.
Unsolicited UDP Packets Timeout	Time to wait to receive a response packet for a sent packet. If time not met, the packet is dropped.
DNS	

Option	Definition
DNS Sinkholing Time-To-Live (TTL)	The TTL to be included in the crafted DNS response packets sent by the Sensor. **NOTE** The default and the maximum values are 720 minutes.
DNS Sinkholing IP Address:	The IP address to which the bot traffic is sinkholed. **NOTE** The default value is the loop back IP address (127.0.0.1 for A records and ::1 for quad-A records present in the actual DNS response). You can configure an IPv4 address for the bot to send the bot traffic to that server. You cannot configure an IPv6 address as a sinkhole server IP address.
FTP	
FTP Acceleration	Set the fast forward FTP data flows feature.
HTTP2	
Flow Allocation %	Set the maximum HTTP2 flows as a percentage of total supported flows. This value differs for each Sensor model. • For NS7500 and NS3600, it can range between 1% to 5%. • For NS9500 and NS7600, it can range between 1% to 10%. **NOTE** The Sensor requires a reboot after updating the flow allocation.
Include decoded packets in attack packet log	While inspecting HTTP2 traffic, the Sensor decodes the HTTP2 packets/frames into HTTP requests/responses. By enabling this, the Manager will include decoded HTTP requests/responses along with HTTP2 packets/frames in the attack packet log.

Option	Definition
Slowloris Attack Configuration	Allows you to configure the values for the following parameters: • **Slow Post Timeout** - Set the value between 5 and 30. • **Slow Post Threshold Frame Size** - Set the value between 1 and 100. • **Slow Post Minimum Number of Streams** - Set the value between 50 and 100. • **Slow Post Min Number of Tiny Frames** - Set the value between 1 and 10. • **Slow Read Timeout** - Set the value between 30 and 300. • **Slow Read Window Size** - Set the value between 1 and 100. • **Slow Read Minimum Number of Streams** - Set the value between 50 and 100. **NOTE** Users are recommended to modify these settings only in consultation with Trellix support team.

How to counter SYN floods with SYN cookies

A SYN flood attack is a series of SYN packets from forged IP addresses targeted at a specific server. When a server is attacked in this manner, the SYN queue in the server fills and all new connection requests are dropped. The SYN cookie feature is a mechanism to counter SYN flood attacks. This feature is an adjunct to the existing statistical anomaly-based Denial of Service detection. In cases where a DoS attack is already underway and there is no time for learning a long-term profile, Trellix IPS provides the ability for the Sensor to proxy all inbound three-way handshakes.

With SYN cookies, whenever a new connection request arrives at a server, the server does not maintain any information about the connection request. Instead it sends back a SYN+ACK with an ISN uniquely generated using the information present in the incoming SYN packet and a secret key. If the connection request is from a legitimate host, the server gets back an ACK from the host.

The Sensor will support a configurable threshold for SYN arrival rate, above which the Sensor will begin using SYN cookies to avoid having to maintain state during the three-way handshake. The Manager provides an interface to the user to enable/disable the SYN cookie feature. It also provides user the ability to configure the threshold values for the SYN cookies.

Asymmetric traffic handling

Traffic that uses different paths for the request and response is termed as asymmetric traffic. There are chances of having asymmetric traffic within a network, when networks increase in size.

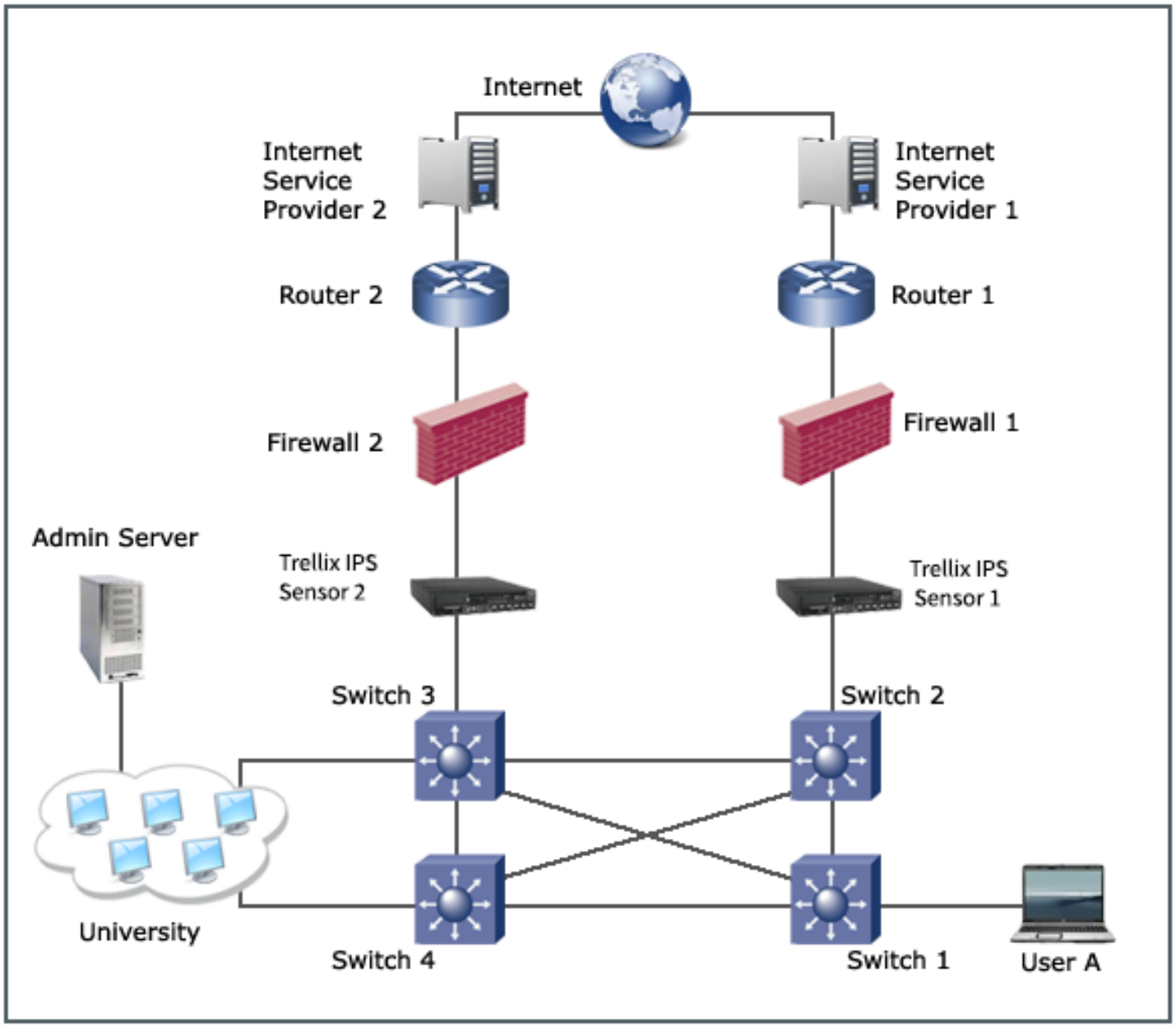
If there are chances of asymmetric traffic in your network, consider the following options:

- Install IPS Sensors at a location where the traffic is symmetric.
- Place an IPS Sensor each on the request and the response path of the asymmetric traffic and create a HA pair to sync up the traffic flow between the two Sensors.

- When the distance between the two IPS Sensors is such that a HA pair cannot be created, consider enabling Stateless Inspection.

> **NOTE**
>
> Sensors in a HA pair scan the traffic independently, but they also share the information with each other during the scanning process. In this way, if a flow happens to be asymmetrically routed across both Sensors, each Sensor will end up with full flow.

Figure 697. Asymmetric traffic representation



The diagram above explains about HTTP traffic flow in an asymmetric network between User A and the University Admin server. The outgoing connection flow from User A is through Switch 1, Switch 2, Sensor 1, Router 1, Internet Service Provider 1, to the

Internet connection. The return path for the packet however, is through Internet Service Provider 2, Router 2, and so on. If traffic flows by the Sensor in an asymmetric manner as described above, all packets of a TCP flow are not visible to a single Sensor. In such a scenario, if Stateless Inspection is enabled, the Sensor will inspect packets without having the valid state for the TCP connection.

CAUTION

When you enable Stateless Inspection, there are chances of false positives, false negatives, and lower detection accuracy compared to when the Sensor sees all traffic. This is because, when a single communication flow is divided across paths, each interface will receive and analyze part of the conversation. Trellix recommends that you use Stateless Inspection only when network configuration does not allow the Sensor to be placed in locations where it could see all traffic.

Configuring non-standard ports

When the destination IP address is listening for a protocol on a port that is not standard, that port is called a *non-standard port*. For example, HTTP by default uses port 80 or 8080; therefore, a Sensor reading a packet with port 80 or 8080 attempts to decode that traffic as HTTP traffic. However, if a user is running an HTTP server on port 2560, it is recommended that the user add this non-standard port parameter. This protects the system from experiencing any false positives from unrecognized port-protocol communication and having malicious activity sent through a "back door."

NOTE

This note is relevant only if you are using the default Service rule objects for features such as Quarantine, Firewall Access Rules, and QoS. The Sensor considers all the standard ports as well as non-standard port numbers that you have defined in the **Non-Standard Ports** page when detecting a protocol. Port numbers are irrelevant if you are using the Application Rule Objects to detect protocols.

You can configure the non-standard ports for the admin domain. These port numbers are inherited by all the Sensors in the admin domain as well as by Sensor ports allocated to a child domain. At the Sensor level, you can append more port numbers to the inherited list. However, you cannot edit or delete the inherited list at the Sensor level. You can define non-standard port numbers at the Sensor level even if you have not configured any at the domain level.

Define the non-standard ports at the domain and Sensor levels

Trellix IPS validates standard ports used across various protocols using the signature set.

You can add more than one non-standard port per protocol; however, you can only add one port at a time. If multiple ports have been added for a single protocol, all entered non-standard ports appear in one entry. Consider you added two non-standard ports, 1121 and 1281 for FTP traffic (standard FTP port is 21). Each non-standard port was added separately, yet both appear in the same entry.

1. To define non-standard ports for an admin domain:
   a. Click the **Devices** tab.
   b. From the **Domain** drop-down list, select the domain you want to work in.
   c. On the left pane, click the **Global** tab.

d. Select IPS Device Settings → **Non-Standard Ports.**

2. To define non-standard ports for a Sensor:

   a. Click the **Devices** tab.

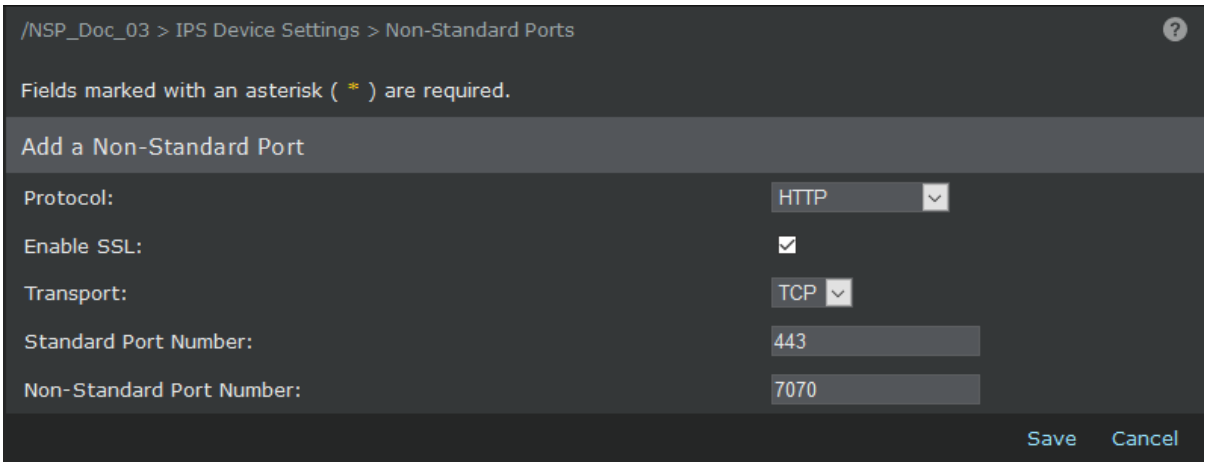
   b. Select the domain from the **Domain** drop-down list.

   c. On the left pane, click the **Devices** tab.

   d. Select the device from the **Device** drop-down list.

   e. Select Setup → Advanced → **Non-Standard Ports.**

3. Click + and specify the options in the corresponding fields.



Option	Definition
Protocol	Lists the protocols for which you can specify the non-standard ports.
Enable SSL	To specify the non-standard port for HTTPS, select HTTP as the **Protocol** and select **Enable SSL**.
Transport	The **Transport** protocol is automatically selected based on the protocol selected. If applicable, you can toggle between TCP and UDP.
Standard Port Number	Automatically displays the standard port number for the selected protocol.
Non-Standard Port Number	Type a port number between 1 and 65535. You cannot enter a standard port number in this field.
Save	Saves the non-standard ports for the corresponding protocol.
Cancel	Ends adding the non-standard ports.

The Manager does not allow you to configure a standard port number for a protocol as the non-standard port. In such an event, the Manager displays the error "The non-standard port number cannot be same as the standard port number."

If the assigned non-standard port is a standard port for another protocol, the Manager displays the error "The input non-standard port number is the standard port number for <protocol name>.The update configuration to Sensor fails on set of this non-standard port number. Please try again with different settings."

If you upgrade from an older version of the Manager, and if there is a conflict between the non-standard port assigned and the standard port in the signature set, the signature set update fails. In this scenario, manually update the conflicting port number.

4. Click **Save**.
5. Perform a configuration update for the Sensor from Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab. Select the Sensor and click **Deploy**. Select the required configurations from **Sync: <Device Name>** window and click **Deploy**. For more information, see Deploy pending changes to a device (page 873).

> **NOTE**
>
> You can also perform configuration update from Devices → <Admin Domain Name> → Devices → <Device Name> → **Deploy Pending Changes**. Select the required configurations and click **Deploy**.

Edit a non-standard port entry

Editing a non-standard port entry means deleting a non-standard port number for a protocol. You cannot add a non-standard port number to an existing record. To add a non-standard port number to an existing record, you have to create a record for the same protocol and specify the required non-standard port number. When you save the record, the new number is automatically appended to the existing record for the protocol.

Editing non-standard port entries is dependent upon the number of non-standard ports you entered for a given protocol. For example, assume that you have employed port 1021 for FTP traffic and added this entry. When you go back to edit the entry, your only option is to delete port 1021, which means deleting the entire non-standard port record for FTP. However, if you separately added entries for ports 1021 and 1121 for FTP traffic, editing this non-standard port entry enables you to delete one of the non-standard ports rather than both.

1. To edit non-standard ports for an admin domain:
   a. Click the **Devices** tab.
   b. From the **Domain** drop-down list, select the domain you want to work in.
   c. In the left pane, click the **Global** tab.
   d. Select IPS Device Settings → **Non-Standard Ports.**
2. To edit non-standard ports for a Sensor:
   a. Click the **Devices** tab.
   b. Select the domain from the **Domain** drop-down list.
   c. On the left pane, click the **Devices** tab.
   d. Select the device from the **Device** drop-down list.
   e. Select Setup → Advanced → **Non-Standard Ports.**
3. Select a record and click 

   At the Sensor level, you can view the inherited list from the admin domain but cannot delete these.

Table 91. Option definitions

Option	Definition
Protocol	Displays the application protocol and the transport protocol you specified when you created the record
Standard Port Number	Automatically displays the standard port number for the selected protocol
Non-Standard Port Number	Displays the non-standard port numbers that you added for the protocol
Delete	Permanently deletes the selected **Non-Standard Port Number**
Cancel	Closes the **View/Delete Non-standard Ports** page

4. For the changes to take effect, perform a configuration update for the Sensor.

Using context-aware data for network forensics

As a security administrator, you may want to analyze the root cause of a specific security event a few hours or days after an event has occurred. You may also want any supporting contextual data for an endpoint during that time interval.

NTBA performs context-aware network forensics to capture connections and layer 7 activity before and after a security event. This helps forensic analysis to be performed on the contextual data, against a set of predefined suspicious activity indicators.

NTBA collects forensic data for a target or attacker that is internal or external to the network. NTBA collects context-aware data as profile and forensic data. Profile data includes details like executables and services launched by an endpoint. Forensic data presents contextual data captured for specific minutes before and after a security event occurs like policy violation or an attack. By default, forensic data is collected for 10 minutes before and after an event.

The network forensics data collected by NTBA provides details such as connections made to a target and attacker, port information, network application, executables, URLs, and files. Metadata information like malware confidence, executable classification, reputation, and location are also shown if available. If a connection is suspicious, a Suspicious Activity indicator briefs the type of suspicious activity performed in the network.

How NTBA collects and stores context-aware data

When a security event like an attack occurs, NTBA performs the following high-level steps to collect context-aware data:

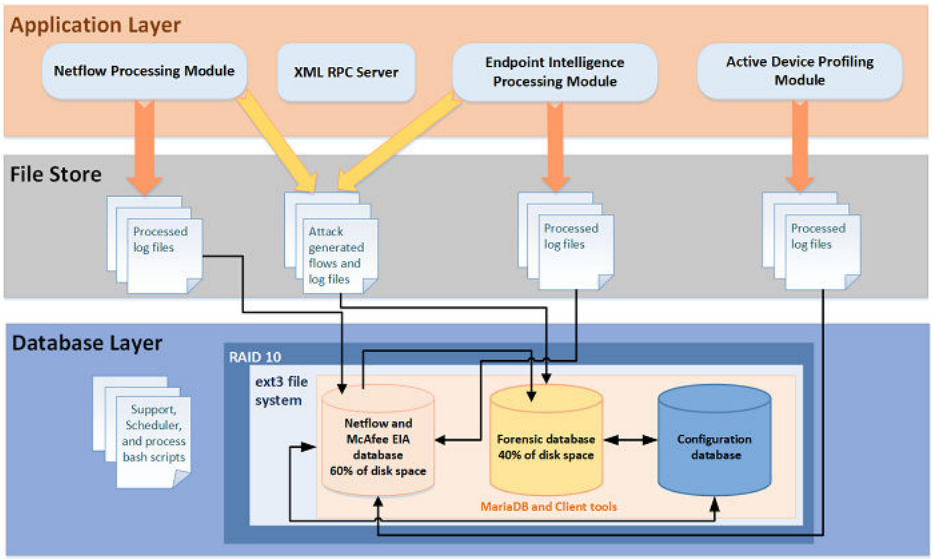
1. Consolidates conversations with attack information like 5-tuple, URLs, files, and programs involved in the connection for a target or attacker.
2. Collects the accessed URLs, files, executables, and connections for the specified time interval based on suspicious activity indicators. By default, these details are collected 60 minutes before and after an event occurred.
3. Checks if the endpoint is an attacker or target.
4. Collects data based on conditions that match the suspicious activity indicators.

Once the context-aware data is collected, NTBA stores this in the database for the configured period. By default, forensic data is stored for 30 days. You can configure the collection settings from Devices → Devices → <NTBA device> → Setup → **Collection Settings**.

The Manager enables you to configure the forensics collection settings, and retrieves the context-aware data from NTBA when you want to perform forensic analysis on a specific endpoint or attack.

The forensic data is stored as part of the virtual disk of NTBA. By default, the netflow data uses 60% and forensic data uses 40% of the disk space. By enabling export of Layer 7, the entire payload is not exported. Only fields related to HTTP, netbios, FTP, SMTP, file hash, and attack ID are exported. In HTTP application, specific fields of HTTP (like URI and host) are exported. Netflow monitoring is not made in real time as the statistics of the particular flow is sent every minute.

Figure 698. NTBA database architecture



The RAID 10 layer is the first layer, followed by ext3 file system, and database layer is the container for the netflow, forensic, and configuration databases.

You can modify the forensic database pruning settings from the Devices → Devices → <NTBA Device> → Maintenance → **Database Pruning** page. For more details, see [Maintenance of system data and files] in [Trellix Intrusion Prevention System Product Guide].

When you analyze an endpoint on the Network Forensics page, the Manager queries all the NTBAs and displays data from the NTBA that is mapped to the endpoint. On the Analysis → **Network Forensics** page, the displayed network forensic data is only from a single NTBA.

NOTE

If an IP address is mapped to more than one NTBA, the Network Forensics page has **Data Source** drop-down list to view network forensics data for NTBA mapped to an endpoint. The drop-down can be used to query the other NTBAs for forensic information.

NOTE

By default, if you directly navigate to the **Network Forensics** page to analyze an endpoint, the current date and time and analysis window of ± 60 minutes is displayed. If you perform forensics from other Manager UI paths for an endpoint, by default, the time of event occurrence and analysis window of ± 10 minutes is displayed.

Suspicious activity indicators

NTBA uses a set of predefined indicators to collect the forensic data. The indicators are triggered only when an attacker or target endpoint, flow, or executable makes a network connection in the configured analysis time window.

For example, on the **Network Forensics** page, you select an IP 1.1.1.6 that is involved in a policy violation. You select an analysis time of ±30 minutes to analyze the collected flows before and after the policy violation happened, and click **Analyze**. The suspicious flows and activity indicators are displayed based on connections made in the network in this defined time window of one hour.

NTBA collects forensic data based on the following rules:

Table 92. Suspicious activity indicators

Suspicious activity indicator	Description
Destination matches attacker in another attack	A target endpoint was involved in another attack or traffic from/to this endpoint.
Source matches attacker in another attack	An attacker endpoint was involved in another attack or traffic from/to this endpoint.
Suspicious endpoint risk	Endpoint made a connection to another endpoint with GTI risk level of **Medium Risk** or **High Risk**.
Unverified endpoint risk	Endpoint made a connection to another endpoint with GTI risk level of **Unverified**.
Executable used in another attack	Executable, for example, chrome.exe was involved in another attack or traffic from/to this endpoint.
Suspicious executable malware confidence	Endpoint accessed an executable that has malware confidence level above **Medium**.
Blocked executable	Endpoint accessed a blocked executable.
New executable	Endpoint accessed a new executable that has not been previously seen in the last x* days. *x refers to the number of days defined on the **Devices | NTBA Device Settings | Device Settings | Setup | Collection Settings** page.
URL used in another attack	Endpoint accessed a URL that was involved in another attack or traffic from/to this endpoint.
Suspicious URL risk	Endpoint accessed a URL with GTI risk level of **Medium Risk** or **High Risk**.
Unverified URL risk	Endpoint accessed a URL with GTI risk level of **Unverified Risk**.
File used in another attack	Endpoint accessed a file that is involved in another attack or traffic from/to this endpoint.
Suspicious file malware confidence	Endpoint accessed a file with suspicious malware confidence of **Medium** or **High**.
Unverified file malware confidence	Endpoint accessed a file with suspicious malware confidence of **Unknown**.
Attack detected	Specific suspicious flow generated an attack in the network.

Suspicious activity indicator	Description
New service detected	A new service was installed on an endpoint that has not been previously seen in the last x* days. *x refers to the number of days defined on the Devices → NTBA Device Settings → Device Settings → Setup → **Collection Settings** page.

On the Analysis → **Network Forensics** page, these are displayed in the **Suspicious Activity** column. You can also use these indicators as filters from the **Any Activity** drop-down list to view specific suspicious activity-based flows in the network.

NOTE

If EIA is disabled, executable-related indicators like executable used in another attack are not available. Similarly, if Trellix GTI is disabled, reputation-based indicators are not functional.

Enable Network Forensics

When network forensics is enabled, the Manager takes advantage of the NTBA Appliance to provide network activity for a given endpoint over a given time span. You can collect network forensic data for a time period for analysis.

1. At the Global level, select Devices → Global → NTBA Device Settings → Device Settings → Setup → **Collection Settings**.

   TIP

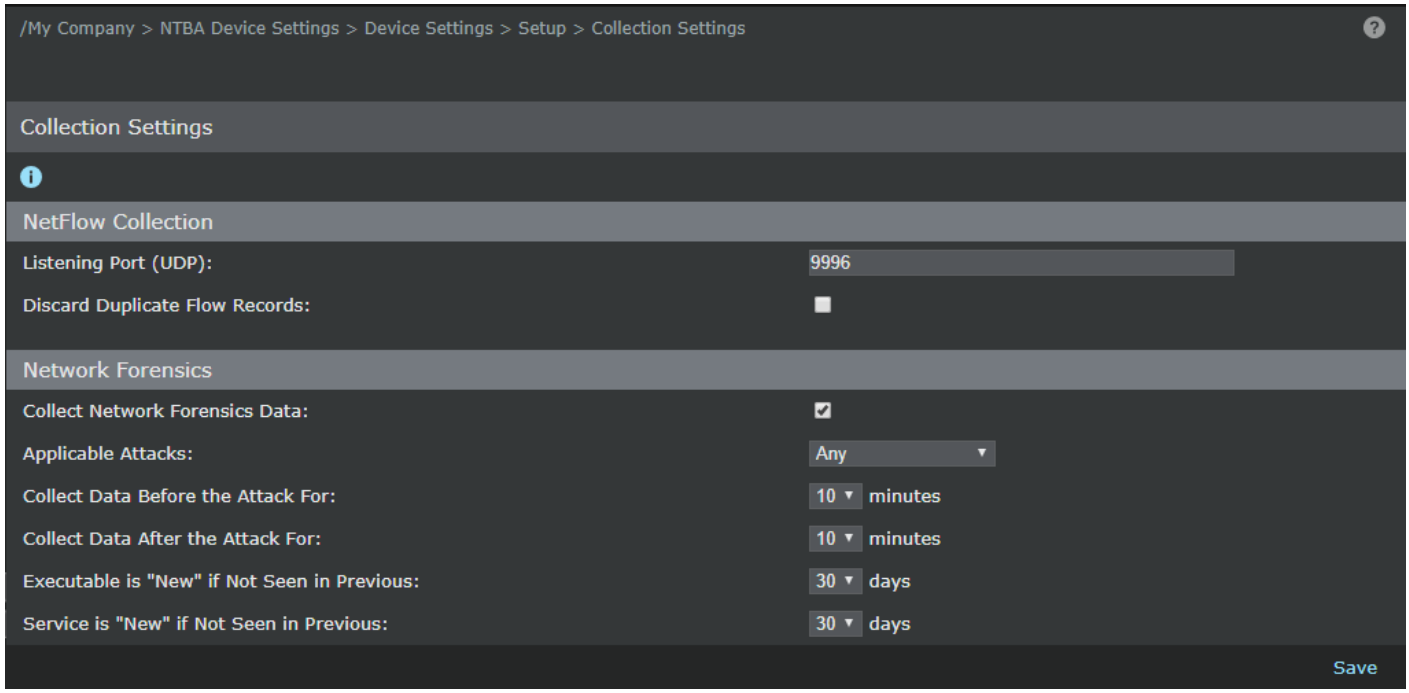
   At a device level, you can navigate to Devices → Devices → <NTBA Appliance> → Setup → **Collection Settings**. If you want to inherit the global level collection settings, select **Use Global Settings**.

2. Enter the listening port and select **Discard Duplicate Flow Records** if you do not wish duplicate records. By default, the UDP port is set to 9996.
3. In the **Network Forensics** area, specify the following:

Item	Description
Collect Network Forensics Data	Select this checkbox to collect network forensics data. By default, this checkbox is selected.
Applicable Attacks	Select **Any**, **IPS Attacks Only** or **NTBA Attacks Only**. By default, this is set to **Any**.
Collect Data Before the Attack For	Select the time for which you wish to collect data before a security event. By default, this is set to 10 minutes. The time range is 1-60 minutes.
Collect Data After the Attack For	Select the time for which you wish to collect data after a security event. By default, this is set to 10 minutes. The time range is 1-60 minutes.
Executable is 'New' if Not Seen in Previous	Collect executable details if the executable is new in the network. By default, this is set to 30 days. The day range is 3-90 days.

Item	Description
Service is 'New' if Not Seen in Previous	Collect service details if the service is new in the network. By default, this is set to 30 days. The day range is 3-90 days.

Figure 699. Forensic data collection



4. Click **Save**.

> **TIP**
>
> If no forensic data is displayed, execute the **`show forensic-db details`** command to check if the network forensics feature is enabled or not. By default, this feature is enabled. You can use the **`set dbdisksize`** and **`show l7dcapstats`** commands to set the percentage of disk size for the forensic data and view layer 7 captured data details.

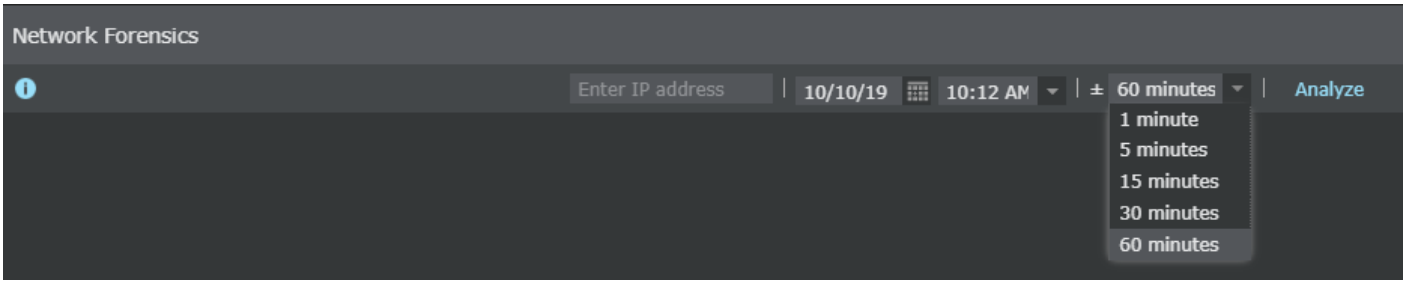
Perform network forensics on an endpoint from the Analysis tab

You can enter an IP address and track its network behavior for a specified time period.

Go to Analysis → **Network Forensics** to analyze the recent behavior of the specific endpoint in the network, including conversations and events in the specified time period.

Filter your view by choosing the time and date of your choice. Use the **±** option to view data before and after an attack. This enables to analyze context-aware data and see network behavior of an endpoint in the network.

Figure 700. Date and time options

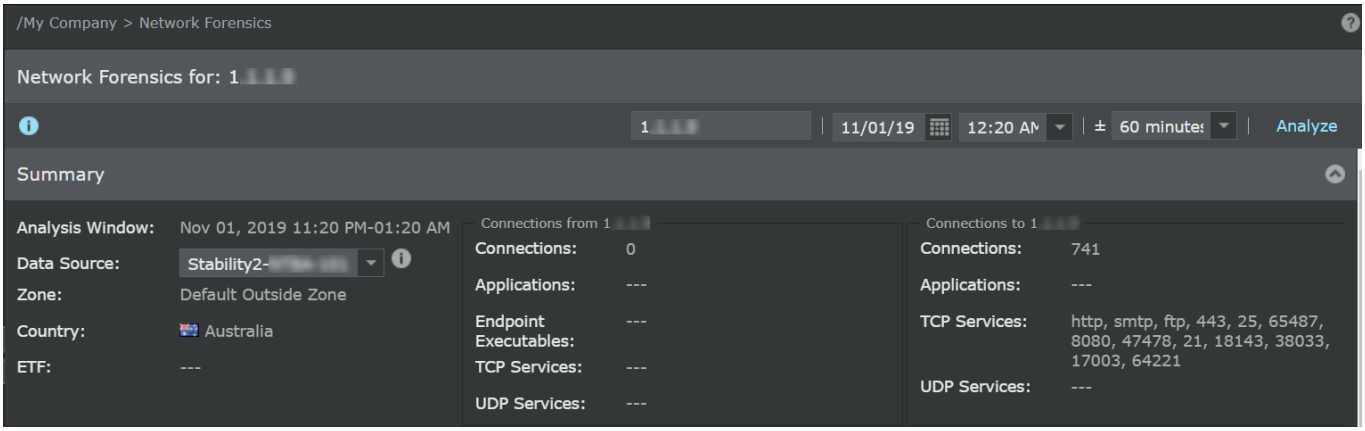


The following table shows the information displayed on the **Network Forensics** page.

Item	Description
Filter Criteria Panel	
Enter IP address	Enter the IP address of the endpoint whose network activities you wish to analyze.
Date	Select the date when the event occurred.
Event occurrence time	Select the time at which the event occurred. The event can be an attack, alert, or policy violation.
Analysis window	Select the time period in which you wish to track an endpoint's activities in the network. This includes activities performed by an endpoint before and after a security event.
Analyze	Retrieves suspicious flows, activities, and indicators for an event in the specified time period.

1. In the **Enter IP address** field, enter an IP address for which you wish to view the suspicious flows and activity. Example: 1.1.1.9.
2. Select the date and time. Use the **±** time to view endpoint behavior before and after an attack.
3. Click **Analyze**.
4. In the top panel, view **Summary** for endpoint details and connections made to and from an endpoint.

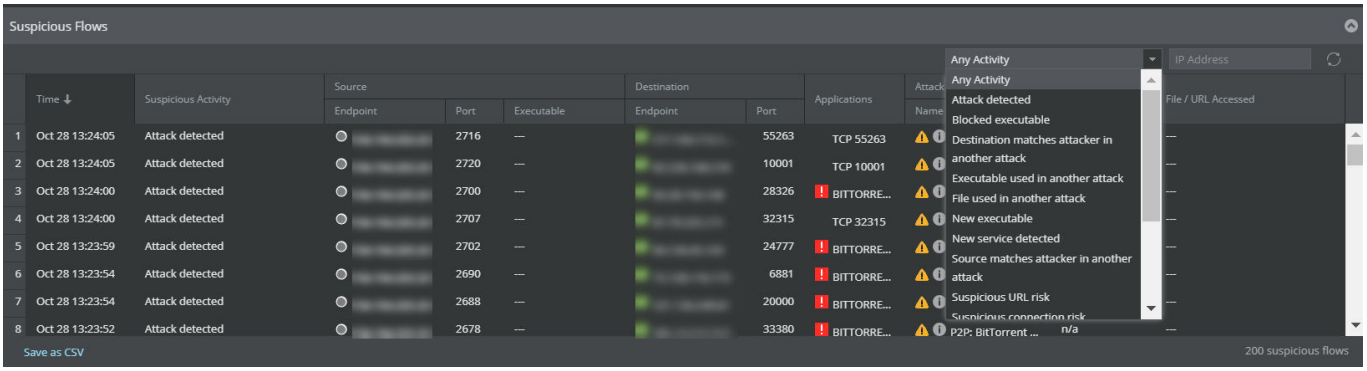
Figure 701. Summary Panel



Item	Description
Summary Panel	
Endpoint Summary	• **Analysis Window** — The period of analysis. • **Data Source** — The NTBA device that is mapped to an endpoint IP address. **NOTE** If one or more NTBAs have an endpoint IP address within the same time range, you can view these NTBA devices from this drop-down list. • **Zone** — The zone to which this endpoint belongs to. • **Country** — The country of the endpoint. • **ETF** — The ETF value assigned by NTBA to an endpoint.
Connections from endpoint	Specifies the client connections from an endpoint that include the TCP and UDP services and ports. • **Connections** — The number of connections made from an endpoint. • **Applications** — The applications accessed from an endpoint. • **Endpoint Executables** — The executables accessed. • **TCP Services** — The tcp services used by an endpoint. • **UDP Services** — The UDP services accessed by an endpoint.
Connections to endpoint	• **Connections** — The number of connections made to an endpoint. • **Applications** — The applications used on an endpoint. • **TCP Services** — The TCP services used on an endpoint. • **UDP Services** — The UDP services accessed on an endpoint.

5. In the lower panel, view **Suspicious Flows** for details like suspicious activity, applications, attack name, and files and URLs accessed.
   - From the flows, select the indicator to view specific activity-based flows. Example: Blocked executable.
   - View suspicious flows that have blocked executables involved in the attack.

Figure 702. Suspicious activity indicator filter



Item	Description
Suspicious Flows Panel	
Suspicious activity indicators	View indicators that map to an event like an alert or attack. • Destination matches attacker in another attack • Source matches attacker in another attack • Suspicious endpoint risk • Unverified endpoint risk • Executable used in another attack • Suspicious executable malware confidence • Blocked executable • New executable • URL used in another attack • Suspicious URL risk • Unverified URL risk • File used in another attack • Suspicious file malware confidence • Unverified file malware confidence • Attack detected • New service detected
IP Address	Specify an IP address and use **Search** to view flows for this address.
Time	Displays the date and time when the suspicious flow for an event occurred. **TIP** You can sort the flows view based on time.

Item	Description
Suspicious Activity	Displays the indicator that specifies the suspicious activity performed like an URL accessed that was involved in another attack, blocked executable accessed and others.
Source	Specifies the source from which the flow was initiated for an endpoint. Details include endpoint and ports used.
Destination	Specifies the destination details like endpoint involved and port.
Applications	Displays the applications accessed from the endpoint.
Attack	Attacks for a specific endpoint that includes attack name and result.
File/URL Accessed	Specifies file or URL access details for a specific endpoint.

6. Click **Save as CSV** to export suspicious flows for analysis.

Managing devices

Management of remote access

From the **Remote Access** tab, you can perform the following actions:

- Adding a device Logon Banner: Add banner messages to be displayed on the Sensor CLI.
- Configure TACACS+ authentication: Use a TACACS+ server to authenticate Sensor logins.
- Managing NMS users: Create NMS users.
- Manage NMS IPs: Add NMS IP addresses.

Add a device logon banner

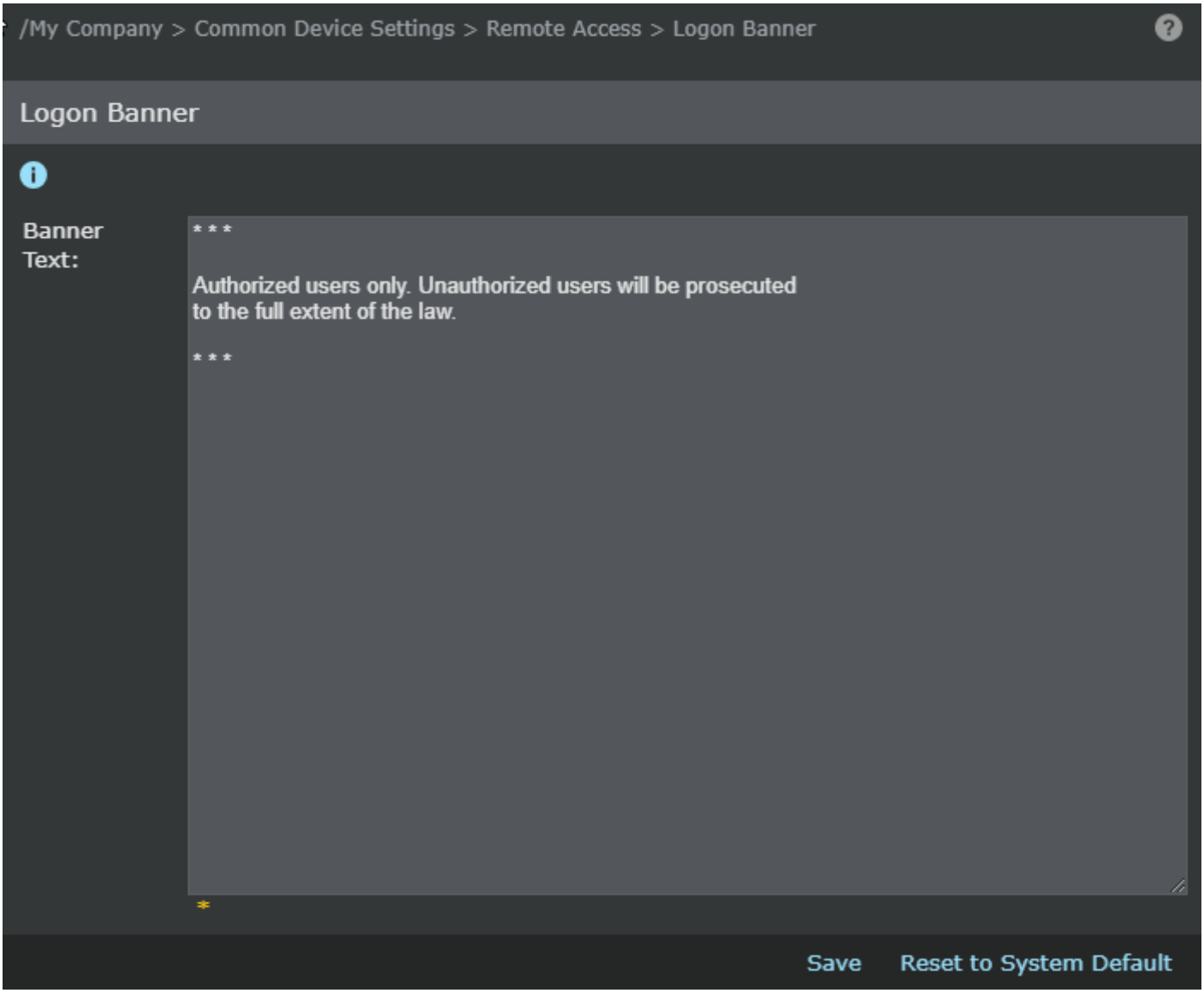
Trellix IPS supports display of messages on the Sensor CLI while logging onto the device. You can customize the message using the Manager.

NOTE

Support for device **Banner** is available for all the hardware devices.

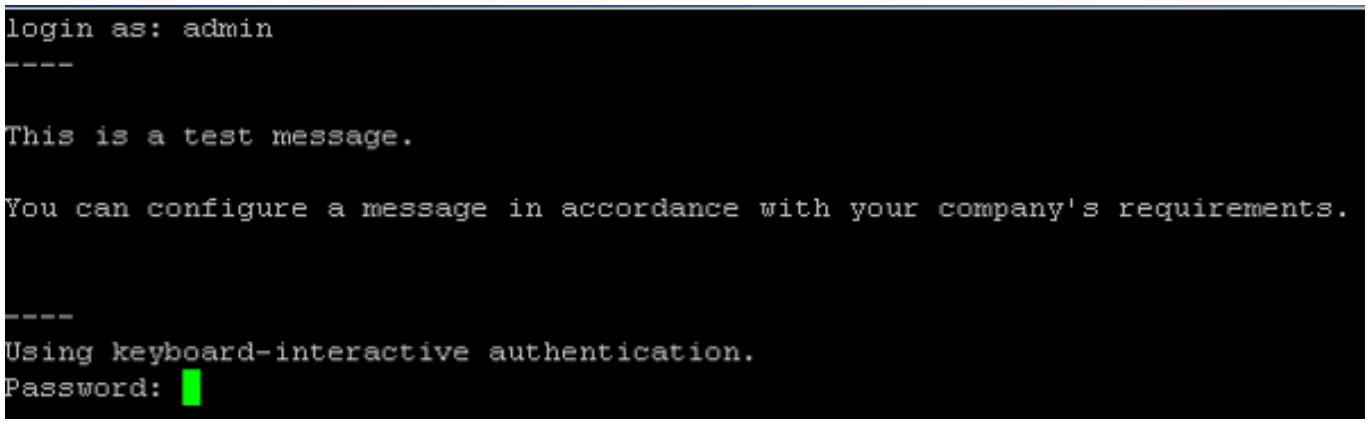
1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → **Logon Banner**.

   A default **Logon Banner** message is displayed.



2. Type a text message that you would like to display on the Sensor CLI.

   You can enter up to 2048 characters.
3. Click **Save** to save the customized message. Click **Reset to System Default** to restore the default **Logon Banner** message.
4. Select Devices → <Admin Domain Name> → Devices → <Device Name> → **Deploy Pending Changes**.
5. View the update information, and select the **Configuration and Signature Set** checkbox.
6. Click **Update**.
7. Log onto the Sensor CLI to view the customized message.



The customized message is displayed on all devices configured to the Manager, and persists across upgrade/downgrade as well as after a **reboot** until **Reset to System Default** from the Manager.

Managing devices access using TACACS+

The **TACACS+** tab enables you to use TACACS+ (Terminal Access Controller Access Control System) to control user access to the device console. With TACACS+, user accounts can be centrally stored and authenticated. TACACS+ is an access-control protocol that allows a device to authenticate all login attempts through a central authentication server. By using TACACS+, the task of administering passwords on each device can be simplified by doing the user authentication on a central server.

Using the Manager, you can configure TACACS+ server at the Admin Domain level and allow devices to inherit this configuration. You can disable this TACACS+ authentication for individual devices using the **Remote Access** option of the device in question.

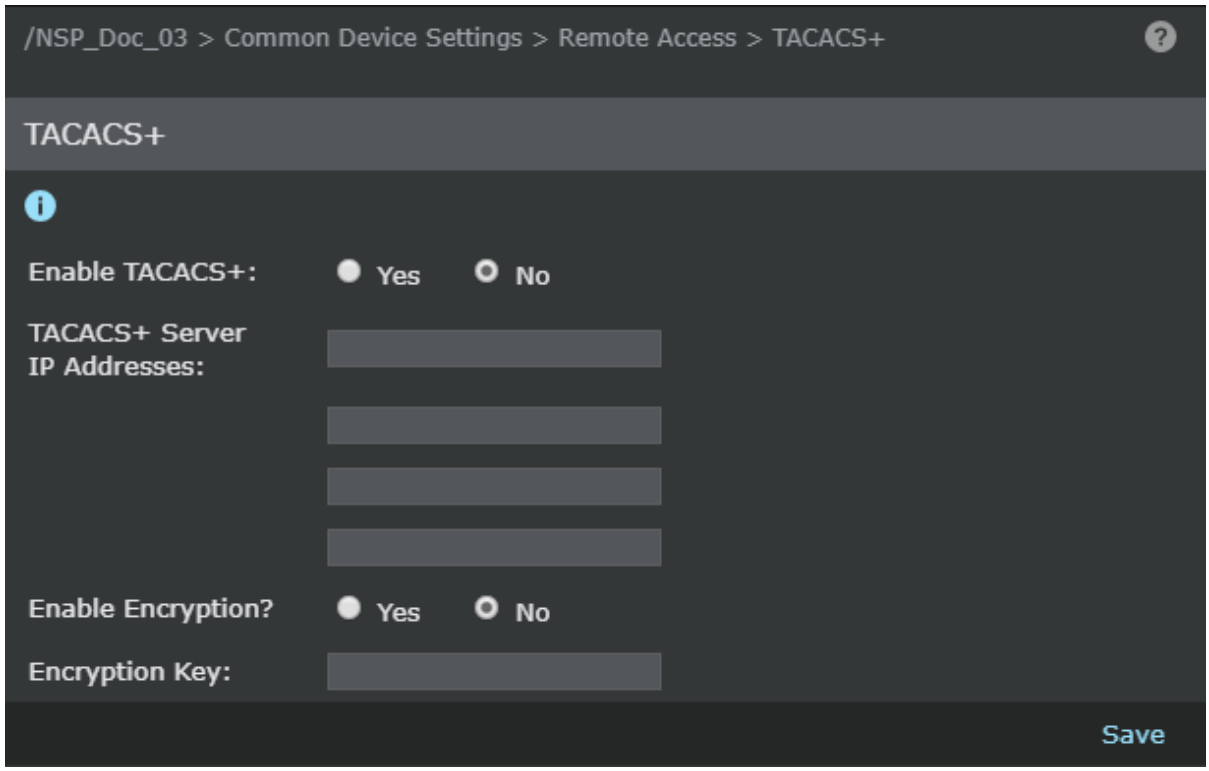
NOTE

Trellix recommends that either TACACS+ users or local users on the Sensor should be configured. If both are required, ensure that users with the same name are not present in the Sensor and the TACACS+ server.

Configure TACACS+ authentication

The **TACACS+** action enables you to enable and disable TACACS+ authentication for the selected admin domain. The Manager does not support TACACS+ and RADIUS authentication at the same time for an admin domain/device. Enabling both the authentication systems may result in conflict, and hence both may not function efficiently. A pop-up message is displayed whenever either one of the authentication system is already enabled.

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → **TACACS+**.



2. Select **Yes** to enable TACACS+.
3. Enter the **TACACS+ Server IP Addresses**; you can enter up to four IP Addresses for the TACACS+ server. At least one IP address is required if you enable TACACS+.
4. To encrypt TACACS+ traffic select **Yes** to **Enable Encryption?**.

   If you select **Yes**, you need to enter an encryption key in the **Encryption Key** field. The maximum length of the key is 64 bytes.
5. To save the changes, click **Save**.

> **NOTE**
>
> The **Inherit Settings** choice is available for the **Enable TACACS+** option from child admin domains.

Managing devices access using RADIUS

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization, and accounting) protocol for applications such as network access.

While connecting to the Sensor CLI through the client program, you are required to enter a user name and password. The information is passed through a Network Access Device (NAD) device, and then to a RADIUS server over the RADIUS protocol. The RADIUS server checks if the information is correct using authentication scheme like PAP. If accepted, the server authorizes the access.

Using the Manager, you can configure a RADIUS server to authenticate users. You can configure a maximum of two RADIUS servers. If the first RADIUS server is not available for communication, due to a network failure, the client program tries to

communicate with the second server. If authentication fails at any available servers, the client program does not communicate with the other available servers.

The RADIUS action enables you to use RADIUS to authenticate existing users on their RADIUS server. Only the PAP (MD5) algorithm is supported for RADIUS user password.

NOTE

Trellix recommends that either RADIUS users or local users on the Sensor should be configured. If both are required, ensure that users with the same name are not present in the Sensor and the RADIUS server.

Consider the following when configuring a RADIUS server:

- The RADIUS service has to be started for it to communicate with its clients.
- The Sensor IP address has to be configured in the RADIUS server.
- Users have to be added to the RADIUS server.
- When users or settings are changed in the files of the RADIUS server, the current service has to be stopped and started for the changes to take effect.

You can configure the RADIUS authentication for the admin domain from Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → **RADIUS**. You can configure RADIUS authentication at the Sensor under Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Remote Access → **RADIUS**.

Configure RADIUS authentication

The RADIUS server is enabled from the Manager for Sensor CLI login authentication. The Manager does not support TACACS+ and RADIUS authentication at the same time for an admin domain/device. Enabling both the authentication systems might result in conflict, and hence both might not function efficiently. A pop-up message is displayed whenever either one of the authentication system is already enabled.

1. Navigate to Devices → <Admin Domain> → Global → Common Device Settings → Remote Access → **RADIUS**.

2. Select **Enable RADIUS CLI Authentication?**.

> **NOTE**
>
> RADIUS authentication is disabled by default.

3. Enter the details for the following fields:

Option	Definition
Primary RADIUS Server	
Server IP Address	IPv4 address of the primary RADIUS server.
Shared Secret	Password that is required on both the Sensor CLI and the RADIUS server. The **Shared Secret** is same as entered in the RADIUS server during configuration. **NOTE** The shared secret should not contain any blank spaces.
Authentication Port (UDP)	Port through which the primary RADIUS server communicates.
Connection Timeout	Time after which the session logs out automatically. You can configure the time anywhere between 2 seconds to 20 seconds.
Enable Accounting?	When enabled, the primary RADIUS server keeps account of the records like the current session duration and information about current data usage. This option is disabled by default.
Accounting Port (UDP)	Port through which the primary RADIUS server communicates to keep account.
Secondary RADIUS Server (optional)	
Server IP Address	IPv4 address of the secondary/backup RADIUS server.
Shared Secret	Password that is required on both the Sensor CLI and the RADIUS server. The **Shared Secret** is same as entered in the RADIUS server during configuration.
Authentication Port (UDP)	Port through which the secondary RADIUS server communicates.
Connection Timeout	Time after which the session logs out automatically. You can configure the time anywhere between 2 seconds to 20 seconds.
Enable Accounting?	When enabled, the secondary RADIUS server keeps account of the records like the current session duration and information about current data usage. This option is disabled by default.
Accounting Port (UDP)	Port through which the secondary RADIUS server communicates to keep account.

4. Click **Save** to save the settings.

> **NOTE**
>
> In case of child domains, you can inherit the same settings using the **Inherit Settings?** option for RADIUS authentication.

Management of SNMPv3 users

SNMP version 3 helps you to manage your network using SNMP protocol to facilitate the exchange of management information between network devices.

Using the Manager, you can add SNMPv3 users at the domain level and allow devices to make use of this configuration or add users at the device level.

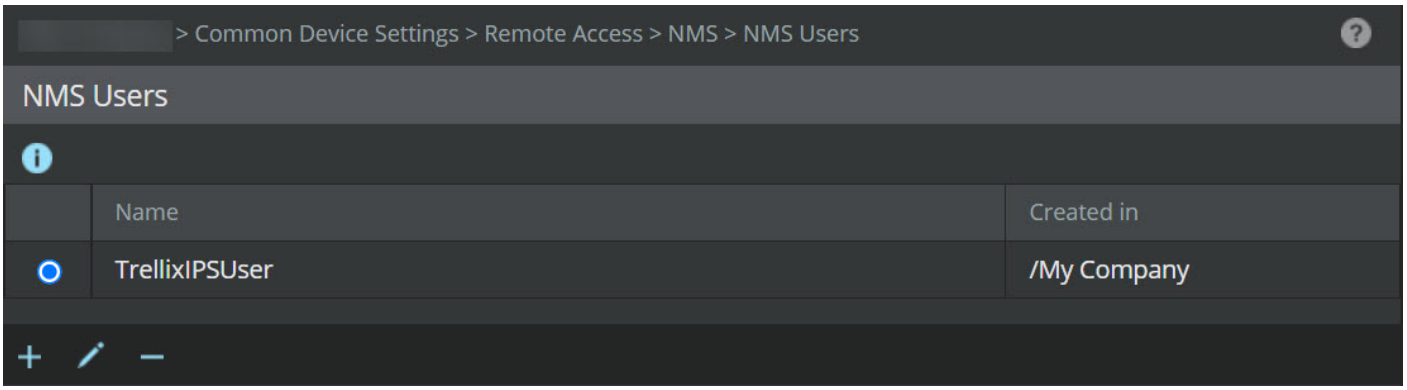
SNMPv3 users created at a domain level are available to the devices and the child domains. Thus, changes done at the domain level are also reflected in the devices using this configuration and the child domains.

Child domains are restricted to only view and use the SNMPv3 users created at the parent domain level.

SNMPv3 in HA pair devices

If both the devices have SNMPv3 configured, before becoming the part of the HA pair, the failover (Stand by) device configuration is deleted and updated with the Primary device configuration. Any configuration changes done after HA pair creation is updated onto both the devices.

Figure 703. SNMPv3 Users sub-tab



The **SNMPv3 Users** action enables you to do the following:

- Adding SNMPv3 users at domain level: Add a NMS user with the authentication and private key.
- Editing SNMPv3 users at domain level: Edit the authentication and private key.
- Deleting SNMPv3 users from the domain: Delete user from NMS database.

> **NOTE**
>
> SNMPv3 users created in the **NMS Users** page under **Global** tab can be added to the SNMPv3 users created at the device level using the **Assign Domain User** button and then assigning the user.

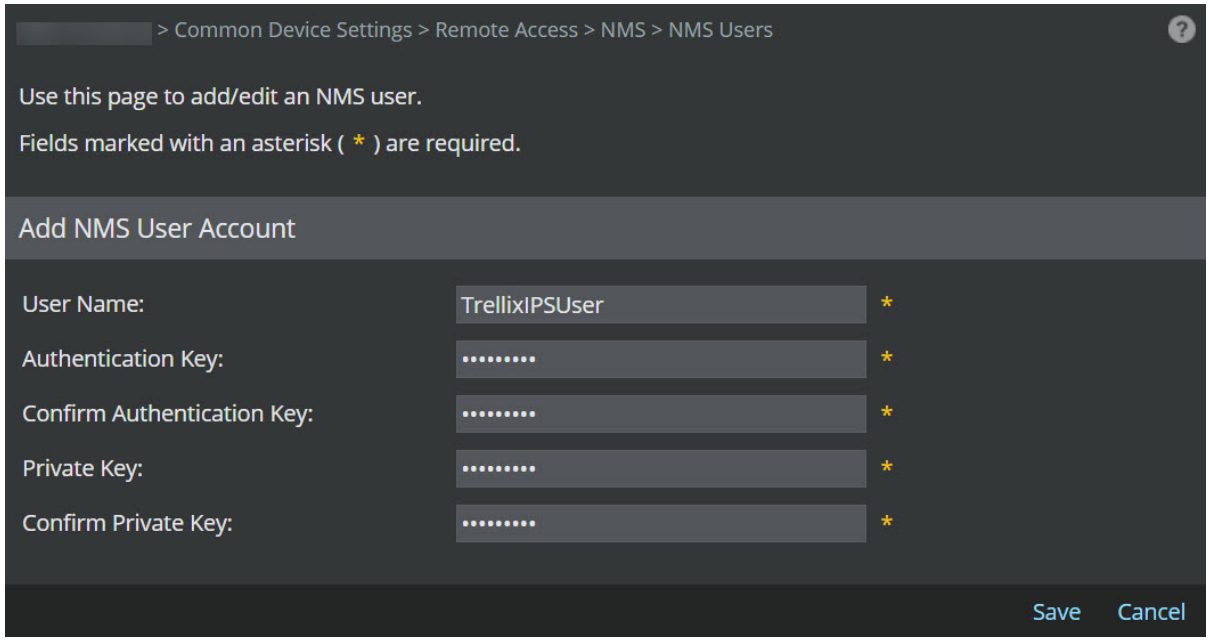
Add SNMPv3 users at admin domain level

SNMPv3 users can be added at the domain level or at an individual device level. Any number of users can be added at the domain level unlike to a device SNMPv3 configuration where it is limited to 10 users.

To add a SNMPv3 user at the domain level, do the following:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → NMS → **NMS Users**.
2. Click +.

   The **Add NMS User Account** dialog is displayed.



3. Enter the **User Name**.

> **NOTE**
>
> The length of the user name should be between 8 to 31 characters. It can consist of alphabets and numerals. Special characters and spaces are not allowed.

4. Enter the **Authentication Key** (re-enter at **Confirm Authentication Key**).
5. Enter the **Private Key** (re-enter at **Confirm Private Key**).

> **NOTE**
>
> The length of the Authentication and Private key should be between 8 to 15 characters. Special characters are not allowed.

NOTE

Since the communication is over SNMP version 3, the supported authentication protocol is "SHA1" and encryption algorithm is "AES128".

6. Click **Save** or **Cancel** to end the authentication.

NOTE

The **User Name**, **Authentication Key** and **Private Key** entered in the Manager should be the same as entered in the SNMP MIB browser.

Edit SNMPv3 users at admin domain level

You are allowed only to change the **Authentication key** and **Private key** parameters of configured users added in database.

To edit a SNMPv3 user at domain level, do the following:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → NMS → **NMS Users**.
2. Click .
3. Enter the **Authentication Key** and **Private Key** (re-enter **Authentication Key** and re-enter **Private Key**).
4. Click **Save**.

Delete SNMPv3 users from the domain

You can delete SNMPv3 users from the domain.

To delete a previously added user:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → NMS → **NMS Users**
2. Select the user from the **NMS Users** table.
3. Click .
4. Confirm the deletion by clicking **OK**.

NOTE

Users deleted from a domain are automatically deleted from the devices.

Management of permitted NMS IP address

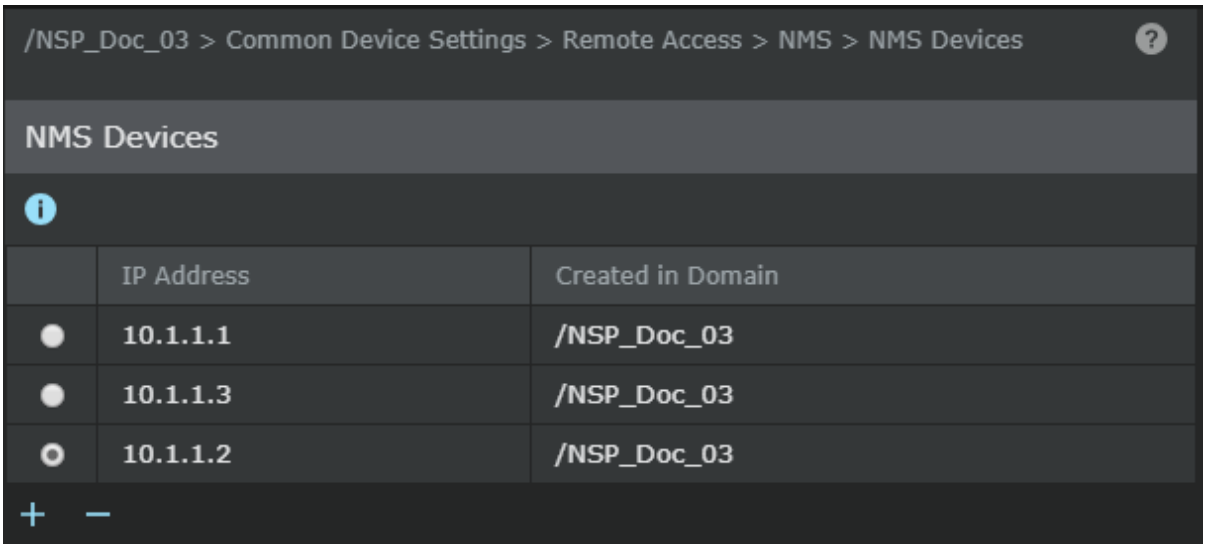
Using the Manager, you can add Permitted NMS IPs at the node at the root admin domain level and allow devices to make use of this configuration or add IPs at the device level.

Permitted NMS IPs added to the devices at the root admin domain level are available to the devices at child domains. Thus, changes done to the devices level at the root admin domain level are also reflected in the devices using this configuration in child domains.

Child domains are restricted to only view and use the NMS IPs created at the parent domain level.

The **NMS Devices** action allows you to do the following:

Figure 704. NMS Devices dialog



- Adding NMS IP addresses — Add NMS IP address.
- Deleting NMS IP addresses — Delete previously configured NMS IP addresses.

Add permitted NMS addresses

To add your NMS device:

1. Go to Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → NMS → **NMS Devices**.
2. Click +.
3. In **Add NMS IP** page is displayed. Enter the **IP Address**. You can enter either an IPv4 or IPv6 address.
4. Click **Save**. The NMS IP is displayed in the **NMS Devices** table.

Delete permitted NMS IP addresses

To delete previously added NMS devices:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Remote Access → NMS → **NMS Devices**.
2. Select the devices from the list.
3. Click −.

4. Confirm your deletion by clicking **OK**.

How to work with the Sensor MIBs

Sensors can monitor SNMP MIBs from a third-party NMS on a read-only basis.

Trellix MIB files

The available MIB files are at the following location:

- Windows based Manager:
  <Trellix IPS install directory>\config\mibs
- Linux based Manager:
  /opt/IPSManager/App/config/mibs

> **NOTE**
> For a list of MIB files in the Linux based Manager, see the output for **show editables** command in the Manager shell.

> **NOTE**
> To edit MIB files in a Linux based Manager, execute **edit <MIB file name>** command in the Manager shell.

The MIB files in the Manager are as follows:

- Trellix-TC: Textual conventions for Trellix enterprise.
- Trellix-SMI: Structure of management information for Trellix enterprise.
- Trellix-SENSOR-CONF-MIB: Sensor configuration MIB.
- Trellix-SENSOR-PERF-MIB: Sensor performance statistics MIB.
- Trellix-SENSOR-SMI: Structure of management information for the Sensor.
- Trellix-INTRUVERT-EMS-TRAP-MIB: SNMP trap messages from Manager to an SNMP manager server.

Work with the MIB files

To configure a third-party NMS to access the Sensor MIBs.

Configure the Sensor:

1. Add the IP addresses of every NMS that will need to have SNMP access to the Sensor using Manager.
2. Create a list of SNMPv3 associations that will provide users with read-only access to the Sensor MIBs.
3. Load and compile the Sensor MIBs onto the third-party NMS for querying the MIB objects.
   Refer to the section below for instructions on how to do this for some of the commonly used NMS applications.

Restricted SNMP write access for third-party NMS users

Sensors provide read-write access to a Host Quarantine Group portion of the MIB tree. To have read-write access to these MIBs, the following configurations are needed:

- Configure third-party NMS users.
- Configure a set of IPv4/IPv6 addresses from where third-party SNMP access would be allowed.

For managing the restricted read-write access, you need to enable/disable it from the Sensor CLI. For more information, see the [CLI commands] section.

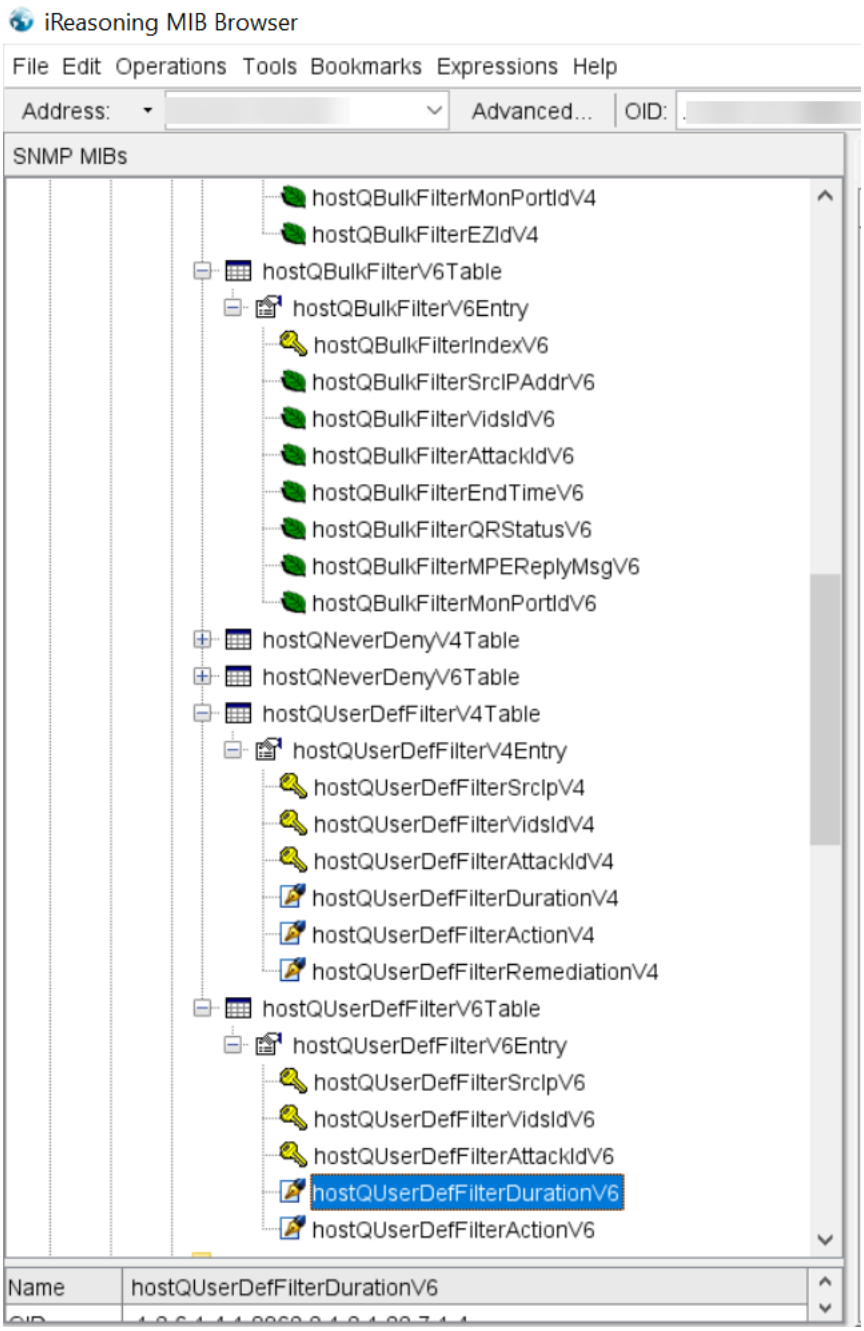
After enabling/disabling the access, the Sensor is to be rebooted only if the SNMP users are already configured. If no SNMP user is configured on the Sensor, then the configuration is done without rebooting the Sensor.

The following write operations are permitted:

- Add an IPv4/IPv6 entry to quarantine the host.
- Extend the quarantine duration of an existing quarantined IPv4/IPv6 host entry.
- Delete the IPv4/IPv6 filter entries one by one.
- Delete all the IPv4/IPv6 filter entries at once.
- Remediation for IPv4.

If the Sensor is in the failover mode, make sure that the entries are created on both the primary and secondary Sensors.

Restricted read-write access is permitted for the section of the MIB tree depicted in the following image.



User scenarios

Scenario 1

To isolate a host in the Sensor from the third-party SNMP application:

Set the **hostQUserDefFilterAction** object of the **hostIsolUserDefFilterTable** to a value 1. For setting this object, the following indices are needed:

- IP Address (To be provided in a dot separated format)

- VidsId (should always be set to 0)
- AttackId (should always be set to 0)

The above action is applicable to both IPv4 as well as IPv6 entries. Consider the following example:

For isolating a host with IPv4 address of **10.12.12.15**, the following OID is to be set with a value 1.

OID - 1.3.6.1.4.1.8962.2.1.2.1.22.6.1.5.**10.12.12.15**.0.0

Scenario 2

To extend the isolation end time of an already isolated host in the Sensor from the third-party SNMP application:

Set the **hostQUserDefFilterDuration** object of the **hostIsolUserDefFilterTable** to a value <time in minutes>. For setting this object, the following indices are needed:

- IP Address (To be provided in a dot separated format)
- VidsId (should always be set to 0)
- AttackId (should always be set to 0)

The above action is applicable to both IPv4 as well as IPv6 entries. Consider the following example:

For extending the isolation duration of an already isolated host with IPv4 address of **10.12.12.15**, by 30 more minutes, the following OID is to be set with a value 30.

OID - 1.3.6.1.4.1.8962.2.1.2.1.22.6.1.4.**10.12.12.15**.0.0

Scenario 3

A list of already isolated hosts can be retrieved by performing an SNMP walk on the **hostQBulkFilterTable.**

To obtain the list of isolated hosts with IPv4 address, perform a walk on the **hostQBulkFilterTableV4.**

Similarly, to obtain the list of isolated hosts with IPv6 addresses, perform a walk on the **hostQBulkFilterTableV6.**

Scenario 4

To delete an already isolated host in the Sensor from the third-party SNMP application:

Set the **hostQUserDefFilterAction** object of the **hostIsolUserDefFilterTable** to a value 2. For setting this object, the following indices are needed:

- IP Address (To be provided in a dot separated format)
- VidsId (should always be set to 0)
- AttackId (should always be set to 0)

The above action is applicable to both IPv4 as well as IPv6 entries. Consider the following example:

For isolating a host with IPv4 address of **10.12.12.15**, the following OID is to be set with a value 2.

OID - 1.3.6.1.4.1.8962.2.1.2.1.22.6.1.5.**10.12.12.15**.0.0

Scenario 5

To delete all the isolated hosts in the Sensor from the third-party SNMP application:

Set the **hostQDeleteAllFilters** object of the **hostQConfigGrp** to a value 2.

OID - 1.3.6.1.4.1.8962.2.1.2.1.22.1.2.0

Scenario 6

To isolate and remediate an IPv4 host in the Sensor from the third-party SNMP application:

Set the **hostQUserDefFilterRemediationV4** object of the **hostIsolUserDefFilterTableV4** to a value 1. For setting this object, the following indices are needed:

- IP Address (To be provided in a dot separated format)
- VidsId (should always be set to 0)
- AttackId (should always be set to 0)

The above action is applicable only to IPv4 entries. Consider the following example:

To isolate and remediate a host with IPv4 address of **10.12.12.15**, the following OID is to be set with a value 1.

OID - 1.3.6.1.4.1.8962.2.1.2.1.22.6.1.6.**10.12.12.15**.0.0

How to load and compile MIBs into a third-party NMS

Most NMSs provide a way for the user to load MIBs. Loading a MIB is a way that an NMS can learn about new MIB objects, such as their names, object identifiers (OIDs), and the kind of data type.

Consult the documentation of the third-party NMS for information on MIB loading and compilation. This document includes instructions for HP OpenView and IBM NetView; but you should still consult the HP or IBM documentation, as those products may change.

Load Trellix IPS MIBs from the UI of HP OpenView or IBM NetView

Follow these steps to load Trellix IPS MIBs:

1. Copy the files into the directory **/usr/OV/snmp_mibs** of the network management server. This is the default directory where HP OpenView and IBM NetView look for MIB documents. If you place them elsewhere, specify the explicit path names in the load mib graphical interface.
2. Set the permissions so that you have read access to the MIBs.
3. From the GUI menu, choose Options → **Load/Unload MIBs**.
4. To compile or load the MIBs, follow the instructions in the platform documentation.

Load the MIB file from the CLI of HP OpenView or IBM NetView

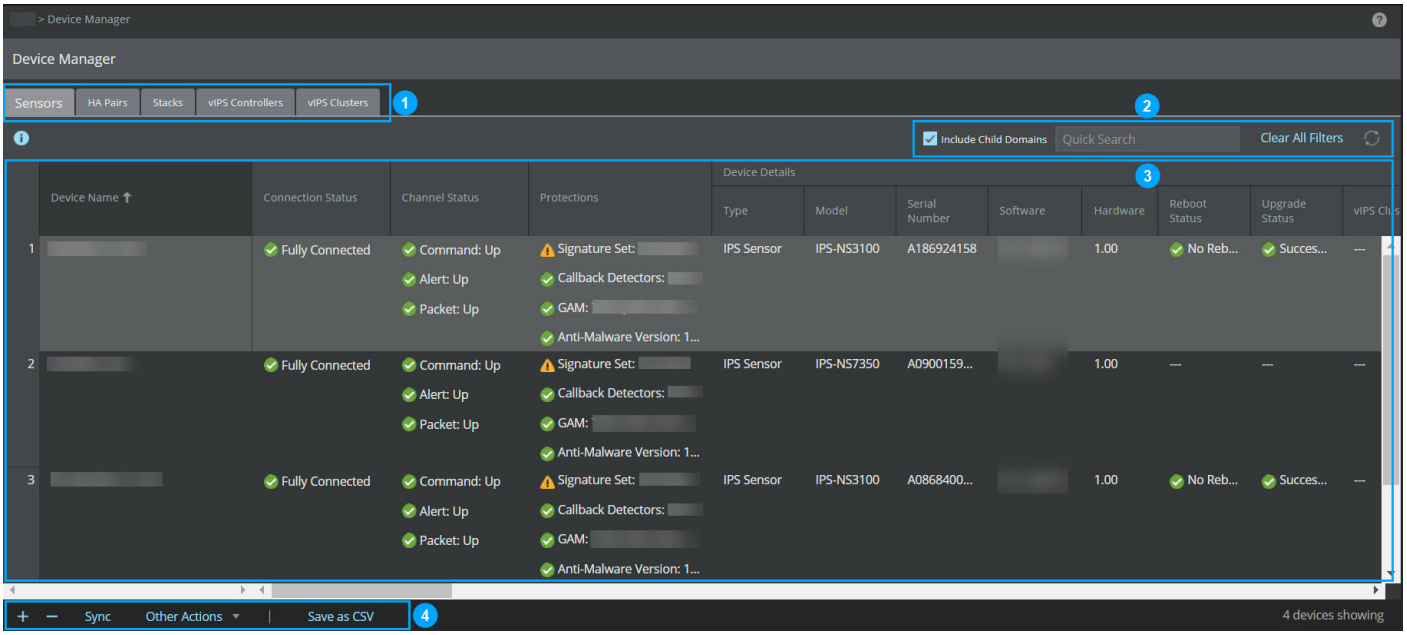
To load the MIB file, issue the command.

```
/opt/OV/bin/xnmloadmib -load filename
```

Device Manager in Trellix IPS Manager

The Devices → <Admin Domain Name> → Global → **Device Manager** page provides a consolidated view of all devices configured in the Manager such as NS-series Sensors, Virtual IPS Sensors, and NTBA Appliances. You can view all devices configured in an admin domain including those configured in the child admin domains. The information-rich **Device Manager** grid view displays general device information, system health and other options such as viewing faults, license assignment to devices etc. from a single page. The Manager also enables you to take actions such as Sensor reboot, shutdown, Sensor CLI password reset, Sensor software upgrade from the **Device Manager**, delivering a comprehensive view of your deployment as well as unification of key configuration options on a single page.

Figure 705. Device Manager



Callout	Description
1	Tabs namely, **Sensors**, **HA Pairs**, **Stacks**, **vIPS Controllers**, and **vIPS Clusters**. **NOTE** **vIPS Controllers** and **vIPS Clusters** tabs are only displayed for the Manager in a cloud environment.
2	Top-right menu
3	Grid view
4	Bottom-left menu

The following options are available in all the tabs of the **Device Manager** page:

Options	Description
Top-right menu	

Options	Description
Quick Search/*Search*	Enter the keyword in the *Quick Search*/*Search* field and the results are automatically displayed.
	Refreshes the tab.
Bottom-left menu	
	Add new devices. For more information, see Add a Sensor to the Manager and Creating a HA Pair (page 642).
	Delete a device. In case of **Sensors** tab, you can delete a single or multiple devices based on the selection. A **Successful/Failed Deletion(s)** dialog box displays the status and device details.
Save as CSV	Downloads the device details for all the devices as a .csv file.

Sensors

Top-right menu

The following options are available on the top-right corner of the **Sensors** tab:

Options	Description
Include Child Domains	Displays the Sensors configured in the child domain.
Clear All Filters	Click **Clear All Filters** to undo all filters applied.

Filter and sort options

The **Device Manager** page can be customized by different options like filtering and sorting which helps to drill-down the necessary details based on your requirement.

- **Filter**: All the columns in the **Device Manager** page can be filtered based on specific fields to view a consolidated list of details.
- **Sort**: All the columns in the **Device Manager** page can be sorted in the ascending or descending order.

Grid view

The following columns are available in the grid view of the **Sensors** tab:

Option	Definition
Name	Displays the name of the device. **NOTE** For vIPS Clusters, it displays the name of the member Sensors.

Option	Definition
Connection Status	Displays the status between the Sensor and the Manager. • **Fully Connected**: Indicates that all channels are up. The Sensor is able to communicate with the Manager. • **Partially Connected**: Indicates that one or more channels are down. • **Disconnected**: Indicates that the command channel is down. This occurs when the Sensor fails to communicate with the Manager. • **Trust Pending**: Indicates that the Sensor is defined on the Manager but not on the Sensor.
Channel Status	Displays the name of the following channels and its status whether "Up" or "Down": • **Command** • **Alert** • **Packet** If the trust is not established between the Manager and Sensor, the **Channel Status** is displayed as **---**.
Protections	Displays if the versions for the following protection parameters are latest not: • **Signature Set** • **Callback Detectors** • **GAM** (Gateway Anti-Malware engine) • **Anti-Malware** engine The icons displayed for the parameters are as follows: • : Displayed when the parameter has the latest version available. • : Displayed when the version available in the Manager differs with the version available in the Sensor. • : Displayed when there is no latest version available on the Manager. • : Displayed when the latest version cannot be determined. This is displayed only for **GAM** and **Anti-Malware**.
Device Details	
Type	Displays if the device is an IPS Sensor or an NTBA Appliance.
Model	Displays the Sensor model.
Serial Number	Displays the Sensor serial number.
Software	Displays the software version running on the Sensor.
Hardware	Displays the current hardware version running on the Sensor.

Option	Definition
Reboot Status	Displays if the Sensor requires a reboot. This is required to deploy configuration changes to the Sensor without any failure. • **Reboot Required**: Indicates that the Sensor requires a reboot. The reason for the reboot is also provided for better understanding. For example, **Reboot Required** (Sensor software change). • **No Reboot Required**: Indicates that the Sensor does not require a reboot. **NOTE** This is not applicable to NTBA appliances. It is displayed as **---**.
Upgrade Status	Displays if the latest software version is installing on the Sensor or downloading the latest software version to the Manager before installing it on the Sensor. • **Successful** : When the Sensor upgrade is successful. • **In-progress**: When the Sensor is upgrading to the latest Sensor software version. • **Failed** : When the Sensor upgrade fails. • **---**: When no upgrade is performed.
vIPS Cluster	
Name	Displays the name of the vIPS Cluster. For non-vIPS Clusters, "---" is displayed. **NOTE** This column is applicable only to Sensors that are members of a vIPS Cluster.
Capacity	Displays the total capacity of license required for all the Sensors in the cluster.

Option	Definition

License	Displays the license status of the cluster.
	
	NOTE
	License assignment is disabled at the member Sensor level within the cluster.
	
	The license status can be one of the following options:
	• **Required**: The reason can be one of the following:
	  • The license has not been assigned.
	  • The license is assigned, but its capacity is less than the cluster's configured capacity.
	
	NOTE
	If a combination of expired and insufficient licenses exists, the insufficient license takes a higher priority.
	• **Present**: The sufficient license is present and valid.
	• **Expired**: The license is assigned, but one or more license is expired.
	• **Grace Period**: The assigned license(s) have expired and are now running on a grace period.
	
	NOTE
	A grace period of **30 days** is provided to subscription based system licenses after they expire.

vIPS Probe	Displays the vIPS Probe version running on the member Sensor. For non-vIPS Probe, "---" is displayed. **NOTE** This column is applicable only to Sensors that are members of a vIPS Cluster.
Cloud Cluster Id	Displays the Cluster ID for the vIPS Clusters. For non-vIPS Clusters, "---" is displayed. **NOTE** This column is applicable only to Sensors that are members of a vIPS Cluster.
Last Upgrade	Displays the date, time, and year of the last software upgrade.

Option	Definition
System	**Running Capacity**: Displays the throughput of the Sensor. **NOTE** The information is displayed only for NS9500, NS7600, NS7500, NS3600, and NS3500 Sensors.

	License: Displays one of the following:
	
	• **Required**: The reason can be one of the following:
	  • License has not been assigned to the device.
	  • The license is assigned, but its capacity is less than the device's configured capacity.
	• **Present**: The license is present and valid.
	• **Expired**: The license is assigned, but has expired.
	• **Grace Period**: The license has expired and is running on grace period.
	
	NOTE
	A grace period of **30 days** is provided to subscription-based **System** licenses after they expire.
	
	Click on the tooltip icon to assign or change the license. For more information, see Assign a license to a Sensor.

Stack	**Name**: Displays the name of the stack of NS9500 Sensors.
	Capacity: Displays the throughput for the stack.

Option	Definition

	License: Displays one of the following:
	• **Required**: The reason can be one of the following:
	  • License has not been assigned to the stack.
	  • The license is assigned, but its capacity is less than the stack's configured capacity.
	• **Present**: The license is present and valid.
	• **Expired**: The license is assigned, but has expired.
	• **Grace Period**: The license has expired and running on grace period.
	NOTE
	A grace period of **30 days** is provided to subscription based system licenses after they expire.
	Click on the tooltip icon to assign or change the license. For more information, see Assign a license to a Sensor.

HA Pair	If the device is a part of a HA pair, it displays the name of the HA pair the device belongs to.
Management IP Address	Displays the IP address of the management interface in the device and the subnet mask IP address.
Default Gateway	Displays the IP address of the default gateway configured on the Sensor.
FIPS Mode	Displays if FIPS mode is enabled or disabled. **NOTE** This is not applicable to NTBA appliances. It is displayed as **---**.
Last Reboot	Displays the date and time of the previous reboot of the Sensor.
Owner Domain	Displays the admin domain name or the child admin domain name to which the device belongs.
Comment	Displays the location and contact information.
System Health	
Overall Health	Displays the overall health of the system. • **Normal**: All the health indicators are normal. • **Abnormal**: One or more health indicators are abnormal. • **---**: Disconnected or trust pending.

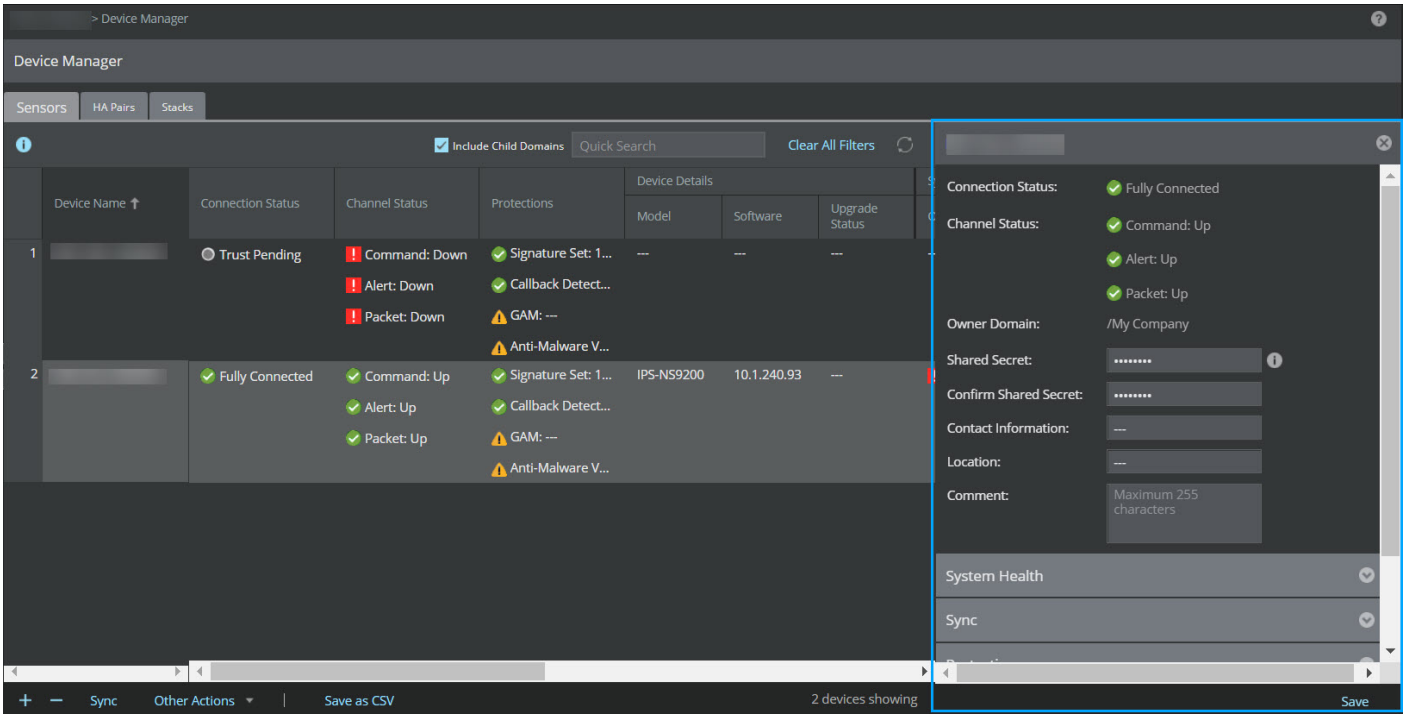
Option	Definition
Internal Health	Displays the Sensor health. • **Normal**: All the health indicators are normal. • **Abnormal**: One or more health indicators are abnormal. • **---**: Disconnected or trust pending.
Physical Ports	Displays if the ports are operating normally or abnormally. • **Normal**: Physical ports are operating normally. • **Abnormal**: One or more ports are down or the failover kit is in bypass mode. • **---**: Disconnected or trust pending. Click the link to navigate to the **Physical Ports** page of the device.
Inspection	Displays if the device is in layer 2 bypass mode. • **Normal** – Traffic inspection is enabled • **Abnormal** – Traffic inspection is disabled. This means that the device is in layer 2 bypass mode. Click the link to navigate to the **Layer 2 Bypass** page of the device.
Performance	Displays if there are any performance related faults for the device. • **Normal** – Indicates that the device has no unacknowledged performance faults Click the link to navigate to the **Performance Charts** page. • **Abnormal** – Indicates that the device has one or more unacknowledged faults **NOTE** This is not applicable to NTBA appliances and vIPS Clusters. It is displayed as **---**.
Hardware	Displays if the hardware has any temperature or power related issues. • **Normal** – Indicates that the device has no unacknowledged faults • **Abnormal** – Indicates that the device has one or more unacknowledged faults

Option	Definition
Power Supplies	Displays the power supply status. The following are the status of the power supply: • **Operational** - Indicates that the power supply is detected and operational. • **Non Operational** - Indicates that the power supply is detected but not operational. • **Absent** - Indicates that the power supply is absent. • **Error** - Indicates Error when the system fails to fetch the real power status. • **---** - Indicates that the trust is not yet established or power supply status is not applicable for it. For NS-series Sensors, two units of power modules and power supply status are displayed: • **A:** Displays the Primary power module and power supply status • **B:** Displays the Secondary power module and power supply status **NOTE** Only for NS9300 Sensor, four units of power modules and power supply status are displayed: • For Primary, **A** and **B** displays the two units of power module and power supply status. • For Secondary, **A** and **B** displays the two units of power module and power supply status. **NOTE** For all untrusted devices and NTBA, it is displayed as **---**. **NOTE** The NS3x00 Sensors do not support Secondary power supply module thus, the status of only Primary power supply module is displayed.
Faults	
Total	Displays the number of unacknowledged faults generated for the device. Click the link to navigate to the **Faults** window.
Critical	Displays the number of critical faults generated for the device.
Error	Displays the number of error faults generated for the device.
Warning	Displays the number of warning faults generated for the device.
Info	Displays the number of info faults generated for the device.
Sync	

Option	Definition
Status	Displays the synchronization state of the Sensor. • **Synchronized**: Indicates that no pending changes are required. • **Sync required**: Indicates if any pending changes are required. • **Sync in progress**: Indicates when the deployment is in progress. • **---**: Indicates that there is no trust established between the Sensor and the Manager.
Pending Changes	Displays the configuration changes updated to the device including signature set or callback detectors.
Last Sync	Displays the date and time of the last configuration change.
Deployment Mode	Displays if the configuration update was online or offline. This is displayed as **Direct** for online update and **Indirect** for offline update.

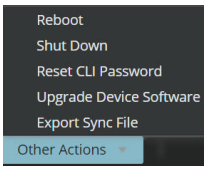
You can also view the device details in the **Details** panel to the right of the page by double-clicking anywhere on the selected device.

Figure 706. Device Details



Bottom-left menu

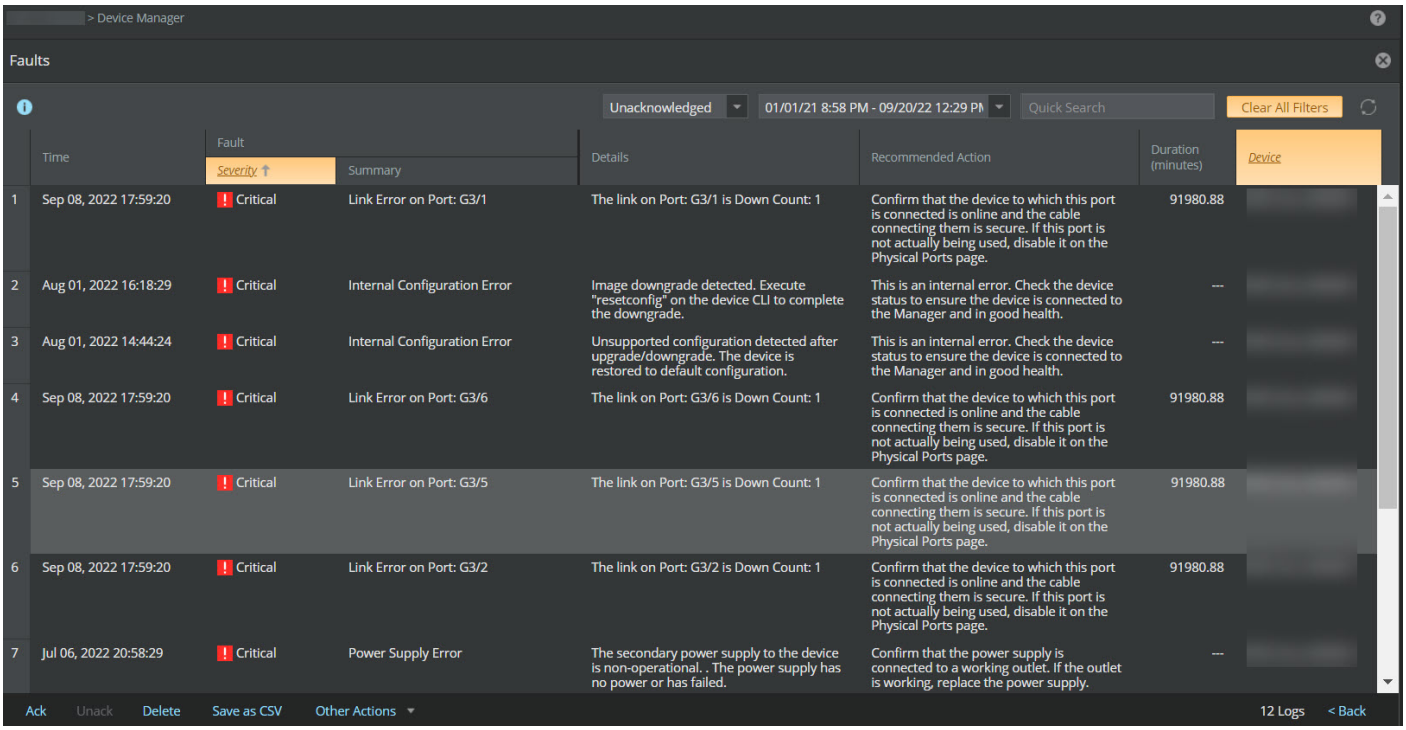
The following options are available on the bottom-left corner of the **Sensors** tab:

Options	Description
Sync	Deploys configuration changes for a single device or multiple devices at the same time. For more information, see Deploy pending changes to a device (page 873).
Other Actions 	You can perform the following actions: • **Reboot**: Perform either partial or a full reboot of the Sensor. • **Shut Down**: Shuts down the Sensor. • **Reset CLI Password**: Resets the CLI password for the Sensor. • **Upgrade Device Software**: Upgrades or downgrades the Sensor software version. For more information, see Update the latest software images on all devices (page 85). • **Export Sync File**: Exports the sync files to the local machine. **NOTE** You can export the sync file only when the **Sync Node** is set to **Indirect**.
<Number> devices showing	Displays the total number of devices connected to the Manager.

Faults

A **Faults** window is displayed on selecting the tooltip icon for a particular fault on the **Device Manager** page. On selecting **Clear All Filters**, the **Faults** window displays all the faults generated for the selected Sensor.

Figure 707. Faults window



This window is similar to the **Faults** tab in the **Logs** page. Except, this window displays just the faults for the selected device based on the severity. All the actions that can be performed in the **Faults** tab in the **Logs** page can also be performed through this window.

For more information, see the Faults (page 343) section.

Click  or  to go back to the **Device Manager** grid view.

HA Pair

To manage a HA pair, go to Devices → <Admin Domain Name> → Global → **Device Manager**. The **Device Manager** page is displayed. Select **HA Pairs** tab. The **HA Pairs** tab displays the following details:

Option	Definition
HA Pair Name	Displays the name of the HA Pair.
Template Sensor	Displays the details of configured primary Sensor as template Sensor in the HA Pair.
Peer Sensor	Displays the details of configured secondary Sensor as peer Sensor in the HA Pair.
Model	Displays the model of the Sensor.
Allow fail open?	Displays the status of fail open as **True** or **False**.
<Number> HA Pair(s)	Displays the total number of HA pair(s) in the Manager.

Stacks

The NS9500 Sensor offers the solution of stacking multiple Sensors to achieve scalability. The individual Sensors in the stack are interconnected using external stacking cables. A stack of Sensors create a unified data plane view across the stack. This allows the Manager to manage the stack as a unified device. In a stack, some of the Sensor properties like signature set and call back detector update etc. are managed at the stack level and remaining like port configuration, troubleshooting etc. are managed at the device level.

To manage a stack, go to Devices → <Admin Domain Name> → Global → Device Manager → **Stacks** tab. The **Stacks** tab displays the following details:

Option	Definition
Stack Name	Displays the name of the device. Double-clicking the name opens the **Stack Details** window where you can view the details of the stack.
Capacity	Displays the throughput of the stack.
Mamber Sensors	Displays the number of devices that are currently part of the stack. Click the number to view the names of devices that are part of the stack.

Option	Definition

License	Displays on of the following:
	• **Required**: The reason can be one of the following:
	  • License has not been assigned to the stack.
	  • The license is assigned, but its capacity is less than the stack's configured capacity.
	• **Present**: The license is present for the stack.
	• **Expired**: The license is assigned, but has expired.
	• **Grace Period**: The license has expired and running on grace period.
	NOTE
	A grace period of **30 days** is provided to subscription-based **System** licenses after they expire.

Deployment Mode	Displays one of the following based on the mode configured during creation of stack: • **Direct** • **Indirect**
HA Pair	If the stack is part of a HA pair, the name of the HA pair is displayed.
Comment	Displays the comment added for the stack.

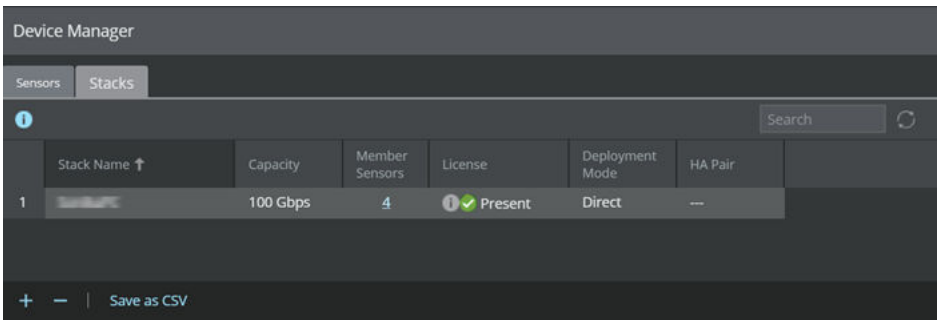
Managing a stack of Sensors

This section describes how to add a stack of Sensors, delete a stack of Sensors, and save the details of the stack to a CSV file.

Add a stack to the Manager

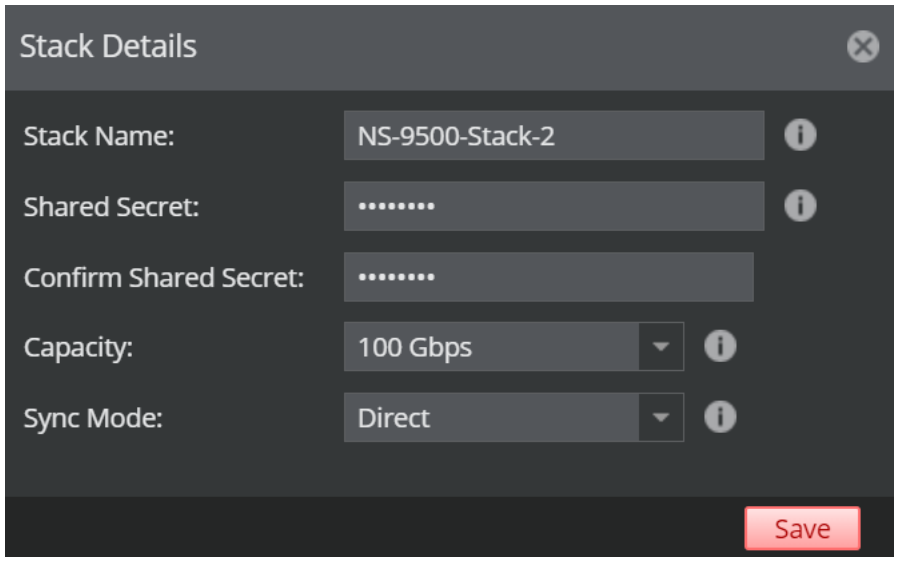
To add a stack of Sensors to the Manager, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager → **Stacks** page.



2. Click + to add a new stack.

   The **Stack Details** window opens.



3. Enter the following mandatory information in the appropriate fields.
   - **Stack Name** — The stack name must begin with a letter. The maximum length of the name is 25 characters.
   - **Shared Secret** — The shared secret must be a minimum of 8 characters and maximum of 25 characters in length. The key cannot start with an exclamation mark nor can have any spaces. The parameters that you can use to define the key are:
     - 26 alphabets: Uppercase and lowercase (A, B, C,...Z and a,b,c,...z)
     - 10 digits: 0 1 2 3 4 5 6 7 8 9
     - 32 symbols: ~ ` ! @ # $ % ^ & * ( ) _ + - = [ ] { } \ | ; : " ' , . <? /

     NOTE

     The Sensor stack name and node ID and shared secret key that you enter in the Manager must be identical to the shared secret that you will later enter during physical installation or initialization of the Sensor (using CLI). If not, the Sensor will not be able to register itself with the Manager.
   - **Confirm Shared Secret** — Confirm the shared secret key.
   - **Capacity** — The throughput for the Stack. Based on the throughput, the number of Sensors will also differ. See the table below:

Capacity	Number of Sensors
40 Gbps	2
60 Gbps	2
100 Gbps	4

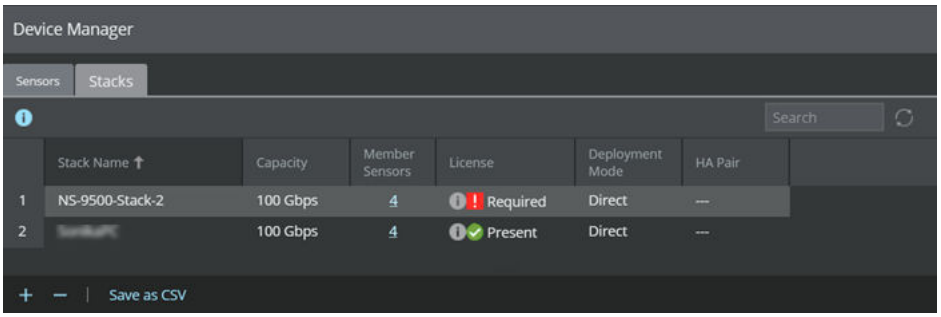
   - **Sync Mode** — Select **Direct** or **Indirect**.

     NOTE

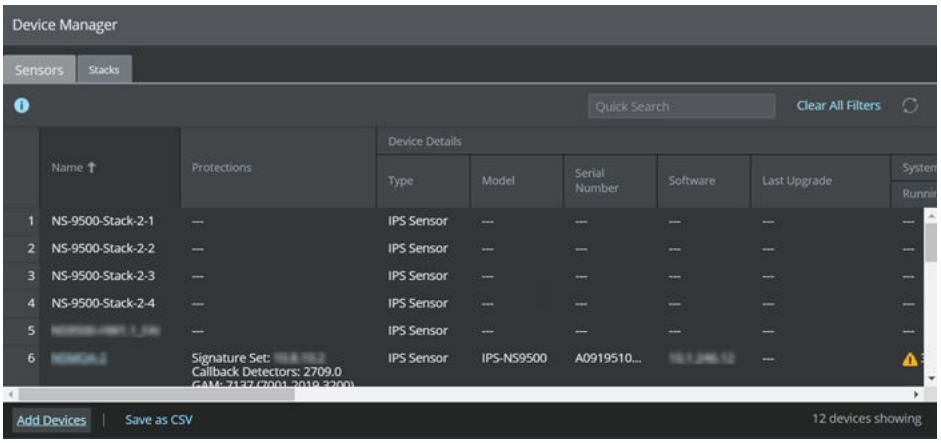
     Selecting **Indirect** enables Offline Sensor update. **Direct** is the default mode.

4. Click **Save**.

   The new stack in displayed in the **Stacks** window.



   In the **Sensors** page, the member Sensor instances are displayed in the **<Stackname-node id>** format. For example, **<Stackname-1>**, **<Stackname-2>**, and so on.

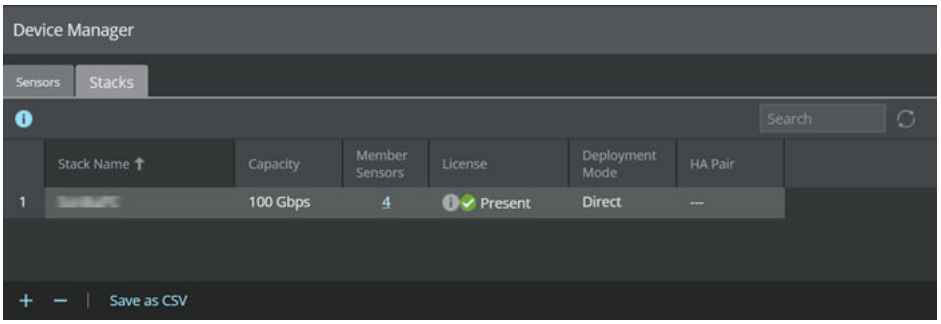


5. Using the Sensor CLI, configure the Sensors with the same name and node ID as the names displayed in the **Sensors** page.
6. In the Manager, go to Manager → <Admin Domain Name> → Setup → **Licenses** and upload the license for the stack. You must manually push the configuration after the license is assigned to the stack.

Delete a stack from the Manager

To delete a stack of Sensors from the Manager, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager → **Stacks** page.



2. Select the stack that you want to delete.
3. Click −.

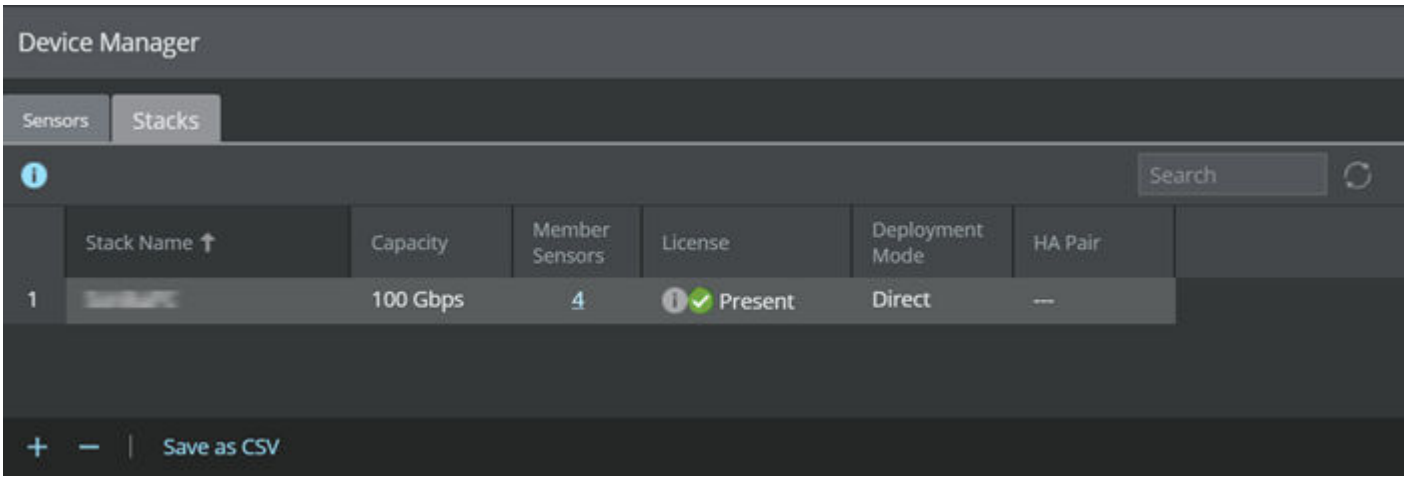
   You will be prompted to confirm the deletion.
4. Click **OK**.

   The selected stack is removed from the Manager.

Save stack details as CSV

To save the stack details from the Manager, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Global → Device Manager → **Stacks** page.



2. Select the stack for which you want to get the details.
3. Click **Save as CSV**.

   A .csv file is saved to your system.

Device Manager in Trellix IPS Central Manager

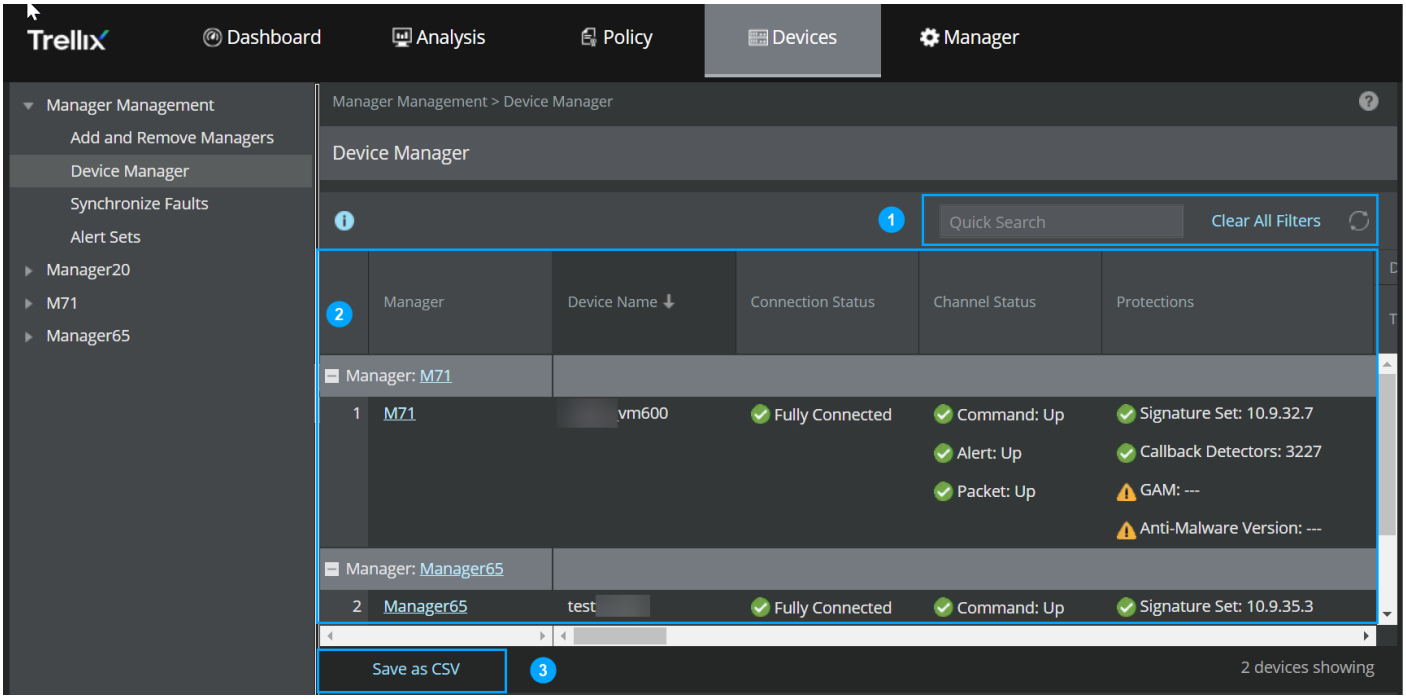
The Devices → Manager Management → **Device Manager** page in Central Manager provides visibility to all devices configured with each of the associated Managers, such as NS-series Sensors, Virtual IPS Sensors, and NTBA Appliances. You can view the devices configured in an admin domain as well as those configured in the child admin domains of any Manager. The **Device Manager** grid view in the Central Manager loads and displays device details in real-time, which include general device information, system health, and faults status, thus offering a comprehensive view of all devices available on individual managers in a single page.

If any of the Managers managed by the Central Manager is in an MDR pair, the Central Manager fetches and displays device data from the active Manager. In case the Central Managers are in an MDR pair, the standby Central Manager displays same device details in the **Device Manager** page as visible in the active Central Manager.

NOTE

You cannot edit, modify, or save any device-related information in the **Device Manager** page in Central Manager. It only provides read-only view of the device details configured with the Managers.

Figure 708. Device Manager page in Central Manager



Callout	Description
1	Top-right menu
2	Grid view
3	Bottom-left menu

The following options are available in the **Device Manager** page of the Central Manager:

Options	Description
Top-right menu	
Quick Search / Search	Enter the keyword in the *Quick Search / Search* field and the results are automatically displayed.
Clear All Filters	Click Clear All Filters to undo all filters applied.
	Click this icon to refresh the page.
Bottom-left menu	
Save as CSV	Downloads the device details for all the devices as a .csv file.

Grid View

The following columns are available in the grid view of the **Device Manager** page in Central Manager:

Option	Definition
Manager	Displays the name(s) of the Manager(s). A header column is available for each Manager. You can expand or collapse the header column of any Manager to view or hide device information specific to them as per your requirement. The Manager name provides a hyperlink which redirects you to the login page of the respective Manager.
Device Name	Displays the name of the device(s) configured with the Manager. **NOTE** For vIPS Clusters, it displays the name of the member Sensors.
Connection Status	Displays the status between the Sensor and the Manager. • **Fully Connected**: Indicates that all channels are up. The Sensor is able to communicate with the Manager. • **Partially Connected**: Indicates that one or more channels are down. • **Disconnected**: Indicates that the command channel is down. This occurs when the Sensor fails to communicate with the Manager. • **Trust Pending**: Indicates that the Sensor is defined on the Manager but not on the Sensor.
Channel Status	Displays the name of the following channels and its status whether "Up" or "Down": • **Command** • **Alert** • **Packet** If the trust is not established between the Manager and Sensor, the **Channel Status** is displayed as **---**.

Option	Definition
Protections	Displays if the versions for the following protection parameters are latest not: • **Signature Set** • **Callback Detectors** • **GAM** (Gateway Anti-Malware engine) • **Anti-Malware Version** The icons displayed for the parameters are as follows: • : Displayed when the parameter has the latest version available. • : Displayed when the version available in the Manager differs with the version available in the Sensor. • : Displayed when there is no latest version available on the Manager. • : Displayed when the latest version cannot be determined. This is displayed only for **GAM** and **Anti-Malware Version**.
Device Details	
Type	Displays if the device is a Sensor or an NTBA appliance.
Model	Displays the Sensor model.
Serial Number	Displays the Sensor serial number.
Software	Displays the software version running on the Sensor.
Hardware	Displays the current hardware version running on the Sensor.
Reboot Status	Displays if the Sensor requires a reboot. This is required to deploy configuration changes to the Sensor without any failure. • **Reboot Required**: Indicates that the Sensor requires a reboot. The reason for the reboot is also provided for better understanding. For example, **Reboot Required (Sensor software change)** . • **No Reboot Required**: Indicates that the Sensor does not require a reboot. **NOTE** This is not applicable to NTBA appliances. It is displayed as **---**.

Option	Definition
Upgrade Status	Displays if the latest software version is being installed on the Sensor or being downloaded to the Manager before installing it on the Sensor. •  **Successful** : Displayed when the Sensor upgrade is successful. •  **In-progress**: Displayed when the Sensor is upgrading to the latest Sensor software version. •  **Failed** : Displayed when the Sensor upgrade fails. • **---**: Displayed when no upgrade is performed.
vIPS Cluster	Displays the name of the vIPS Cluster. For non-vIPS Clusters, "---" is displayed. **NOTE** This column is applicable only to Sensors that are members of a vIPS Cluster.
vIPS Probe	Displays the vIPS Probe version running on the member Sensor. For non-vIPS Probe, "---" is displayed. **NOTE** This column is applicable only to Sensors that are members of a vIPS Cluster.
Cloud Cluster Id	Displays the Cluster ID for the vIPS Clusters. For non-vIPS Clusters, "---" is displayed. **NOTE** This column is applicable only to Sensors that are members of a vIPS Cluster.
Last Upgrade	Displays the date, time, and year of the last software upgrade.
System	**Running Capacity**: Displays the throughput of the Sensor. **NOTE** The information is displayed only for NS9500, NS7600, NS7500, NS3600, and NS3500 Sensors.

Option	Definition

	License: Displays one of the following:
	• **Required**: The reason can be one of the following:
	  • License has not been assigned to the device.
	  • The license is assigned, but its capacity is less than the device's configured capacity.
	• **Present**: The license is present and valid.
	• **Expired**: The license is assigned, but has expired.
	• **Grace Period**: The license has expired and is running on grace period.
	NOTE
	A grace period of **30 days** is provided to subscription-based **System** licenses after they expire.

Stack	**Name**: Displays the name of the stack of NS9500 Sensors.
	Capacity: Displays the throughput for the stack.

	License: Displays one of the following:
	• **Required**: The reason can be one of the following:
	  • License has not been assigned to the stack.
	  • The license is assigned, but its capacity is less than the stack's configured capacity.
	• **Present**: The license is present and valid.
	• **Expired**: The license is assigned, but has expired.
	• **Grace Period**: The license has expired and running on grace period.
	NOTE
	A grace period of **30 days** is provided to subscription based system licenses after they expire.

HA Pair	If the device is a part of a HA pair, it displays the name of the HA pair the device belongs to.
Management IP Address	Displays the IP address of the management interface in the device and the subnet mask IP address.
Default Gate-way	Displays the IP address of the default gateway configured on the Sensor.

Option	Definition
FIPS Mode	Displays if FIPS mode is enabled or disabled. **NOTE** This is not applicable to NTBA appliances. It is displayed as **---**.
Last Reboot	Displays the date and time of the previous reboot of the Sensor.
Owner Domain	Displays the admin domain name or the child admin domain name to which the device belongs.
Comment	Displays the location and contact information.
System Health	
Overall Health	Displays the overall health of the system. • **Normal**: All the health indicators are normal. • **Abnormal**: One or more health indicators are abnormal. • **---**: Disconnected or trust pending.
Internal Health	Displays the Sensor health. • **Normal**: All the health indicators are normal. • **Abnormal**: One or more health indicators are abnormal. • **---**: Disconnected or trust pending.
Physical Ports	Displays if the ports are operating normally or abnormally. • **Normal**: Physical ports are operating normally. • **Abnormal**: One or more ports are down or the failover kit is in bypass mode. • **---**: Disconnected or trust pending.
Inspection	Displays if the device is in layer 2 bypass mode. • **Normal** – Traffic inspection is enabled • **Abnormal** – Traffic inspection is disabled. This means that the device is in layer 2 bypass mode.

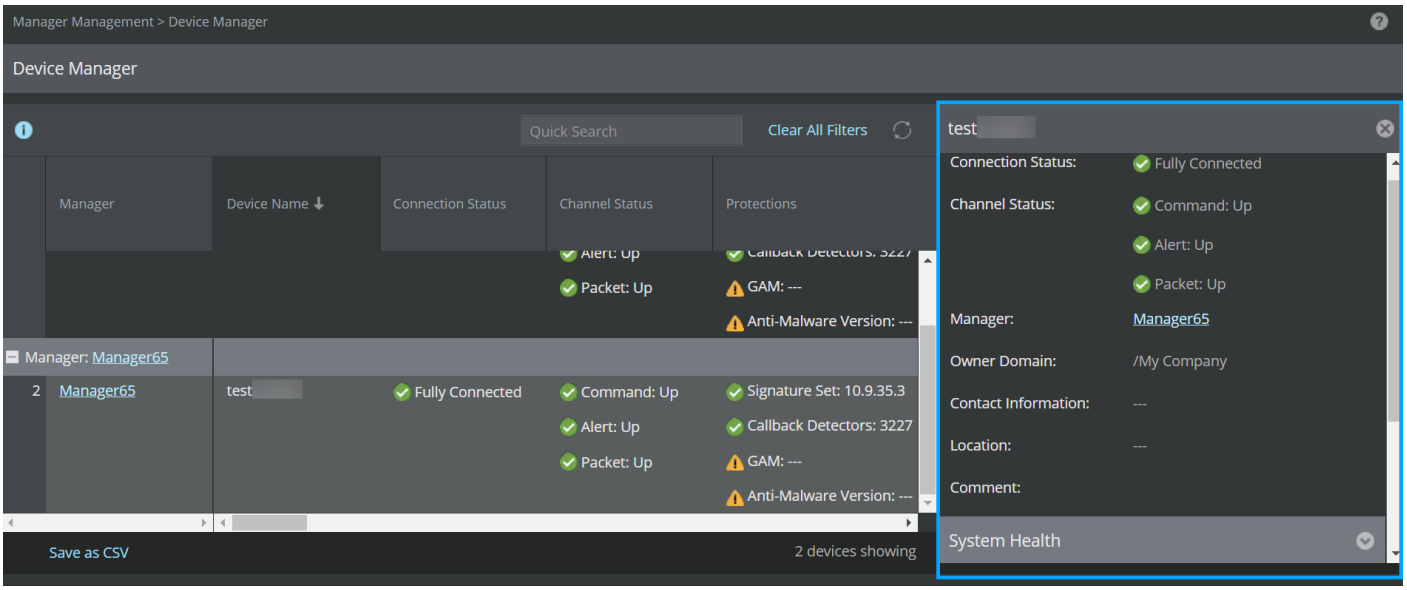
Option	Definition
Performance	Displays if there are any performance related faults for the device. • **Normal** – Indicates that the device has no unacknowledged performance faults. • **Abnormal** – Indicates that the device has one or more unacknowledged faults. **NOTE** This is not applicable to NTBA appliances and vIPS Clusters. It is displayed as **---**.
Hardware	Displays if the hardware has any temperature or power related issues. • **Normal** – Indicates that the device has no unacknowledged faults • **Abnormal** – Indicates that the device has one or more unacknowledged faults

Option	Definition
Power Supplies	Displays the power supply status. The following are the status of the power supply: • **Operational** - Indicates that the power supply is detected and operational. • **Non Operational** - Indicates that the power supply is detected but not operational. • **Absent** - Indicates that the power supply is absent. • **Error** - Indicates Error when the system fails to fetch the real power status. • **---** - Indicates that the trust is not yet established or power supply status is not applicable for it. For NS-series Sensors, two units of power modules and power supply status are displayed: • **A:** Displays the Primary power module and power supply status • **B:** Displays the Secondary power module and power supply status **NOTE** Only for NS9300 Sensor, four units of power modules and power supply status are displayed: • For Primary, **A** and **B** displays the two units of power module and power supply status. • For Secondary, **A** and **B** displays the two units of power module and power supply status. **NOTE** For all untrusted devices and NTBA, it is displayed as **---**. **NOTE** The NS3x00 Sensors do not support Secondary power supply module. So, the status of only Primary power supply module is displayed.
Faults	
Total	Displays the number of unacknowledged faults generated for the device. Click the tooltip icon to navigate to the **Faults** window.
Critical	Displays the number of critical faults generated for the device.
Error	Displays the number of error faults generated for the device.
Warning	Displays the number of warning faults generated for the device.
Info	Displays the number of info faults generated for the device.
Sync	

Option	Definition
Status	Displays the synchronization state of the Sensor. • **Synchronized**: Displayed there are no pending changes. • **Sync required**: Displayed when there are pending changes on the Sensor. • **Sync in progress**: Displayed when the deployment is in progress. • **---**: Indicates that there is no trust established between the Sensor and the Manager.
Pending Changes	Displays the configuration changes updated to the device including signature set or callback detectors.
Last Sync	Displays the date and time of the last configuration change.
Deployment Mode	Displays if the configuration update was online or offline. This is displayed as **Direct** for online update and **Indirect** for offline update.

You can also view these device details in the **Details** panel to the right of the page by double-clicking anywhere on the selected device.

Figure 709. Details panel



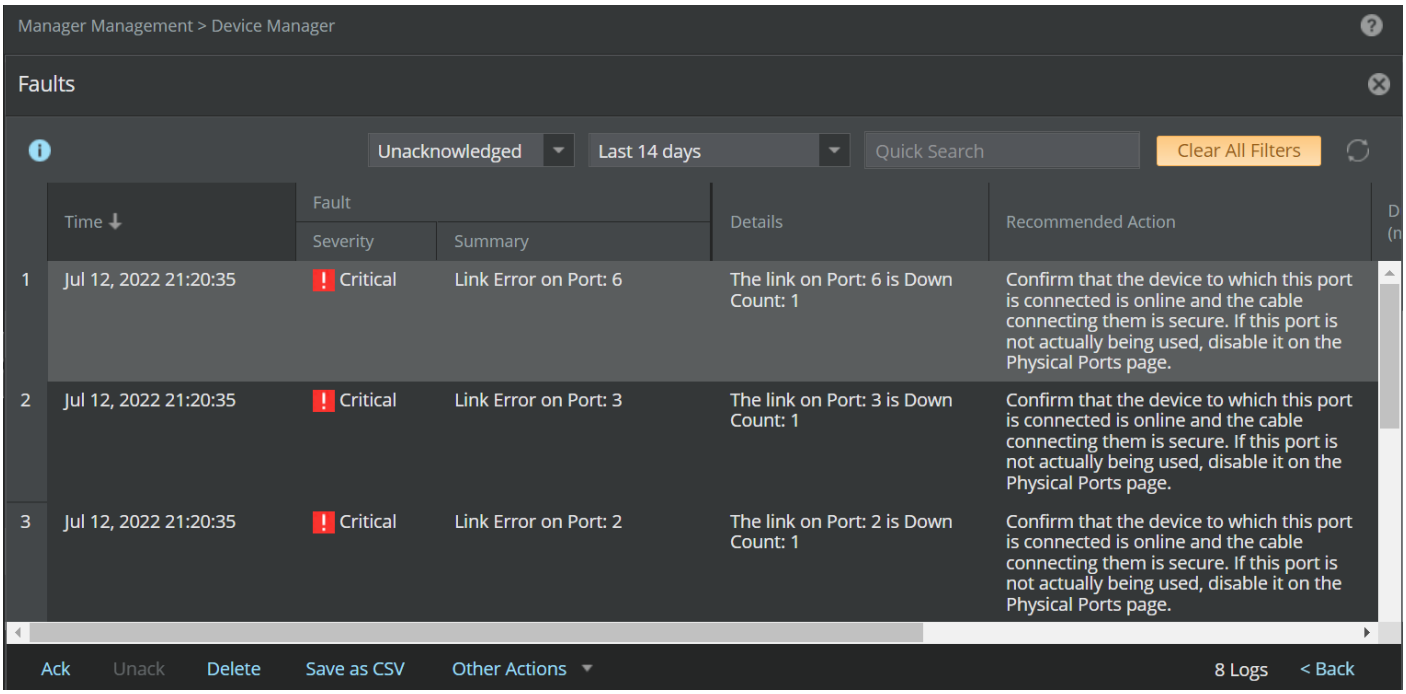
NOTE

You cannot edit, modify, save any device-related information in the **Details** panel of the **Device Manager** page in Central Manager. It only provides read-only view of the details of the selected device.

Faults

A **Faults** window is displayed on selecting the tooltip icon for a particular fault in the **Device Manager** page of the Central Manager. On selecting **Clear All Filters**, the **Faults** window displays all the faults generated for the selected device.

Figure 710. Faults window



This window is similar to the **Faults** tab in the Manager → Troubleshooting → **Logs** page, except that this window displays the faults for the selected device only based on the severity. All the actions that can be performed in the **Faults** tab in the **Logs** page can also be performed through this window.

For more information, refer to the Faults (page 343) section.

Click ⊗ or < Back to go back to the **Device Manager** grid view.

View device summary details

The Devices → <Admin Domain Name> → Devices → <Device Name> → **Summary** action presents a view of the configured information for an installed device. For HA pair, Devices → <Admin Domain Name> → Devices → Member Sensors → <HA Pair Node> → **Summary** action presents a view of the configured information for an installed device that is part of a HA pair. For Sensors in a stack, the Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node Id> → **Summary** action presents a view of the configured information for an installed device that is part of a stack.

The information displayed is configured during the installation and initialization of the selected device through the device command line interface.

In the **Device Details** monitor, verify that the Name, IP address, subnet mask, and default gateway IP address are the same as what you set through the command line interface for the selected device.

When the Sensor is configured with dual stack (IPv4 and IPv6 addresses), following fields in the **Summary** page displays only the IP address on which trust was established between the device and the Manager.

- **IP Address Connected to Manager**

- **Subnet Mask**
- **Default Gateway**

For example, if you configure both IPv4 and IPv6 addresses in the Sensor, but establish trust with the Manager on IPv4, then the **Summary** page displays only the IPv4 address for **IP Address Connected to Manager**, **Subnet Mask**, and **Default Gateway**.

Follow this procedure to view the summary of the device configurations:

For standalone Sensors, go to Devices → <Admin Domain Name> → Devices → <Device Name> → **Summary**.

For HA pair, go to Devices → <Admin Domain Name> → Devices → Member Sensors → <HA Pair Node> → **Summary**.

For Sensors in a stack and a HA pair of stack Sensors, Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → **Summary**.

The **Summary** page is displayed. It contains the following information:

Device details	Definition

General Settings	Displays the following parameters:
	• **Connection Status** - Displays the status between the Sensor and the Manager as **Fully Connected**, **Partially Connected**, **Disconnected**, or **Trust Pending**.
	• **Channel Status** - Displays the name of the following channels and its status whether "Up" or "Down":
	  • **Command**
	  • **Alert**
	  • **Packet**
	  If the trust is not established between the Manager and Sensor, the **Channel Status** is displayed as **---**.
	• **Owner Domain** - Displays the name of the owner domain.
	• **Shared Secret** - You can edit the shared secret key.
	  The device shared secret key can contain up to 25 alphanumeric characters, including hyphens, underscores, and periods.
	  CAUTION
	  This should only be performed if the shared secret in the device shell (command line interface) has been changed. When one of the shared secrets is changed, the device loses communication with the Manager.
	• **Confirm Shared Secret** - Confirm the shared secret key.
	• **Contact Information** - Type the details of the person responsible for this device.
	• **Location** - Type the geographic (city, building, and others) location.
	• **Comment** - Type the comments.
	To update the modified configurations, click **Save**.

Device details	Definition
System Health	• **Overall Health** - Displays the overall health of the system as **Normal**, **Abnormal**, or **---**. • **Internal Health** - Displays the Sensor health as **Normal**, **Abnormal**, or **---**. • **Physical Ports** - Displays the status of ports operating as **Normal**, **Abnormal**, or **---**. Click the link to navigate to the **Physical Ports** page of the device. • **Inspection** - Displays if the device is in layer 2 bypass mode as **Normal** or **Abnormal**. Click the link to navigate to the **Layer 2 Bypass** page of the device. • **Performance** - Displays the performance related faults for the device as **Normal** or **Abnormal**. Click the link to navigate to the **Performance Charts** page. • **Hardware** - Displays if the hardware has any temperature or power related issues as **Normal** or **Abnormal**. • **Power Supplies** - Displays the power supply status as **Operational**, **Non Operational**, **Absent**, **Error**, and **---**. **NOTE** • For NS9300 Sensor, four units of power modules and power supply status are displayed. • The NS3x00 Sensors do not support Secondary power supply module thus, the status of only Primary power supply module is displayed.

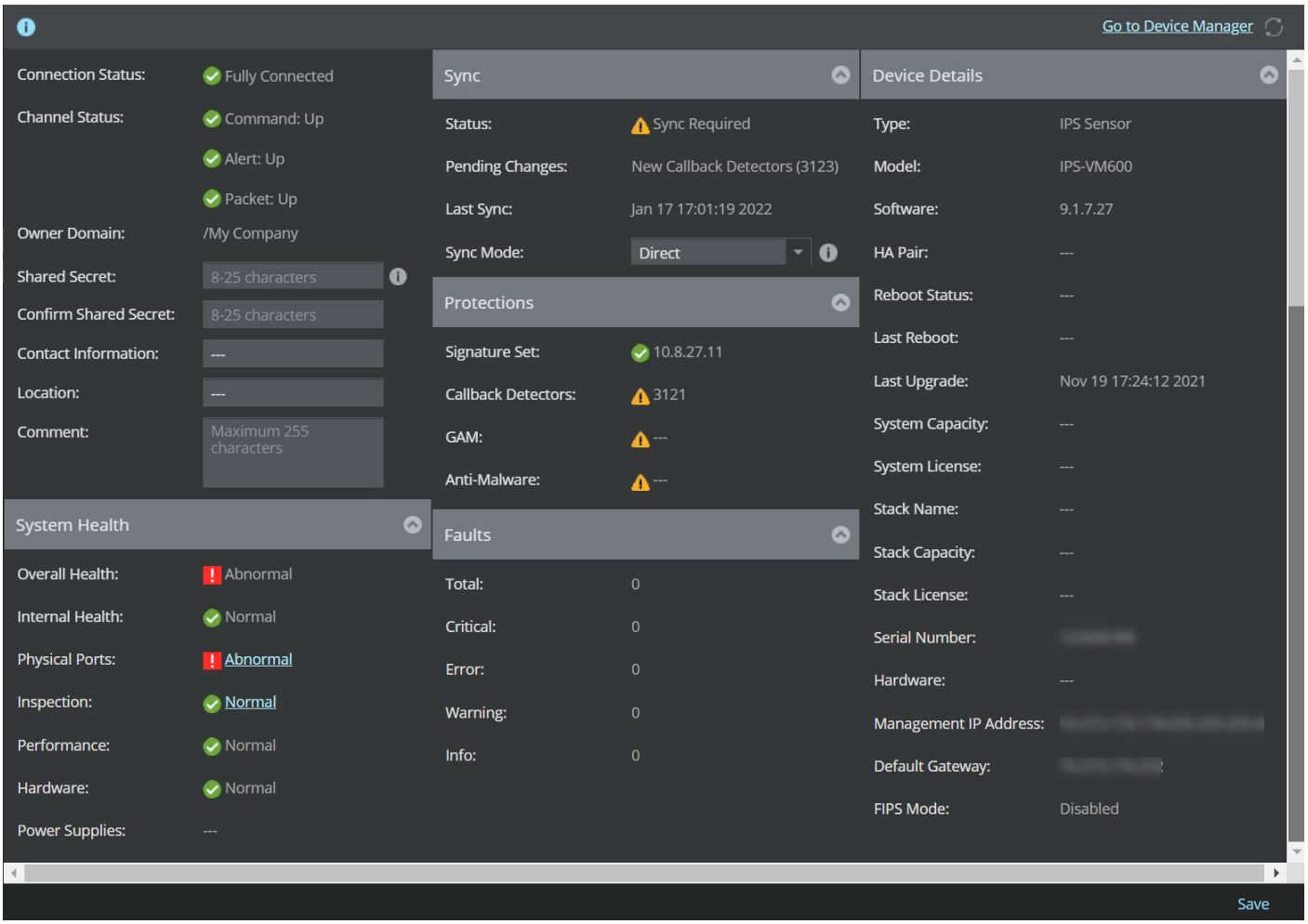
<table>
<tr><th>Device details</th><th>Definition</th></tr>
<tr><td>Sync</td><td>Displays the sync details for the following parameters:
Status - Displays the following status:<table><tr><th>Status</th><th>Description</th></tr><tr><td> 
Synchronized</td><td>Indicates that no pending changes are required.</td></tr><tr><td> 
Sync in progress</td><td>Indicates if any pending changes are required.</td></tr><tr><td>Sync required</td><td>Indicates when the deployment is in progress.</td></tr><tr><td>---</td><td>Indicates that there is no trust established between the Sensor and Manager.</td></tr></table>
Pending Changes - Displays the configuration changes updated to the device including signature set or callback detectors.
Last Sync - Displays the date and time of the last sync.
Sync Mode - Displays the configuration mode as Direct for online updates and Indirect for offline updates.
You can edit the mode from Sync mode drop-down. Select the required mode and click Save.</td></tr>
<tr><td>Protections</td><td>Displays if the versions for the following protection parameters are latest not:
Signature Set
Callback Detectors
GAM (Gateway Anti-Malware engine)
Anti-Malware engine
The following icons are displayed:  : Displayed when the parameter has the latest version available  : Displayed when the version available in the Manager differs with the version available in the Sensor.  : Displayed when there is no latest version available on the Manager.  : Displayed when the latest version cannot be determined as the deployment is possibly in an air-gap network.
NOTE
This is displayed only for GAM and Anti-Malware.</td></tr>
</table>

Device details	Definition
Faults	Displays the number of system faults generated for the following parameters: • **Total** - Displays the number of unacknowledged faults generated for the device. • **Critical** - Displays the number of critical faults generated for the device. • **Error** - Displays the number of error faults generated for the device. • **Warning** - Displays the number of warning faults generated for the device. • **Info** - Displays the number of info faults generated for the device. A **Faults** window is displayed on selecting the tooltip icon for a particular fault.

Device details	Definition
Device Details	Displays the device details for following parameters: • **Type** - Displays the type of device. • **Model** - Displays the model of device. • **Software** - Displays the device software version. • **HA Pair** - Displays the name of HA pair. • **Reboot Status** - Displays if the Sensor requires a reboot. This is required to deploy configuration changes to the Sensor without any failure. **NOTE** This is not applicable to NTBA appliances. It is displayed as **---**. • **Last Reboot** - Displays the time stamp of last reboot. • **Upgrade Status** - Displays the status of the upgrade as **Successful** , **In-progress**, **Failed** , or **---**. • **Last Upgrade** - Displays the time stamp of last upgrade. • **System Capacity** - Displays the throughput for the Sensor. **NOTE** The information is displayed only for NS3500, NS9500, and NS7500 Sensors. • **System License** - **License**: Displays the license details of Sensor. Click on the tooltip icon to assign or change the license. For more information, see Assign a license to a Sensor. • **Stack Name** - Displays the name of the Stack. • **Stack Capacity** - Displays the throughput for the stack. • **Stack License** - Displays the license details of stack. • **Serial Number** - Displays the device serial number. • **Hardware** - Displays the version details of hardware. • **Management IP Address** - Displays the IP address/subnet mask of device. • **Default Gateway** - Displays the IP address of the default gateway configured on device. • **FIPS Mode** - Displays if FIPS mode is enabled or disabled.

Device details	Definition
	NOTE This is not applicable to NTBA appliances. It is displayed as **---**.
Go to Device Manager	You can access the **Device Manager** from this link.
Save	Saves the modified updates.
	Refreshes the page.

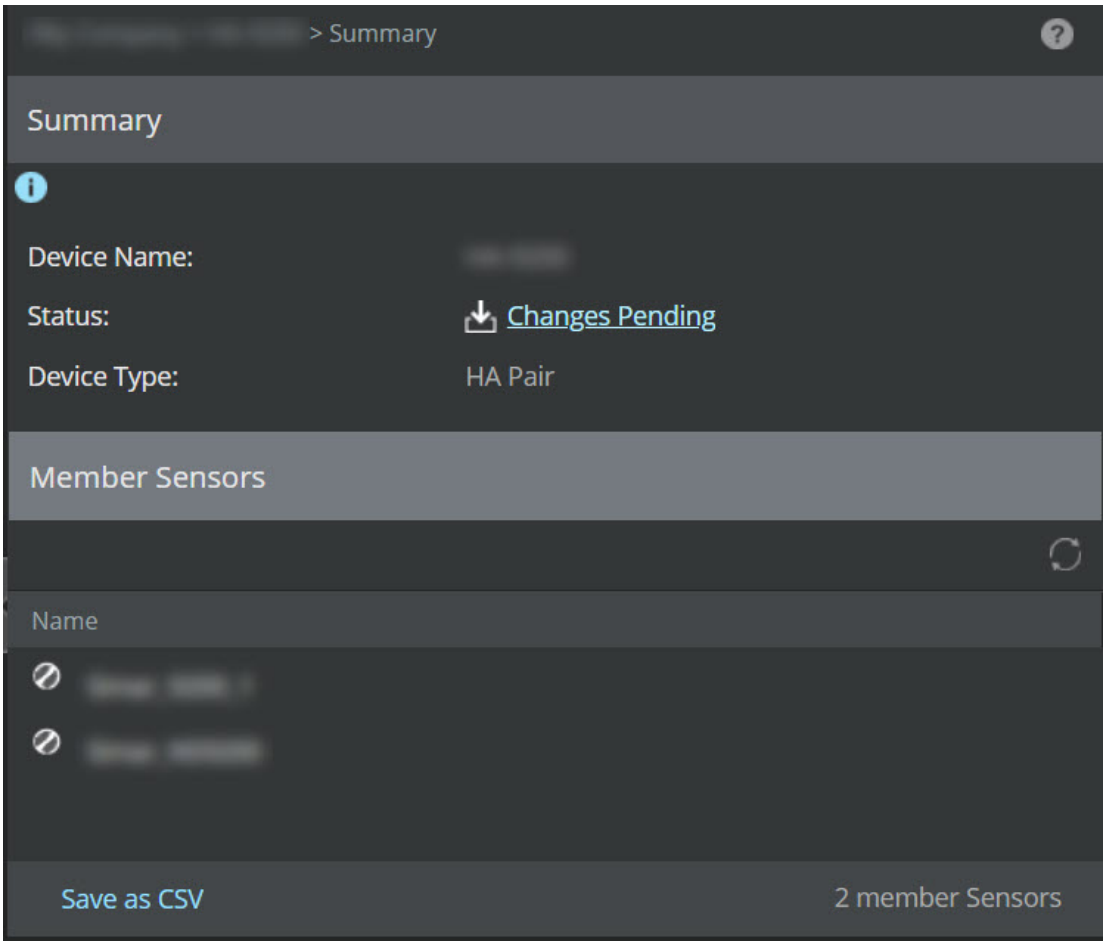
For more information, refer Sensors (page 1587) tab.



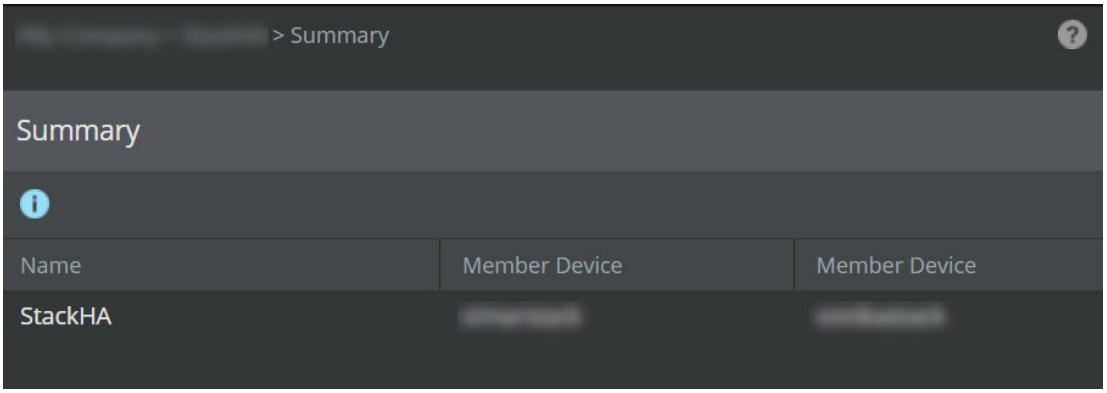
Summary details of HA Pairs

The Devices → <Admin Domain Name> → Devices → <HA Pair Name> → **Summary** action presents a view of the configured information for installed HA Pairs. It displays the following details:

Options	Definition
Device Name	Displays the name of configured HA Pair.
Status	Displays the status of device.
Device type	Displays the device type as HA Pair.
Member Sensors	
	Refreshes the page.
Name	Displays name of the Sensors configured as HA Pair. If the Sensor is connected,  **<Sensor Name>** is displayed. If the Sensor is disconnected,  **<Sensor Name>** is displayed.
Save as CSV	Downloads the device details for all the devices as a .csv file.
<Number> member Sensors	Displays the total number of member Sensors available in the Manager.



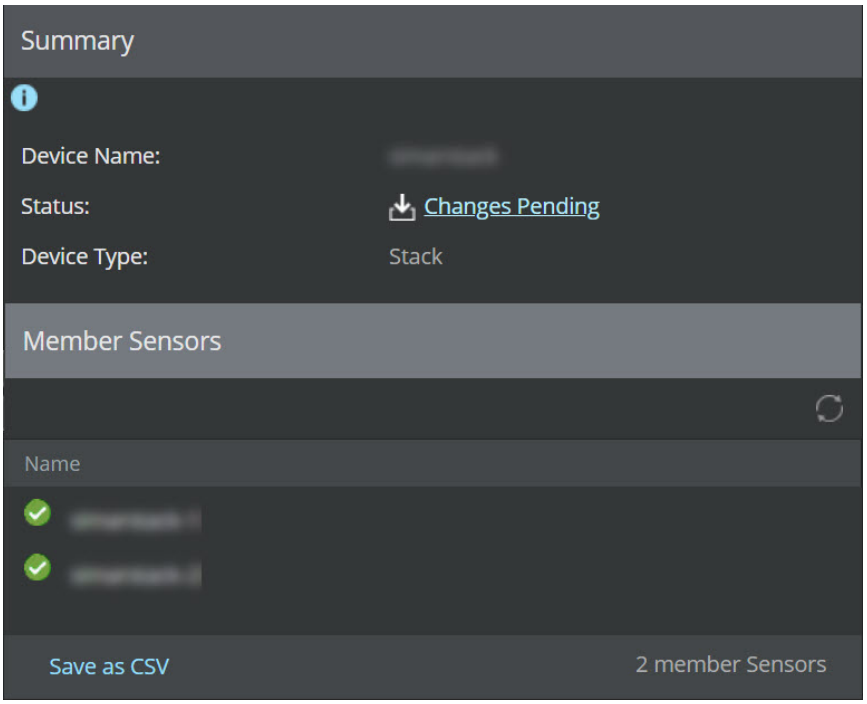
If the HA Pair is a HA Pair of Stacks, the **Name** and **Member Device** details are displayed.



Summary details of the Sensors in Stack

The Devices → <Admin Domain Name> → Devices → <Stack Name> → **Summary** action presents a view of the configured information for the Sensors in Stack. It displays the following details:

Options	Definition
Device Name	Displays name of the configured Sensors in Stack.
Status	Displays the status of device.
Device type	Displays the device type as Stack.
Member Sensors	
	Refreshes the page.
Name	Displays name of the Sensors in Stack. If the Sensor is connected, **<Sensor Name>** is displayed. If the Sensor is disconnected, **<Sensor Name>** is displayed.
Save as CSV	Downloads the device details for all the devices as a .csv file.
<Number> member Sensors	Displays the total number of member Sensors available in the Manager.



Monitoring Sensor Health

The Devices → <Admin Domain Name> → Global → Sensor Health → **Health Status** page provides a consolidated view of all health-related faults generated for the Sensor in Manager. You can view these faults in admin domain including those configured in the child admin domains. The **Health Status** page provides a cumulative view of system health, processor health, resource usage, and traffic nature of all devices configured in the Manager.

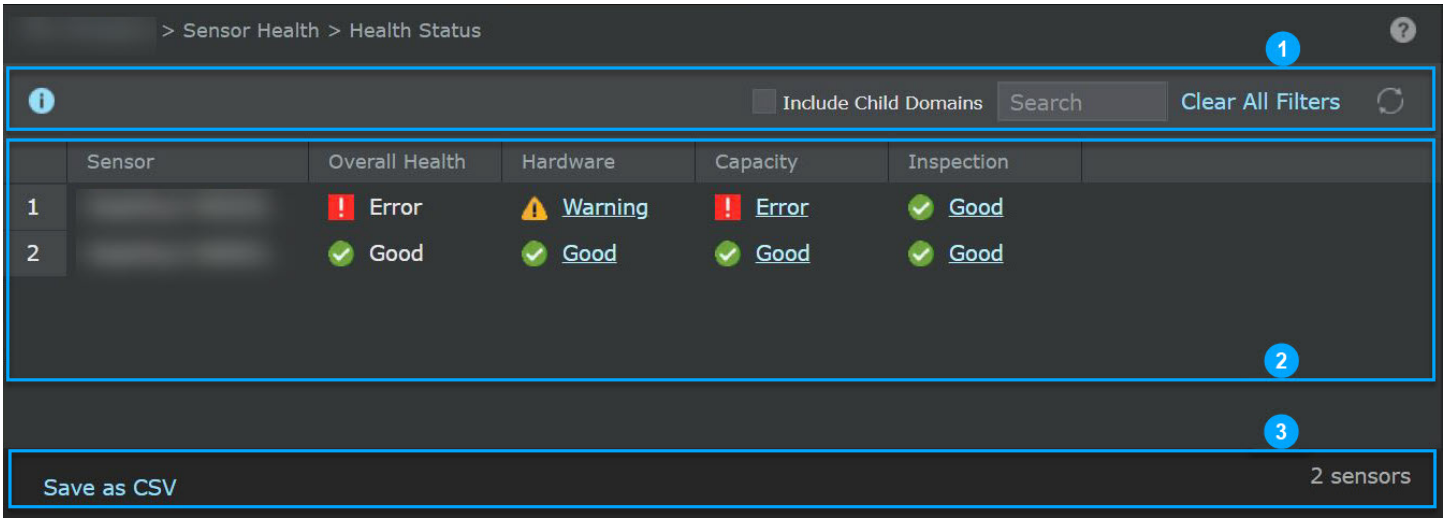
NOTE

This feature is not applicable for NS3x00, NS9300, and Virtual-IPS Sensors.

Health Status

The **Health Status** page allows you to monitor the Sensor health and take necessary actions, if required. The following options are available in the **Health Status** page:

Figure 711. Health Status page



Callout	Description
1	Top menu
2	Grid view
3	Bottom menu

The details of callout options are as listed below:

Options	Description
Top Menu	
	Provides an overview of Sensor Health page.
Include Child Domains	Displays the Sensors configured in the child domain.
Search	Enter a keyword in the *Search* field and results are automatically displayed.
Clear All Filters	Click **Clear All Filters** to undo applied filters.
	Refreshes the tab.
Grid View	
Sensor	Displays the name of the device.
Overall Health	Displays the following faults for overall health of the Sensor: • **Good**: All indicators are good • **Error**: One or more indicators have error • **Warning**: One or more indicators have warning

Options	Description
Hardware	Displays the following faults when there are any abnormalities in the hardware: • **Good**: All indicators are good • **Error**: When any indicators possess a critical or a major abnormality • **Warning**: When any indicators possess a minor abnormality
Capacity	Displays the following faults when the memory, CPU, and throughput usages of the Sensor breaches the threshold: • **Good**: All indicators are good • **Error**: When any indicators possess a critical or a major abnormality • **Warning**: When any indicators possess a minor abnormality
Inspection	Displays the following faults for inspection summary: • **Good**: All indicators are good • **Error**: When any indicators possess a critical or a major abnormality • **Warning**: When any indicators possess a minor abnormality
Bottom Menu	
Save as CSV	Downloads the device details for all devices as a .csv file.
<Number> sensor	Displays a total number of Sensors configured in the Manager.

The **Health Status** page can be customized by different options like sorting, filtering, and grouping which helps to drill-down the details based on your requirement. The following options are available:

- **Sort Ascending**: You can sort all columns in the ascending order.
- **Sort Descending**: You can sort all columns in the descending order.
- **Columns**: You can view the required columns by selecting each category from the list.
- **Group by this field**: You can group the device details based on specific sub category.
- **Show in Groups**: It allows you to disable **Group by this field** filter. By default, it is disabled.
- **Filters**: You can filter the faults based on its severity.

Hardware Summary

You can view the details of generated faults for all Hardware indicators by selecting the hyperlink from the **Hardware** column of **Health Status** page. You can monitor the device performance and take necessary actions. For the following parameters, faults are displayed:

Voltage Error: The device supplying the voltage or the device using the voltage can trigger the voltage error. Faults are generated, when this device voltage is outside its normal range.

System Firmware Error: The BIOS logs any POST (Power On Self Test) errors to the System Event Logs (SEL). This event is logged every time a POST error is displayed. Even though this event indicates an error, it might not be a fatal error.

Temperature Error: Multiple varieties of temperature Sensors can be implemented on Trellix IPS system. Now, they are split into three types: Regular, Thermal Margin, and Discrete temperature Sensors. Each of them have there own types of events and when their device temperature goes outside its normal range, faults are generated.

Memory Error: Trellix IPS system's BIOS reports multiple error codes from sticks of memory that populate slots in board. For example, DIMM (Dual In-line Memory Module) failed test/initialization or is disabled.

Fan Error: On the Trellix IPS system, speed Sensor fans are available. Faults are generated, when the device fan is not performing at expected capacity.

Processor Error: This event occurs only due to failures of thermal solution. Each processor has a status Sensor. This status Sensor indicates the processor presence or a thermal tip condition.

Logging Error: The Baseboard Management Controllers (BMC) logs a system clear event. This is the first event in the SEL. When logging is disabled for the device manually using any Intelligent Platform Management Interface (IPMI)-aware utility or in factory (as part of manufacturing process), faults are generated.

Power Supply Error: The Sensors monitors the status of power supplies in the system. If there is a failure, predictive failure, or a configuration error it generates faults.

Physical Security Error: Two Sensors are included in the physical security subsystem: Chassis intrusion and LAN leash lost.

- **Chassis Intrusion:** It is monitored on supported chassis. Faults are generated when the chassis lid is opened or closed.
- **LAN Leash Lost:** It monitors the physical connection on the onboard network ports. If a LAN leash lost event is logged, it indicates that the network port lost its physical connection.

Watchdog Error: Trellix IPS Server supports a watchdog timer, to check whether the operating system is still responsive. By default, this timer is disabled. An IPMI-aware utility is required to reset this timer before its expiry. If the timer expires, you can configure the BMC to take necessary actions.

Operating System Shutdown Error: An IPMI-driver integrated in the operating system aids the capability to log SEL events. When the system shuts down from the Windows operating system, multiple events could be logged such as, operating system stop/shutdown event and OEM record events.

Generic Hardware Error: The BMC is configured to send alerts for events logged into the SEL. These alerts are called as Platform Event Filters (PEF). By default, it is disabled. You can enable the PEF filters manually using any IPMI-aware utility. PEF events are logged, if the BMC responds due to a PEF configuration. The BMC event triggers the PEF action in SEL. This function is built into BMC to allow it to send alerts (SNMP or other) for any event that gets logged to the SEL.

Physical Interrupt Error: The following includes types of physical interrupt error:

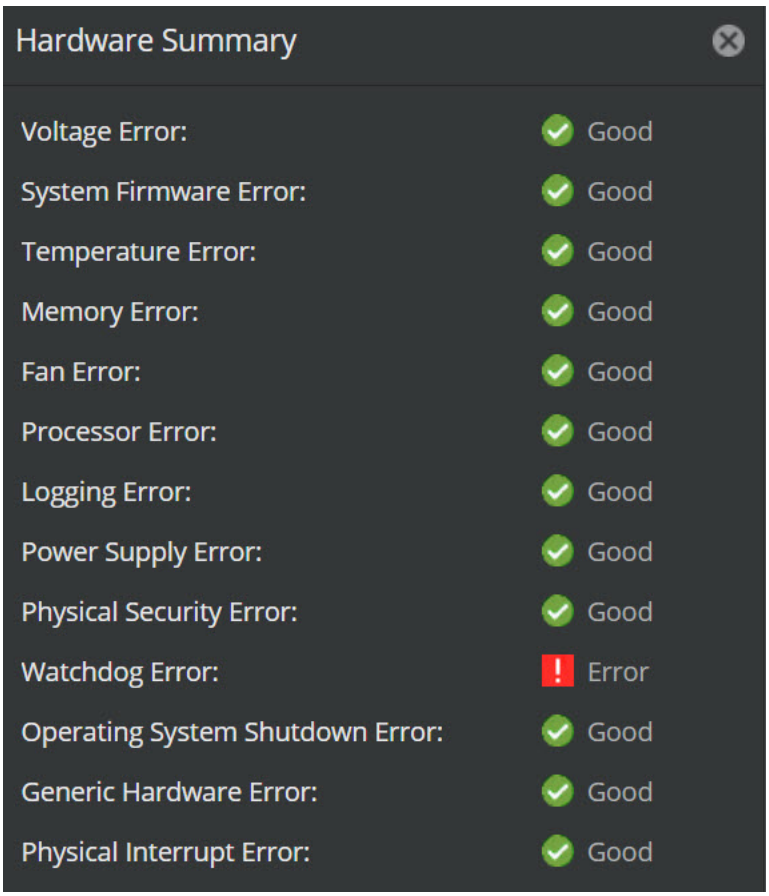
- **Frontend Panel Non-Maskable Interrupt Error:** The front panel interrupt button (also referred as NMI button) is a recessed button, that allows you to force a critical interrupt which triggers a crash error or kernel panic.
- **Peripheral Component Interconnect express Error:** PCIe stands for Peripheral Component Interconnect express. It is an interface standard that is used to connect high-speed components. The motherboard has several PCIe slots to connect different components such as GPU (or video cards or graphics cards), Wi-Fi cards, SSD (Solid-state drive).

  PCIe error events are either correctable (informational event) or fatal. In both cases information is logged to help identify the source of the PCIe error and the bus, device, and function is included in the extended data fields. The PCIe devices are

mapped in the operating system by bus, device, and function. Each device is uniquely identified by the bus, device, and function. PCIe device information can be found in the operating system.

For more information about Hardware Summary, see [Intel-SEL Troubleshooting guide].

Figure 712. Hardware Summary



NOTE

The faults for **Voltage Error**, **System Firmware Error**, **Memory Error**, **Processor Error**, **Logging Error**, **Physical Security Error**, **Watchdog Error**, **Operating System Shutdown Error**, and **Physical Interrupt Error** are displayed only for 10.1.5.190 Sensors and above.

Faults are generated based on severity. Trellix recommends you to take required actions to correct the generated faults. For more information, see Sensor Faults (page 2426) section.

Capacity Summary

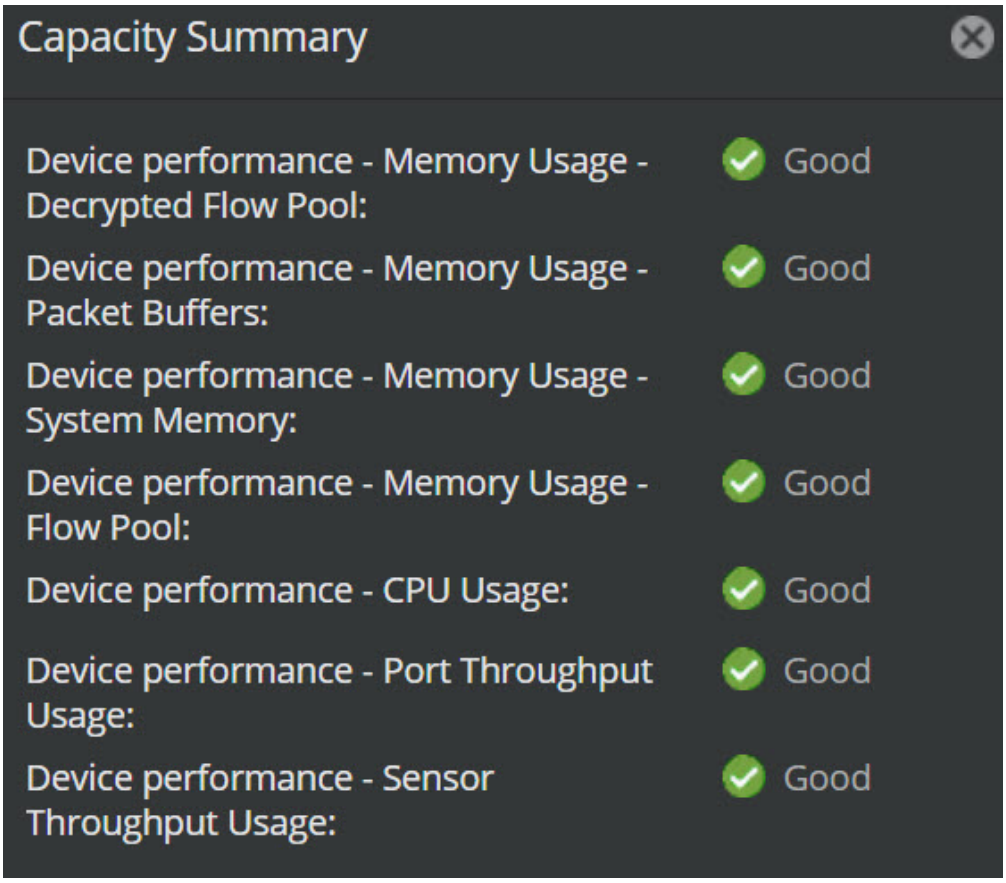
You can view the details of generated faults by selecting the hyperlink from the **Capacity** column of **Health Status** page. For the following parameters, faults are displayed:

- **Device Performance - Memory Usage**: When the memory usage breaches the threshold, faults are generated. You can view the faults for the following metrics:

- **Device Performance - Memory Usage - Decrypted Flow Pool**: Memory allocated to inspect decrypted SSL flows.
- **Device Performance - Memory Usage - Packet Buffers**: Packet buffer used by the Sensor.
- **Device Performance - Memory Usage - System Memory**: System memory used by the Sensor.
- **Device Performance - Memory Usage - Flow pool**: Memory allocated to inspect all flows.

- **Device Performance - CPU Usage**: CPU Usage is the usage that represents the combined usage of software processing in the datapath together with the throughput usage in the Sensor. You can monitor the CPU usage before it reaches the threshold limit. By default, a fault message is generated if the CPU usage goes beyond 90%.
- **Device Performance - Port Throughput Usage**: Displays the faults, when the port throughput utilization breaches the threshold value for a selected device.
- **Device Performance - Sensor Throughput Usage**: Displays the faults, when the Sensor throughput utilization breaches the threshold value for a selected device.

Figure 713. Capacity Summary



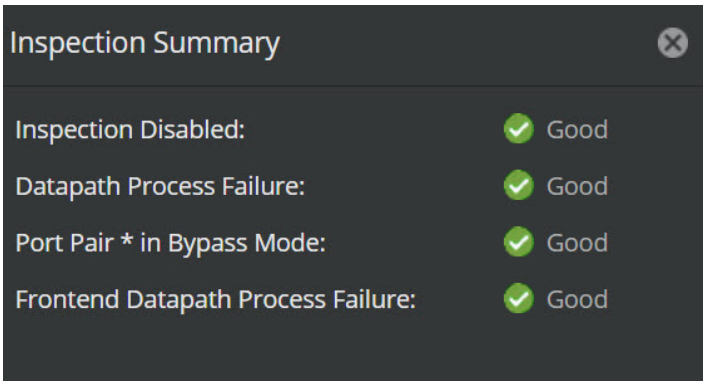
Inspection Summary

You can view the details of generated faults by selecting the hyperlink from the **Inspection** column of **Health Status** page. For the following parameters, faults are displayed:

- **Inspection Disabled**: When the device is operating in layer 2 bypass mode, inspection is disabled.

- **Datapath Process Failure**: When the device has detected a failure in the datapath process, which might impact datapath inspection.
- **Port Pair * in Bypass Mode**: When the device is configured in the inline fail-open mode, but it is in bypass mode. The port pair is not inspecting traffic.
- **Frontend Datapath Process Failure**: When the device has detected a failure in the front-end datapath process, which might impact datapath inspection.

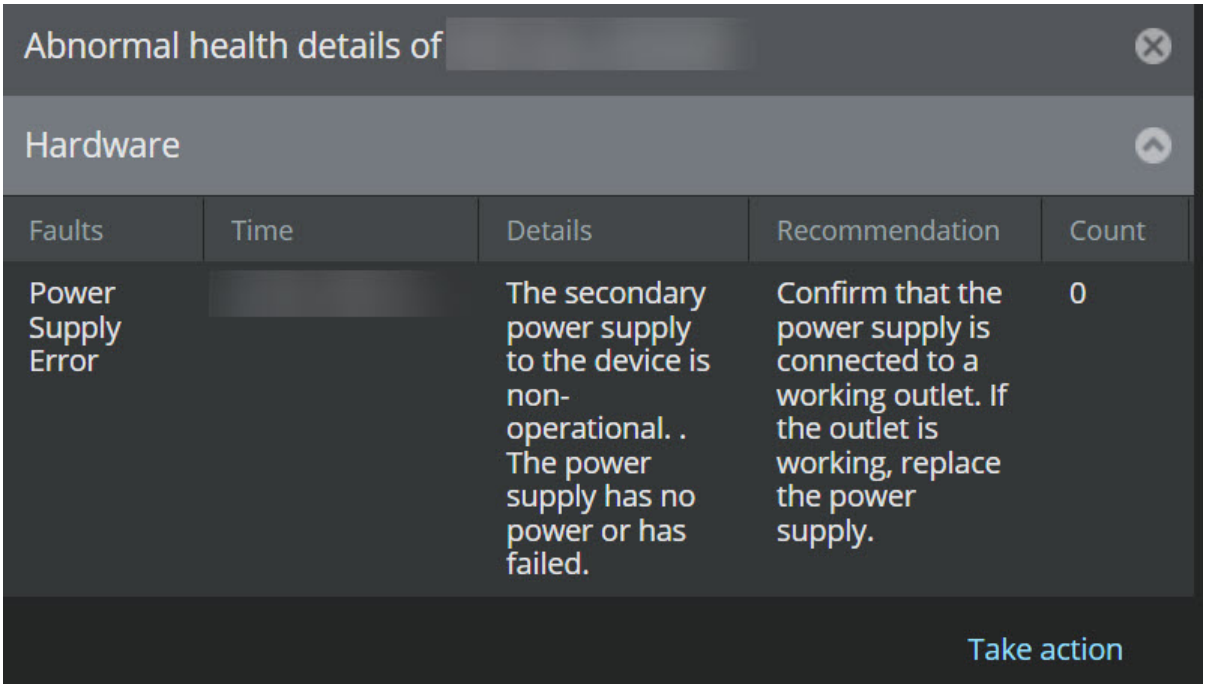
Figure 714. Inspection Summary



Details Panel

For a particular Sensor, you can view the device details by double-clicking anywhere on the selected device. An **Abnormal health details of <Sensor Name>** panel is displayed at the right end of the page .

Figure 715. Abnormal health details panel

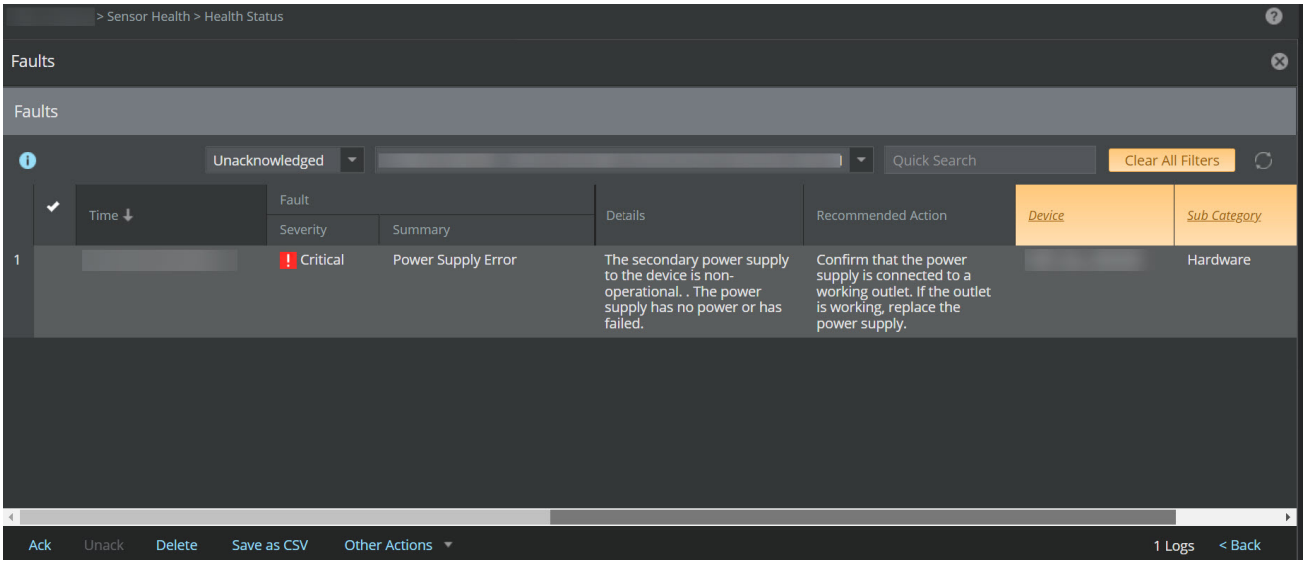


This panel displays the following details:

- **Faults**: Displays the name of the indicators where the faults are observed.
- **Time**: Displays the time stamp for all generated faults.
- **Details**: Displays the details of all factors that trigger faults.
- **Recommendation**: Displays a few basic troubleshooting steps for resolving the generated faults.
- **Count**: Displays a total number of the same faults generated for the Sensor.

The **Take action** enables you to access the **Faults** window. It displays all faults generated within the time range i.e., the interval between the occurrence of the first fault and the present time. By default, the **Faults** window displays all faults generated for a selected **Device** and its **Sub Category**. On selecting **Clear All Filters**, you can remove all applied filters and view overall faults.

Figure 716. Faults Window



This window is similar to the **Faults** tab in the Manager → Admin Domain Name → Troubleshooting → **Logs** except, it displays the faults only for a selected **Device**, **Time**, and its **Sub Category**. All actions that can be performed in the **Faults** tab of **Logs** page can be performed through this window. You can click ⊗ or < Back to go back to the **Health Status** page. For more information, see the Faults (page 343) section.

How to reboot devices

Rebooting a device shuts down all its processes and then restarts them. You can reboot a device from the Manager or from the device's CLI. By default, when you reboot a device, it restarts the entire system. So, until the device is fully up again, there is a break in the device's functions. For example, in case of an inline Sensor with no fail-open kit, the traffic flow is interrupted until the Sensor is up again.

Trellix IPS provides two reboot options:

- Full reboot: This is the default reboot option where the entire system, including the hardware, restarts.
- Hitless reboot: This option restarts only those software processes of a device that require to be restarted. When you do a hitless reboot, the device goes into Layer 2 pass-through mode and restarts the required processes, but the data path continues to pass traffic. After restarting the required processes, it automatically comes out of Layer 2 pass-through mode. This reduces the reboot time and also prevents traffic interruption during the reboot.

If you have enabled autorecovery, a Sensor attempts to recover automatically without loss of traffic, when it determines internal errors or process failures. If it is unable to recover from the error, it goes into Layer 2 pass-through mode or goes through a full reboot. Functionally, hitless reboot is to some extent similar to the autorecovery feature, but they are two independent features. That is, you can use one without enabling the other. One difference is, you can trigger hitless reboot, whereas autorecovery is triggered by the Sensor itself, provided you have this feature enabled. Also, hitless reboot cannot recover a Sensor from internal errors because the Sensor must be in good health for it to undergo hitless reboot.

Notes regarding hitless reboot:

- Hitless reboot is supported only on NS-series Sensors.

  NOTE

  For NS-Series Sensors, hitless reboot is not supported when SSL decryption is enabled.

- A Sensor must be in good health for hitless reboot. If the health turns bad during a hitless reboot, it undergoes a full reboot.
- If for some reason, a Sensor is unable to undergo a hitless reboot, a fault is raised in the Manager and the Sensor undergoes a full reboot.
- Hitless reboot is supported only if Layer 2 pass-through monitoring is enabled. Though not mandatory, Trellix recommends that you also enable autorecovery and Sensor watchdog features when using the hitless reboot feature. For information on how to enable these features, see the [IPS Administration] section.

For the relevant devices, the hitless reboot option is available from the Manager and from the Sensor CLI. This section provides information on how to reboot a device from the Manager. For information on how to reboot from the CLI, see the [CLI commands] section.

Reboot a device from the Manager

You can reboot the device from the Manager. Certain devices support full reboot and hitless reboot. Full reboot restarts the entire system, whereas a hitless reboot restarts select processes but not the entire system.

NOTE

Full reboot can take up to 10 minutes, whereas hitless reboot can be completed in about 3-4 minutes.

1. For a standalone Sensor, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → **Reboot**.

   For Sensors in a stack, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Maintenance → **Reboot**.

   The **Reboot** page is displayed.

2. Click **Reboot Now**.
   - To perform a hitless reboot, clear the **Full Reboot** checkbox, then click **Reboot Now**.
3. Click **OK** to confirm reboot.

NOTE

You can also perform the Sensor reboot from Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab and choose the required Sensor from list. Select **Reboot** from **Other Actions** drop-down. A **Warning** dialog box is displayed. You can perform either partial or full reboot depending on the requirement.

Add multiple user accounts to devices

Users added to devices, manage the different activities required to maintain the device. This provides granular access control for the CLI commands. You can create users from the Sensor CLI and assign different roles to them. Only the administrator has the rights to add new users and edit existing roles of users. A maximum of 100 users can be added to the devices from the Sensor CLI. The various roles for users are:

- ReadWrite
- ReadOnly
- Updater
- Maintainer

For more information, see the section [Granular access control for CLI commands] in the [CLI commands] section.

Import a Sensor configuration file

Prerequisites:

The Manager from which configuration is exported and the one to which configuration is imported must be identical. They should be of the same model, and same software version.

Both Managers must have the same admin domain hierarchy, or at a minimum, the same admin domain hierarchy starting from the domain wherein the Sensor resides.

For example, if you exported a Sensor belonging to /My Company/Domain A, and below Domain A, there is:

- /My Company/Domain A/Domain B
- /My Company/Domain A/Domain B/Domain C

The importing Sensor must reside in a domain that has the following sub-domains:

- Domain B
- Domain B/Domain C

CAUTION

Trellix recommends that the Sensor receiving the import has the same signature set as the exporting Sensor. It is recommended that both the Managers have the same set of policies if policies have also been exported/imported.

The **Import Configuration** option enables you to overwrite the current configuration on a saved (exported) Sensor configuration file.

Importing a saved configuration is useful in a test-to-production environment where you configure your settings on a test (non-production) Manager system, then import to a Sensor in your live environment.

Importing is also useful in the event a Sensor fails and you replace the failed Sensor with a new Sensor, which requires the same configuration as the previous Sensor.

Steps:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → **Import Configuration**.

   NOTE

   The **<Device Name>** here refers to a Sensor.

   The **Import Configuration** page is displayed.
2. Click **Browse** to locate your saved Sensor configuration.
3. Click **Apply**.
4. Upon completion of import, reboot the Sensor.
5. Run a Sensor report to verify settings.

Export the Sensor configuration

The **Export Configuration** feature enables you to save the configuration of a Sensor (including NTBA Appliance configuration settings of the Sensor) into a single file for later application to the same Sensor or another Sensor of the same model.

The **Export Configuration** feature helps to avoid duplication of work when it comes to configuring Sensors. For example, if you are deploying multiple Sensors of the same model with similar configuration, you can configure one Sensor and export its configuration to the rest. This feature is also useful if you plan on restoring the configuration back on the same Sensor or its replacement.

You can include the following when you export a Sensor configuration. The choices vary depending on the Sensor model and software version:

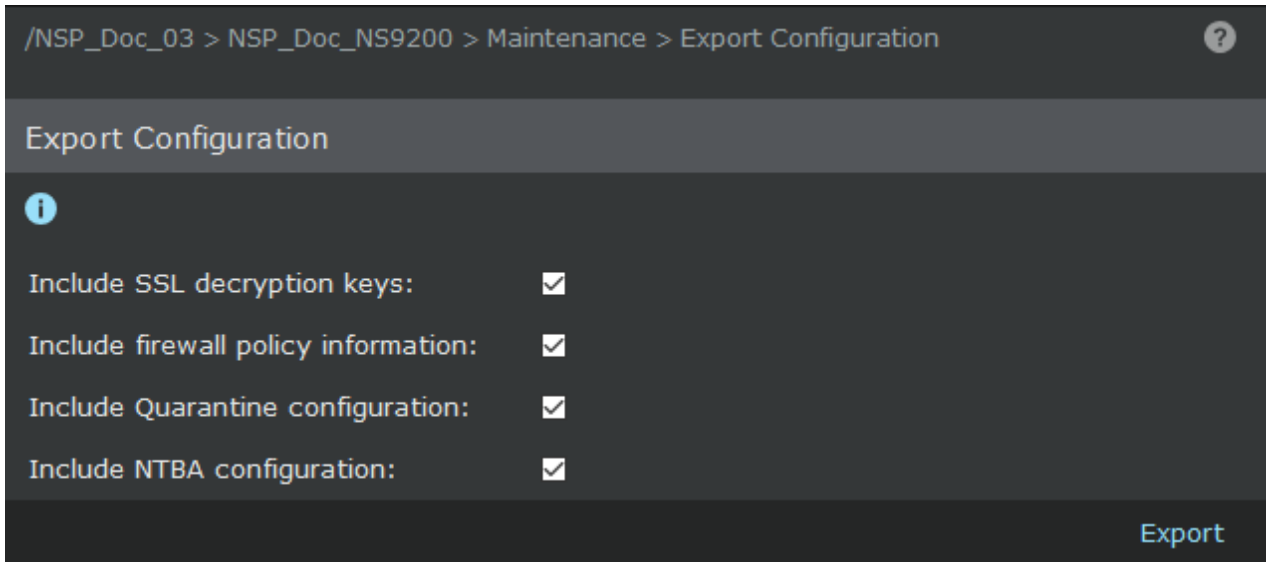
- **Include HA pair configuration** — Includes HA pair information.
- **Include SSL decryption keys** — Includes the SSL decryption keys.
- **Include firewall policy information** — Includes firewall policy information.
- **Include monitoring port information** — Includes monitoring ports configuration information.
- **Include Quarantine configuration** — Includes Quarantine-related configuration for the Sensor and its ports but does not include monitoring port IP addresses.
- **Include NTBA configuration** — This option exports NTBA configuration set.

NOTE

The exported configuration for a Sensor does not include firewall policies and exception objects details, but includes only the firewall policy name. To export firewall policies and exception objects details for a Sensor, go to Policy → <Admin Domain Name> → Intrusion Prevention → Advanced → **Policy Export**.

1. Select Devices → <Admin Domain Name> → Devices → <IPS Sensor> → Maintenance → **Export Configuration**.

   The **Export Configuration** page is displayed.



2. Select the configurations that you want to include in the export.
3. Click **Export** and save the file to a location of your choice.

Enable Sensor CLI activity log events to the Manager

Trellix IPS allows you to view the Sensor CLI user actions, such as user login and command execution, on the Manager.

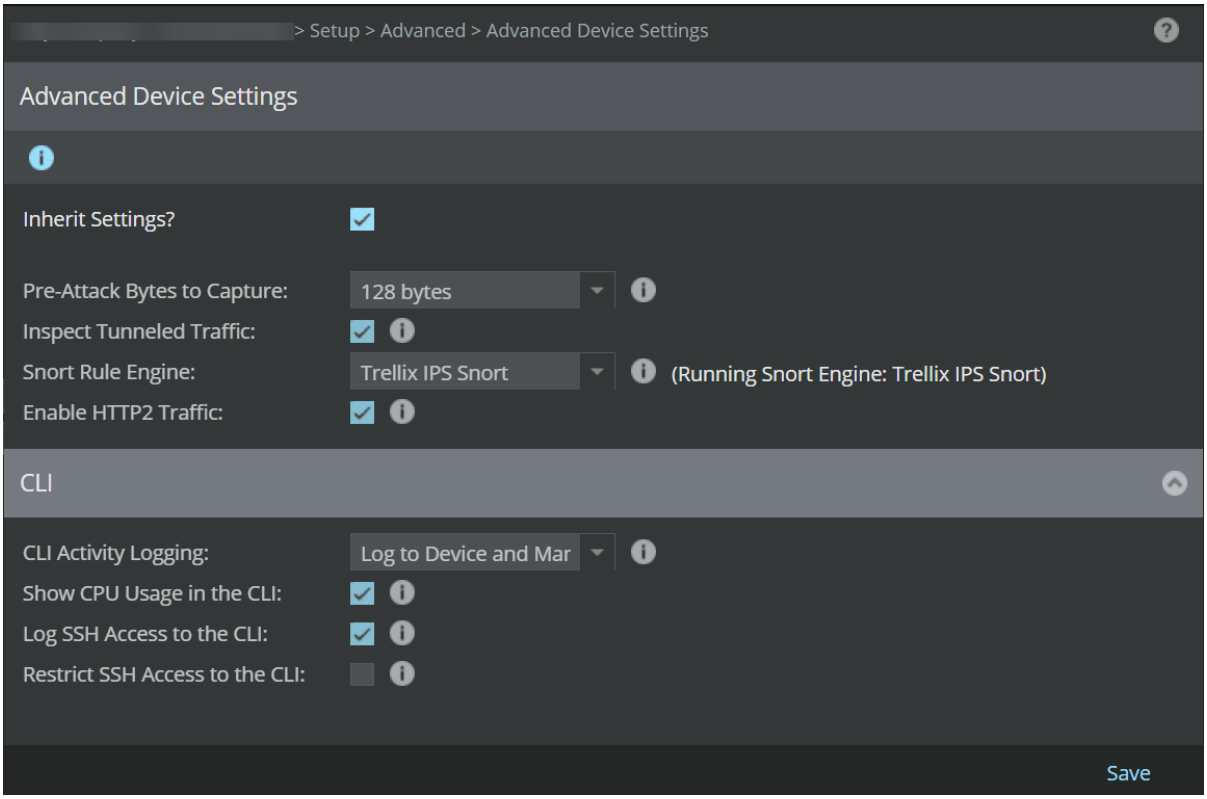
By default, this feature is disabled.

To enable activity log events from the Manager:

1. Select Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings**.

   The **Advanced Device Settings** page appears.

2. In **CLI** options, go to **CLI Activity Logging** and select **Log to Device Only**, **Log to Manager Only**, or **Log to Device and Manager**.
3. Click **Save**.



To view Sensor CLI user activity log, see [Trellix Intrusion Prevention System Product Guide].

To view Sensor CLI user activity report, see the section [Generate User Activity Reports] in [Trellix Intrusion Prevention System Product Guide].

Configure advanced device settings

Use the **Advanced Device Settings** page to configure settings for packet captures, tunneled traffic, and CLI activity.

1. At an Admin domain level, select Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings**.

   The **Advanced Device Settings** page appears.

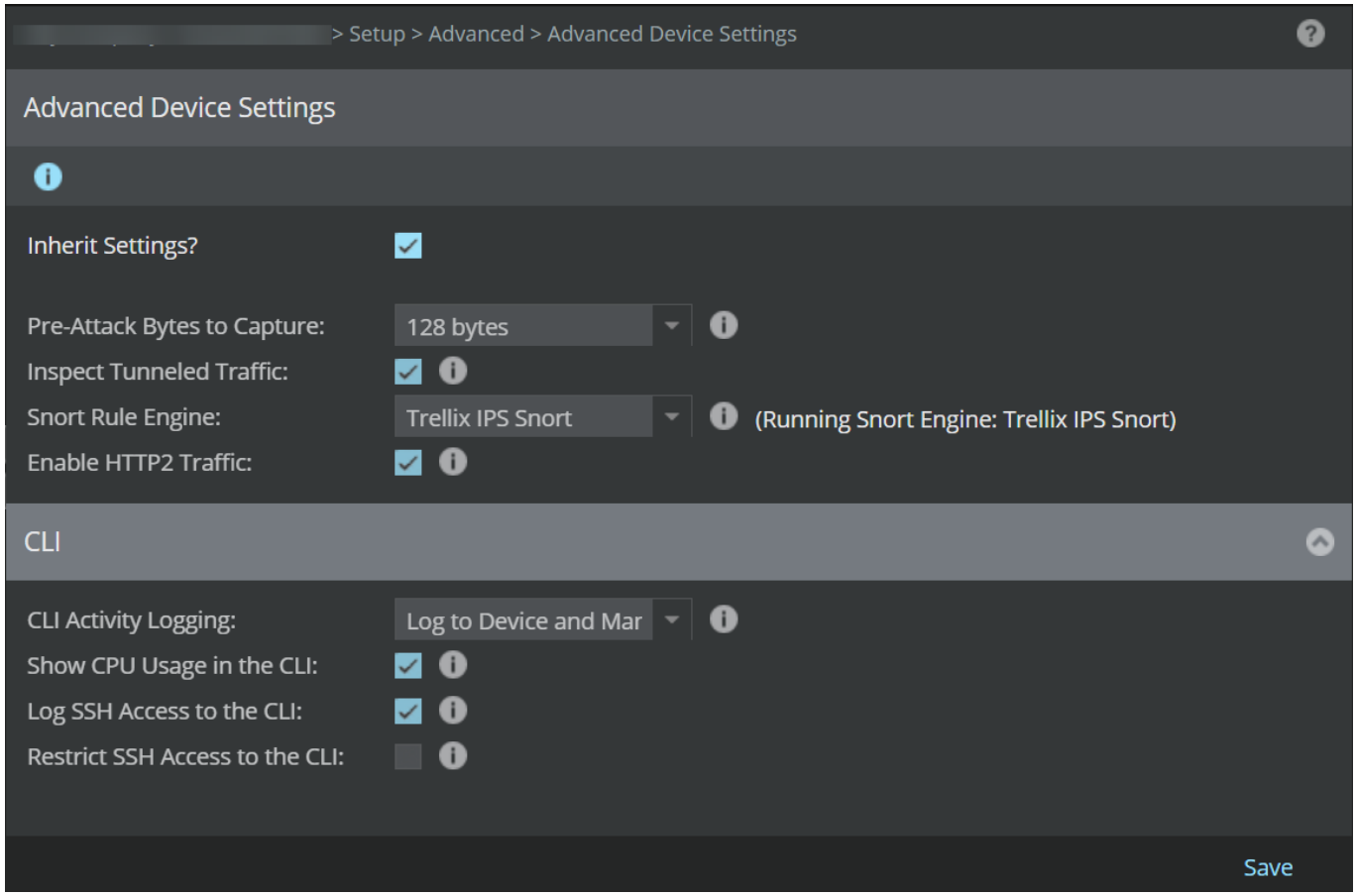
   > **NOTE**
   >
   > Alternatively, you can configure these settings for a Sensor from Devices → <Admin Domain Name> → Devices → <Sensor_name> → Setup → Advanced → **Advanced Device Settings**.

2. The bytes to be captured when pre-attack capturing is enabled is set in the IPS Policy and is displayed on this page. Valid values are 128 and 256 bytes.
3. Select the Inspect Tunneled traffic checkbox to parse IPv4 and IPv6 traffic for all supported tunneling protocols like GRE, GTP for malware detection. By default, this checkbox is deselected.

4. Select a Snort Rule Engine. You can select either the **Trellix IPS Snort** engine or the **Suricata Snort** engine. By default, the **Snort Rule Engine** is set to **Trellix IPS Snort**.

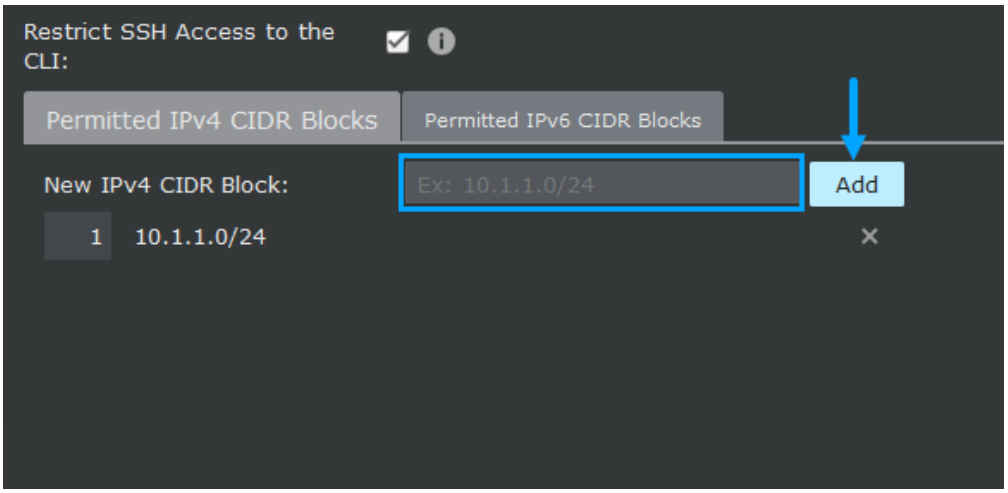
> **NOTE**
>
> The Suricata Snort engine is not available on NS7600 and NS3600 Sensors.

5. From **CLI Activity Logging** options, select **Log to Device Only**, **Log to Manager Only**, or **Log to Device and Manager** to track executed CLI commands. By default, this is set to **Disabled**.



6. Select **Show CPU usage in the CLI** to determine the Sensor load. By default, this checkbox is deselected.
7. Select **Log SSH Access to the CLI** to log all attempts to access CLI on the device. By default, this checkbox is deselected.
8. Use the **Restrict SSH Access to CLI** checkbox to configure IP addresses or CIDR blocks to restrict SSH access. You can set IPv4 and IPv6 blocks and click **Add**. By default, this checkbox is deselected.

> **NOTE**
>
> For Virtual IPS Sensors in the AWS environment, this checkbox must be selected and the IPv4/IPv6 CIDR blocks must be added to restrict SSH access from external invalid IPs.



9. Click **Save**.

HTTP2 traffic inspection

Introduction

IPS supports HTTP2 inspection for the following scenarios:

- HTTP2 Prior Knowledge
- Externally decrypted HTTP2 over TLS

> **NOTE**
>
> HTTP2 upgrade (h2c) scenario is not supported.

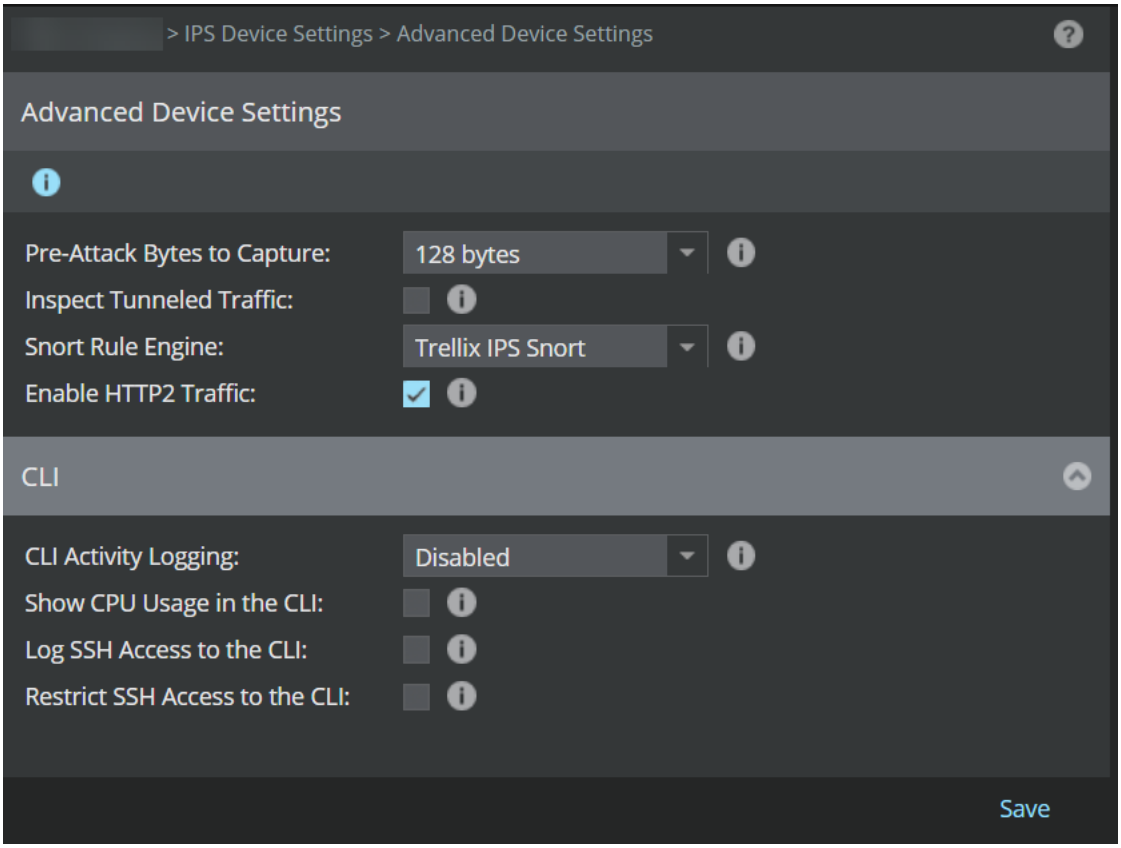
When you install/upgrade the Manager, by default, HTTP2 traffic inspection is not enabled.

Enable HTTP2 traffic inspection from the Manager

You can enable HTTP2 traffic inspection at both Global and Devices level in the Manager.

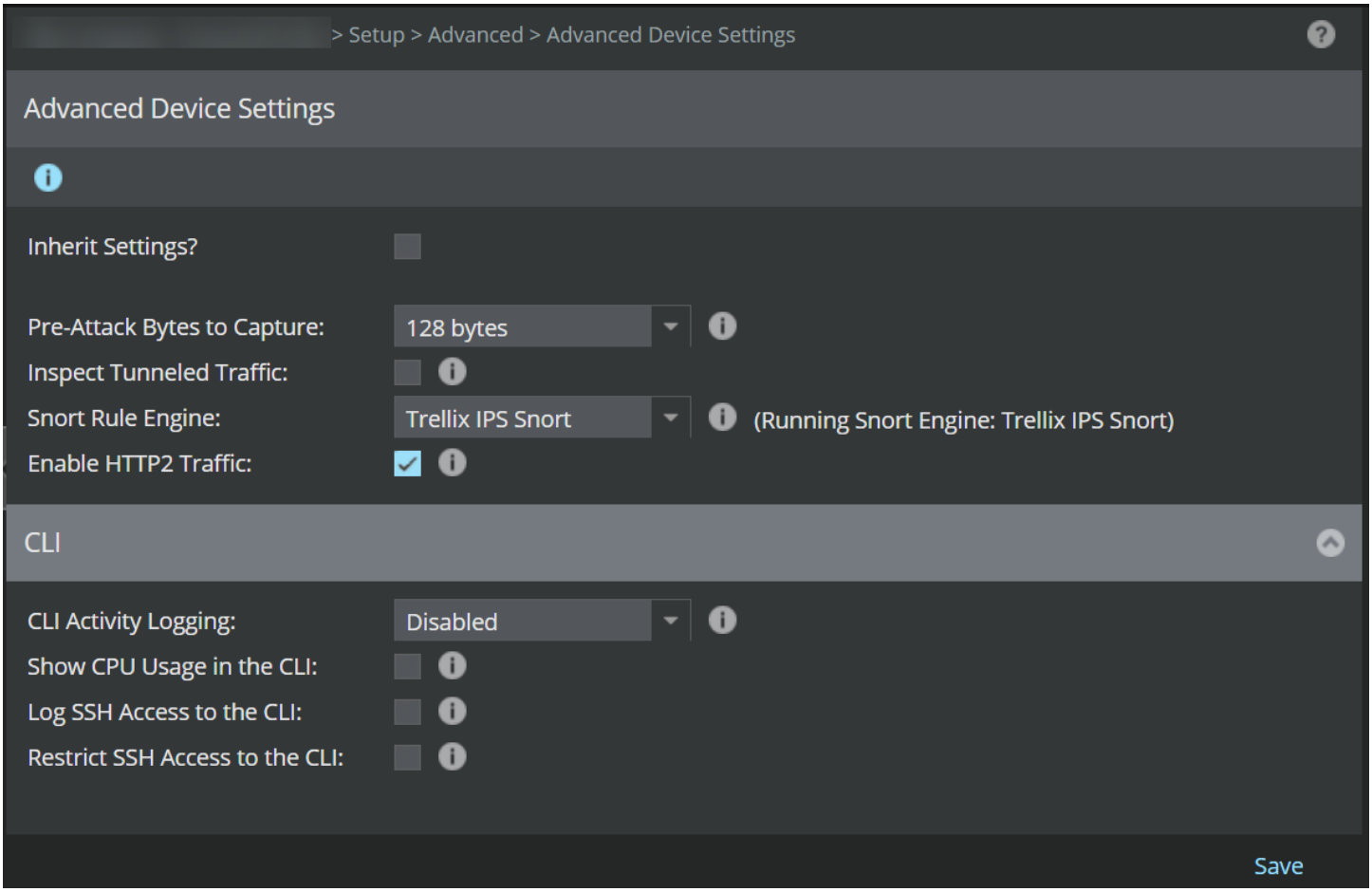
To enable HTTP2 traffic inspection at Global level, go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings** and select **Enable HTTP2 Traffic**.

Figure 717. Advanced Device Settings at Global level



To enable HTTP2 traffic inspection at Devices level, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **Advanced Device Settings** and select **Enable HTTP2 Traffic**.

Figure 718. Advanced Device Settings at Device level



NOTE

By default, **Enable HTTP2 Traffic** is disabled.

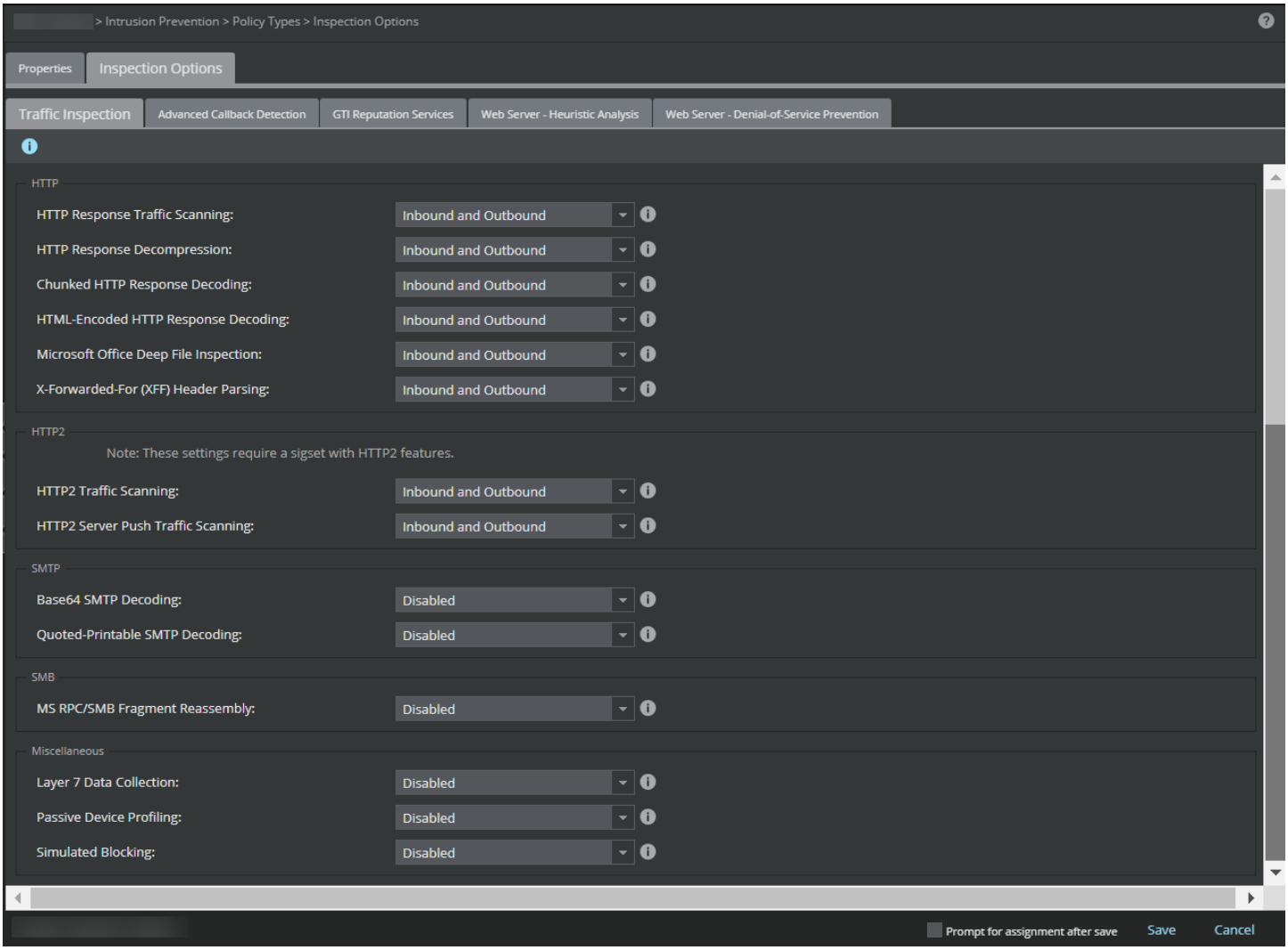
After enabling the HTTP2 traffic inspection from **Devices** tab, follow the below steps:

1. Go to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **Inspection Options**.
2. Navigate to **Inspection Options** tab and click **Traffic Inspection** tab.
3. Configure **HTTP Response Traffic Scanning** based on your requirement.
4. Go to **HTTP2** section, configure **HTTP2 Traffic Scanning** and **HTTP2 Server Push Traffic Scanning** based on your requirement.
5. Click **Save**.

IMPORTANT

- The Sensor requires a reboot when you enable or disable **HTTP2 Traffic Scanning**. You can check the Sensor reboot status from **Device Manager** or **`status`** CLI.
- **HTTP2 Traffic Scanning** can be enabled only when **HTTP Response Traffic Scanning** is enabled.
- **HTTP2 Server Push Traffic Scanning** can be enabled only when **HTTP2 Traffic Scanning** is enabled.
- HTTP2 traffic inspection requires a sigset with HTTP2 features.
- Only NS9500, NS7600, NS7500, and NS3600 Sensors support HTTP2 traffic inspection.
- HTTP2 performance numbers align with HTTP 1.1 for supported Sensor models.

Figure 719. Inspection Options: Traffic Inspection

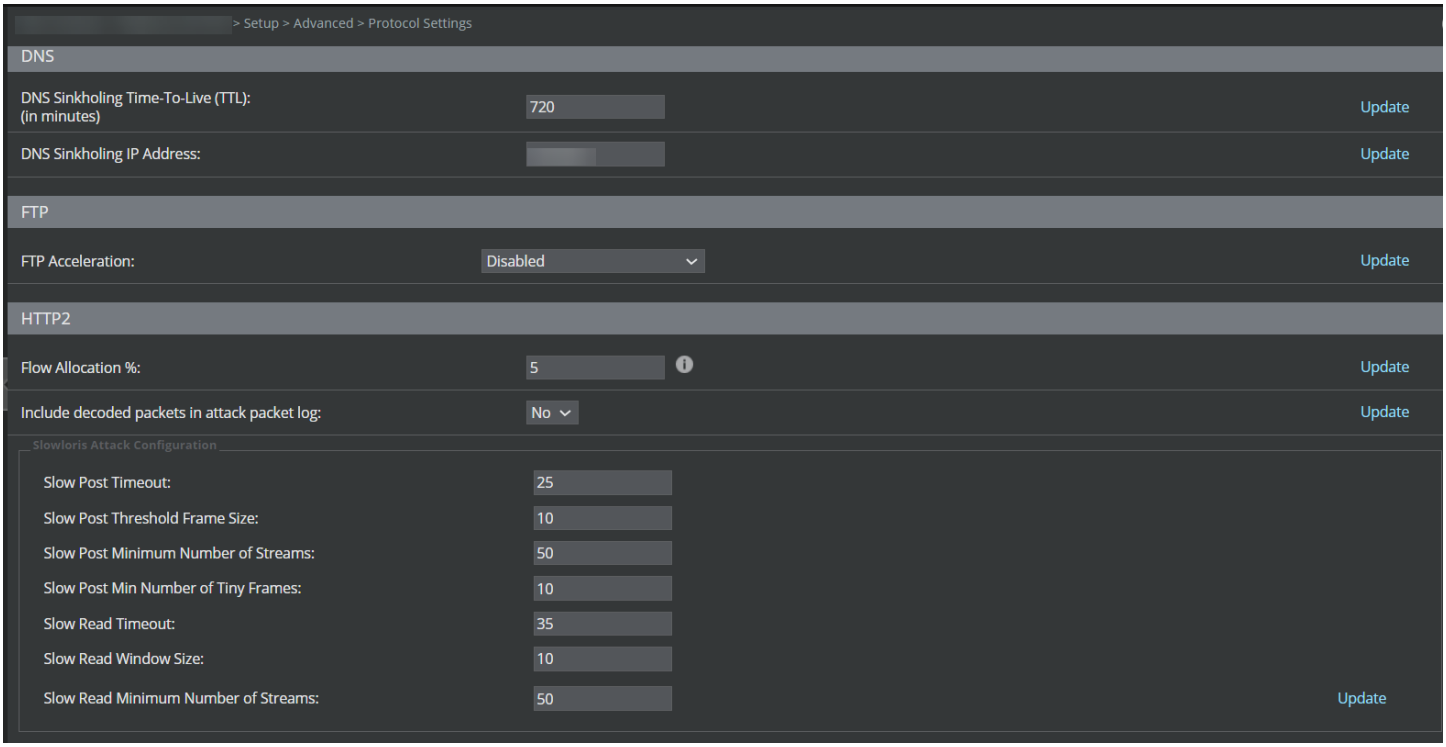


HTTP2 Protocol settings

You can configure the HTTP2 protocol settings for any required Sensor from Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **Protocol Settings**. Go to **HTTP2** section, and configure the following:

Parameters	Description
Flow Allocation %	Set the maximum HTTP2 flows as a percentage of total supported flows. Flow allocation differs for each Sensor model. For NS3600, NS7500, NS7600, and NS9500 Sensors the min and max flow allocation are as follows: • NS3600 and NS7500 - It can range from 1% to 5%. • NS7600 and NS9500 - It can range from 1% to 10%. After configuring, click **Update** to apply the changes. **NOTE** The Sensor requires a reboot after updating the flow allocation.
Include decoded packets in attack packet log	While inspecting HTTP2 traffic, the Sensor decodes the HTTP2 packets/frames into HTTP requests/responses. By enabling this, the Manager will include decoded HTTP requests/responses along with HTTP2 packets/frames in the attack packet log. After configuring, click **Update** to apply the changes.
Slowloris Attack Configuration	Allows you to configure the values for the following parameters: • **Slow Post Timeout** - Set the value between 5 and 30. • **Slow Post Threshold Frame Size** - Set the value between 1 and 100. • **Slow Post Minimum Number of Streams** - Set the value between 50 and 100. • **Slow Post Min Number of Tiny Frames** - Set the value between 1 and 10. • **Slow Read Timeout** - Set the value between 30 and 300. • **Slow Read Window Size** - Set the value between 1 and 100. • **Slow Read Minimum Number of Streams** - Set the value between 50 and 100. **NOTE** Users are recommended to modify these configurations only in consultation with Trellix support team.

Figure 720. HTTP2 Protocol Settings



Alert enhancements for HTTP2

The following new alert fields are included in Layer 7 data:

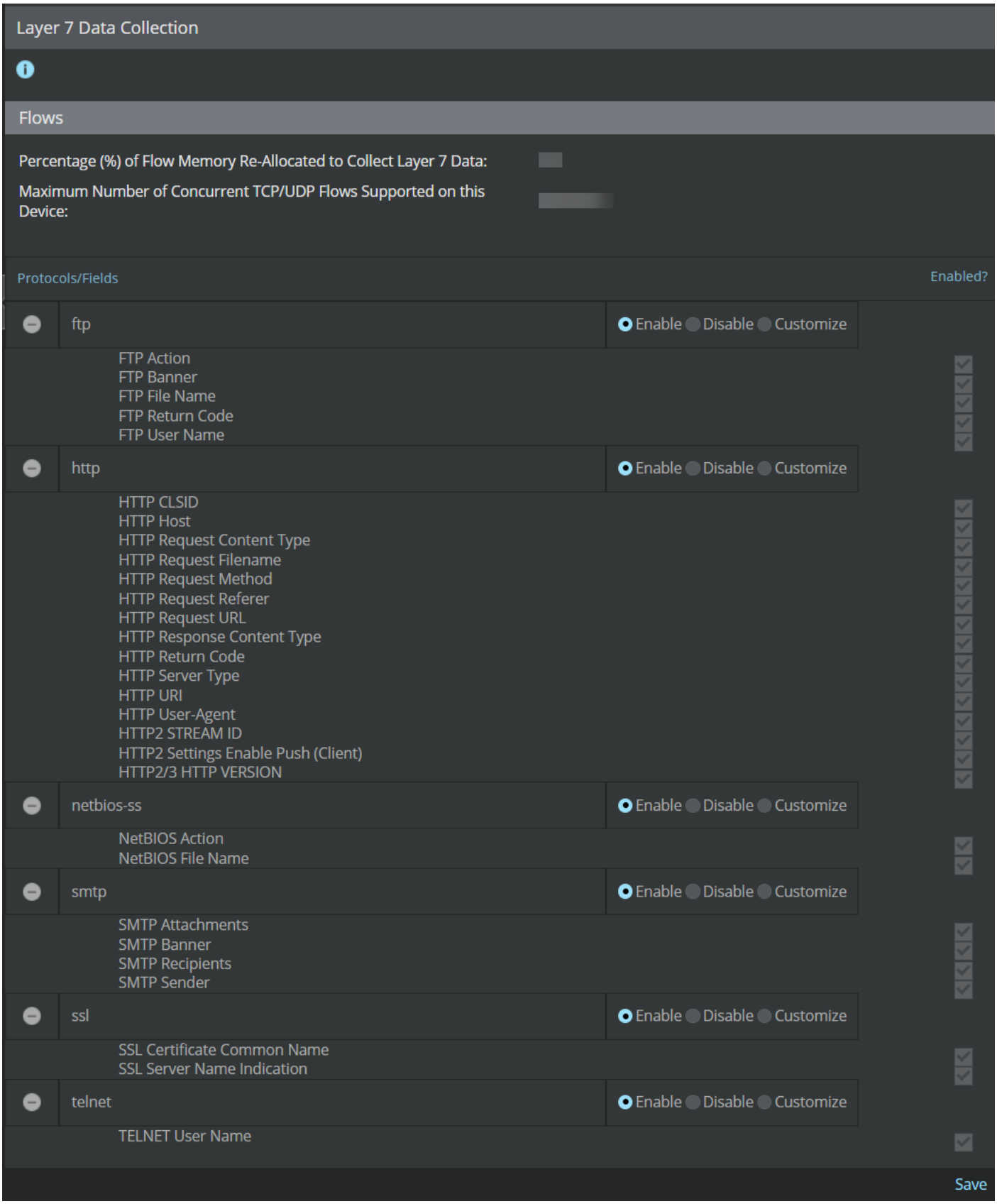
- HTTP2_STREAM_ID
- HTTP2_SETTINGS_ENABLE_PUSH
- HTTP2/3_HTTP_VERSION

You can **Enable**, **Disable**, or **Customize** the alert fields from Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Advanced → **L7 Data Collection**.

NOTE

HTTP2/3 HTTP VERSION is always enabled.

Figure 721. Layer 7 Data Collection



Filter HTTP2 alerts

You can filter HTTP2 alerts through the **Attack Log** or **Reports** page in the Manager.

Attack Log

To focus on attacks detected on HTTP2 traffic, you can apply the filter in the **Attack Log**. To apply the filter, select **Filters** from **Layer 7 Data** column drop-down and in the search field, enter **HTTP2/3 HTTP VERSION: HTTP2**.

Figure 722. Layer 7 Data: Filter value

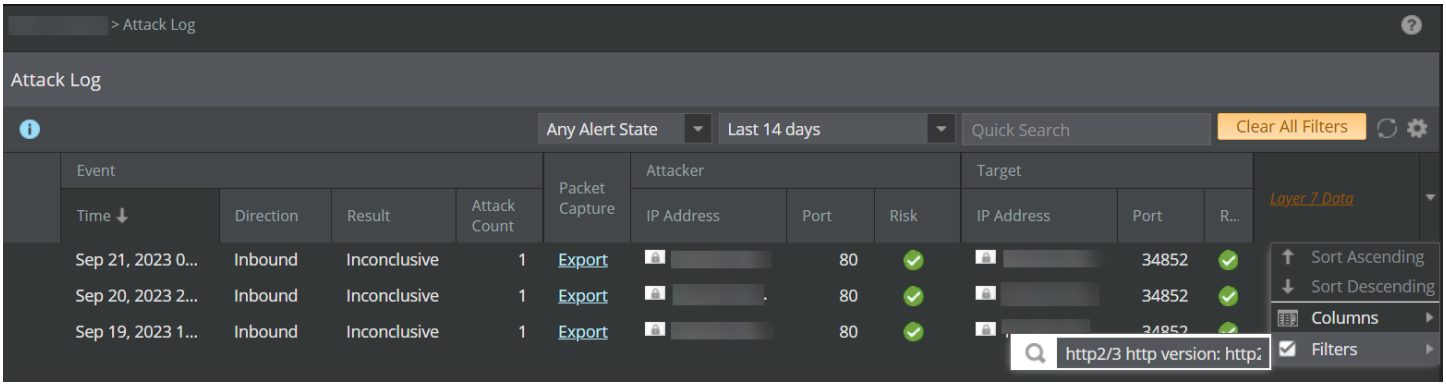
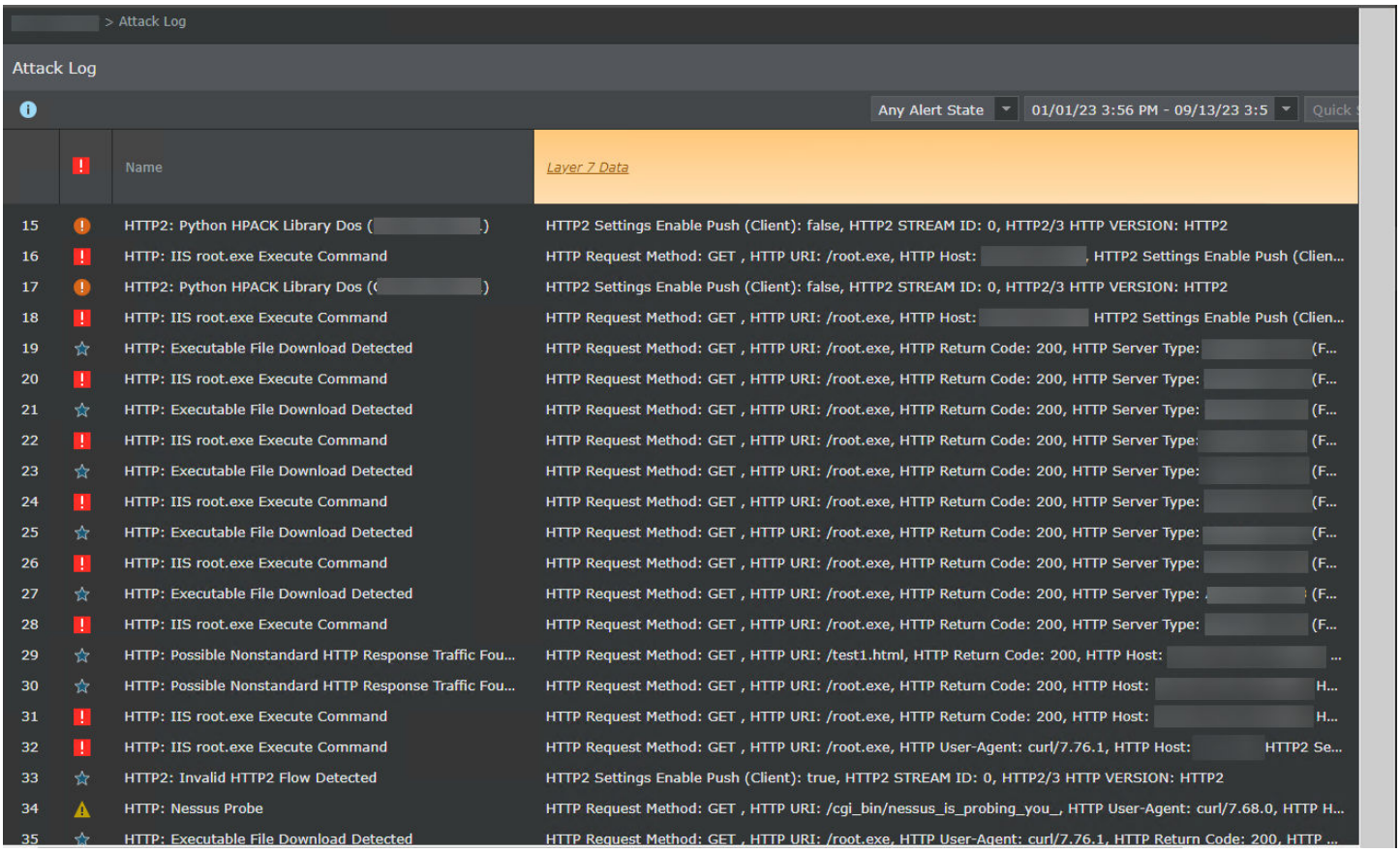
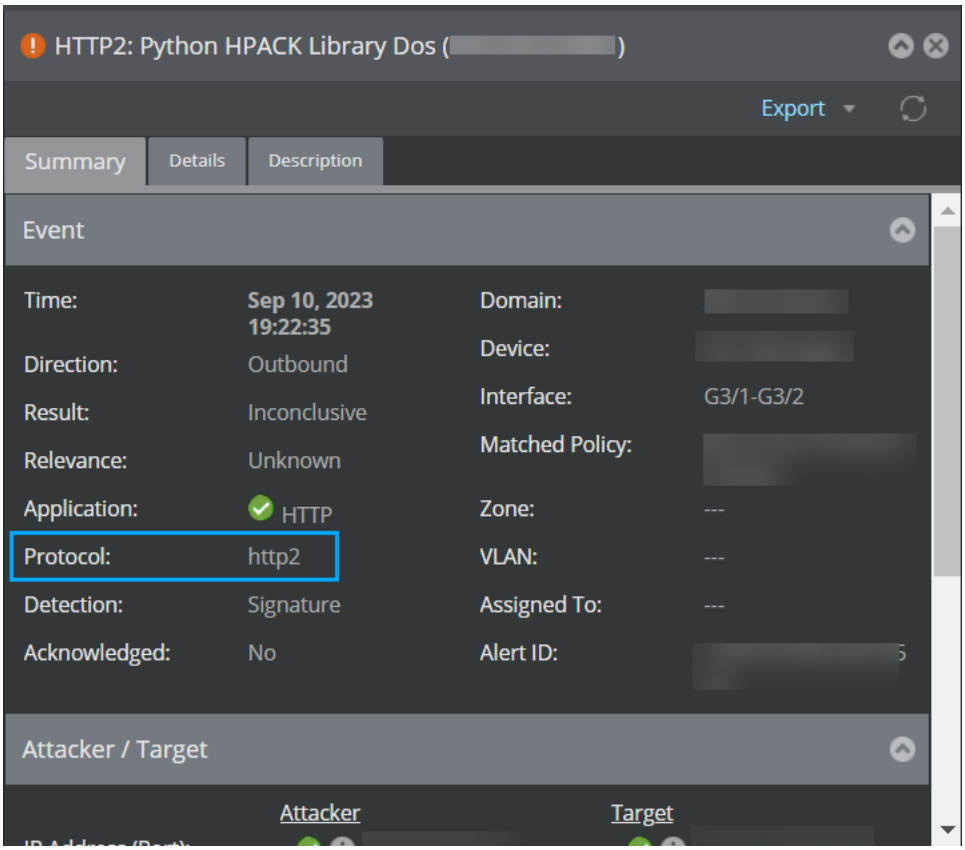


Figure 723. Alerts for attacks detected on HTTP2 traffic



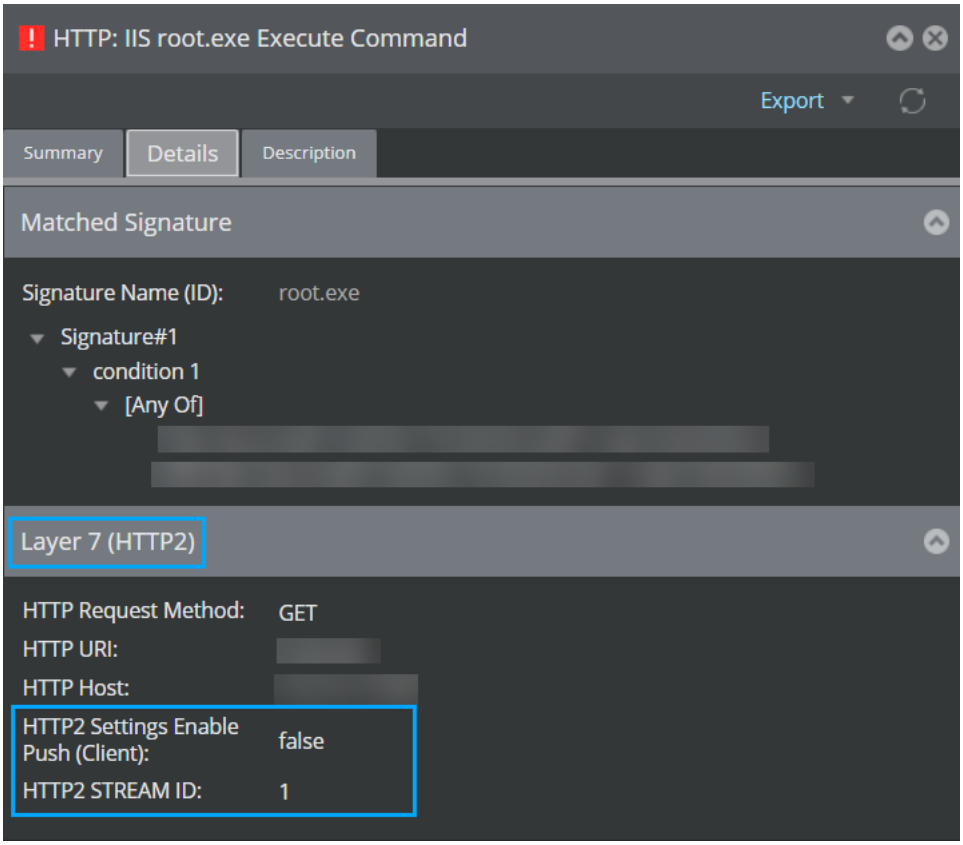
For a particular alert, you can differentiate the HTTP2 alerts by verifying the **Protocol** data in **Summary** tab of **Details** panel in **Attack Log** page.

Figure 724. Summary tab



You can also verify the HTTP2 alerts through the **Layer 7** section in **Details** tab of **Details** panel in **Attack Log** page.

Figure 725. Details tab



Reports

You can follow the below steps to create HTTP2 reports:

1. Go to Analysis → <Admin Domain Name> → Event Reporting → **Next Generation Reports**.
2. In the **Next Generation Reports** page, select **New**.
3. Select the type of data as **Alert Data** and click **Next**.
4. Specify the required display and click **Next**.
5. Specify the required fields and click **Next**.
6. Select **Protocol** and set the property value to be equal to **HTTP2** and click **Next**.
7. Configure the **Date Options** and **Report Format**.
8. Click **Run**.

Supported features with HTTP2

In this release, IPS supports following HTTP2 attack categories:

- Attack content in a single HTTP2 stream
- Attack content across multiple HTTP2 stream

- HTTP2 protocol compliance attacks
- HTTP2 DoS attacks

Unsupported features with HTTP2

In this release, the following features are not supported over HTTP2 connections:

- Malware scanning
- URL Reputation
- Application Identification
- SSL (Known Key, Agent, Proxy)
- Mandate Authentication/HTTP Redirection
- Layer 7 Distributed DoS
- Trellix Snort Rules
- Botnet detection over HTTP
- Connection limiting
- X-Forwarded-For Header Parsing (XFF)
- Decompression (Gzip, Deflate) and Decoding (Chunk, HTML)
- Shell Code Detection
- Firewall
- File Reputation
- Web Security
- IPS Quarantine

Monitoring Sensor Performance

How to configure and monitor device performance

Device **Performance Monitoring** features offer a practical way to monitor load on the devices configured in the Manager. Pro-active capacity planning is made possible by the metrics that can be configured and monitored in the Manager interface. The metrics and thresholds provide an easy way to isolate the device as the root cause of a network failure or to rule it out as the cause. It is possible to view the values of key metrics in 'real-time' (every few seconds) as a way to see how the device is behaving at any given moment in time. Decisions on capacity planning to determine when to replace the device in favor of a larger one are facilitated by device **Performance Monitoring**. Troubleshooting is a special use case for when more information is needed in order to identify where things are going wrong.

NOTE

In case of MDR, the device will try to send alerts and system events to both the Managers. If one of the Managers is not reachable, only the reachable one will get the event. Consequently, **Performance Monitoring** threshold faults are generated only in respect of the reachable Manager. So there are chances that some of the alarms might get missed or not get cleared in the Managers.

View device performance settings summary

Device performance metrics and thresholds can be configured through the **Performance Monitoring** page of the **Global** tab in the root admin and child admin domains and that of the specific **Device** tab.

Click on either of the following to view the Summary tab:

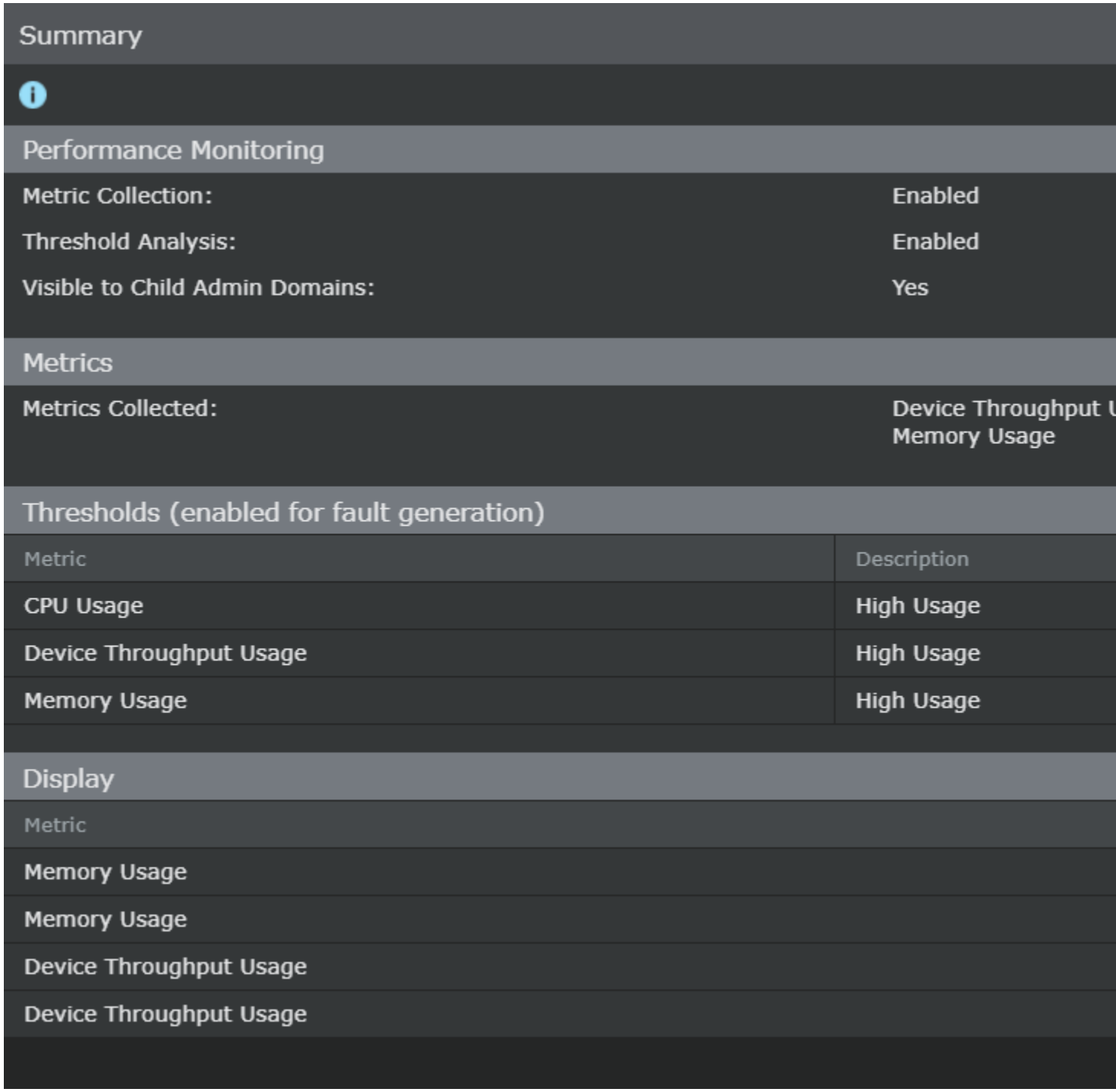
1. For the root admin domain, select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Summary**.
2. For the child domain, select Devices → <Child Domain Name> → Global → Common Device Settings → Performance Monitoring → **Summary**.
3. For the specific device, select Devices → <Admin Domain Name> or <Child Admin Domain> → Devices → <Device Name> → Setup → Performance Monitoring → **Summary**.
4. For the HA pair in the root admin domain, select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Summary**.

   The **Summary** page has four subtabs: **Performance Monitoring**, **Metrics**, **Thresholds**, and **Display**. The **Summary** page summarizes device performance monitoring settings in the **Enable**, **Metrics**, and **Thresholds** tabs. The values displayed under the **Summary** tab are read-only information.

   NOTE

   The **Display** tab is available only at the global level.

Figure 726. Summary window



Enable device performance monitoring

The overall state of device **Performance Monitoring** can be controlled in the **Enable** sub-tab of the performance monitoring tab. The device **Performance Monitoring** can be enabled with the relevant choice settings in the following locations in the Manager:

1. For the root admin domain, select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. For the child admin domain, select Devices → <Child Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**
3. For the specific device, select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Enable** or Devices → <Child Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Enable**.

   The procedure to enable device performance monitoring is detailed in the following sections:

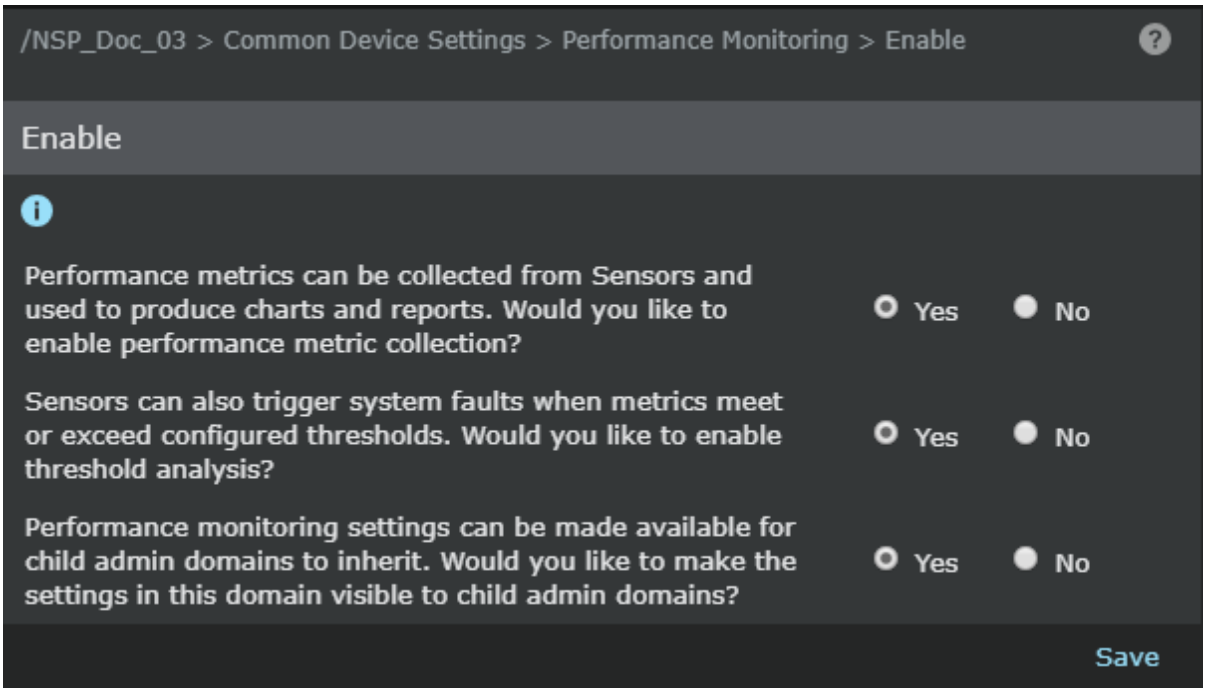
   - Enable device performance monitoring for the admin domain
   - Enable device performance monitoring for specific devices

Enable device performance monitoring for the admin domain

The **Enable** page when accessed from the **Global** tab of the admin domain is used to control the overall state of device **Performance Monitoring** at the admin domain level.

Performance **Metrics** are collected from devices and used to produce performance-related graphs and reports. The Enable page provides the option to enable or disable performance metric collection.

Figure 727. Enable dialog



Follow this procedure to enable or disable metric collection at the admin domain level:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. Against **Performance metrics can be collected from sensors and used to produce charts and reports. Would you like to enable performance metric collection?** choice, select **Yes** to enable metrics collection or select **No** to disable metrics collection.
3. Click **Save**.

Enable or disable system faults at the admin domain level

Devices can also trigger system faults when performance metrics meet or exceed specific thresholds. The **Enable** page provides the option to enable or disable threshold analysis.

Follow this procedure to enable or disable system faults at the root admin domain level:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. Against **Sensors can also trigger system faults when metrics meet or exceed configured thresholds. Would you like to enable threshold analysis?** choice, select the **Yes** to enable to trigger system faults or select **No** to disable triggering of system faults.
3. Click **Save**.

Enable or disable visibility of settings to child admin domains

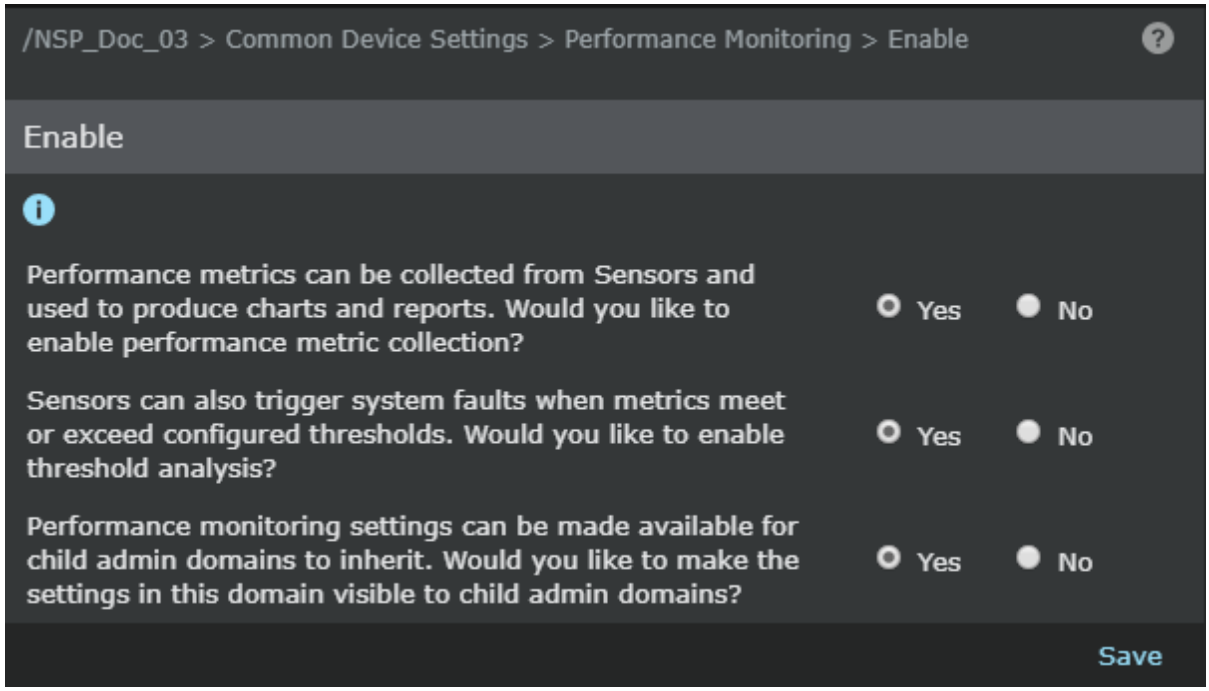
Performance monitoring settings can be made available for child admin domains to inherit. The **Enable** page provides the option to enable or disable visibility of settings to child admin domains.

Follow this procedure to enable or disable visibility of settings to child admin domains:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. Against **Performance monitoring settings can be made available for child admin domains to inherit. Would you like to make the settings in this domain visible to child admin domains?** choice, select the **Yes** to enable to visibility of settings to child admin domains or select **No** to visibility of settings to child admin domains.
3. Click **Save** to save your selection.

   The **Enable** page when accessed from **Global** tab of the child admin domain is used to control the overall state of Sensor **Performance Monitoring** at the child admin domain level.

Figure 728. Performance monitoring



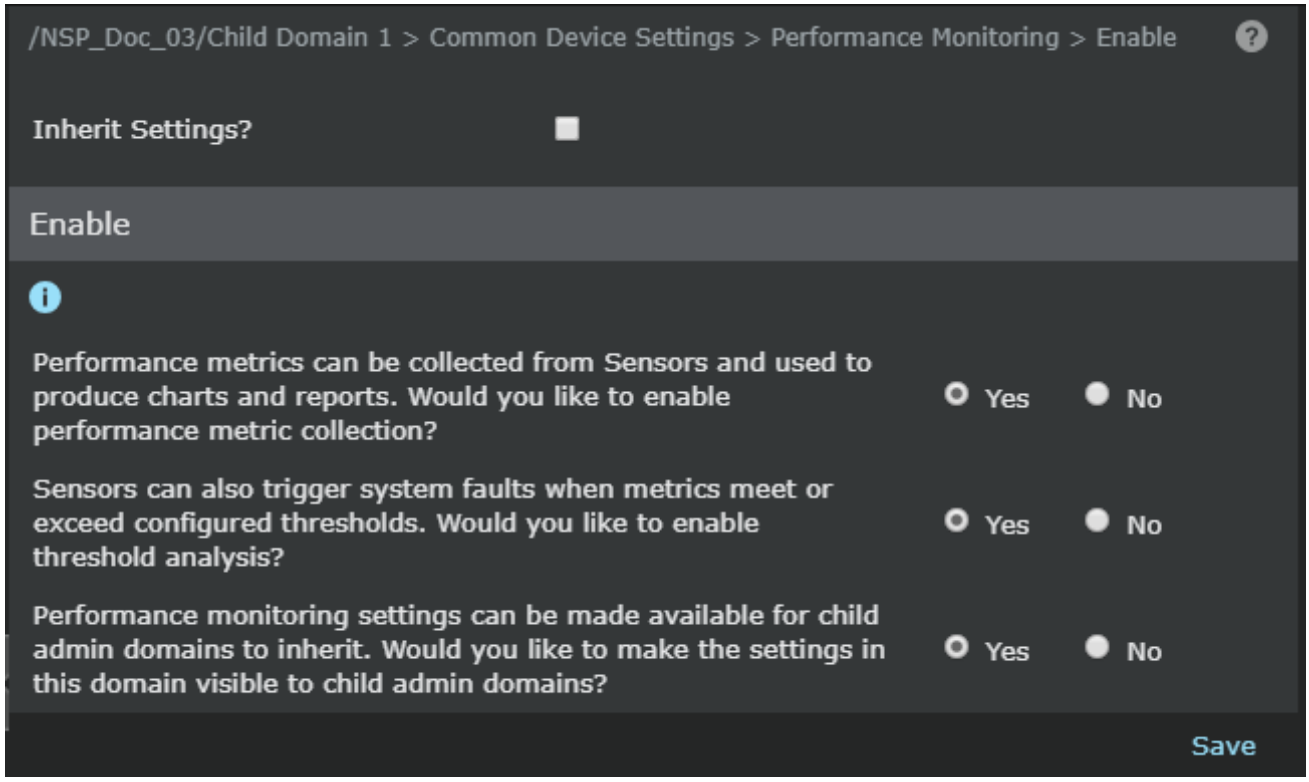
Enable or disable inheritance of settings from the parent admin domain

The **Enable** page at the child admin domain level provides the option to enable or disable performance metric collection with choices relevant to the child admin domain. The choice to inherit or not inherit the settings from the parent admin domain is available at the child admin domain.

Follow this procedure to enable or disable inheritance of settings from the parent admin domain:

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. Select the checkbox against **Inherit Settings?** to inherit settings from the parent admin domain. Deselect this checkbox to disable inheritance of settings from the parent admin domain.
3. Click **Save**.

Figure 729. Inherit settings from the parent domain



Enable or disable metric collection for devices within the child admin domain

Performance metrics are collected from devices and used to produce performance-related graphs and reports.

Follow this procedure to enable or disable metric collection at the child admin domain level:

1. Select Devices → <Child Admin Domain Name> → Devices → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. Against **Performance metrics can be collected from sensors and used to produce charts and reports. Would you like to enable performance metric collection?** choice, select the **Yes** to enable metrics collection or select **No** to disable metrics collection.
3. Click **Save**.

Enable or disable system faults for devices within the child admin domain

Devices can also trigger system faults when performance metrics meet or exceed specific thresholds. The **Enable** page provides the option to enable or disable threshold analysis.

Follow this procedure to enable or disable system faults at the child admin domain level:

1. Select Devices → <Child Admin Domain Name> → Devices → Global → Common Device Settings → Performance Monitoring → **Enable**.

2. Against **Sensors can also trigger system faults when metrics meet or exceed configured thresholds. Would you like to enable threshold analysis?** choice, select the **Yes** to enable to trigger system faults or select **No** to disable triggering of system faults.
3. Click **Save**.

Enable or disable visibility of settings to child admin domain levels

Performance monitoring settings can be made available for child admin domains to inherit. The **Enable** page provides the option to enable or disable visibility of settings to child admin domains.

Follow this procedure to enable or disable visibility of settings to child admin domains (In this case sub-domains of child admin domains):

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Enable**.
2. Against **Performance monitoring settings can be made available for child admin domains to inherit. Would you like to make these setting visible to child admin domains?** choice, select the **Yes** to enable to visibility of settings to Child Admin Domains or select **No** to visibility of settings to Child Admin Domains.
3. Click **Save**.

   If the visibility of settings to child admin domains is enabled, the settings at the parent admin domain are inherited by the child admin domains. However the child domains have the choice of inheriting or not inheriting the settings from the parent admin domain. The reference to child admin domain here refers to the child admin domain of the root admin domain as also the sub-domains of a child admin domain. If the settings are not inherited by the child admin domain, a set of default settings become operational at the child admin domain level. These default settings can be changed at the child admin domain level. If the visibility of settings to child admin domains is disabled the checkbox for inheriting the settings from the admin domain is grayed out at the child admin domain level.

Enable device performance monitoring for specific devices

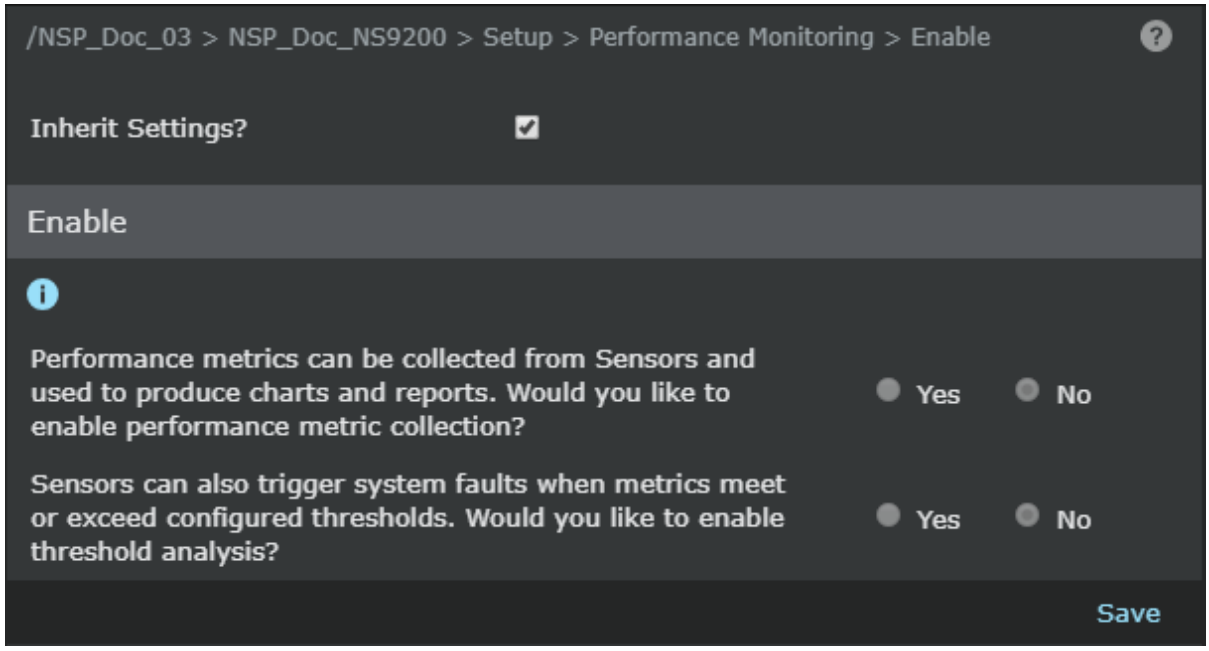
The **Enable** page, when accessed from the **Devices** tab, is used to control the overall state of device **Performance Monitoring** at a specific device level.

The **Enable** page, when accessed from the **Devices** tab, provides the option to enable or disable performance metric collection with choices relevant to the chosen device. The choice to inherit or not inherit the settings from the parent admin domain is available when accessed from the **Devices** tab.

Follow this procedure to enable or disable inheritance of settings from the root admin domain:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Enable**.

Figure 730. Enable area



2. Select the checkbox against **Inherit Settings?** to inherit settings from the parent admin domain. Deselect this checkbox to disable inheritance of settings from the parent admin domain.
3. Click **Save**.

Enable or disable metrics collection for specific devices

Performance metrics are collected from devices and used to produce performance-related graphs and reports.

Follow this procedure to enable or disable metrics collection for a specific device:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Enable**.
2. Against **Performance metrics can be collected from sensors and used to produce charts and reports. Would you like to enable performance metric collection?** choice, select the **Yes** to enable metrics collection or select **No** to disable metrics collection.
3. Click **Save**.

Enable or disable system faults for specific devices

Devices can also trigger system faults when performance metrics meet or exceed specific thresholds. The **Enable** page provides the option to enable or disable threshold analysis.

Follow this procedure to enable or disable system faults for a specific device:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Enable**.
2. Against **Sensors can also trigger system faults when metrics meet or exceed configured thresholds. Would you like to enable threshold analysis?** choice, select the **Yes** to enable to trigger system faults or select **No** to disable triggering of system faults.

3. Click **Save**.

Configure of metrics collection

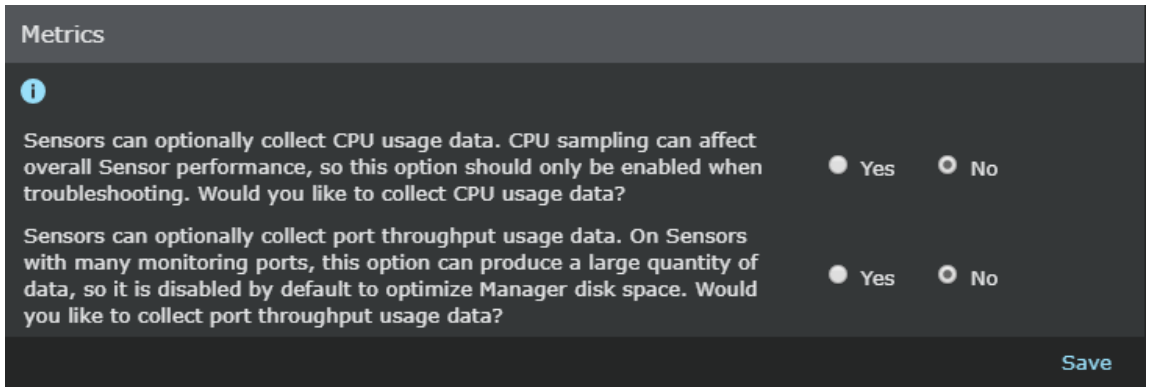
Metric collection can be configured from the root admin domain **Global** device settings tab, child admin domain **Global** device settings tab, or the **Devices** tab. You can enable metric collection so that devices automatically forward core metrics to the Manager. The core metrics show Sensor throughput usage, Sensor memory usage, and Sensor CPU usage.

Configure metrics collection for the admin domain

You can enable metrics collection for all devices that belong to the root admin domain:

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Metrics** to view the **Metrics** page.

Figure 731. Metrics dialog



2. Select **Yes** or **No** against **Sensors can optionally collect CPU usage data. CPU sampling can affect overall sensor performance, so this option should only be enabled when troubleshooting. Would you like to collect CPU usage data?** (This is disabled by default).
3. Select **Yes** or **No** against the choice **Sensors can optionally collect port throughput usage data. On sensors with many monitoring ports, this option can produce a large quantity of data, so it is disabled by default to optimize Manager disk space. Would you like to collect port throughput usage data?**.
4. Click **Save**.

> **NOTE**
>
> When metrics collection is enabled, Sensors automatically forward core metrics to the Manager.

Enable metric collection at the child domain Device list node

You can enable metric collection at the child domain Device list node:

1. Select Devices → <Child Admin Domain Name → Devices → <Device Name> → Setup → Performance Monitoring → **Metrics** to view the **Metrics** page.
2. Select the **Inherit Settings?** checkbox to inherit the settings from Parent Admin Domain. Deselect this checkbox if you do not want to inherit settings from Parent Admin Domain.
3. Select **Yes** or **No** against the choice **Sensors can optionally collect CPU usage data. CPU sampling can affect overall sensor performance, so this option should only be enabled when troubleshooting. Would you like to collect CPU usage data?**. This choice is available only if the **Inherit Settings** checkbox is deselected.
4. Select **Yes** or **No** against the choice **Sensors can optionally collect port throughput usage data. On sensors with many monitoring ports, this option can produce a large quantity of data, so it is disabled by default to optimize Manager disk space. Would you like to collect port throughput usage data?**. This choice is available only if the **Inherit Settings?** checkbox is deselected.
5. Click **Save**.

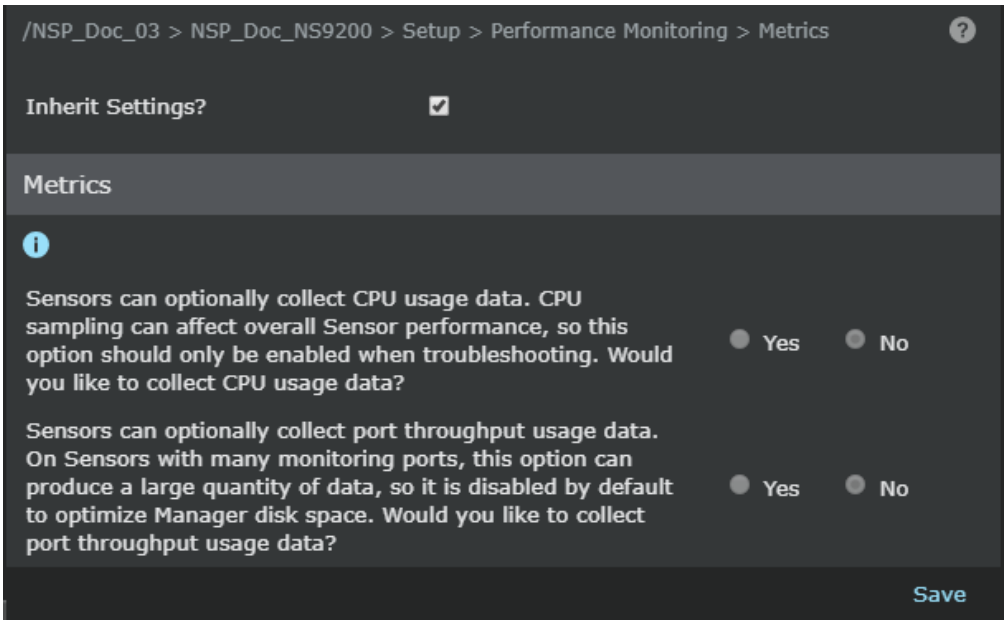
> **NOTE**
>
> When metric collection is enabled, devices automatically forward core metrics to the Manager. The reference to child admin domain here refers to the child admin domain of the root admin domain as well as the sub-domains of a child admin domain.

Configure metrics collection for specific devices

Follow this procedure to enable metrics collection for a specific device:

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Metrics** or Devices → <Child Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Metrics** to view the **Metrics** page.

Figure 732. Enable Metrics



2. Select the **Inherit Settings?** checkbox to inherit the settings from parent admin domain. Deselect this checkbox if you do not want to inherit settings from parent admin domain.
3. Select **Yes** or **No** against the choice **Sensors can optionally collect CPU usage data. CPU sampling can affect overall sensor performance, so this option should only be enabled when troubleshooting. Would you like to collect CPU usage data?**.
4. Select **Yes** or **No** against the choice **Sensors can optionally collect port throughput usage data. On sensors with many monitoring ports, this option can produce a large quantity of data, so it is disabled by default to optimize Manager disk space. Would you like to collect port throughput usage data?**.
5. Click **Save**.

> **NOTE**
>
> When metrics collection is enabled, devices automatically forward core metrics to the Manager.

Set thresholds

Thresholds can be set with a view to alert the user by raising a system fault when the set threshold value is crossed. An example would be a system fault raised when the Sensor CPU usage crosses an upper threshold value of say 90%.

Thresholds can be set for CPU usage, Sensor throughput, port throughput, L2 error drop (Layer 2 here refers to too many CRC and Ethernet Packet Compliance errors) and L3/L4 error drop (Layer 3/4 here refers to too many checksum and protocol errors) and memory usage. Thresholds can be set at the root admin domain device list node, child admin domain device list node and the Device_Name node. The threshold page is used to change threshold values for select metrics and optionally generate system faults when those thresholds are exceeded. Thresholds set represent the average values for every minute.

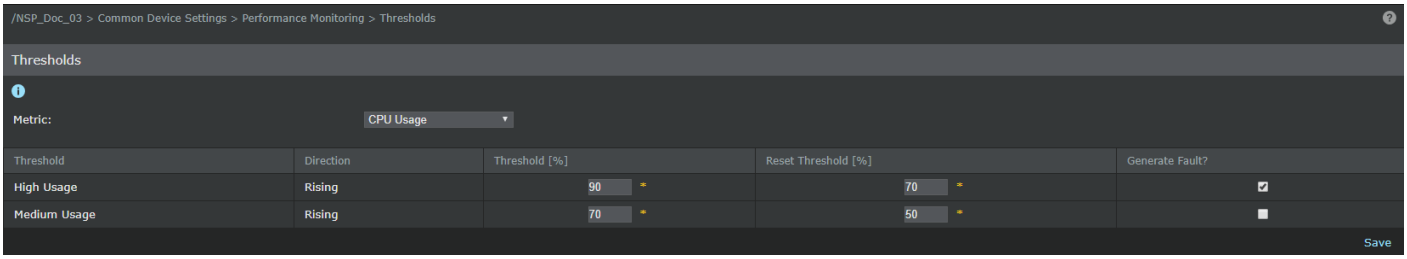
> **NOTE**
>
> Threshold generated faults for a given device are flushed out on reboot. Settings can be inherited upto two admin domain levels

Set the CPU usage threshold for the admin domain

Follow this procedure for setting the CPU usage threshold for all devices that belong to the root admin domain.

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 733. Thresholds sub-tab



2. Select **CPU Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select **Generate Fault?** to generate fault.
5. Click **Save** to save your settings.

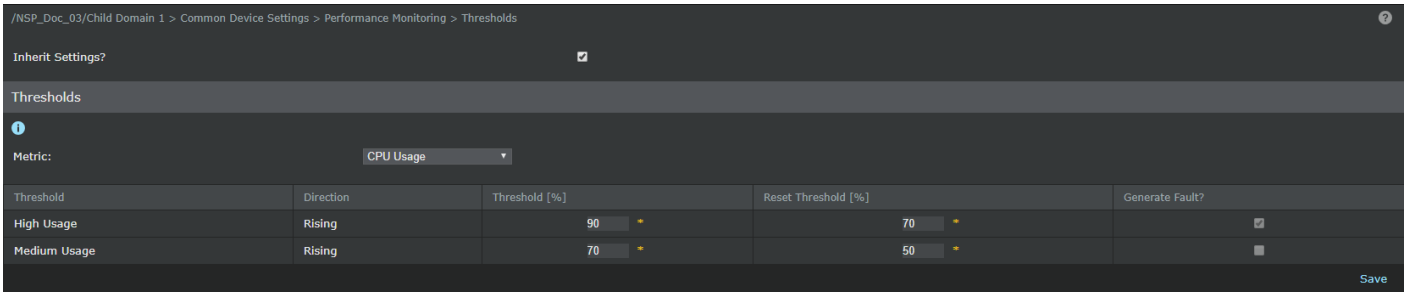
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values

Set the CPU usage threshold for devices within a child domain

Follow this procedure for setting the CPU usage threshold for all devices within the child admin domain.

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 734. Thresholds area



2. Select **CPU Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select the **Generate Fault?** checkbox to enable generation of fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

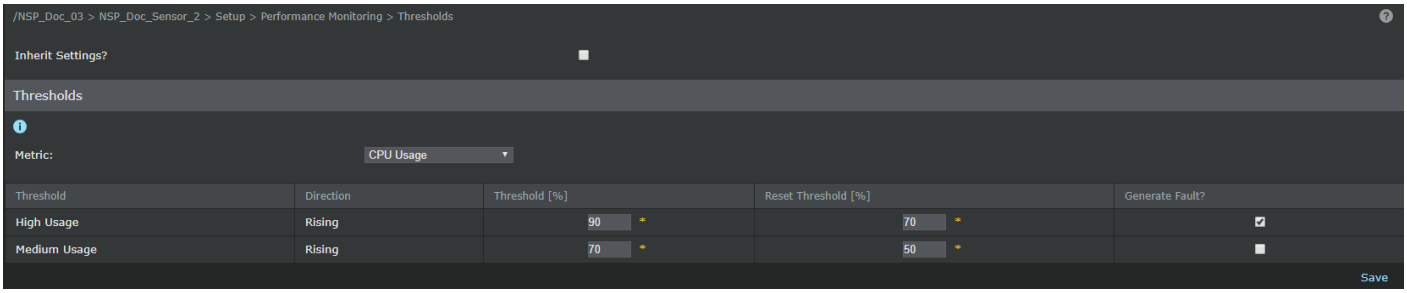
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected. If this checkbox is checked the settings from the parent admin domain are automatically inherited.

Set the CPU usage threshold for specific devices

Follow this procedure for setting the CPU usage threshold for a specific device.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Thresholds**.

Figure 735. Thresholds dialog



2. Select **CPU Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select **Generate Fault?** to generate fault.
5. Click **Save** to save your settings.

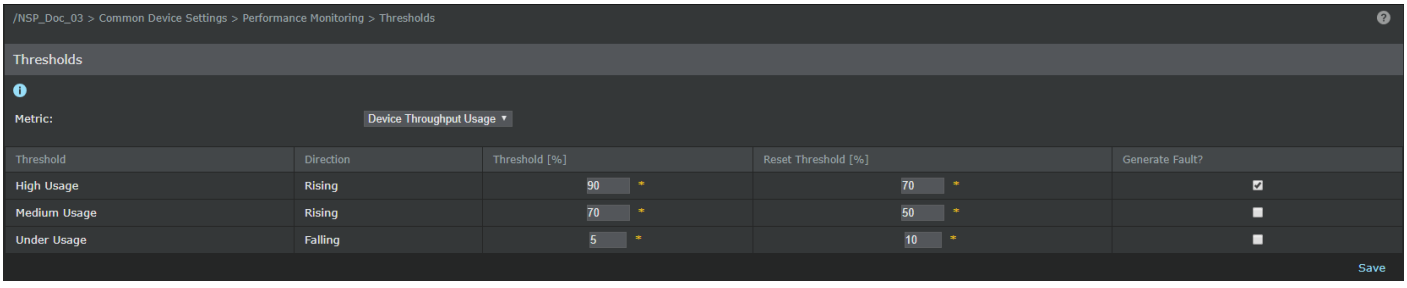
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. This option is available only when **Inherit Settings?** is deselected.

Set the Sensor throughput threshold for devices within the admin domain

Follow this procedure for setting Sensor throughput threshold for all devices within the admin domain.

1. Click Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 736. Thresholds area



2. Select **Device Throughput Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select **Generate Fault?** to generate fault.
5. Click **Save** to save your settings.

NOTE

Click **Defaults** to set the threshold settings to the default values. "Under Usage" in the context of the throughput usage threshold is a 'falling threshold'. Alarm is generated when the throughput % drops below a certain value. This is helpful on very busy networks, where a certain amount of traffic is always expected to be seen. This type of alarm is a good indication that there is a communication problem on the network.

NOTE

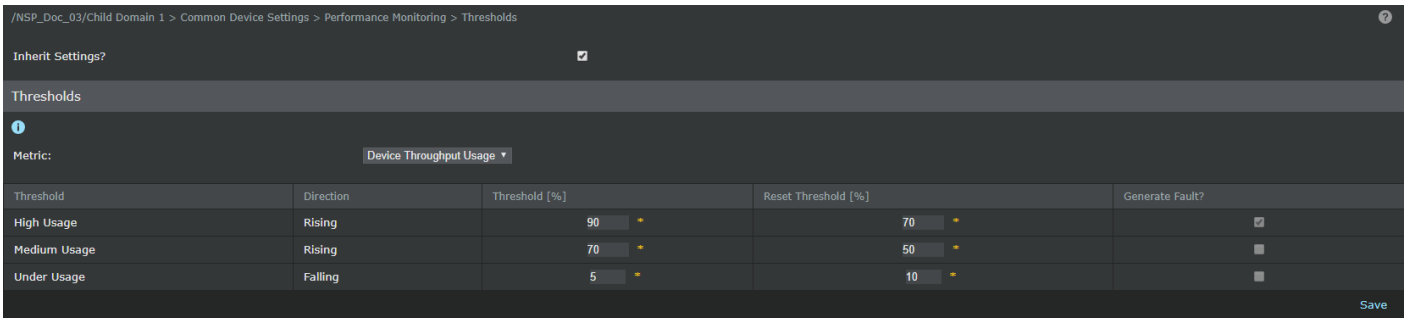
By default **High Usage** setting of Sensor throughput usage threshold alarm is enabled and the rest are disabled at root domain.

Set the Sensor throughput threshold for devices within the child admin domain

Follow this procedure for setting the Sensor throughput threshold for devices within the child admin domain.

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 737. Thresholds area



2. Select **Device Throughput Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select **Generate Fault?** to generate fault.
5. Click **Save** to save your settings.

NOTE

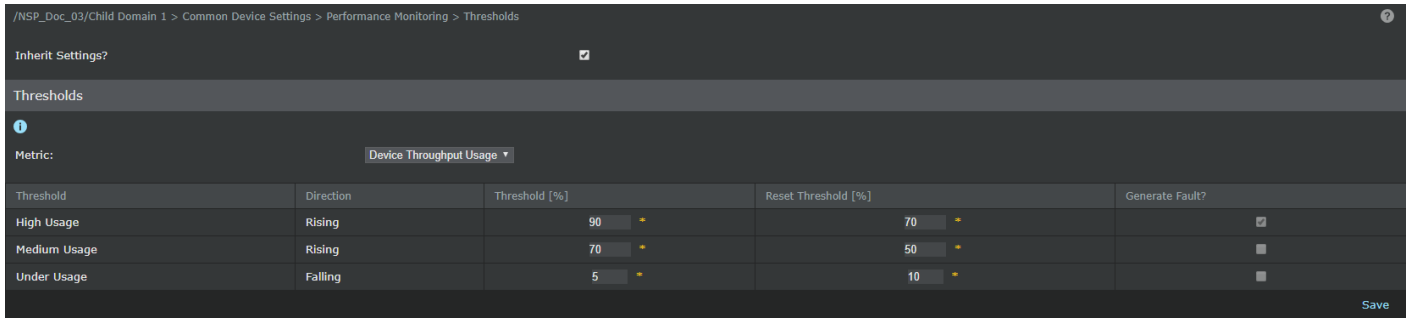
Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected. If this checkbox is selected, the settings from the parent admin domain are automatically inherited.

Setting the Sensor throughput threshold for specific devices

Follow this procedure for setting the Sensor throughput threshold for a specific device within a domain.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Thresholds**.

Figure 738. Thresholds sub-tab



2. Select **Device Throughput Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select **Generate Fault?** generate fault.
5. Click **Save**.

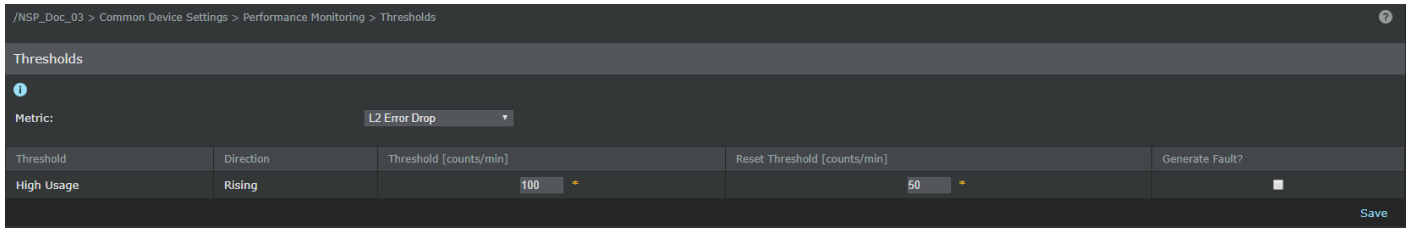
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. **Under Usage** in the context of the throughput usage threshold is a 'falling threshold'. A fault is generated when the throughput % drops below a certain value. This is helpful on very busy networks, where a certain amount of traffic is always expected to be seen. This type of fault is a good indication that there is a communication problem on the network.

Set the L2 error drop threshold for devices within the admin domain

Follow this procedure for setting the L2 Drop threshold for devices within the admin domain.

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 739. Thresholds dialog



2. Select **L2 Error Drop** in the drop down list against **Metric**.
3. Enter the required threshold in the **Threshold [counts/min]** column (this value should be higher than the value in the **Reset Threshold [counts/min]** column).

4. Select **Generate Fault?** to generate fault.
5. Click **Save** to save your settings.

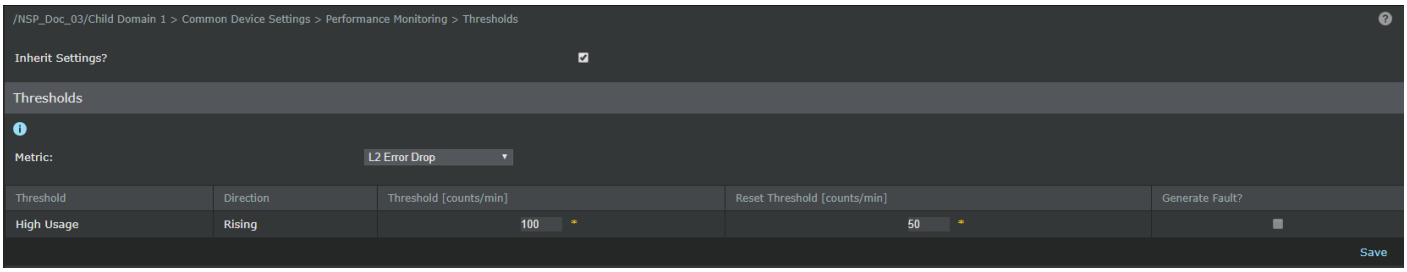
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values.

Set the L2 error drop threshold for devices within the child admin domain

Follow this procedure for setting the L2 Error Drop threshold for devices within a child admin domain.

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 740. Thresholds area



2. Select **L2 Error Drop** in the drop down list against **Metric**.
3. Enter the required threshold the **Threshold [counts/min]** column (this value should be higher than the value in the **Reset Threshold [counts/min]** column).
4. Select **Generate Fault?** to enable fault.
5. Click **Save** to save your settings.

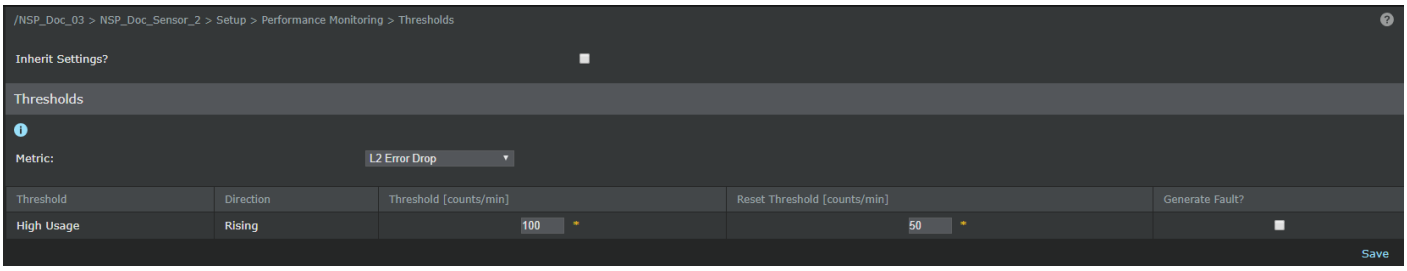
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected. If this checkbox is selected, the settings from the parent admin domain are automatically inherited.

Set the L2 error drop threshold for specific devices

Follow this procedure for setting the L2 Error Drop threshold for a specific device within a domain.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Thresholds**.

Figure 741. Thresholds area



2. Select **L2 Error Drop** in the drop down list against **Metric**.
3. Enter the required threshold in the **Threshold [counts/min]** column (this value should be higher than the value in the **Reset Threshold [counts/min]** column).
4. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

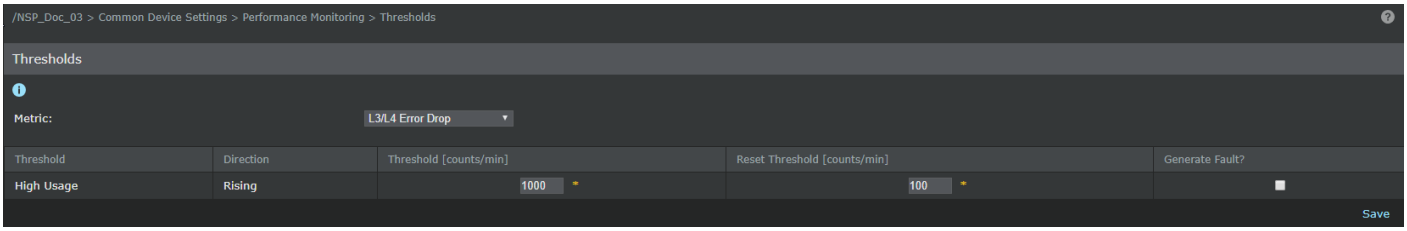
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected.

Set the L3/L4 Error Drop threshold for devices within an admin domain

Follow this procedure for setting the L3/L4 Drop Threshold for devices within the root admin domain.

1. Select Device → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 742. Thresholds dialog



2. Select **L3/L4 Error Drop** in the drop down list against **Metric**.
3. Enter the required threshold in the **Threshold [counts/min]** column (this value should be higher than the value in the **Reset Threshold [counts/min]** column).
4. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

NOTE

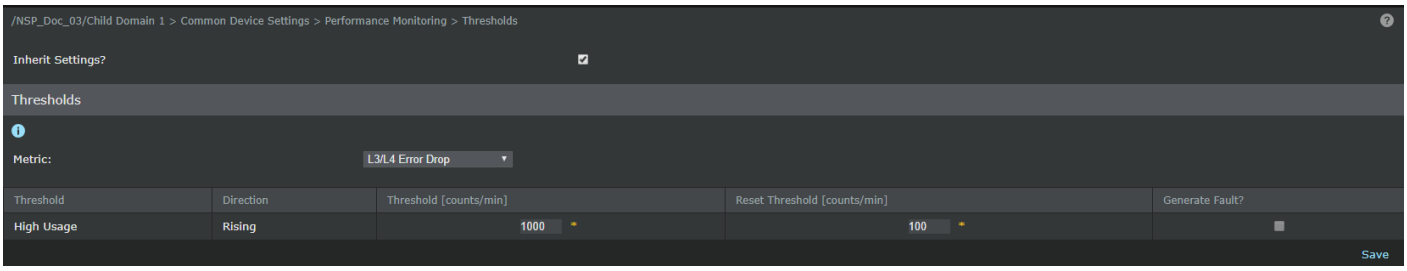
Click **Defaults** to set the threshold settings to the default values.

Set the L3/L4 error drop threshold for devices within the child admin domain

Follow this procedure for setting the L3/L4 Error Drop threshold at the child admin domain Device list node.

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 743. Thresholds area



2. Select **L3/L4 Error Drop** in the drop down list against **Metric**.
3. Enter the required threshold in the **Threshold [counts/min]**column (this value should be higher than the value in the **Reset Threshold [counts/min]** column).
4. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

NOTE

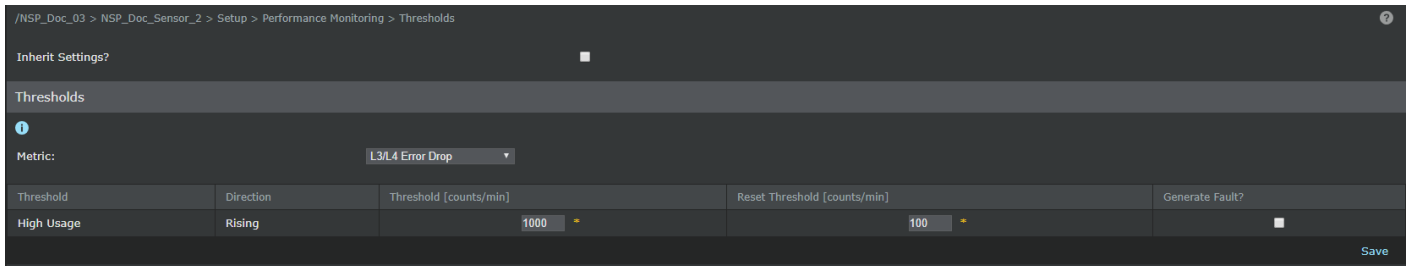
Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected. If this checkbox is selected, the settings from the parent admin domain are automatically inherited.

Set the L3/L4 error drop threshold for specific devices

Follow this procedure for setting the L3/L4 Drop threshold for a specific device.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Thresholds**.

Figure 744. Thresholds area



2. Select **L3/L4 Error Drop** in the drop down list against **Metric**.
3. Enter the required threshold in the **Threshold [counts/min]** column (this value should be higher than the value in the **Reset Threshold [counts/min]** column).
4. Select the **Generate fault?** checkbox to generate fault. Deselect the **Generate fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

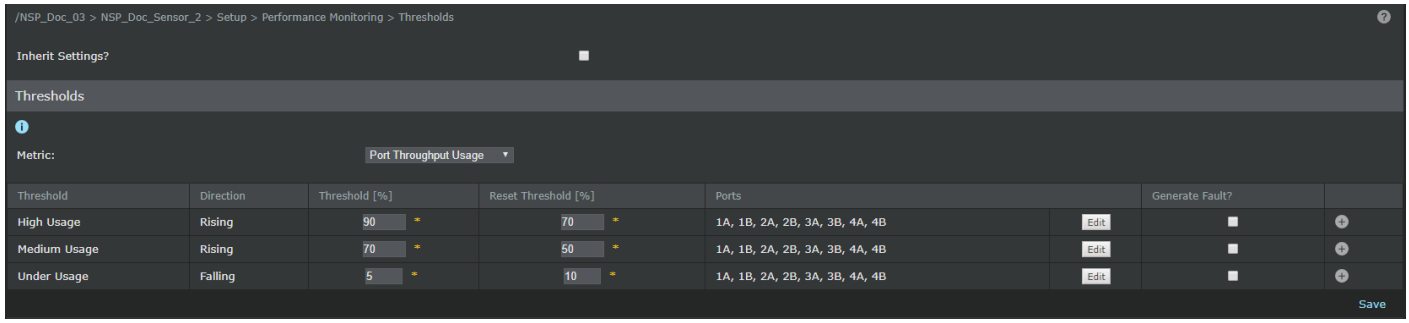
> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected. If this checkbox is selected, the settings from the parent admin domain (the Device list) are automatically inherited.

Set the port throughput usage threshold for specific devices

Port throughput usage is configurable for specific devices within a given network domain. Follow this procedure for setting the port throughput usage threshold for each device within a domain.

1. Click Devices → <Admin Domain Name> → <Device Name> → Setup → Performance Monitoring → **Thresholds**.

Figure 745. Thresholds area



2. Select **Port Throughput Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Click ⊕ against a row to clone that row.

5. In the **Ports** column, click Edit to assign or remove the port values in the **Assign Ports** window.

> **NOTE**
>
> If none of the ports are selected, the threshold is applied to all the ports. In such a case, the **Ports** column displays **All Ports**.

6. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
7. Click **Save** to save your settings.

> **NOTE**
>
> Click on **Defaults** to set the threshold settings to the default values. **Under Usage** in the context of the Throughput Usage threshold is a 'falling threshold'. Alarm is generated when the Throughput % drops below a certain value. This is helpful on very busy networks, where a certain amount of traffic is always expected to be seen. This type of alarm is a good indication that there is a communication problem on the network.

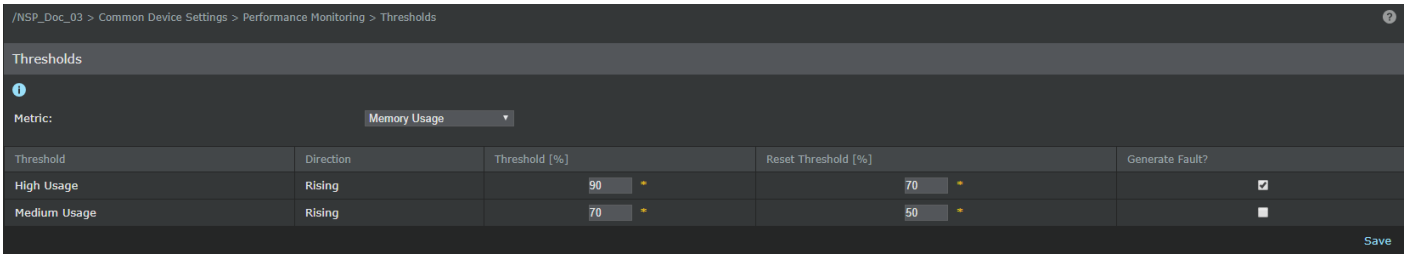
> **NOTE**
>
> **Port Throughput Usaage** metric is applicable at device level configuration but not at admin domain level.

Set the memory usage threshold for the admin domain

Follow this procedure for setting the memory usage threshold for all devices that belong to the root admin domain.

1. Select Devices → <Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 746. Memory usage for admin domain



2. Select **Memory Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

NOTE

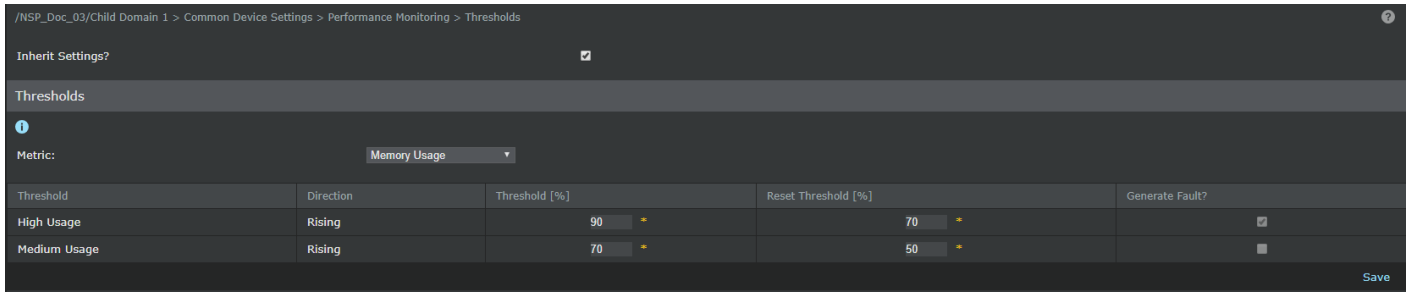
Click **Defaults** to set the threshold settings to the default values

Set the memory usage threshold for devices within a child domain

Follow this procedure for setting the CPU usage threshold for all devices within the child admin domain.

1. Select Devices → <Child Admin Domain Name> → Global → Common Device Settings → Performance Monitoring → **Thresholds**.

Figure 747. Memory usage for child domain



2. Select **Memory Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

NOTE

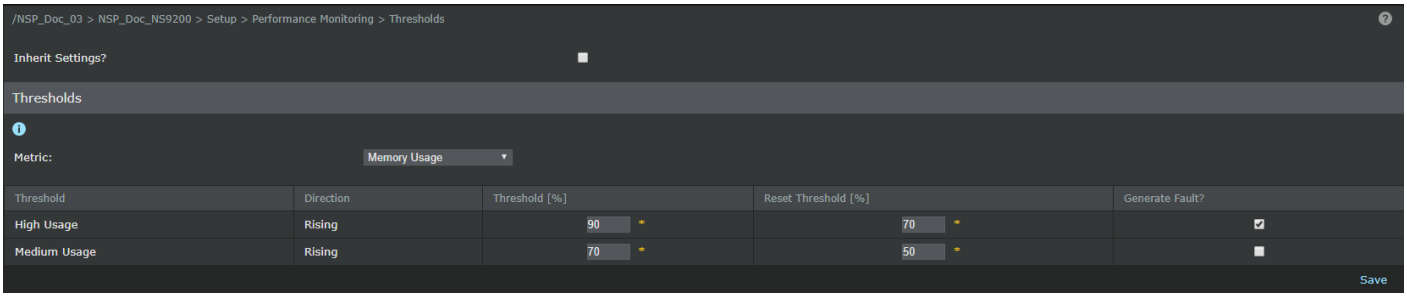
Click **Defaults** to set the threshold settings to the default values. The threshold values can be changed only if the checkbox against **Inherit Settings?** is deselected. If this checkbox is checked the settings from the parent admin domain are automatically inherited.

Set the memory usage threshold for specific devices

Follow this procedure for setting the memory usage threshold for a specific device.

1. Select Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Performance Monitoring → **Thresholds**.

Figure 748. Memory Usage



2. Select **Memory Usage** in the drop down list against **Metric**.
3. Enter the required threshold percentage in the **Threshold [%]** column (this value should be higher than the value in the **Reset Threshold [%]** column).
4. Select the **Generate Fault?** checkbox to generate fault. Deselect the **Generate Fault?** checkbox to disable generation of fault.
5. Click **Save** to save your settings.

> **NOTE**
>
> Click **Defaults** to set the threshold settings to the default values. This option is available only when **Inherit Settings?** is deselected.

How to monitor the device performance

Device performance can be monitored through information on the metrics and through warnings when thresholds set are crossed. Monitoring based on the four core usage metrics related to CPU, memory, device throughput and port throughput can be done in **Performance Charts**. Monitoring based on the thresholds configured for **CPU Usage**, **Memory Usage**, **Sensor Throughput Usage**, **Port Throughput Usage**, **L2 Error Drop**, and **L3/L4 Error Drop** are shown under Sensor Performance Monitoring Threshold faults on the **Faults** tab in **Logs** page of the Manager.

How to monitor thresholds

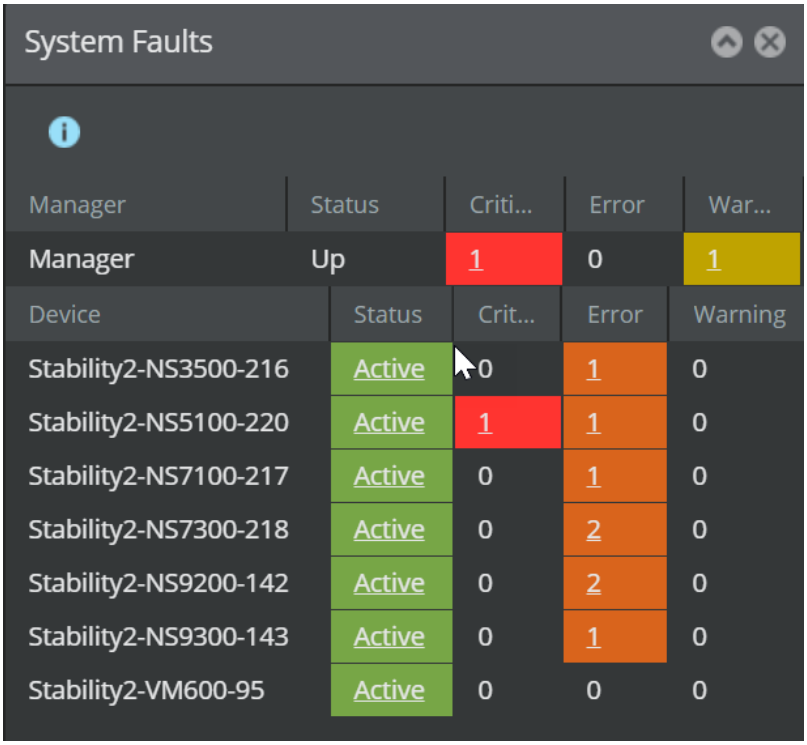
Thresholds configured for CPU usage, memory usage, device throughput usage, L2 error drop, L3/L4 error drop and port throughput usage are monitored as part of the number of warnings generated in the **System Faults** monitor in the **Dashboard** of the Manager. Clicking on the numbers listed under the Warning column in the **System Faults** monitor takes you to more detailed table on the **Faults** tab in **Logs** page of the Manager. Here more information on the warnings generated is available. Threshold warnings are listed under Device Performance - Memory Usage - System Memory fault in the **Summary** column. You can drill down for specific fault information.

Monitor thresholds from the Manager Dashboard page

You can monitor thresholds from the Manager Dashboard pages.

1. Click the numbers listed against the device to be monitored under the warnings column of the **System Faults** monitor.

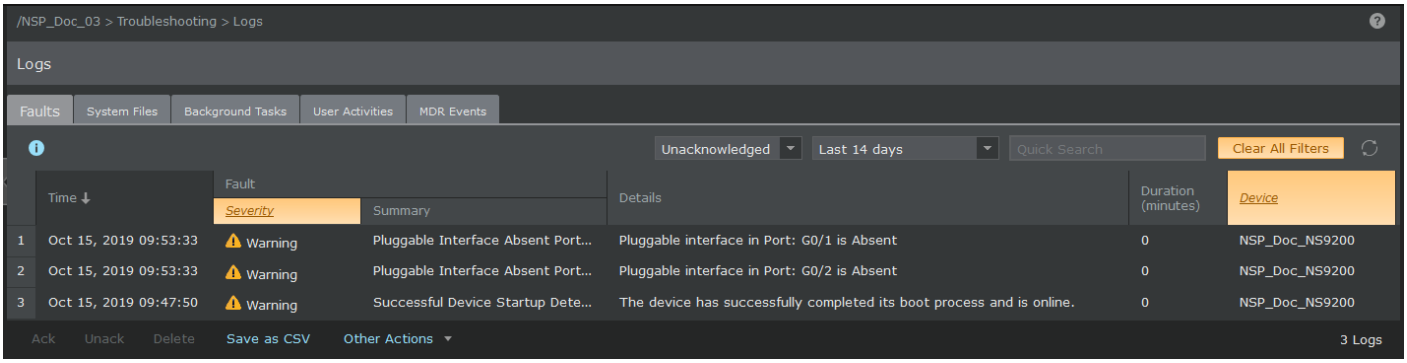
Figure 749. System Faults monitor



2. The **Faults** tab in the **Logs** page displays the list of warnings for the selected device.

   The warnings relating to the Sensor performance monitoring thresholds are listed as a **Device Performance - Memory Usage - System Memory** fault type.

Figure 750. Warning dialog



View Monitoring thresholds

To view Monitoring thresholds:

1. Select Manager → <Admin Domain Name> → Troubleshooting → **Logs** and select **Faults** tab.

   The **Faults** tab displays the Operational Status of the Manager, Database, and Sensors.

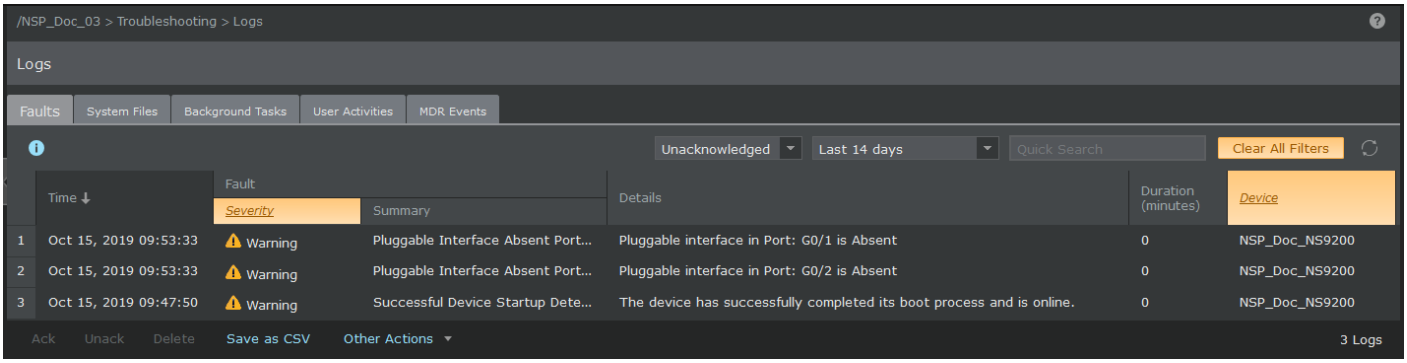
NOTE

The numbers listed are in "Unacknowledged Fault Count / Total Fault Count" format.

2. In the Device pane, click on the total listed under the **Warning** column to view all warnings.

   The warnings relating to the Sensor performance monitoring thresholds are listed as a **Device Performance - Memory Usage - System Memory** fault type.

Figure 751. Fault Count page



How to monitor Device performance metrics

Core Sensor performance metrics can be monitored using Performance Charts. The core metrics are **CPU Usage**, **Memory Usage**, **Port Throughput Usage**, and **Device Throughput Usage**.

Monitoring of core metrics is possible only if Performance Monitoring is enabled in the **Global** tab or **Devices** tab from the Manager configuration pages.

Monitor device usage metrics

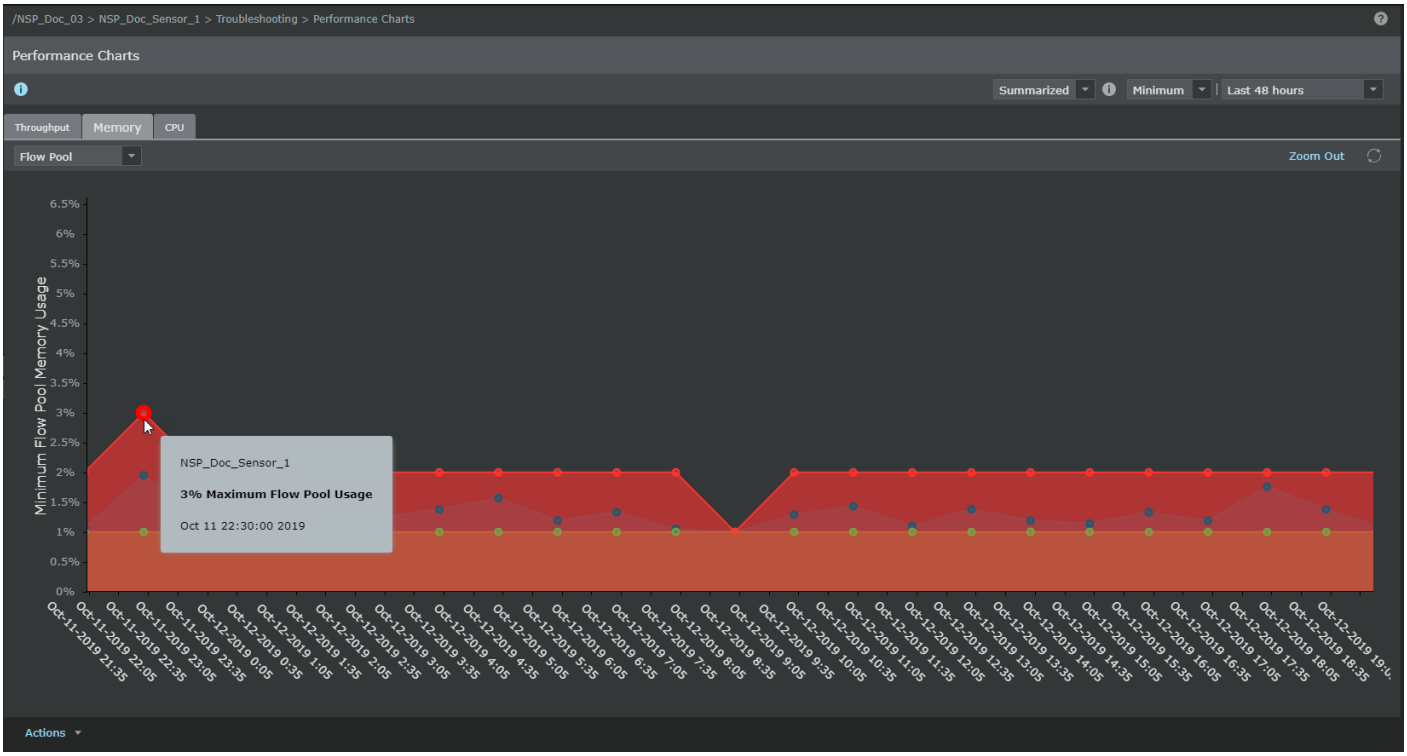
You can view the device usage metrics in the **Performance Charts** page. In order to view the device usage values, performance monitoring has to be enabled for data collection. The list of metrics available for monitoring are as follows:

- **Throughput** — Displays the Sensor and port throughput usage.
- **Memory** — Displays the memory usage which helps monitor the usage before reaching the threshold limit.
- **CPU** — Displays the device CPU usage which helps monitor the usage before reaching the threshold limit.

Follow this procedure to view memory usage (this example demonstrates steps for viewing memory usage):

1. Navigate to Devices → <Admin Domain Name> → Devices → Device Name → Troubleshooting → **Performance Charts**.
2. Select the **Memory** tab.

Figure 752. Memory



The memory usage chart will display data as per your selection in the drop-down menus. Click the refresh icon to refresh the data.

The display of options vary according to the Sensor model type and version. Sometimes the chart may not be available for some options if the option is not applicable to the configured Sensor (Example: **Decrypted Flow Pool** option is only applicable to sensors that support SSL decryption).

View default Device performance monitors

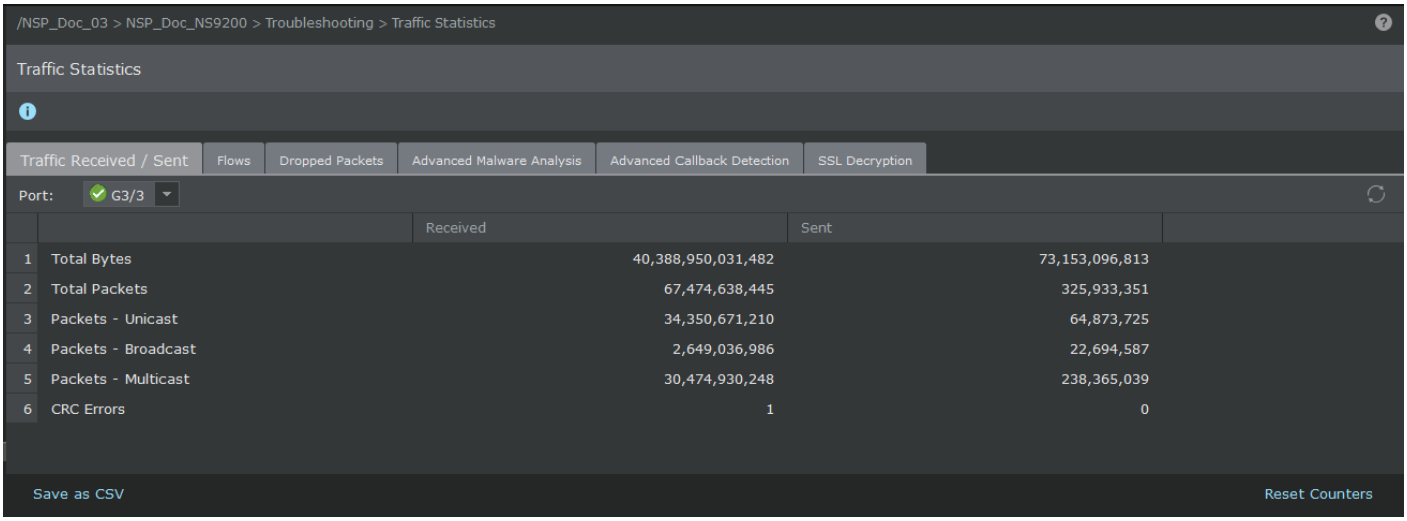
Sensor performance statistics can be viewed in the **Traffic Statistics** page that displays different type of Sensor statistics. The list of options available for Sensor performance statistics are:

- **Traffic Received / Sent** — Statistics of the total number of packets received (Rx) and transmitted (Tx) for a given device
- **Flows** — Statistical view of the TCP and UDP flow data processed by a device. Checking your flow rates can help you determine if your device is processing traffic normally, while providing you with a view of statistics, such as the maximum number of flows supported as well as the number of active TCP and UDP flows.
- **Dropped Packets** — Packet drop rate on a port
- **Advanced Malware Analysis** — Statistics of the malware detected for a given device
- **Advanced Callback Detection** — Statistics on the amount of callback activity and communication attempts to the C&C servers
- **SSL Decryption** — Traffic statistics for inbound and outbound SSL decryption

Follow this procedure to view Sensor performance statistics (this example demonstrates steps for creating Flow statistics):

1. Navigate to Devices → <Admin Domain Name> → Devices → Device Name → Troubleshooting → **Traffic Statistics**.
2. Select the **Traffic Received / Sent** tab.

Figure 753. Traffic Received / Sent statistics



Click the refresh icon to refresh the data for the port selected.

Generation of device performance reports

Device performance reports provide flexible data on device configuration and performance. Three default reports give information on CPU usage, memory usage and device throughput usage for a selected period. New reports on Sensor performance can be generated as per user needs. These reports can be generated in hourly, daily, weekly or monthly time frames.

Device performance — Next Generation default reports

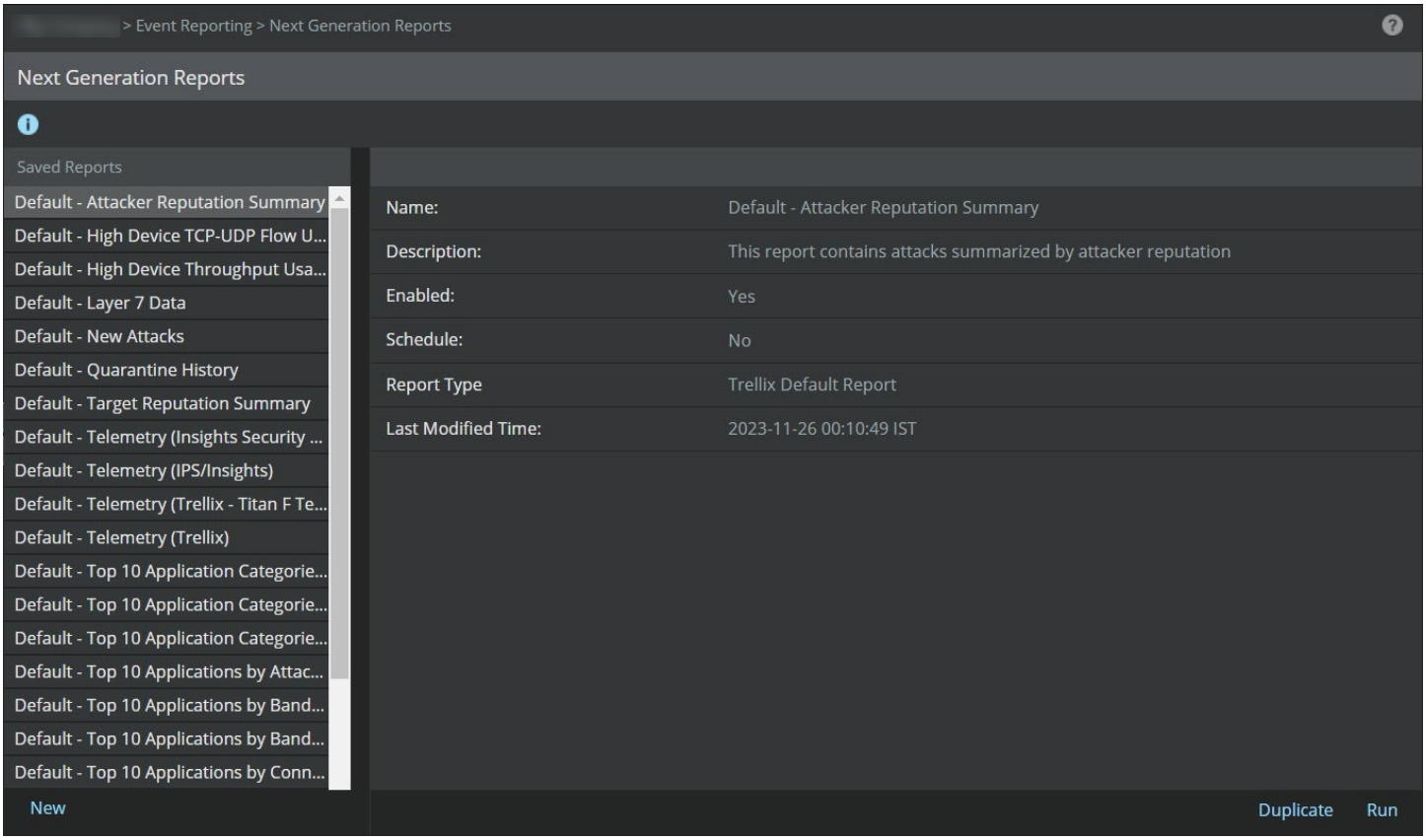
The Next Generation report option allows you to generate customized reports. You can make selections, such as the type of data to base the report on, and the format in which you want the data to be presented such as table, bar chart, or a pie chart, etc. From a list of fields that are applicable for a report, you can select the fields that you want to display; you can also specify the conditions that must be met to include the information for those fields in the report.

Generate the default Sensor performance reports

Next Generation default reports can be generated from Analysis → <Admin Domain Name> → Event Reporting → **Next Generation Reports** menu in the Manager.

When you select the Analysis → <Admin Domain Name> → Event Reporting → **Next Generation Reports**, the **Next Generation Reports** page is displayed. The **Saved Reports** section on the left pane comes up by default.

Figure 754. Next Generation report



The four default reports related to Sensor performance monitoring; **Default - High Device Throughput Usage**, **Default - High Device TCP–UDP Flow Usage**, **Default - Quarantine History**, and **Default - Top 10 Attacks** are displayed on the left pane along with other reports.

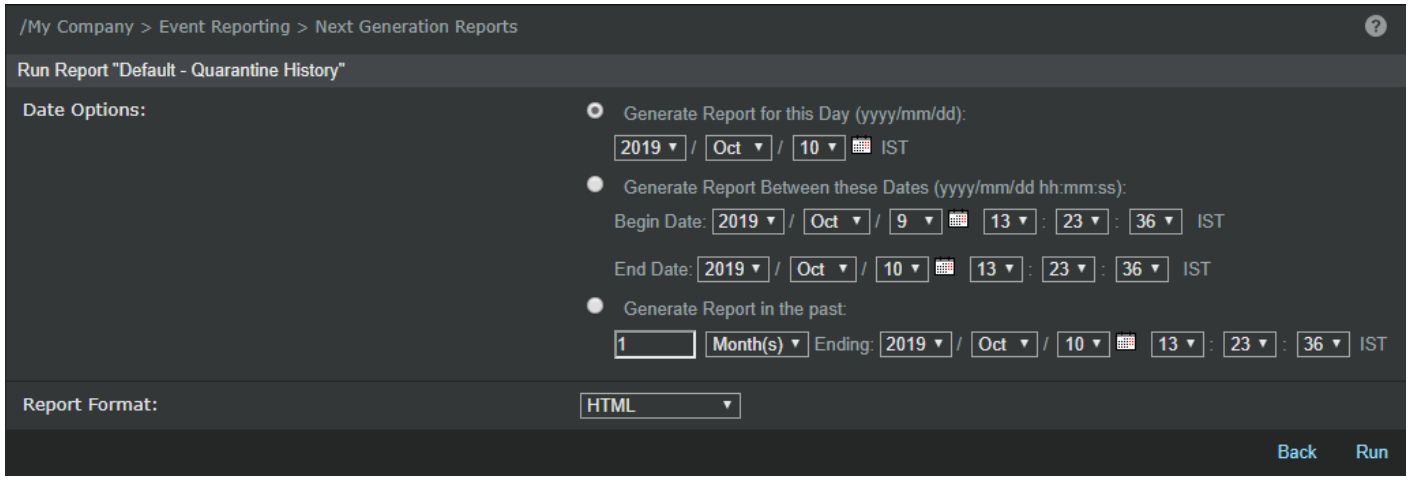
The procedure to view one of the defaults reports related to Sensor performance monitoring, the **Default - Quarantine History** is detailed below.

NOTE

The admin domain filter in the main **Analysis** tab (provided in the left pane) does not impact the report generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

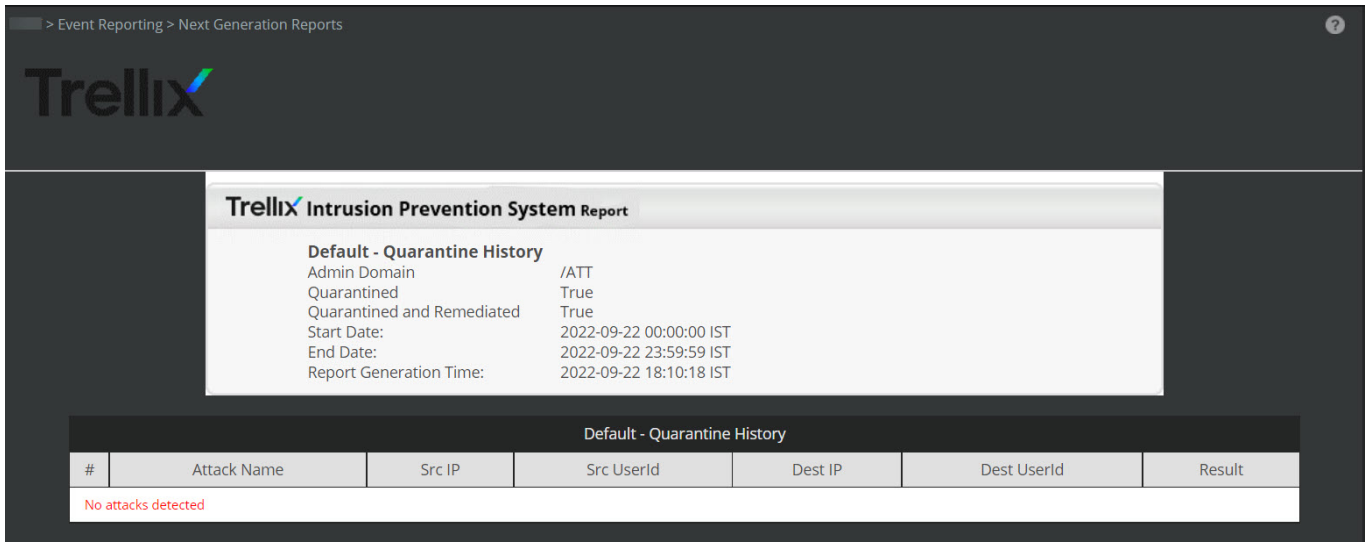
1. Select **Default - Quarantine History** listed on the left pane to view the details of this report on the right pane.
2. Click **Run** to view the Run Query choices.
3. Select one of the **Date Options** (either query for the day or between two dates or for a selected period in the past).
4. Select the report format (**HTML**, **PDF Portrait**, **PDF Landscape**, **Save as CSV** or **Save as HTML**) and click **Run**.

Figure 755. Report Format option



5. The **Default - Quarantine History** report is generated.

Figure 756. Default - Quarantine History report



> **NOTE**
>
> In step 1 above, select **Default - High Device Throughput Usage** or **Default - High Device TCP–UDP Flow Usage** or **Default - Top 10 Attacks** and follow a similar procedure to generate the corresponding Sensor performance reports. Default reports are generated only if the data values are higher than or equal to 95 %.

Device performance — Next Generation user defined reports

The Next Generation report option allows you to generate customized reports. You can make selections such as the type of data to base the report on, the format in which you want the data to be presented such as table, bar chart, or a pie chart, etc. From a list of fields that are applicable for a report, you can select the fields that you want to display; you can also specify the conditions that must be met to include the information for those fields in the report.

Next generation User defined reports on Sensor performance can be generated for a specific interval / period.

NOTE

The admin domain filter in the main **Analysis** tab (provided in the left pane) does not impact the report generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

Generate period-specific reports on device performance

Follow this procedure to generate a period specific Next Generation report on device performance.

1. Navigate to Analysis → <Admin Domain Name> → Event Reporting → **Next Generation Reports**.
2. Click **New** at the bottom of the left pane.
3. Select **Application Data** and select the option **Hourly** in the **Data Source** page.

   Daily, weekly and monthly period specific reports can be generated by selecting the option **Daily**, **Weekly** or **Monthly**.
4. Click **Next**.
5. Click the **Table** option under **Display Options** and click **Next**.
   - Click the desired fields in the **Available Fields** pane to move it to the **Selected Fields** pane (You can click the left / right arrow on each columns to change the position of the column. You can click **X** on each column to remove the column). Click **Next**.
6. Click the properties listed on the left pane and move them to the right pane to reduce the quantity of information shown in the report. Click **Next** to select the date option in the next page, click **Save As** to save the report.
7. Select one of the **Date Options** (either query for the day or between two dates or for a selected period in the past). Select the report format (**HTML**, **PDF Portrait**, **PDF Landscape**, **Save as CSV** or **Save as HTML**) and click **Finish**.
8. To generate the report, select the report created in the left pane and click **Run**.

   The hourly report is generated.

Sensor performance — Configuration reports

Configuration reports are a category of reports where you can generate configuration reports based on pre-defined conditions. There are two configuration reports related to Sensor performance.

Generate Performance Monitoring - Admin Domain Configuration reports

The **Performance Monitoring - Admin Domain Configuration** report displays information on admin domain wise configuration made in the Manager.

Follow this procedure to generate the admin domain report.

Steps:

1. Click the **Manager** tab from the Manager home page.

2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Performance Monitoring - Admin Domain Configuration**.

   The configuration options of the **Performance Monitoring - Admin Domain Configuration** is displayed.

3. Select a filter from the **Admin Domain** drop down list.

   > **NOTE**
   >
   > The admin domain selected in the left pane has no impact on the reports generated. The **Admin Domain** drop-down list is explicitly to filter the reports that are generated.

4. Select or clear the checkboxes against **Metrics**, **Thresholds** and **Display**.
5. Select the **Output Format**.
6. Click **Submit**.

   The **Performance Monitoring - Admin Domain Configuration** report is generated.

Generate Performance Monitoring - Sensor Configuration reports

The **Performance Monitoring - Sensor Configuration** report displays information on Sensor configuration settings made in the Manager.

Steps:

1. Click the **Manager** tab from the Manager home page.
2. Select <Admin Domain Name> → Reporting → Configuration Reports → **Performance Monitoring - Sensor Configuration**.

   The configuration options of **Performance Monitoring - Sensor Configuration** report is displayed.

3. Select the Sensors to be included against Sensors. Select or clear checkboxes against **Metrics** and **Thresholds**.
4. Select the **Output Format**.
5. Click **Submit**.

   The **Performance Monitoring - Sensor Configuration** report is generated.

Custom Attack Definitions

Custom attacks

Trellix IPS uses a variety of methods to detect aberrant network activity. The main detection method used is attack definition. An attack defines either a rule or related signatures that specify a set of checks for capturing various attempts at exploiting a given vulnerability or creating other threat conditions.

> **NOTE**
>
> Throughout this guide, the terms attack and attack definition are used interchangeably.

Trellix IPS regularly supplies you with its own attack definitions (signature set) to protect your network. Additionally, it also provides ad hoc signature sets in case of emergencies and zero-day vulnerabilities. Trellix's research team develops these signatures and tests them thoroughly before releasing them to its customers.

There could be unique security requirements that would not be possible to be covered in the Trellix IPS-supplied signature set. For such cases, you have the option of developing your own attack definitions. Such user-defined attacks are referred to as custom attack definitions or custom attacks.

Reasons to create your own attack definitions

If the Trellix IPS-supplied signature set is adequate to protect your network, then why create one yourself?

The reasons you might want to create an attack definition will vary widely based on the usage scenario for your IPS Sensor and the environment in which it is deployed. The sections below attempt to describe some common scenarios and the actions that might be taken when they occur.

- **Emergency situations** - Trellix follows strict quality assurance processes and requires high-quality information before providing updates to customers. Thus, there may be situations where an attack covering particular vulnerabilities may be a very high priority for your network but might not be provided as swiftly as your security policy might require. In this case, you might need to write and deploy strategic attacks based on your knowledge of your network's vulnerabilities until an update from Trellix is available.
- **Forensic analysis** - It may be useful to deploy specialized attacks to investigate suspicious activity on your network and possibly to track intrusions.
- **Custom attacks for Your particular environment** - Writing custom attacks for your network environment may be necessary for a variety of reasons. The most common is policy enforcement. For example, your security policy may dictate that certain traffic or usage patterns are disallowed. In such cases, it may be useful to write and deploy attacks that can alert your IT or security staff.
- **To preserve legacy attack definitions** - If you are migrating from an open-source IPS or IDS solution, such as Snort, you may want to import the attacks in their current format into Trellix IPS.

Types of custom attacks

In Trellix IPS, you have the flexibility to create custom attacks in two ways:

- You can create custom attacks in Trellix IPS's proprietary format. This type of custom attacks are signature-based. You can define one or more signatures per attack. Such attack definitions are called **Trellix IPS Custom Attacks** in this guide.

  NOTE

  The Trellix IPS Custom Attacks in the earlier releases were called User-Defined Signatures (UDS). The interfaces of the UDS Editor are now available within the Custom Attack Editor.

- You can write rule-based custom attacks using Snort rules language, which is open-source. Such attack definitions are called **Snort Custom Attacks** in this guide.

  NOTE

  These two formats are not interchangeable. That is, you cannot convert a Trellix IPS Custom Attack to Snort Custom Attack or the other way around.

You can use Snort rules in your existing Trellix IPS setup without having to modify it in any way or install any Snort-related components. These rules could be your own or from sources such as the Snort user-community; the critical thing is that the rules should conform to the Snort syntax for you to use them in Trellix IPS.

A Snort Custom Attack is converted into Trellix IPS's format internally when you save it in the Manager server. This translation enables you to use Snort rules directly in Trellix IPS without the need for any Snort-related components.

Trellix IPS signature terminology

To be able to create effective custom attacks, you need to understand how Trellix IPS detects attacks. To be able to understand this mechanism, you need to be familiar with some terms listed below:

- Signatures and rules
- Attacks
- Policies
- Alerts

Signatures and rules

A signature or rule is a set of checks (for example, string matches or IP-port comparisons) that are applied to network traffic seen by the Sensor. The term signature is relevant for Trellix IPS Custom Attacks (that is, custom attacks in Trellix IPS format) or the Trellix IPS-supplied signature set. The term rule applies to Snort Custom Attacks.

In case of Snort Custom Attacks, the Manager parses them to check the syntax. Then it converts the valid attack definitions to Trellix IPS's format and saves them in the Manager database. Once in the database, the converted Snort rules function like any other Trellix IPS signature. So, in Trellix IPS, both signatures and rules are functionally similar. What applies to a signature is also applicable to a rule unless stated otherwise.

NOTE

Throughout this guide, Snort Custom Attacks are also referred to as Snort rules or just rules. This is not to be confused with the Trellix IPS rule sets, which are a collection of attack definitions that meet certain criteria.

The attack detection mechanism in Trellix IPS relies on comparison of traffic to a database of signatures or rules. Trellix IPS enables you to define checks using combinations of string matches and checks for other anomalies such as excessive field lengths. When all the necessary conditions for a given rule of set of signatures are satisfied, an event is raised in the Sensor; all signatures and rules defined are checked against the traffic simultaneously and all matching events within the context of a given attack are correlated by the Sensor to generate a single alert.

Attacks, policies, and alerts

In Trellix IPS, attack definitions are a mechanism used to identify and protect against malicious actions taken against your network. An attack definition is the aggregation of the signatures (or rule) and other supporting data that can identify a specific network event. When you select an attack, you are essentially selecting a group of conditions defined in a rule or signature(s).

NOTE

A rule in a Snort Custom Attack corresponds to the signatures in a Trellix IPS Custom Attack.

Policies are applied to the Sensor and consist of one or more attacks. Traffic passing through the Sensor is compared to the attacks enabled in the policies, and if any traffic is identified as malicious by an attack definition, an alert is triggered to notify you of the incident.

Custom attack editor

Custom Attack Editor provided in the Manager is the tool that you use to create custom attacks. Custom Attack Editor enables you to create Trellix IPS Custom Attacks as well as in Snort Custom Attacks. Using this tool, you can also import custom attacks in bulk against defining them individually.

Audience

Custom Attack Editor is designed for sophisticated users with expertise in networking and intrusion prevention. The ability to create a custom attack is a double-edged sword. It can be a very powerful detection and defense mechanism, but at the same time, when used without training and experience, a custom attack can cause harm to your network and the business that depends on it. In addition, without a significant amount of experience in both using and configuring detection mechanisms for network intrusion detection devices, it is possible to make mistakes that can render your detection device essentially useless. For example, a mistake in implementation of a signature on a high-traffic network could cause such a large number of alerts to be generated that it would render the Manager unusable. On the opposite end of the spectrum, without proper experience and expertise, it is likely that a user might create a signature that would never detect security incidents (due to errors in tests or detection window, for example), despite the fact that the signature might be intended to detect very important events specific to your network.

Since a poorly written custom attack can cause many more problems than it solves, Trellix recommends that an attack writer possesses the following knowledge:

- A strong understanding of computer networking
- Experience with networks running the protocol for which you intend to create a custom attack, including a good packet-level understanding of the protocol
- The ability to recognize the difference between "good" and "bad" traffic. That is, traffic that is correct and valid for your network and the devices that comprise it, and traffic that is anomalous to your network's configuration and security policies.
- A strong understanding of Snort rules language, if you plan to use Snort Custom Attacks

While the fact that Trellix IPS provides deep parsing of application protocols and supports complex attack-definition structures may seem overwhelming to first-time users, it is reasonably straightforward to create custom attacks after crossing this initial hurdle.

Getting started with custom attacks

Creating a custom attack requires certain experience as well as a number of different pieces of information, both technical and policy-oriented. This chapter describes the information you should have before you start creating custom attacks in Trellix IPS.

Before you create a custom attack

Creating attack definitions is a complex topic on which books have been written. It is highly recommended that you refer to one of these books if you are not an experienced attack definition author. Pay close attention to detail when you define your attacks, as there are many ways to shoot yourself (and your network!) in the foot as you develop expertise with attack definitions.

Before creating a custom attack, you should carefully consider the requirement that you are trying to address. This means that you should have a clear understanding of the attack's purpose, such as a specific business or policy requirement.

You should have a clear rationale for using a custom attack instead of another mechanism. In some cases, a custom attack may not be the appropriate solution. For this reason, you should consider whether you can address your need with other technical means, such as router ACLs, firewall rules, or a network sniffer.

Finally, you should verify that the custom attack you intend to create does not duplicate any attack provided in Trellix IPS. However, in case of a duplicate, you have the flexibility to use both or just the custom attack instead of the Trellix IPS-supplied attack. If you choose to use both, note that the Sensor may raise two alerts for the same attack traffic.

Required information for creating a custom attack

The following is a list of the information you should have in hand as you create your custom attacks and the constituent signatures or rule. A signature or rule can range from very simple (for example, checking the value of a header field) to highly complex checks of different information in a specific order. You must have good bit of data to aid yourself in creating an accurate attack definition, such as the following:

- Reason for creating this custom attack
- Technical information references for this custom attack
- Protocol in which this custom attack will search the traffic (also known as the impact protocol)

- Specific hardware or software platforms affected by this traffic (also known as impact packages)
- Severity of this event
- The direction in which the "traffic to be watched for" occurs
- Specific criteria that comprise the attack, such as field values and patterns to match
- A method, data, or tool to be used for testing the attack before you use it in your production environment

Understanding impact packages and protocols

Trellix IPS policies define what hardware and software platforms are present on a network and what should be monitored. The platforms can be as generic as the HTTP protocol or as specific as Microsoft Internet Explorer running on Windows Server 2016.

After a policy is configured and saved, the Manager searches through the database and generates a list of attacks that will be enabled when that policy is applied to an interface. Attacks specify what platforms they affect as part of their impact construct.

In case of Trellix IPS Custom Attacks, the impact construct of an attack can contain references to protocols, and the packages that provide support for those protocols. Protocol references refer to protocols defined by Trellix as well as the custom-defined ones. Package references refer to particular software or hardware platforms, which can include a specific OS.

The platforms that can be selected are those for which Trellix IPS has specific support in some form. If you do not see a particular platform, you can choose the one which is similar, or specify **`tcpip-machine`** as the package, or specify just the impact protocol for the attack.

For Snort Custom Attacks, you cannot choose an impact package. By default, **`tcpip-machine`** is selected as the package, and this cannot be modified. Additionally, the Manager identifies the impact protocol for the attack definition.

How Trellix IPS prevents intrusions

The attack prevention mechanism of Trellix IPS is very powerful, but may also be difficult to understand. A good analogy is to that of a DNA test. DNA testing allows biology experts to obtain a DNA sample from a member of a species, and use the sample to determine the individual from which the particular sample came. Trellix IPS provides much of the same capability, but oriented toward detecting and accurately identifying network events. As an example, Trellix IPS's detection mechanisms can allow your signature to identify every HTTP traffic flow, every HTTP traffic flow using the GET mechanism, every HTTP traffic flow using GET with `/cgi-bin/calendar.pl` as the path, and even every GET with that path and a parameter named **month** with a value of **February**.

This is why Trellix IPS supports the aggregation of multiple conditions into every attack. Each signature or rule within an attack can be more or less specific so as to identify everything from generic network activity that affects a given platform in a particular way to a specific piece of code that has very specific and identifiable effects. Based on their specificity and severity, signatures and rules are assigned different confidence and severity values.

When a network event occurs that matches an existing attack definition, the rule or signature(s) (generic and specific) within that attack definition may be triggered. When alert throttling is enabled, the Sensor correlates the multiple triggering events automatically to raise a single alert with the highest confidence level.

How attack detection works

The Sensor performs different levels of traffic processing and analysis. Signatures and rules operate on traffic that has passed through these higher-level processing phases. Understanding how attack detection works can enable you to create effective Custom Attacks.

Flows

At the highest level, the Sensor addresses UDP and TCP traffic based on the concept of a flow. Flows are defined by their protocol (UDP/TCP), the source and destination ports, and IP addresses of their endpoints. As you might be aware, UDP does not contain the concept of "state" that TCP does. So the Sensor implements a timer-based flow context for UDP traffic. After dividing traffic into flows, the Sensor makes use of port mappings or, in the case of traffic running on non-standard ports, intelligent protocol identification, to pass each flow to the appropriate protocol parsing mechanism.

For a custom attack, you can specify whether the Sensor should look at the complete flow, one direction of the flow, or restrict itself to data occurring within single packets of the flow. Precise control of this detection window is necessary for accurate detection of attacks.

Protocol parsing specifications

Protocol specifications (Trellix IPS's protocol parsing mechanisms) parse through network flows to validate traffic and divide it into protocol fields which may then be actively tested against Trellix IPS-supplied attacks or Custom Attacks. By dividing protocol traffic into the appropriate fields, a Sensor can perform matches against the most specific field or subfield pertinent to an effective attack, thus resulting in very low false-positive rates. Since the parsing process is fully stateful, it allows detection of anomalies in the protocol's behavior. Additionally, this parsing makes it possible to provide an additional benefit to Trellix IPS Custom Attack writers in the form of qualifiers. Qualifiers are tests that are embodied in the name of a particular protocol field. For example, rather than specifying that an HTTP request method must be "GET", the Trellix IPS system allows you to use "http-get-req-uri" as the name of the field, saving you the requirement of providing that test in the Custom Attack, and the Sensor from having to perform an extra pattern match.

Packet searches

Traffic flows that are not identified as belonging to any particular protocol are passed to the packet search protocol specification engine for further parsing. Trellix IPS presents each direction of the flow to Trellix IPS-supplied attacks and any Custom Attacks. Tests against packet search traffic typically take the form of specific ordered pattern matches so as to prevent false positives and performance problems.

Attack definitions

Attack definitions tie together elements of the above-described framework to derive specific "fingerprints" for network traffic from smaller building blocks.

In essence, attack definitions are like DNA tests. They can identify both specific people and relatives of that person. In the IPS case, the relatives may be a collection of buffer overflow attacks against a certain piece of software, and the particular person would be a specific piece of exploit code.

While the two are not greatly different, Trellix IPS adopts a convention of differentiating between attacks based on abnormality and attacks based on specific traffic. The main difference is while anomaly-based attack detection process examines the network for unexpected or non-conforming behavior, specific attack definitions will often look for a very particular indicator, such as

a flag with a particular value, or a specific string's presence. Anomaly attacks know what to expect in normal traffic, and are triggered when they get something else. Normal attack definitions look for specific misbehavior. The custom attacks that you define must check for behavioral anomalies as well as specific exploit strings. Thus, all possible attempts to exploit a vulnerability can be detected.

Technical information references

A Custom Attack definition is generally based on an advisory or some other description of a known vulnerability. You should have in hand whatever information you can find regarding the attack definition. This can include traffic dumps of an attack in progress or the exploit code itself. You can use this information to determine the characteristics of the vulnerability.

You should know the specific criteria that the attack definition should comprise of, such as field values and patterns to match. Your research may lead to a long list of characteristics specific to the exploit traffic. However, bear in mind that an attack definition based on all suspicious characteristics may be too specific. Although it would be precise, it may impact a Sensor's throughput or lead to detection problems. On the other hand, an attack definition based on only one of the characteristics may be too broad and generate false positives.

Importance of testing custom attack definitions

It is imperative that you thoroughly test your attack definitions before deploying them in a production environment. Incorrect definitions can lead to false positives, false negatives, and performance problems, any of which could be very detrimental to the security and reliability of your network. The best way to avoid these problems is to make use of a comprehensive test plan that puts the attack definition through the full deployment process and verifies that it performs as expected.

Trellix recommends that at a minimum you include the following verification exercises in your test plan:

- Use traffic generation tools or packet dumps to verify that your attack definitions match the traffic they are supposed to detect.
- If possible, verify that any custom attack definition is not duplicating functionality already available in Trellix IPS. For example, check if there is Trellix IPS-supplied attack definition for the same condition. You can do this by examining whether your test traffic raises duplicate alerts - one for Trellix IPS-supplied attack and another for custom attack.
- Deploy the custom attacks on a non-production Sensor connected to either a test network that mirrors your production network traffic or a non-production Sensor connected to your production network in SPAN or Tap mode.

Quick tour of the custom attack editor

To create and import Custom Attacks, you use the Custom Attack Editor - a powerful tool available in the Manager. Using this tool, you can define both Trellix IPS Custom Attacks and Snort Custom Attacks. This section explains the user interfaces and features of the Custom Attack Editor.

Basics of the custom attack editor interface

There could be unique security requirements that would not be possible to be covered in the Trellix IPS-supplied signature set. For such cases, you have the option of developing your own attack definitions. Such user-defined attacks are referred to as Custom Attack definitions or Custom Attacks.

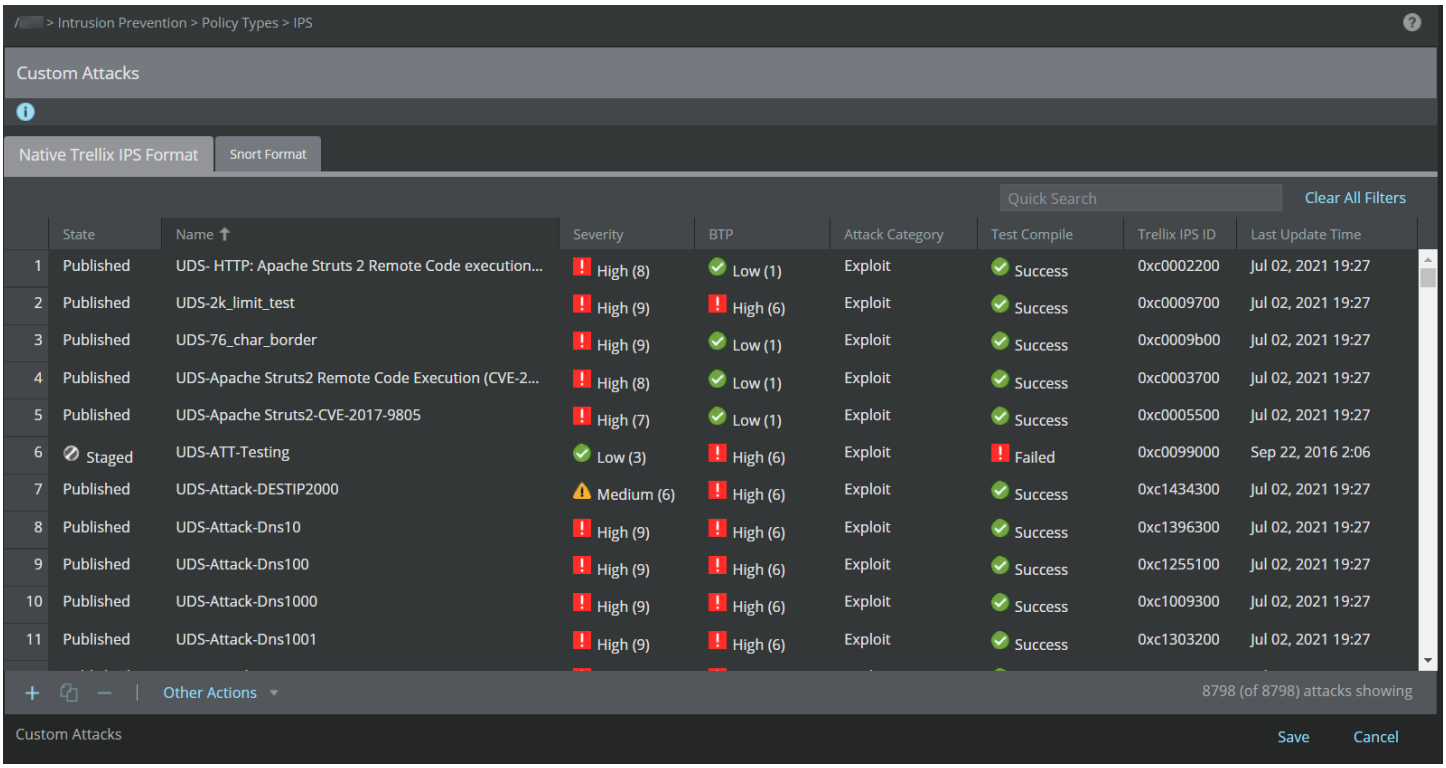
Custom Attack Editor enables you to create Trellix IPS Custom Attacks as well as Snort Custom Attacks. Using this tool, you can also import custom attacks in bulk against defining them individually. You use the Custom Attack Editor to manage custom attacks. You can launch it from the **Custom Attacks** page of the Manager. From the Manager, select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

NOTE

The Custom Attacks menu option is available only for the root admin domain.

The **Custom Attacks** page provides the following options:

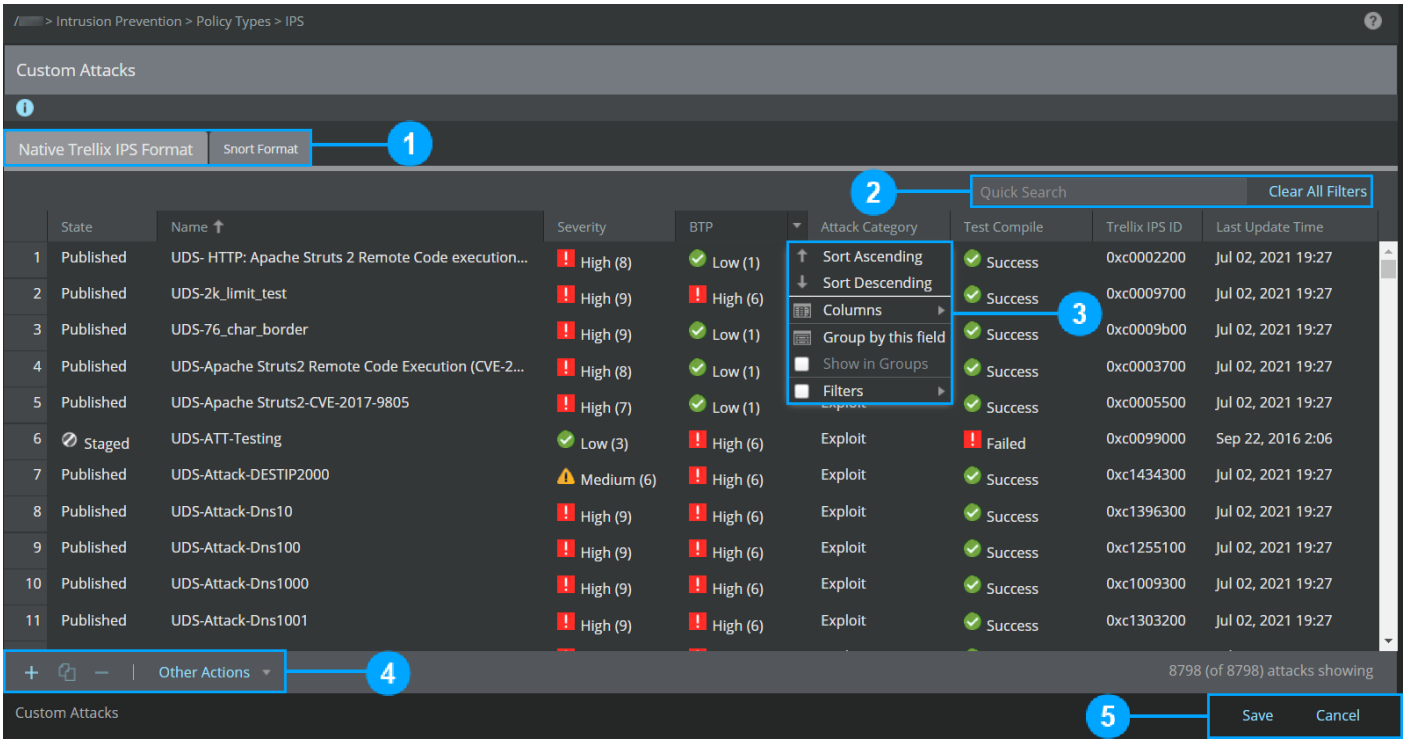
- **Native Trellix IPS Format**: You can create custom attacks in Trellix IPS's proprietary format. This type of custom attacks are signature-based. You can define one or more signatures per attack. Such attack definitions are called Native Trellix IPS Format Custom Attacks.
- **Snort Format**: You can write rule-based custom attacks using Snort rules language, which is open-source. Such attack definitions are called Snort Custom Attacks. In case of Snort Custom Attacks, the Manager parses them to check the syntax. It then converts all valid attack definitions to Trellix IPS's format and saves them in the Manager database. Once in the database, the converted Snort rules function like any other Trellix IPS signature. So, in Trellix IPS, both signatures and rules are functionally similar implying that what applies to a signature also applies to a rule unless stated otherwise.



Default page of the Custom Attack Editor

This section explains the default page that is displayed when you launch the Custom Attack Editor.

Figure 757. Default page of Custom Attack Editor



Item	Description
1	Tabs
2	Regular expression search
3	Viewing options
4	Menu options
5	Save/Cancel buttons

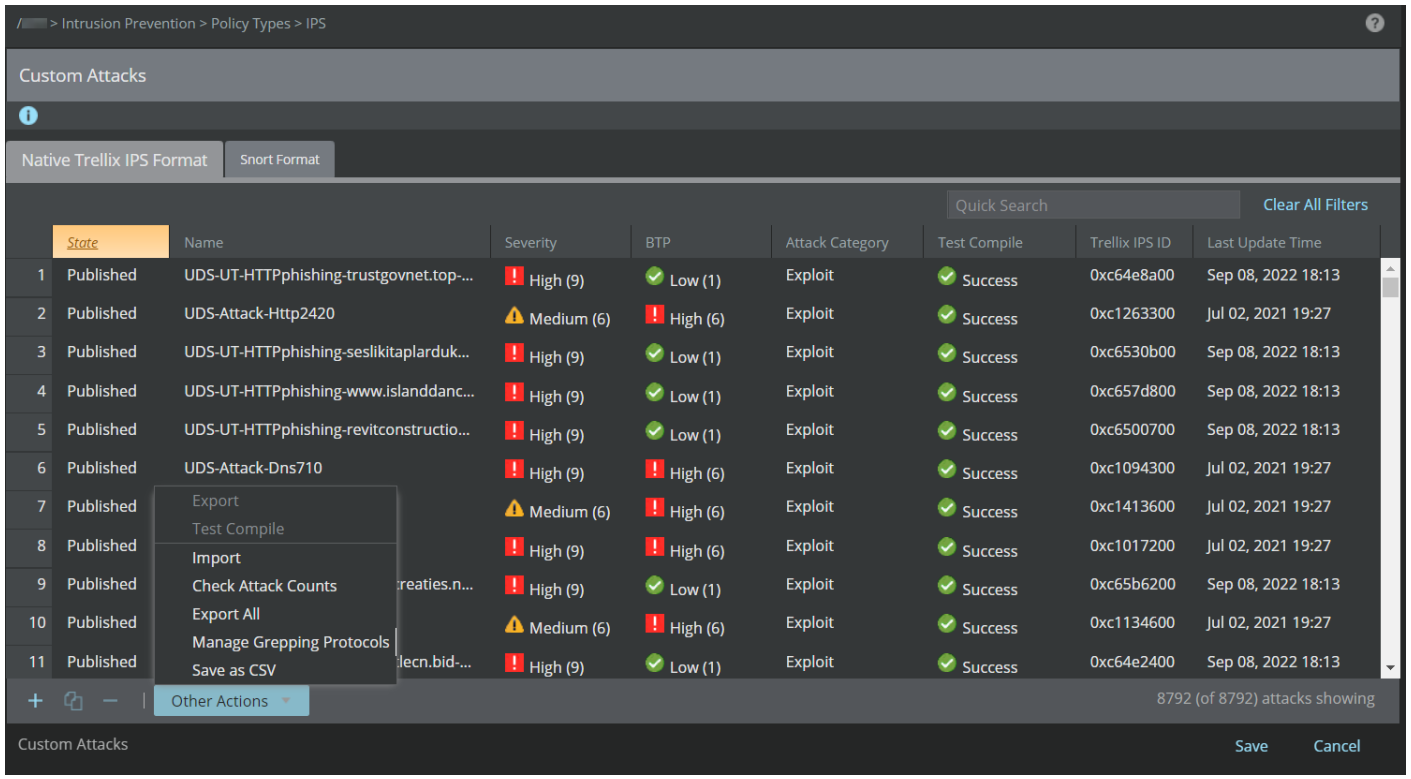
The default page of the Custom Attack Editor has the following areas:

- **Tabs** — All the custom attacks are displayed in tabbed regions in the Custom Attack Editor. There are two tabs in the Custom Attack Editor:
  - **Native Trellix IPS Format** tab is the default tab that is displayed when you launch the Custom Attack Editor. It lists all the Native Trellix IPS Format custom attacks that are currently stored in the Manager server as well as newly created custom attacks.

    You can use this tab to perform the following actions on Native Trellix IPS Format Custom Attacks:
    - Add, copy, or delete
    - Other actions such as:
      - Export
      - Test Compile
      - Import

- Check Attack Counts
- Export All
- Manage Grepping Protocols
- Save as CSV

Figure 758. Native Trellix IPS Format tab

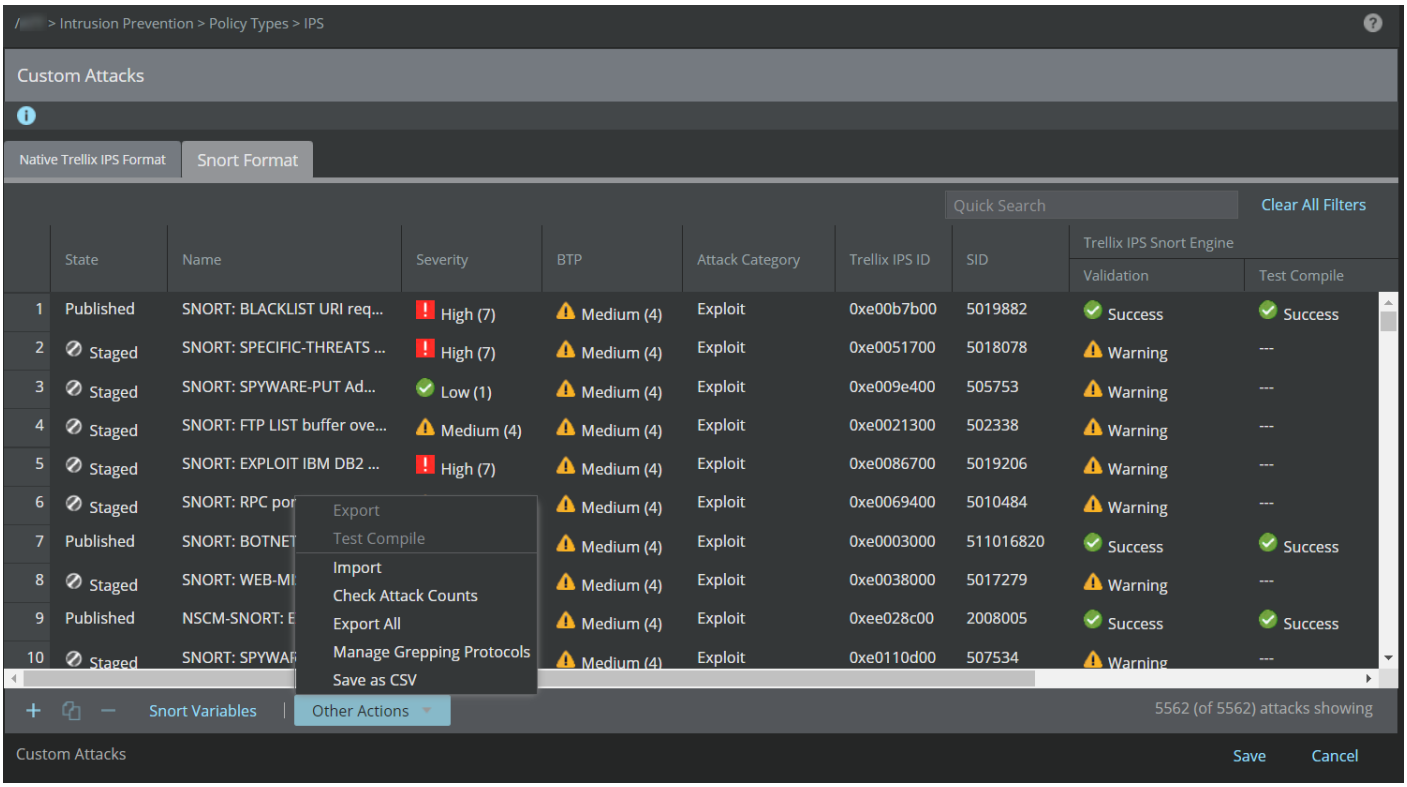


- **Snort Format** tab displays all the Snort Custom Attacks.

  You can use this tab to perform the following actions on Snort Format Custom Attacks:

  - Add, copy, or delete
  - View Snort variables
  - Other actions such as:
    - Export
    - Test Compile
    - Import
    - Check Attack Counts
    - Export All
    - Manage Grepping Protocols
    - Save as CSV

Figure 759. Snort Format tab



- **Regular expression search** — You can use Java regular expressions to ensure a quicker search. The following table shows some of the important expressions that can be used for quick filter option.

Regular expression	Description
^	Matches beginning of line
$	Matches end of line
abc*xyz	String starts with abc and ends with xyz
\A	Beginning of entire string
\z	End of entire string
.	Matches any single character

- **Viewing options** — This area contains the options you can use to list just the custom attacks that you wish to view. These options can be helpful when you are trying to locate specific custom attacks from a large set.

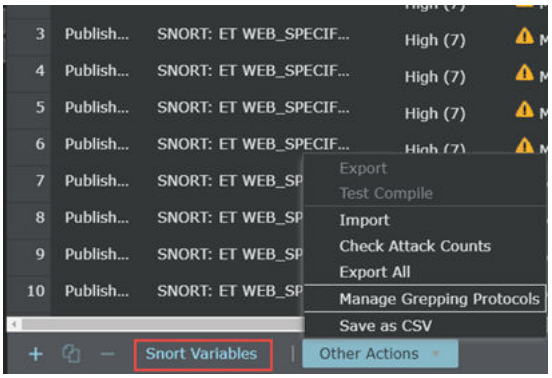
  You can hide a column. You can also modify the way the content is aligned in each of the columns.

- **Menu Options** — The main actions that you can perform in the Custom Attack Editor.
- **Save\Cancel buttons** — These options are used to Save or Cancel the changes that you have made.

Menu items

This section describes the menu options that are available in Custom Attack Editor.

Figure 760. File menu



Option	Definition
Applicable to Native Trellix IPS Format and Snort Format	
+	Click to define a custom attack. You can either create an exploit attack or a reconnaissance attack. You need to create an attack before adding signatures to it.
	Click to copy an existing custom attack.
−	Click to delete the selected attack from the Manager client. To delete it from the Manager server, you need to click **Save** after you delete it from the client.
Export	Select this option to export the custom attacks in the Manager to a file.
Test Compile	Click to Test Compile the selected custom attacks.
Import	Select this menu to import Native Trellix IPS Format or Snort Format custom attack from files to the Manager.
Check Attack Counts	Click to view the count of published custom attacks.
Export All	Click to export all the custom attacks in the Manager to a file.
Manage Grepping Protocols	Click to Manage Grepping Protocols.
Save as CSV	Click to save the custom attacks in CSV format.
Applicable to Snort Format	
Snort Variables	Click to manage Snort Variables.

IMPORTANT

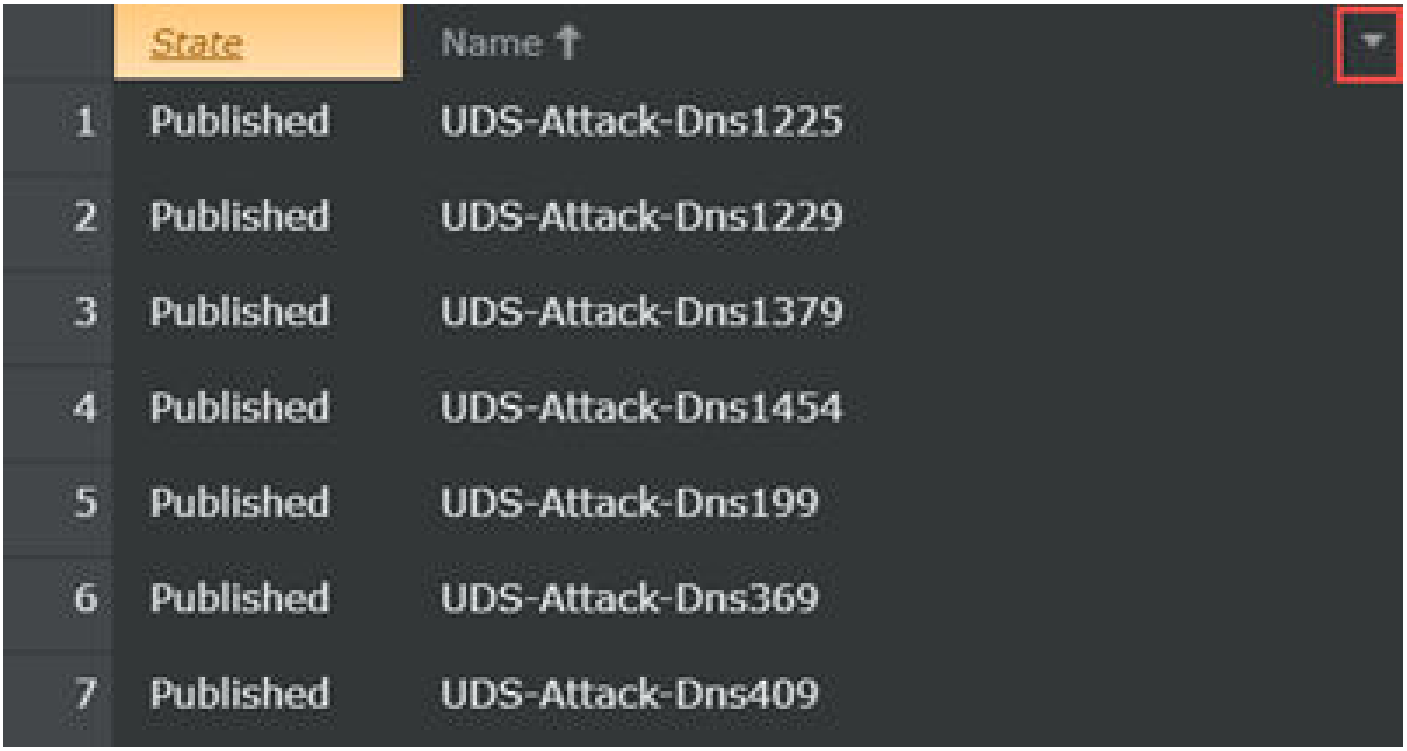
Before you delete a custom-defined protocol, make sure it is not used in any of the Trellix IPS Custom Attacks.

Tab regions

To enable easy viewing, Custom Attacks are listed in tabbed regions in the **Custom Attack Editor**. The **Native Trellix IPS Format** tab is the default tab that is displayed when you launch the **Custom Attack Editor**. It displays all the Native Trellix IPS Format custom attacks. The **Snort Format** tab displays all the Snort Custom Attacks.

You can click on a column heading and drag-and-drop it to suit your viewing preference. Click on the arrow at the end of the column heading to:

- Hide the column
- Display any hidden columns
- Sort or filter the contents in the column



NOTE

What you see in the figure below are the default column headings.

Figure 761. Tab regions

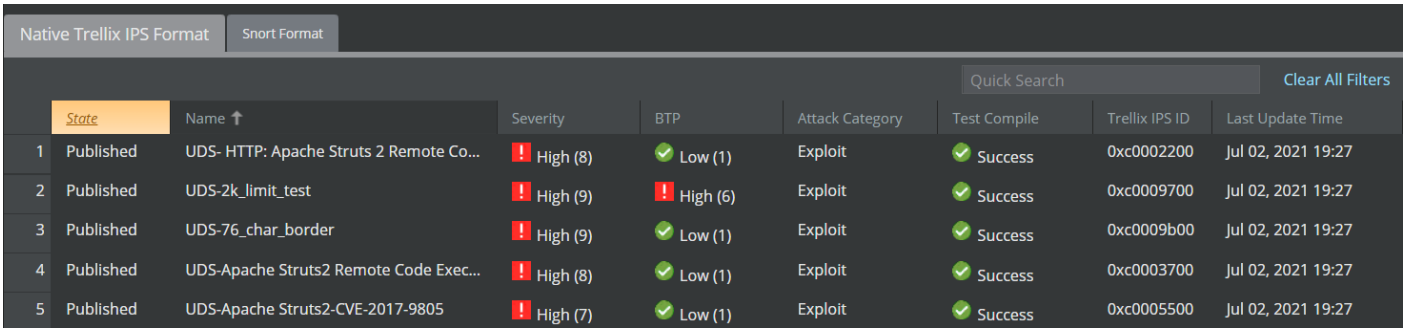


Table 93. Tab regions

Item	Description
Trellix IPS ID	When you save the added/imported custom attacks to the database, the Manager assigns a unique attack ID to each rule. For native Trellix IPS attacks, the ID starts with 0xc and for Snort attacks, it starts with 0xe. **NOTE** Until you save the newly-added attacks to the Manager database, they are assigned the same temporary ID.
SID	Snort rule ID (SID) is the ID assigned to a Snort rule by you or the party that provided the rule. The Snort attack definitions that you want to save in the Trellix IPS database must have a unique SID. Make sure that the SIDs of the attacks that you are writing or importing have not been used by the definitions that are already in the database. For attack definitions that failed to import, the Trellix IPS assigns -1 as the SID.
Trellix IPS Snort Engine	The imported rules are available for both the Trellix IPS Snort and the Suricata Snort. This column indicates whether the rule was validated successfully. Some rules may have been converted but with warnings. For example, rules for which an equivalent Trellix IPS signature exists are converted with warnings. Some rules may have failed to convert. For example, rules that use undefined variables fail to convert. The **Validation** field displays status of attack validation from the Trellix IPS Snort Engine. Validation results can be Success, Failed, or Warning. The **Test Compile** column displays the status of test compilation.
Suricata Snort Engine	The **Validation** column displays status of attack validation from the Suricata Snort Engine. Validation results for the Suricata Snort rules can be Success or Failed.
Last Updated Time	This is the time stamp when a rule was imported or modified.

Item	Description
State	This column indicates whether a rule will be published and therefore made available for inclusion in the IPS policies. You can click on a rule to publish or stage it. **NOTE** • If you publish a Snort rule that overlaps with a native Trellix IPS attack definition, you can expect two alerts to be generated for the same rule. • Only the **Published** rules are considered for inclusion in the IPS policies. For more information, see the tables *Rules for determining the state of a Custom Attack in Native Trellix IPS format* and *Rules for determining the state of a Custom Attack in Snort format below*.
Name	The name for the attack that the Manager assigns post-import. The format that the Manager uses for the name is SNORT:<the text specified for the msg rule option in the rule> (<SID>). So this name is modified accordingly if you modify the msg text or the SID of the rule. Note that msg rule option and a unique SID are required in a rule for you to import it into the Manager.
Severity	The Manager assigns a severity of Low, Medium, or High based on the priority value of the rule. • A priority 1 Snort attack definition is assigned a severity of High. • A priority 2 Snort attack definition is assigned a severity of Medium. • A priority of 3 or higher is assigned a severity of Low. You can set the priority for a rule by using the priority keyword in the rule definition. If the priority keyword is not present in the rule, the Manager derives the priority value based on the classtype of the rule. However, if the classtype is not available for the rule and there is no priority set in the rule definition, the Manager assigns a priority value of 0 to the rule. **TIP** Severity is often used in attack set profiles to include/exclude attacks from IPS policies. To ensure inclusion of a rule in a policy, assign a Severity value as per the policy profile settings.

Item	Description
BTP (Benign Trigger Probability)	This column indicates the possibility of producing false positives. The lower the BTP value, higher is the accuracy of the rule. **TIP** BTP is often used in attack set profiles to include/exclude attacks from IPS policies. To ensure inclusion of a rule in a policy, assign a BTP value as per the policy profile settings.
Attack Target	This column indicates the type of attack target such as client, server, and so on.
Test Compile	This column indicates the compilation status of the attack.
Attack Category	This column indicates the category of the attack such as malware, exploit, policy violation, and so on.
Protection Category	Indicates the Protection Category to which the Trellix IPS Custom Attack belongs. You specify this when you create a Trellix IPS Custom Attack.
Supported Device Types	This column indicates the supported devices for the Snort Rule.

NOTE

The columns **SID**, **Trellix IPS Snort Engine**, and **Suricata Snort Engine** are available only on the **Snort Format** tab.

Table 94. Rules for determining the state of a Custom Attack in Native Trellix IPS format

State of the Custom Attack	Trellix IPS Snort Engine Validation Status	Test Compile Status
Published	Success	Success
Published	Warning	Success
Staged	Warning	Failed
Staged	Failed	Pending
Staged	Success	Failed

Table 95. Rules for determining the state of a Custom Attack in Snort format

State of the Custom Attack	Trellix IPS Snort Engine Validation Status	Test Compile Status	Suricata Engine Validation Status
Published	Success	Success	Success
Published	Success	Failed	Success
Published	Success	Success	Failed
Published	Failed	Pending	Success
Published	Warning	Success	Success

State of the Custom Attack	Trellix IPS Snort Engine Validation Status	Test Compile Status	Suricata Engine Validation Status
Published	Warning	Failed	Success
Staged	Warning	Success	Failed
Staged	Warning	Failed	Failed
Staged	Failed	Pending	Failed
Staged	Success	Failed	Failed

View options

Various options are available on the tabs of the Custom Attack Editor to enable you to easily locate the information that you require. The options are:

- Sorting based on column values
- Group By
- Display Filter

Sorting Assending/Descending — You can sort the list of Custom Attacks based on the values of one or more columns. This can be in the ascending or descending order for the selected columns.

To sort the display information based on a column, click on the column heading. To base it on multiple columns, click on the required column headings (in the order that you want).

Group By this field — This option enables you to view the aggregate attack count based on certain values. For example, out of the attacks listed in a tab view, you can view the number of high, medium, and low-severity attacks.

Filter — To locate custom attacks based on values such as severity and conversion result, you can just sort the listed attack definitions based on these values by clicking on the corresponding column heading. For advanced search capabilities, you can use the Display Filter feature. You can create a display filter with a set of criteria to view only those attack definitions that meet the criteria. For example, you can locate attack definitions based on what is contained in the attack names. This way you can easily locate specific attack definitions from a larger set.

NOTE

A Filter that you define is always applied to the attacks listed on the both the tabs and not just to the attacks on the currently selected tab.

Attack creation interfaces

As discussed earlier, there are two types of custom attack definitions: Native Trellix IPS Format custom attack and Snort Format custom attack. The methods to create these two types of attacks are different. So, the interfaces where you define them also differ accordingly. This section describes these interfaces in detail.

Trellix IPS custom attack creation interfaces

To access the Trellix IPS Custom Attack creation interface:

1. In the Custom Attack Editor, Click  .

The New Custom Attack creation interface presents information related to naming, describing, and categorizing the attack. You can either create an Exploit Attack or a Reconnaissance Attack.

Attack tab

The **Attack** tab enables you to name your attack and type a description.

Option	Definition
State	Select the state of the custom attack. The choices are **Published** and **Staged**.
Name	The name you assign to the attack. "UDS" is automatically prefixed before every created attack name. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor, as well as in the attack database when you subsequently save the attack in the Manager server.
Description	Use this area for notes and other pertinent information. **TIP** We recommend that you enter useful information in the **Description** field for easy future reference.
Severity	Select a severity from the drop-down list. Choices are as follows: • High (most severe): High severity is divided into three categories — High 9, High 8, and High 7. • Medium: Medium severity is divided into three categories — Medium 6, Medium 5, Medium 4. • Low (least severe): Low severity is divided into three categories — Low 3, Low 2, and Low 1.

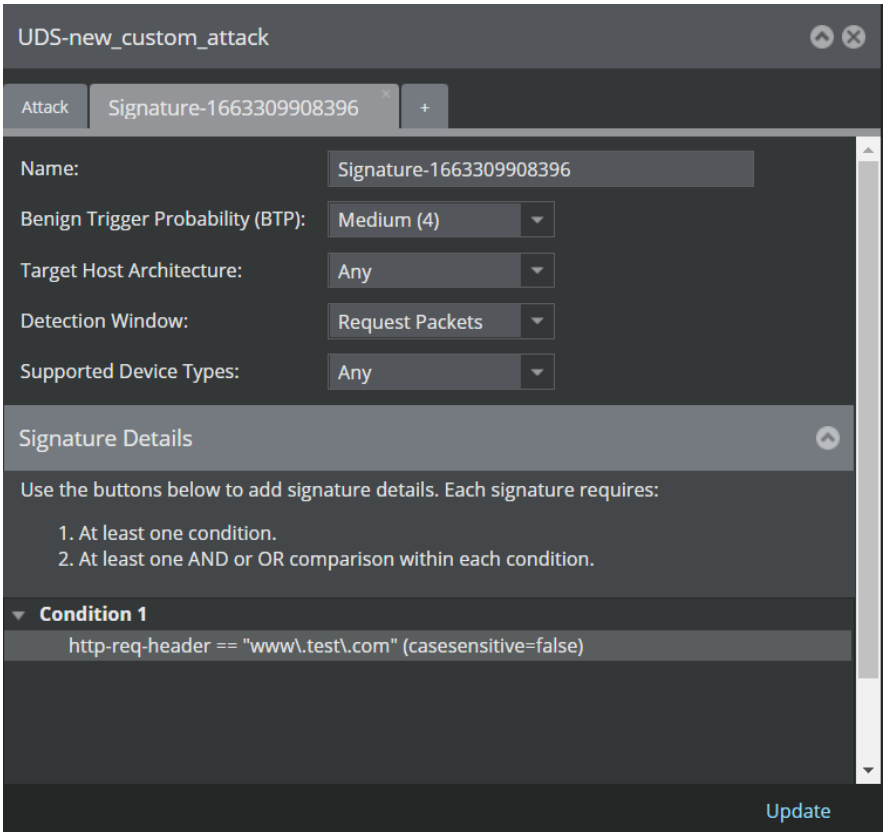
Option	Definition
Protection Category	You must choose a Protection Category from the available options. The Protection Category indicates the intent of the attack and the intended target. For example, you can choose **Client Protection/Operating Systems** for an attack targeting vulnerabilities in client operating systems. In this example, Client Protection is the category and Operating Systems is a subcategory. The list of Protection Categories is pre-defined and provided by Trellix Advanced Research Center. You cannot modify it. This list is updated when you update the Signature Set.
Detection Type	Select the type of detection from the options that relisted.
Attack Target	Select the appropriate attack target.
Blocking	Select the appropriate blocking. You can either block only the attack packet or the entire flow.
Non-editable Fields	
Benign Trigger Probability	This is an indication of the probability that the Snort Custom Attack will alert on traffic that may not be an attack. The default value is Medium, which you cannot modify.
Attack Category	This column indicates the type of attack.
Trellix IPS ID	The numeric ID assigned for the attack by the Manager for database archival. The Manager assigns the ID after you save it in the Manager server. For Snort Custom Attacks, the IDs begin with 0xe. For Snort Custom Attacks created in the Central Manager, the IDs begin with 0xee.
Supported Device Types	You can apply a Custom Attack signature for just the available device types. The value for this field depends on what you select for the corresponding rule. You cannot edit this field at the attack level, but the Manager modifies it accordingly when you change it for the corresponding rule.
Last Updated	Displays the time at which the signature was last updated

Signature creation interface

After you define the details for a Trellix IPS Custom Attack, you need to define one or more signatures for that attack. To access the signature creation interface, in the **New Custom Attack** interface, click on the **Signature-<signature name>** tab.

The signature creation interface presents the details related to the signature you are creating. These details are used to provide further information about the suspicious activity for which you are attempting to capture and analyze through Custom Attacks. By configuring each field, you are further refining the signature's search, which raises the probability your attack will successfully detect the desired activity, thus preventing false positives.

Figure 762. New Signature window



The signature detail fields are as follows:

Option	Definition
Name	The name you give to the signature. If the attack is detected, the Attack Log displays the detecting signature in the attack's details window.
Benign Trigger Probability (BTP)	This is an indication of the probability that your signature will alert on traffic that may not be an attack. The choices are High, Medium, and Low, with Low representing approximately a 0% to 33% chance of your signature raising a false positive. For example, your signature may be a generic string search, such as "Confidential", thus the BTP would be best graded as High. If you know a specific file name that is infected or sensitive, such as "program.exe", you could set your BTP to Low to reflect your confidence in your signature.
Target Host Architecture	You can define a specific machine architecture targeted by an attack with shellcode. For example, to detect a Intel-specific shellcode, you can select i386 as the architecture. The default is **any**.

Option	Definition
Detection Window	This field describes where in a flow you want your signature to actively check traffic. The choices are as follows: • **Single Packet** — Check each packet for your signature condition(s). If your condition is xyz, and the Sensor sees xy in one packet and z in the next, no alert is generated. Each condition you specify must be found in one packet. • **Request Packet** — Check only the request direction of a flow. • **Response Packet** — Check only the response direction of a flow. • **Entire Flow** — Check the entire flow (between two hosts) for your condition(s). If your condition is xyz, and the Sensor sees xy in one packet and z in the next of the same flow, an alert is generated.
Supported Device Types	You can apply a Trellix IPS Custom Attack signature for any of the following device type options: • **NS-Series Only** • **VM-Series Only** • **Any** The value for this field depends on what you select for the constituent signatures. For example, if the attack contains signatures with **Supported Device Types** set only to NS-series, then the value displayed here is **NS-series Only**. You cannot edit this field at the attack level, but the Manager modifies it accordingly when you change it for the corresponding signatures.
Conditions	A condition is the test or group of tests that, if met, raises an alert. Conditions are made up of protocol field tests, or comparisons. A signature may have multiple conditions, each with multiple comparison tests. If you configure multiple conditions for a signature, each condition must be met in order (ANDTHEN logic) before an alert is raised. • + — Add a new condition. • − — Delete a selected condition.
Comparisons	Within a condition, you add one or more comparison tests. Comparisons can be AND or OR in nature. AND comparisons must be met for an alert to be generated for malicious traffic. OR comparisons allow for multiple comparisons within a condition, of which only one of the OR tests must be met to raise an alert. You must start a condition with an AND comparison. You may have up to 32 comparisons per condition. • AND — Add an AND comparison. • OR — Add an OR comparison. You must have already added an AND comparison. • × — Delete a selected condition.

Snort custom attack interfaces

You create Snort Format custom attacks using the Snort Rules Language. When you write a Snort rule in the Custom Attack Editor and save it in the Manager server, an attack definition is automatically created and the rule associated with this attack.

Interface to write Snort rules

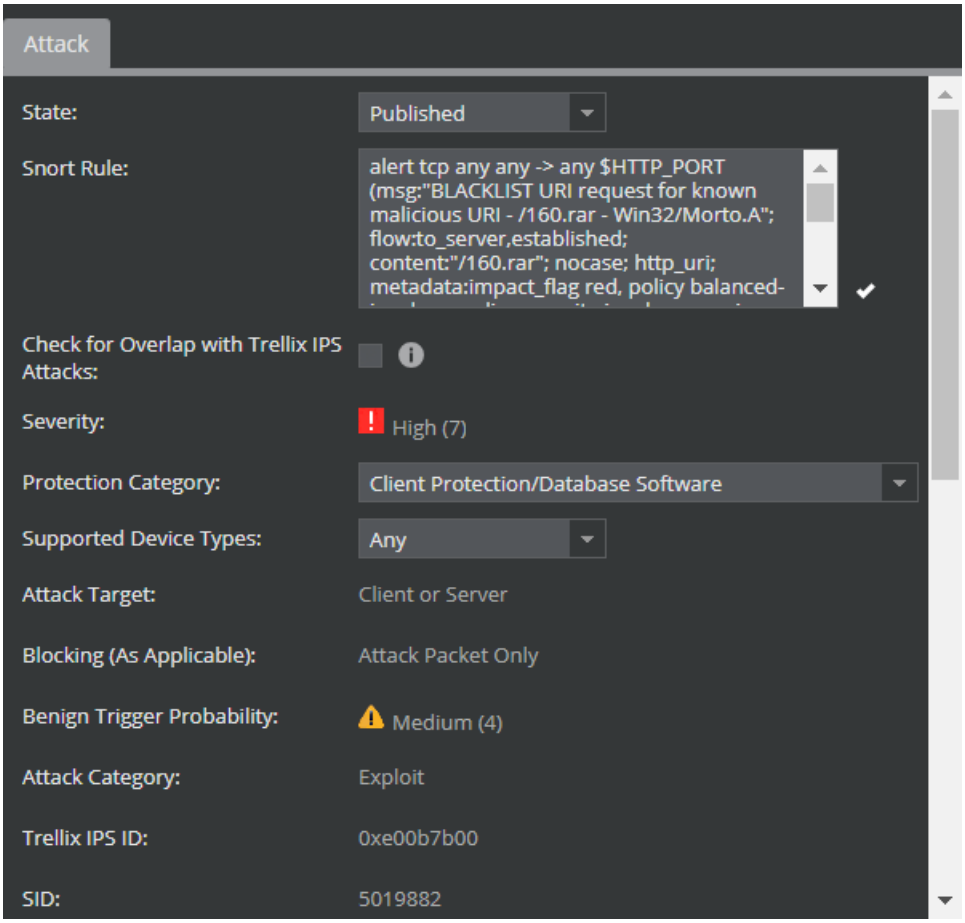
The interface for writing a Snort rule is a free-text editor within the Custom Attack Editor. To access the Add Snort Rule editor in the Custom Attack Editor, click the **Snort Format** tab.

Enter the Snort rule in the Add Snort Rule editor and click **Save**. The rule and the associated Custom Attack are saved in the Manager client. You can view this attack on the currently selected tab as well as on the **All Custom Attacks** tab.

Interface to edit snort custom attacks

To access the **Edit Snort Attack** interface, click a Snort Custom Attack .

Figure 763. Edit Snort Attack window



When you create a Snort rule in the Manager, based on the elements of the rule, the Manager assigns values to some of the fields. If you modify the rule in the **Raw Snort Rule Text** section, the Manager modifies the field values accordingly. For example, if you change the msg in the rule, the attack and signature names also change because the Manager assigns the attack and rule names as per the msg keyword in the rule.

NOTE

Every time you modify the rule in the **Raw Snort Rule Text** section, you need to check if the rule is conforming to Snort rules syntax by clicking ☑. After the Manager translates the rule to Trellix IPS's format, click **Save** to save the changes in the Manager client. The changes are saved in the Manager server only when you click **Save** in the Custom Attack Editor.

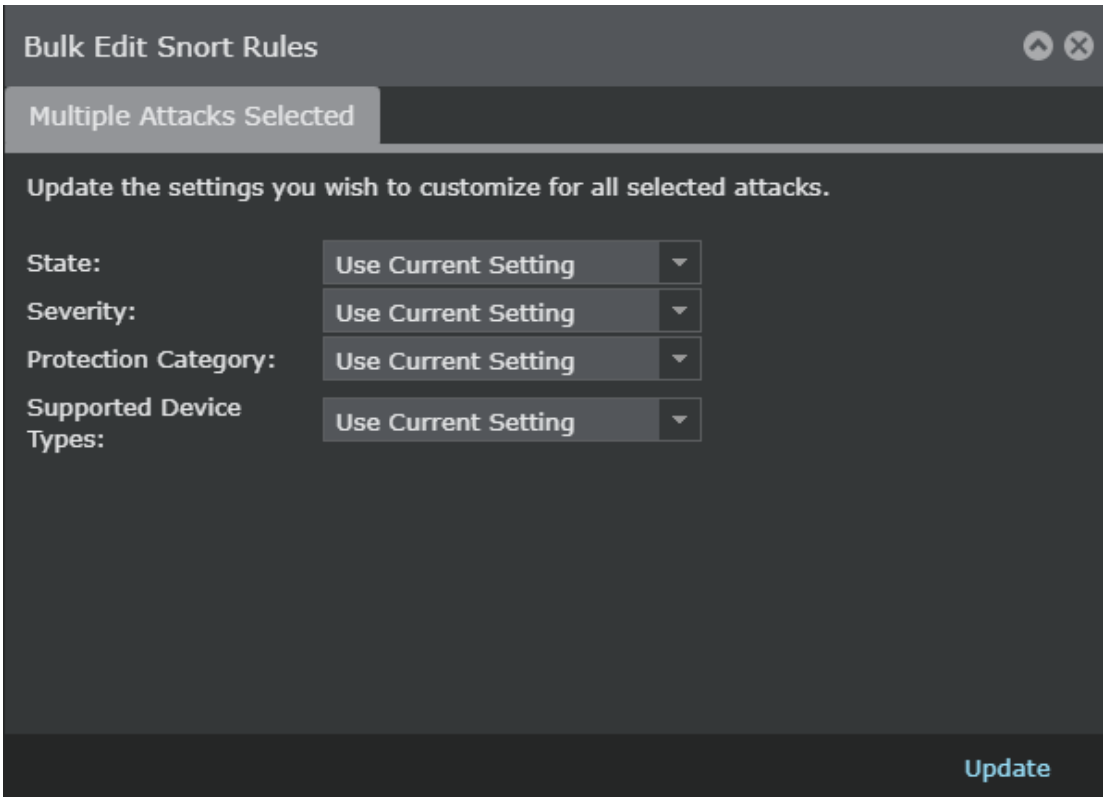
The following the fields displayed on the **General** tab for a Snort Custom Attack:

Option	Definition
Editable Fields	
State	Select the state of the custom attack. the choices are **Published** and **Staged**. • Published — An attack in the Published state means that it is published in the policies of Trellix IPS. • Staged — An attack in the Staged state means that it is not published in the policies of Trellix IPS.
Snort Rule	You can modify the rule in this section.
Check for Overlap with Trellix IPS Attacks	Verifies if the rule matches an existing Trellix IPS attack definition. If the rule matches then the Snort Rule will be **Staged**.
Protection Category	Displays the Protection Category assigned to the attack. The Protection Category indicates the intent of the attack and the intended target. The list of Protection Categories is pre-defined and provided by Trellix Advanced Research Center. You cannot modify it. This list is updated when you update the Signature Set.
Attack Target	Indicates the target that is being exploited
Supported Device Types	You can apply a Snort Custom Attack signature for just the NS-series Sensors or Virtual IPS Sensors, or for both of them. The value for this field depends on what you select for the corresponding rule. You cannot edit this field at the attack level, but the Manager modifies it accordingly when you change it for the corresponding rule. By default, you can apply up to 5000 per NS-series and Virtual IPS Sensors.
Non-editable Fields	
Severity	This priority is derived from the classtype or the priority tag.
Attack Target	This column indicates the target that is being exploited.
Blocking (As Applicable)	In case of Snort Custom Attacks, the Sensor drops just the packet that matches the rule. You cannot edit this field.
Benign Trigger Probability	This is an indication of the probability that the Snort Custom Attack will alert on traffic that may not be an attack. The default value is Medium.
Attack Category	This column indicates the type of attack.
Trellix IPS ID	The numeric ID assigned for the attack by the Manager for database archival. The Manager assigns the ID after you save it in the Manager server. For Snort Custom Attacks, the IDs begin with 0xe. For Snort Custom Attacks created in the Central Manager, the IDs begin with 0xee.

Option	Definition
SID	Snort rule ID (SID) is the ID assigned to a Snort rule by you or the party that provided the rule. The Snort attack definitions that you want to save in the Trellix IPS database must have a unique SID. Make sure that the SIDs of the attacks that you are writing or importing have not been used by the definitions that are already in the database. For attack definitions that failed to import, SID is set to -1.
Trellix IPS Snort Engine	The **Validation** field displays status of attack validation from the Trellix IPS Snort Engine. The **Test Compile** field displays the status of test compilation.
Suricata Snort Engine	The **Validation** field displays status of attack validation from the Suricata Snort Engine.
Last Updated	This is the time stamp when a rule was imported or modified.

To access the **Bulk Edit Snort Rules** interface, select multiple snort rules by pressing the **Ctrl** key.

Figure 764. Bulk Edit Snort Rules window



The following the fields displayed on the **General** tab for a Snort Custom Attack:

Option	Definition
State	This column indicates whether a custom attack is published in the Trellix IPS policies. This column can have one of the following values: • Published — An attack in the Published state means that it is published in the policies of Trellix IPS. • Staged — An attack in the Staged state means that it is not published in the policies of Trellix IPS. • Use Current Setting — Retains the current value
Severity	Select a severity from the drop-down list. This column can have one of the following values: • High (most severe): High severity is divided into three categories — High 9, High 8, and High 7. • Medium: Medium severity is divided into three categories — Medium 6, Medium 5, Medium 4. • Low (least severe): Low severity is divided into three categories — Low 3, Low 2, and Low 1. • Informational: Informational has 0. • Use Current Setting: Retains the current value
Protection Category	You must choose a Protection Category from the available options. The Protection Category indicates the intent of the attack and the intended target. For example, you can choose **Client Protection/Operating Systems** for an attack targeting vulnerabilities in client operating systems. In this example, Client Protection is the category and Operating Systems is a subcategory. The list of Protection Categories is pre-defined and is provided by Trellix ARC. You cannot modify it. This list is updated when you update the Signature Set.
Supported Device Types	You can apply a Snort Custom Attack signature for just NS-series Sensors or Virtual IPS Sensors, or for both of them. The value for this field depends on what you select for the corresponding rule. By default, you can apply up to 5000 Snort signatures per NS-series Sensors and Virtual IPS Sensors. This column can have one of the following values: • **NS-Series Only** • **VM-Series Only** • **Any**

Matching Criteria section

The **Matching Criteria** section enables you to categorize your attack for eventual submission to your Manager's attack database. Once exported to the attack database, selection of your attack is published by one of several rule sets, which are then added to policies for enforcement.

A rule set is defined as a set of ordered rules used to determine what attacks or conditions are of interest, and thus should be monitored when applied as part of a policy. A rule set is configured based on attack category (Exploit, Reconnaissance), operating system (Windows, UNIX), protocol (HTTP, DNS), application (SendMail, Apache), severity (High, Low), and benign trigger probability (High, Low) options. Except for benign trigger probability, you need to indicate these options when defining at the attack level. You can indicate the value for benign trigger probability when creating the signatures for an attack definition. Based on the values that you set for these options, the attack is available for policy enforcement.

- **Protocol** — This is the identified impact protocol for the Snort Custom Attack.
- **Software Package (OS)** — Manager assigns tcpip-machine to all Snort Custom Attacks. You cannot edit this value.

Packet Grep protocol interface

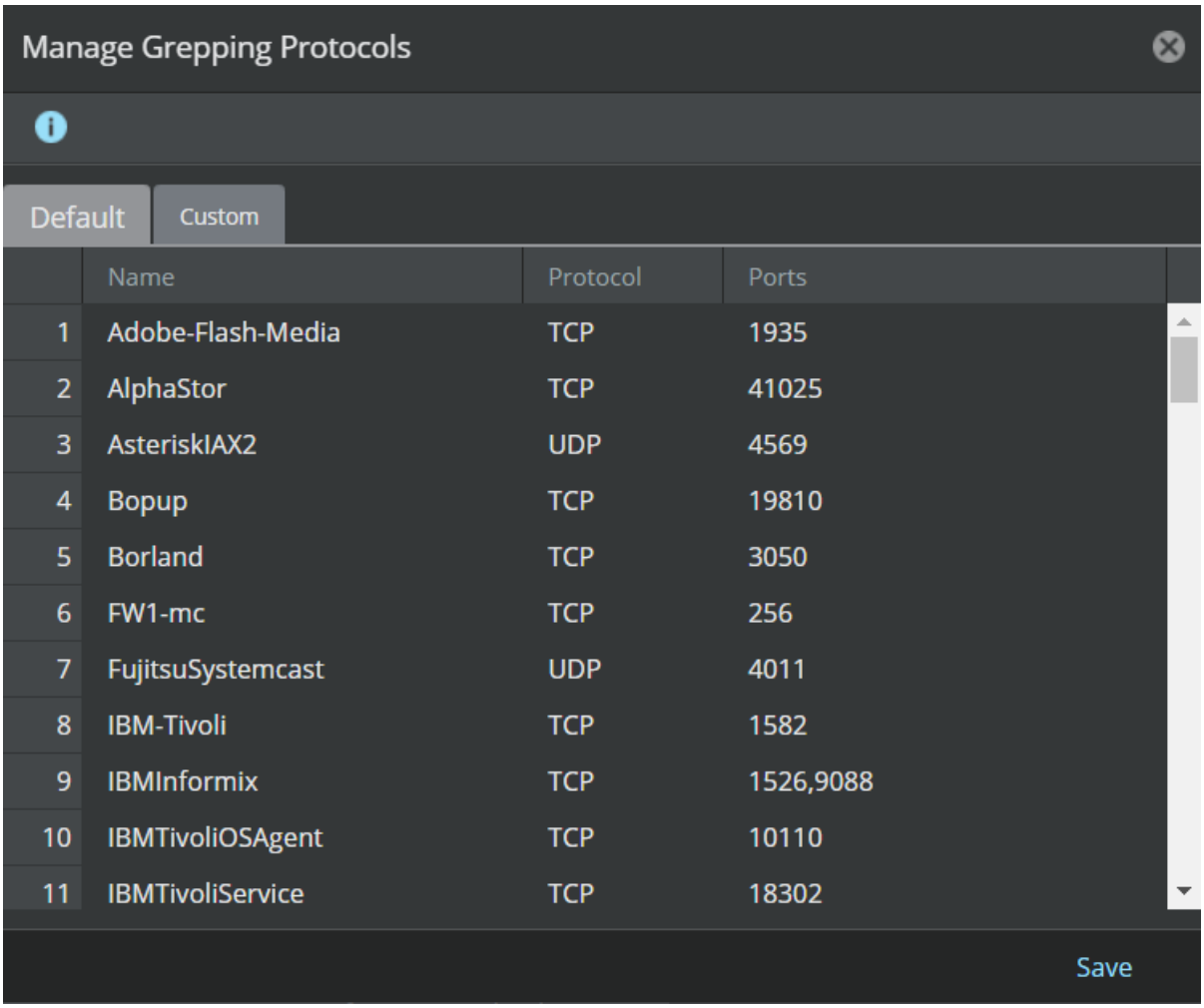
Not all traffic can be supported by standardized protocol specifications. There are cases that require a different means of identifying an attack based on packet grepping. Trellix IPS has a pre-defined list of packet grep protocols. You can view this list of protocols in the Packet Grep interface. Using this interface, you can also create packet grep protocol in case the one that you need is not in the list of Trellix IPS-defined packet grep protocols.

To access the Packet Grep protocol interface in the Custom Attack Editor, select Other Actions → **Manage Grepping Protocols**.

Trellix IPS default protocols

The Default section displays applications which support TCP, UDP, and IP that are commonly used/allowed, but do not use a standardized protocol and may be used for malicious purposes. The Custom Attack Editor enables you to monitor usage of programs such as NetMeeting and PCAnywhere in order to prevent external attacks. For example, your security policy may allow the use of PCAnywhere to resolve desktop/server issues remotely, but the program can also be used to infiltrate your network and perform malicious acts. The Custom Attack Editor enables you to create a pattern-matching signature for responses or requests to/from any of the listed programs for monitoring purposes.

To create a signature for any of these instances, simply create a signature instance, and select Packet Grep Protocol Match as a comparison for a condition.



Custom-defined packet grep protocols

Custom-defined packet grep protocols section is where you can view the list of custom-defined packet grep protocols and also create new ones. Custom-defined packet grep protocols can be used when creating a Native Trellix IPS Format custom attack with **Text in Custom Application** template.

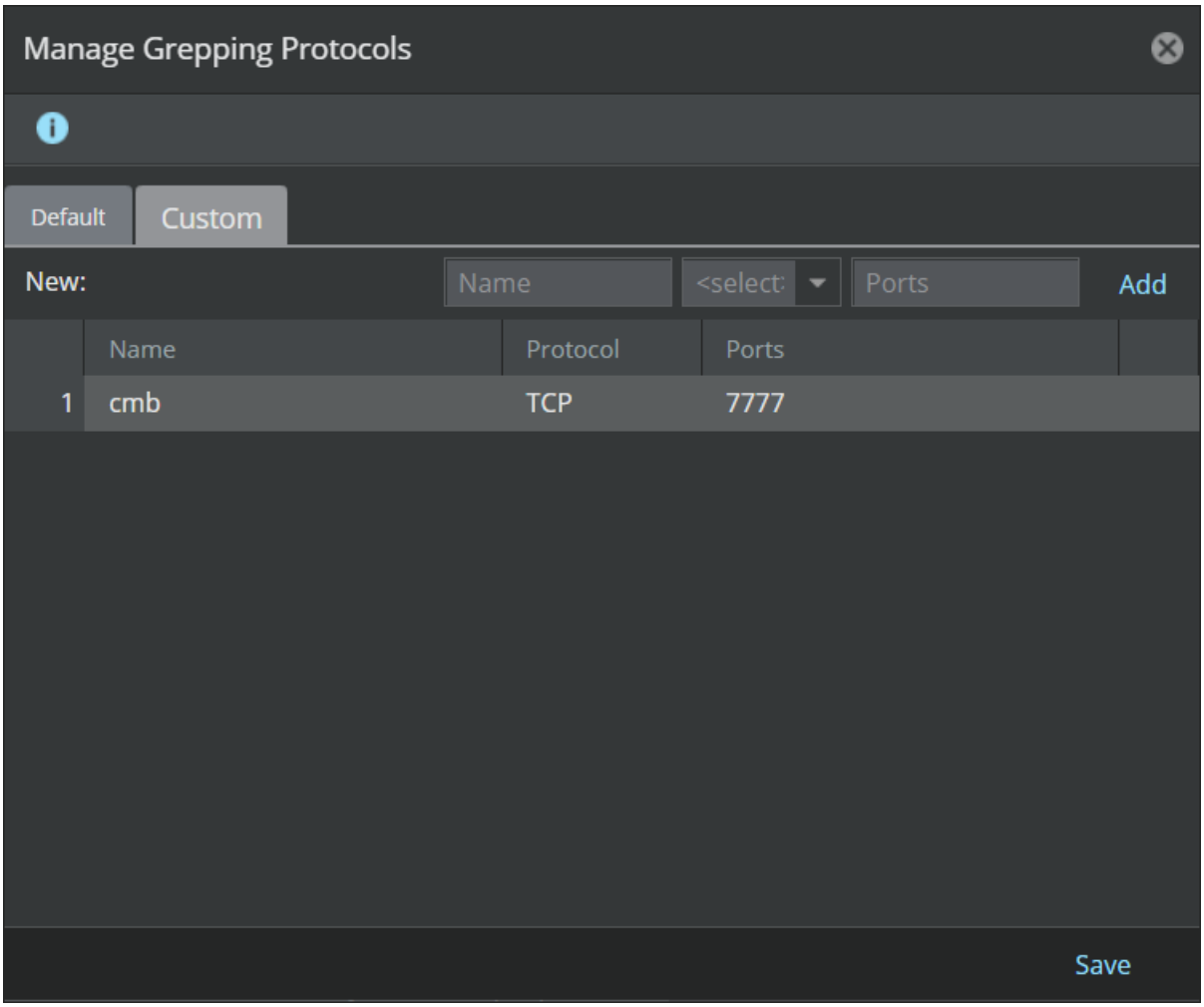
- Add

  — Add a new packet grep protocol instance.

- × — Delete a created instance.

> **NOTE**
>
> You cannot modify a default custom-defined packet grep protocol.

Figure 765. Custom-defined Packet Grep Protocols window



When you add a packet grep protocol, you need to specify the transport layer protocol and the identifying port(s) for locating those attacks that use an application protocol unknown to Trellix IPS.

The interface fields and options are as follows:

- **Name** — Name displayed during selection. For example, type "Custom-Adobe-Flash" for the Name.
- **Transport Protocol** — Specify the transport protocol that will be used by the application whose protocol details that you are defining.
  - TCP
  - UDP
- **Ports** — Target ports that have been added for the current custom protocol. Type the number in this field, and then click **Add** to add a port that can be used to identify the unknown traffic.

> **NOTE**
>
> Do not enter any standard port number.

Other Actions

Following are the other actions that can be performed using the custom attack editor.

Work with packet search protocol

This section deals with creating a packet search protocol and a signature using your new packet search protocol.

Create a packet search protocol

Not all traffic can be supported by previously defined protocol specifications. Thus, in some cases, you may need to define a different means of separating out certain protocol traffic. The Packet Grep Protocol feature (Packet Search > Manage Packet Search Protocol) enables you to create pattern matching searches in a particular protocol traffic that is not separately parsed.

Packet searching is commonly known as packet grepping. The term grep refers to the Unix command "g/re/p," which executes a global search for a regular expression, and prints the lines that contain pattern matches. In essence, a protocol packet grep is a search for a fixed pattern in either the request or response of an unsupported protocol flow.

Protocols, such as HTTP and FTP, have defined specifications and destination ports. For example, HTTP primarily uses port 80, but is also common on port 8080. A Sensor monitoring traffic identifies the HTTP traffic by the protocol's common traits, and checks the traffic against standardized (RFC) HTTP traffic specifications. If packets are determined to be suspicious through signature tests, an alert is sent from the Sensor to the Manager. In the event that a Sensor does not recognize the protocol of a monitored transmission through signature, anomaly, or packet search tests, the packets are sent to a general state machine and examined against user-configured pattern-matching checks. If a pattern is matched, an alert is raised.

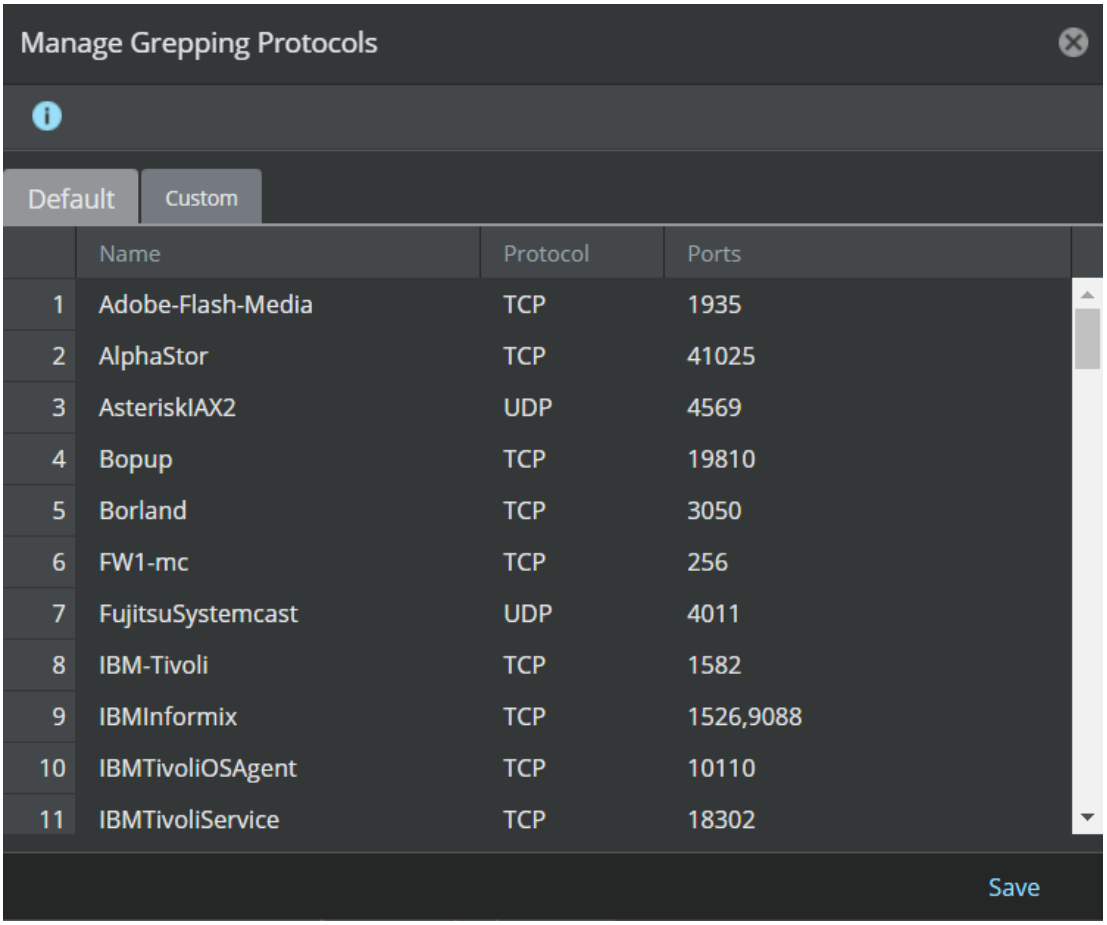
For example, port 1387 on one of your Payroll servers is receiving undetermined protocol connection requests atop TCP. You have confidential information on this server, so protecting your data from suspicious searches or requests is crucial. You can create a packet search instance in requests via TCP to port 1387, then create a Trellix IPS Custom Attack that defines a regular expression pattern that alerts upon being matched.

Several packet search protocol instances are provided with Trellix IPS. These applications use protocols that are not defined by an RFC nor by a defined Trellix IPS protocol specification. Some of these instances, such as pcAnywhere and NetMeeting, represent legitimate applications that are allowed by network policy within/into some networks, but which may be used for malicious purposes.

NOTE

You cannot delete any of the Trellix IPS-defined packet grep protocols.

Figure 766. Manage Grepping Protocols window



Create a packet search protocol instance

Several packet search protocol instances are provided with Trellix IPS. You can create a packet search protocol instance. These applications use protocols that are neither defined by an RFC nor by any Trellix-defined protocol specification.

Steps:

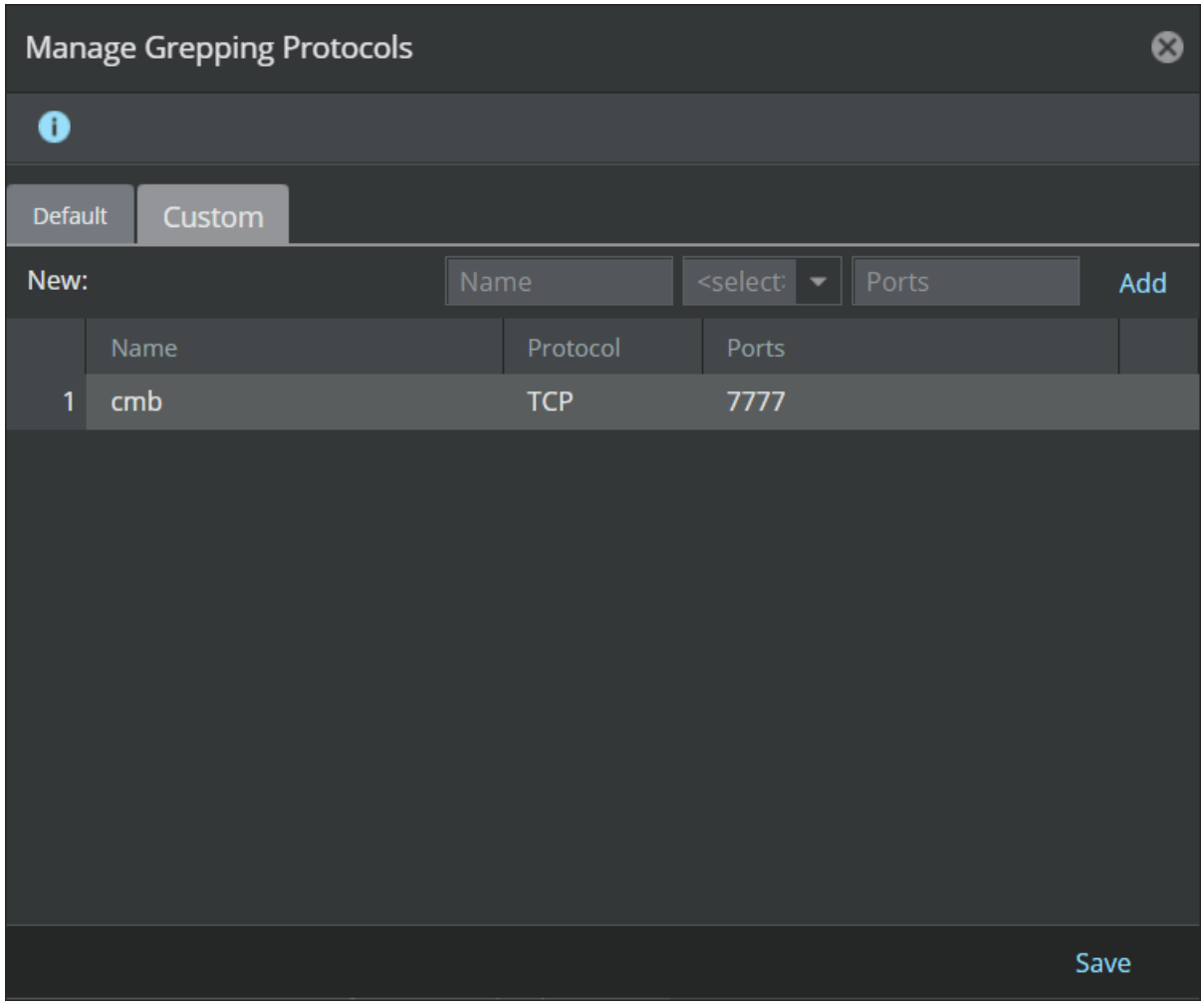
1. In the Custom Attack Editor, select Other Actions → **Manage Grepping Protocols**.

   The **Manage Grepping Protocols** dialog box opens.
2. Go to **Custom** tab.
3. Type a name. This name is listed in the "Select Protocol" step during signature creation.

   Type a verbose name. This name is for reference purposes.
4. Select the transport protocol as either **TCP** or **UDP**.
5. Type a port number in the **Ports** field, then click **Add**. Repeat for multiple port numbers.

NOTE

You cannot add a port number that is already used by a defined protocol, such as 21 (FTP) or 80 (HTTP). Also, if you create a packet grep instance for port 888, you cannot create another packet grep instance for that port.



6. Click **Save** when finished.
7. Create a new signature instance that utilizes your created packet grep instance.

Create a signature using your new packet search protocol

Prerequisite:

Create a Trellix IPS Custom Attack definition and in the **Matching Criteria** section and select **tcpip-machine** as the **Software Package**.

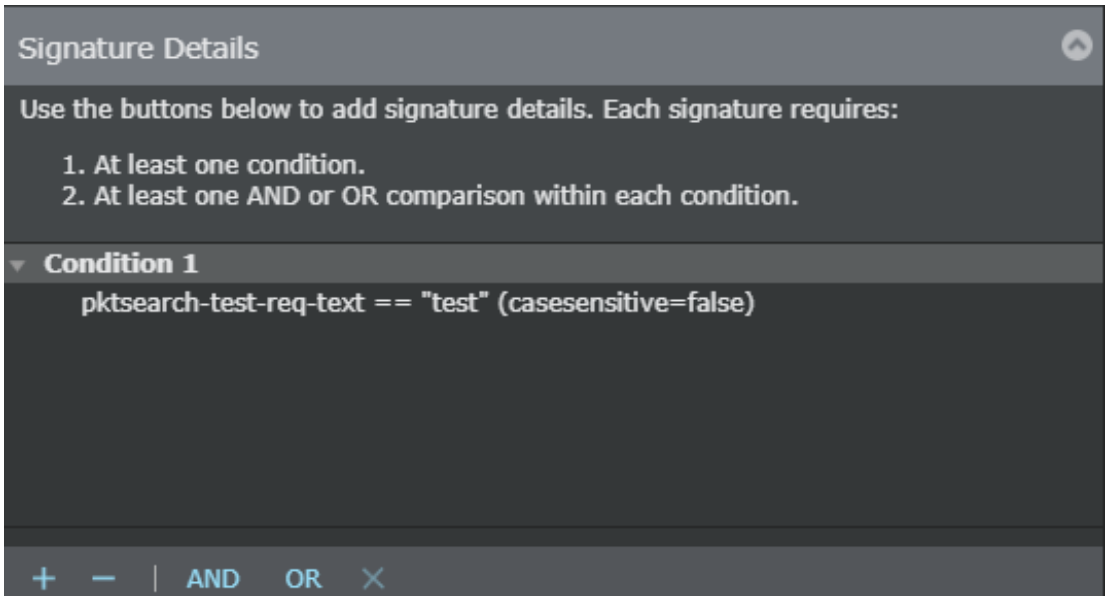
Steps:

1. Click **Signature-<Signature ID>** tab.

   The **Signature Details** section is visible.

2. Add a comparison with at least one condition. Do the following:
   a. Click **Condition 1** so that it is highlighted.

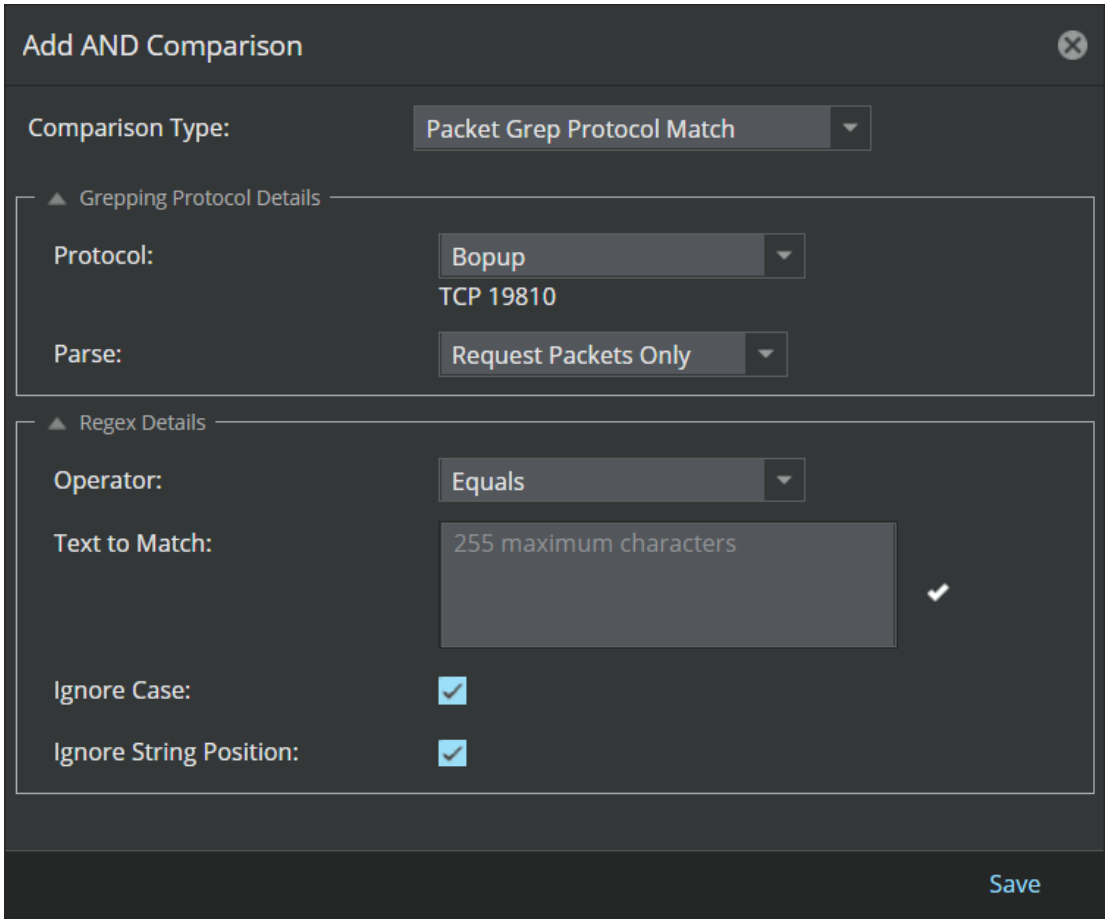
Figure 767. Creating a condition



   b. Click **AND**.

      The **Add ADD Comparision** dialog box opens.

Figure 768. Adding comparators



c. Select **Packet Grep Protocol Match** from the **Comparison Type** drop-down menu.

d. Select the protocol name that you defined from the **Protocol** drop-down menu.

e. Select the signature search direction from the **Parse** drop-down menu. The choices are as follows:

- Request Packets Only
- Response Packets Only

f. Select the regular expression matching criteria as **Equals** or **Does NOT equal** from the **Operator** drop-down menu.

g. Add a pattern to match in the **Text to Match** text box.

h. Optionally, click the **Ignore Case** check box if you want the pattern to be matched regardless of [letter] case.

i. Optionally, click the **Ignore String Position** check box.

j. Click **Save** after adding the condition details. Your comparison appears under **Condition 1**.

3. Click **Update** in the attack editor window.

4. Click **Save** in the **Custom Attacks** window.

Import previously exported custom attacks

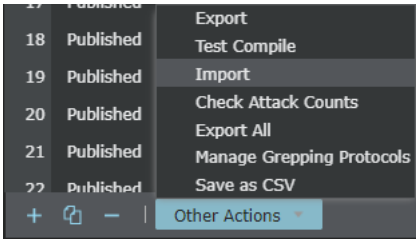
If you had exported any Trellix IPS Custom Attacks, you can import it back into the Manager. Note that this should be the same ZIP file that was created at the time of export. If this ZIP file contains any Snort Custom Attacks, those are imported as well. This feature enables you to import custom attack definitions created on a different Manager as well as the Trellix IPS-defined custom attacks.

NOTE

When you import the ZIP file containing the exported attack definitions, only the attacks not present in the Manager are imported.

To import the previously exported Trellix IPS Custom Attacks, perform the following steps:

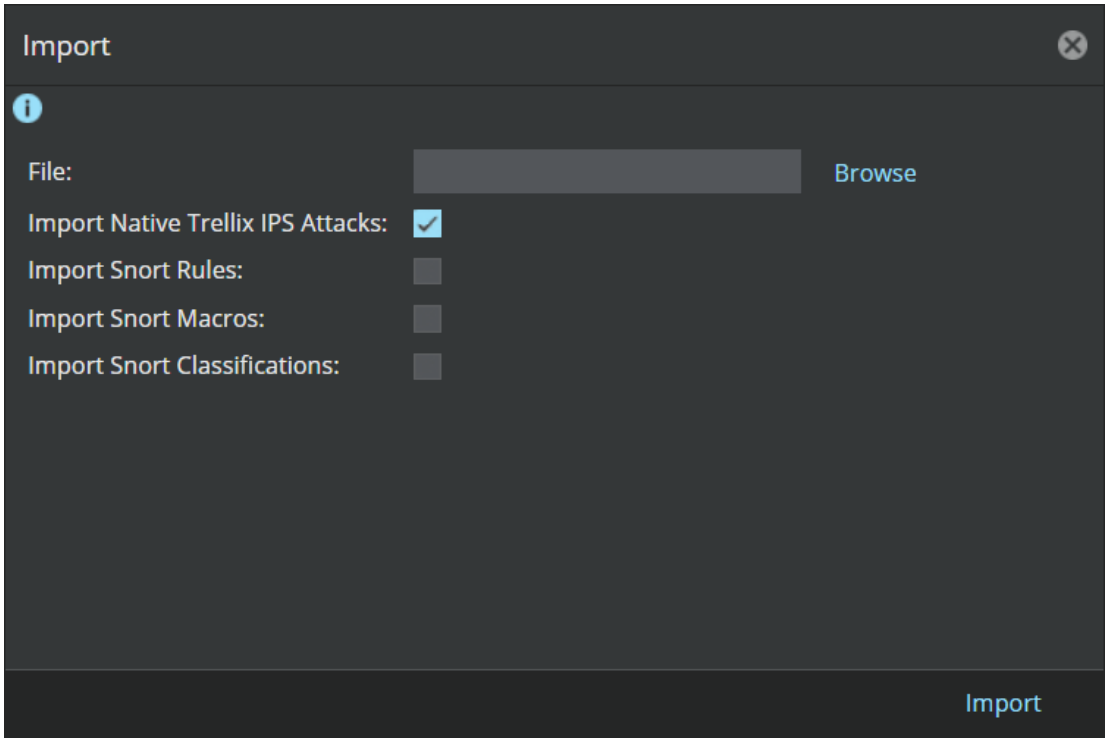
1. In the Custom Attack Editor, go to Other Actions → **Import**.



2. Browse to the location of your saved Trellix IPS Custom Attack ZIP file.
3. Click **Open**.

   The imported attacks are listed in a new tab in the Custom Attack Editor. If the ZIP contains Snort Custom Attacks, those two types of attacks are listed on separate tabs.
4. If you are importing Native Custom Attacks:
   a. Select **Import Native Trellix IPS Attacks**.

Figure 769. Import Native Trellix IPS Attacks



b. Deselect **Import Snort Rules**.

c. Deselect **Import Snort Macros**.

d. Deselect **Import Snort Classification**.

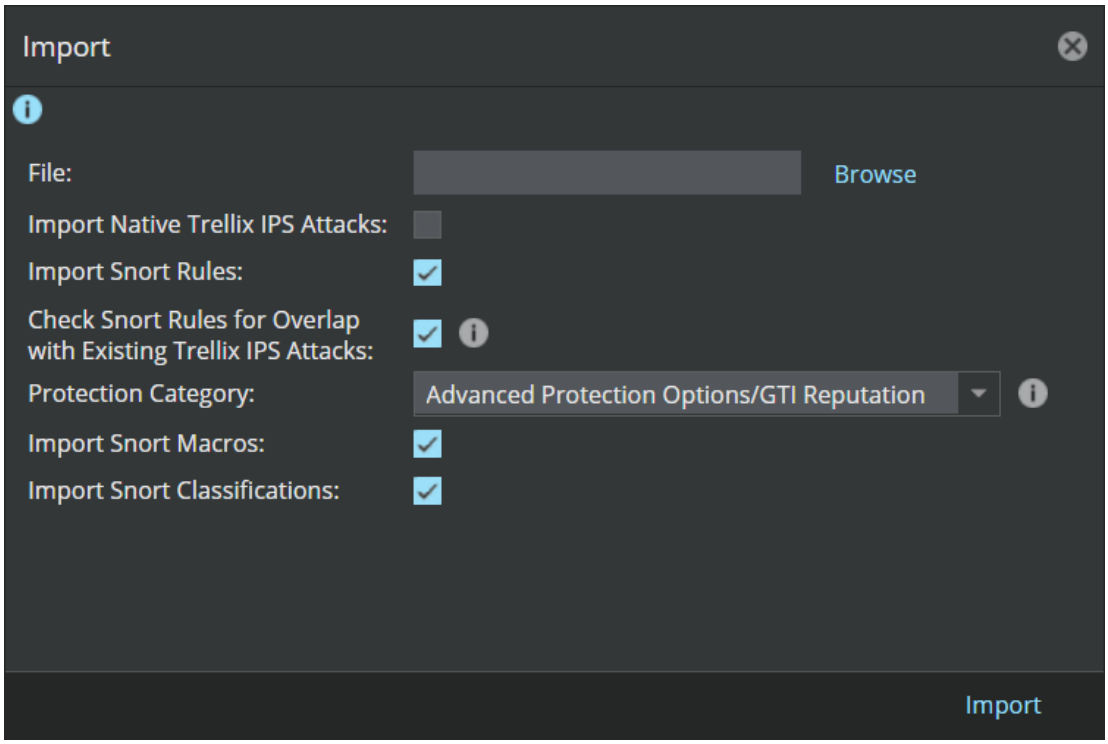
e. Click **Import**.

If you are importing Snort Rules:

a. Deselect **Import Native Trellix IPS Attacks**.

b. Select **Import Snort Rules**.

Figure 770. Import Snort Rules



c. Select **Check For Overlaps With Existing Trellix IPS Attacks**.

d. Select a **Protection Category** value.

e. Select **Import Snort Macros**.

f. Select **Import Snort Classification**.

g. Click **Import**.

5. Verify if the attack is published in the policies.
6. Publish the attack with its signatures to the Sensors for attack detection.

Importing Trellix IPS-defined custom attacks

To quickly address the latest threats, Trellix IPS periodically provides attack definitions before they are incorporated in official signature sets. These Trellix IPS-defined custom attacks (ID-UDS) are automatically deprecated when they are incorporated in a regular signature set.

NOTE

When an ID-UDS is deprecated, the Manager generates an Informational alert that you can view in the Attack Log.

NOTE

You cannot edit the attributes of an ID-UDS using the Custom Attack Editor.

You can export and import an ID-UDS just like you would with any other Custom Attacks.

Importing snort custom attacks

Using the Custom Attack Editor, you can import Snort rules from a file against constructing them one by one. Sources such as the Snort user community distribute files containing the rules which you can directly import. The import feature is helpful when you want to create a large number of Snort Custom Attacks in one go.

You can use files to import Snort rules into the Manager following any one of the two methods described below:

- Import a .zip file that contains all the required files.
- Import files individually in a specific order.

If you are importing the files individually, they have to be imported in the following order:

1. Import the Snort Configuration file (.conf)
2. Import the Snort variable files
3. Import the Snort rules files (.rules)

Check for overlaps with Trellix IPS attacks

When you create a Snort rule in the Custom Attack Editor or when you import Snort rules, the Custom Attack Editor checks if there is an equivalent Trellix IPS attack signature based on the CVE IDs. If a Trellix IPS attack signature exists, the corresponding Snort rule is referred to as a *duplicate Snort custom attack* or *duplicate Snort rule.* Such rules are imported into the Custom Attack Editor but staged in the policies by default when you save them. You can manually change the **State** of such rules to **Published.**

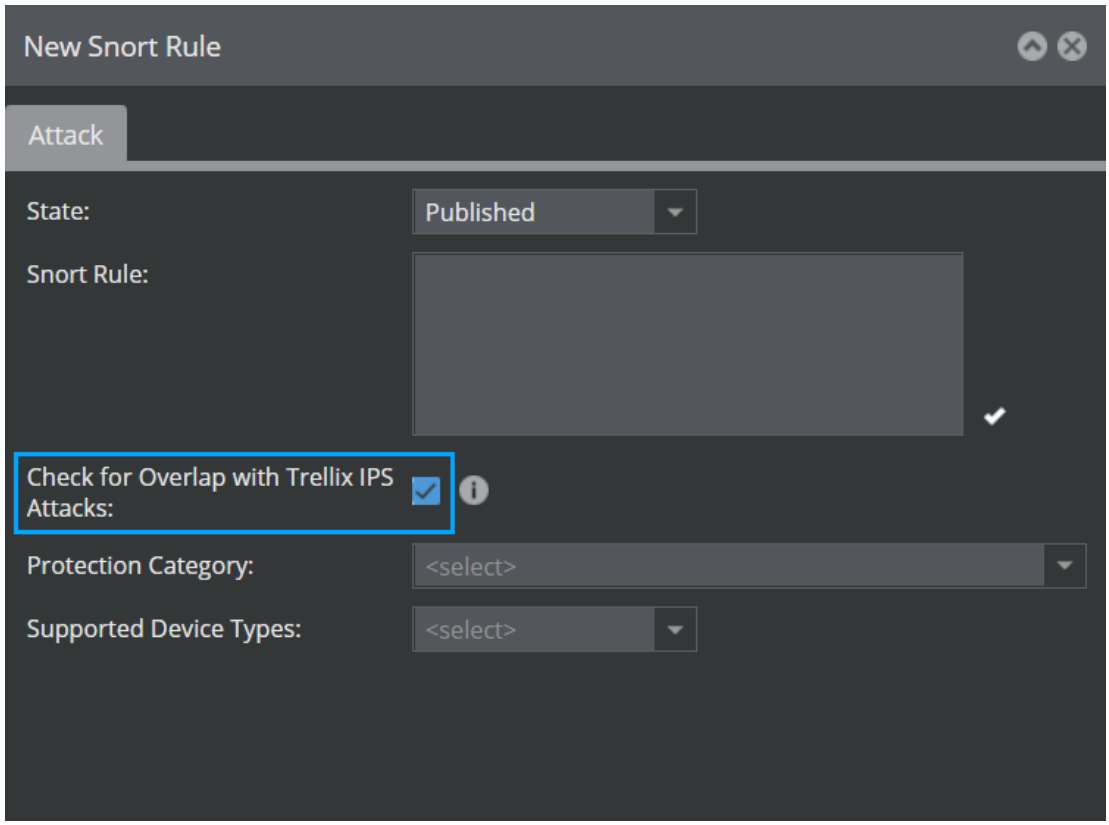
Alternatively, you can specify your preference in the Custom Attack Editor so that, going forward, the duplicate Snort custom attacks are published in the corresponding policies by default.

When you publish duplicate Snort custom attacks and enable alerting for the corresponding Trellix IPS signature as well, two alerts might be raised for the same attack traffic — one triggered by the Snort custom attack and the other by the Trellix IPS attack.

Steps:

1. In the Custom Attack Editor, click  .
2. Select **Check for Overlap with Trellix IPS Attacks.**

Figure 771. Publish duplicate Snort custom attacks



- This selection applies only to the Snort custom attacks that you will create or import from now on and not to the already staged duplicate Snort custom attacks. You can only manually publish the previously staged duplicate Snort custom attacks by changing the **State** of the corresponding attack.
- This feature compares only the CVE IDs in Snort rules with the CVE IDs in the Trellix IPS attack signatures.
- The CVE ID that you mention in the Snort rule must be of the universal format for this feature to work.

Correct	Incorrect
`reference:cve, 2010-0249;`	`reference:cve, CVE-2010-0249;` The rule is published even though there is an equivalent Trellix IPS signature because the Custom Attack Editor looked for CVE-2010-0249 instead of just 2010-0249.

Import snort rules through a conf file

Prerequisites:

Make sure of the following before you begin importing the conf file:

- You have all the rules files containing the rules that you want to import.

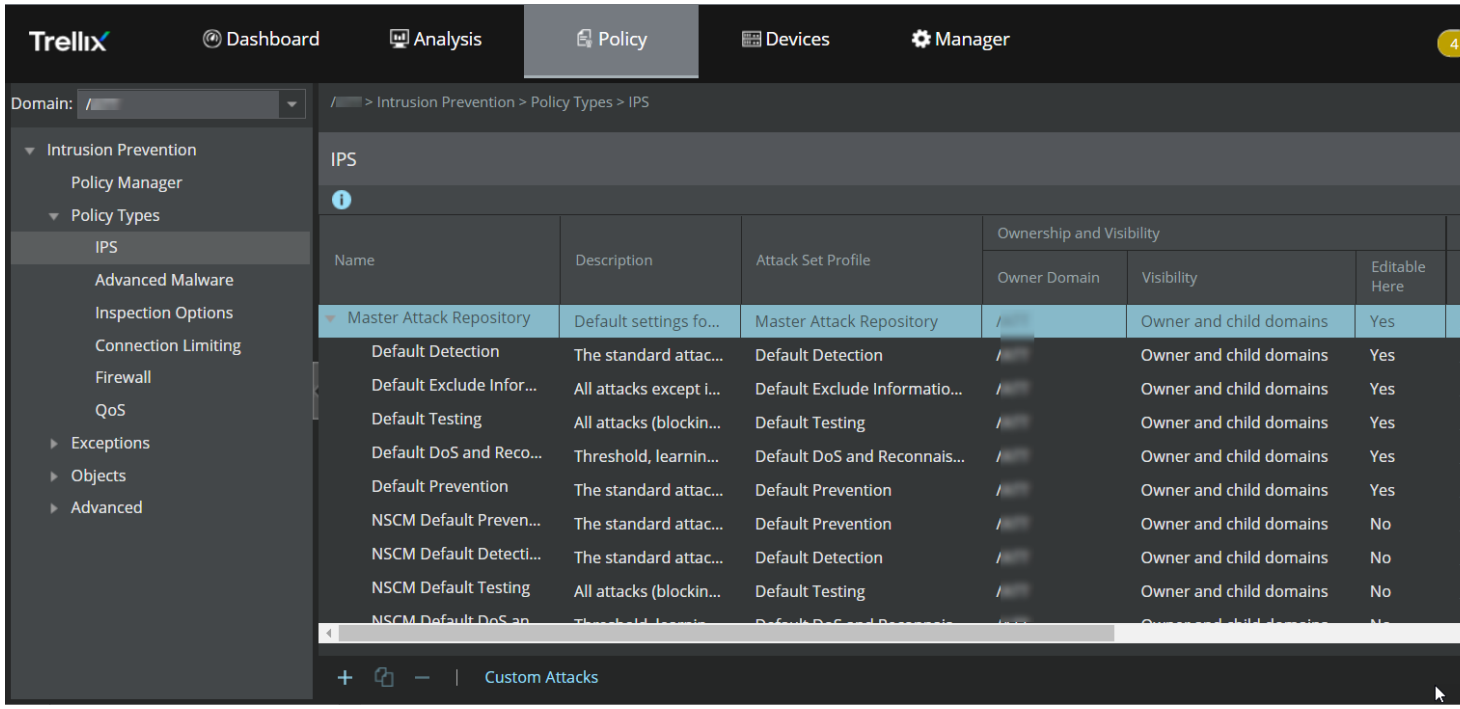
  The conf file has references to each rules file that you want to import. That is, the rules files are called from the config file using the include keyword and the absolute or relative path to the files. You can also use a variable to denote the path.

- All the variables, classifications, and references used in the rules are either defined in the conf, or the rules files up front, or available already in the Manager.
- Depending on how the rules have been constructed, the conf file may be referencing some files in addition to the rules files. Make sure all the files called by the conf file are in place.
- Each rule must have a globally unique Snort rule ID (SID) for it to be converted and saved in the Manager database. A rule is not considered for import, if the SID and revision number are same as that of a rule imported earlier. If the SID is same but not the revision number, then the rule with the highest revision number is retained.

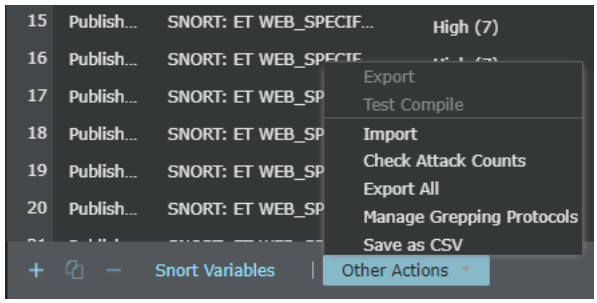
This section provides the steps for importing Snort rules into the Manager using a conf file.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.



2. In the **Custom Attack Editor** of the **Snort Format** tab, click Other Actions → **Import** .

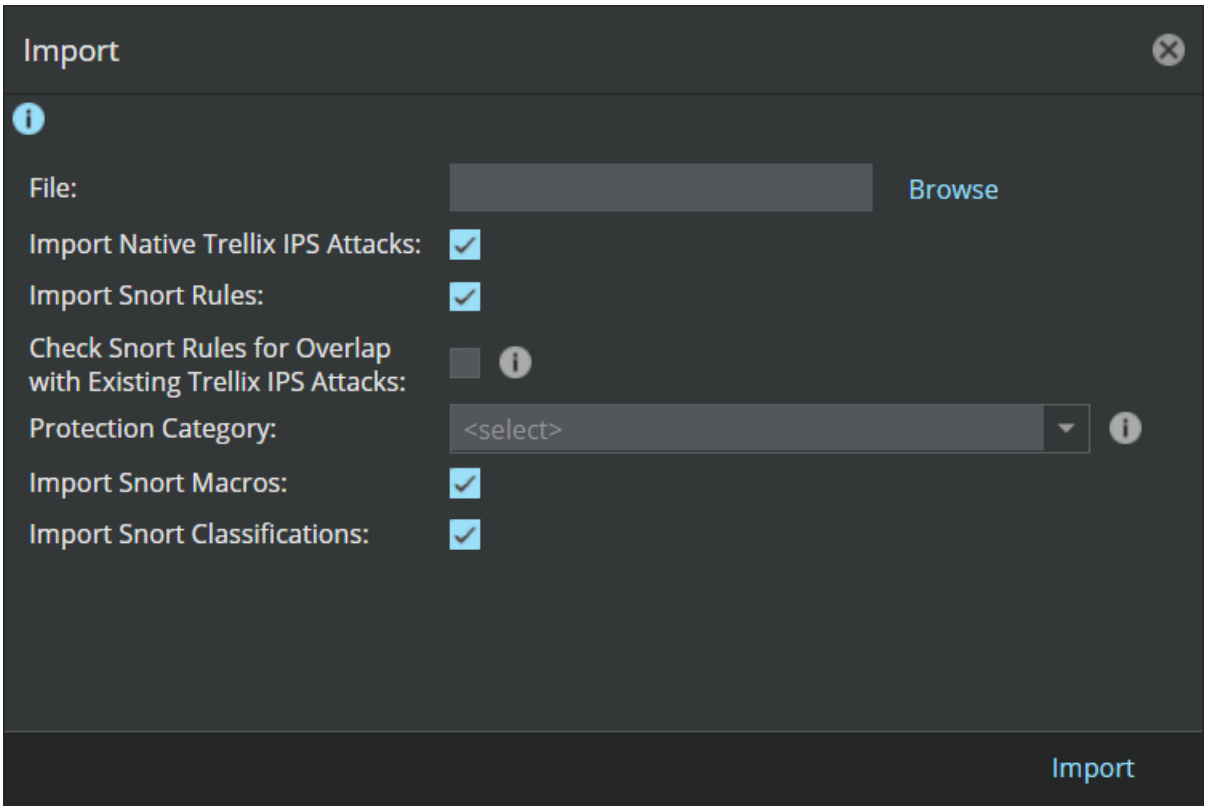


3. Navigate to the .conf file to be imported.
4. Click **Open**.

All the rules are imported into the Manager and the valid ones are converted to Trellix IPS's format. There could be some rules that were successfully converted to Trellix IPS's format, some converted with warnings, and some that failed to convert.

5. Select a **Protection Category** value.

Figure 772. Import rules window



6. Click **Import**.
7. You can refer to the section Managing Snort rules (page 1717) to:
   - View the details of the imported Snort rules
   - Know which rules converted successfully, which converted with warnings, and which failed to convert

Import snort rules through a rules file

Prerequisites:

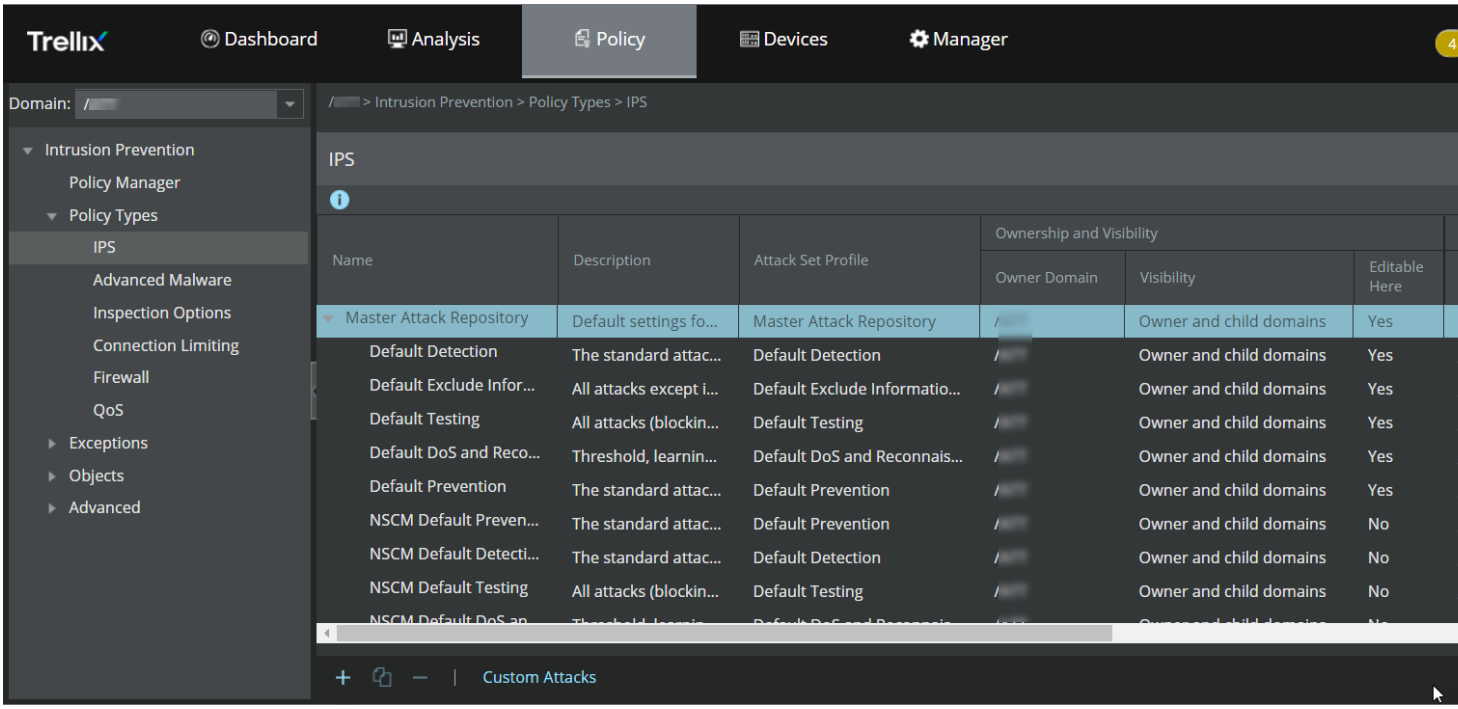
Make sure of the following before you begin importing a rules file:

- All the variables, classifications, and references used in the rules are either defined in the rules files up front or already available in the Manager.
- Just like a conf file, a rules file too can call other files. So, make sure the files called by a rules file are in place.

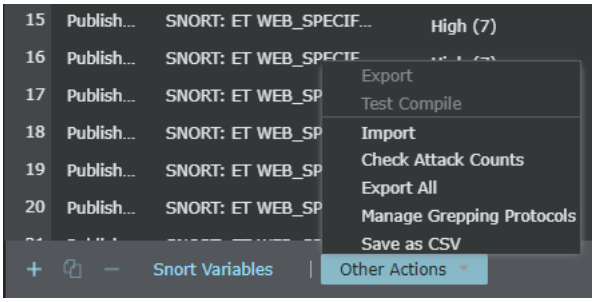
You can import rules directly from a rules file without a conf file. This section provides the steps for importing Snort rules into the Manager using a rules file.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.



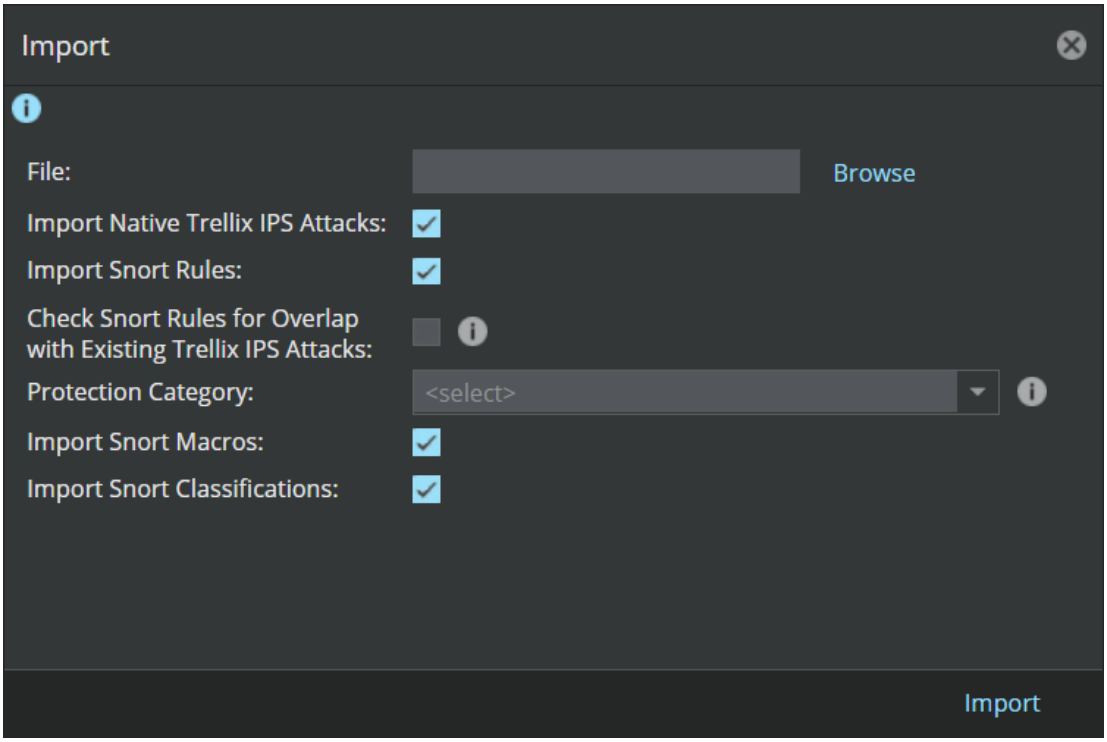
2. In the **Custom Attack Editor** of the **Snort Format** tab, click Other Actions → **Import** .



3. Navigate to the .rules file to be imported.
4. Click **Open**.

   All the rules are imported into the Manager and the valid ones are converted to Import snort rules through a conf file's format. There could be some rules that were successfully converted to Import snort rules through a conf file's format, some converted with warnings, and some that failed to convert.
5. Select a **Protection Category** value.

Figure 773. New Signature window

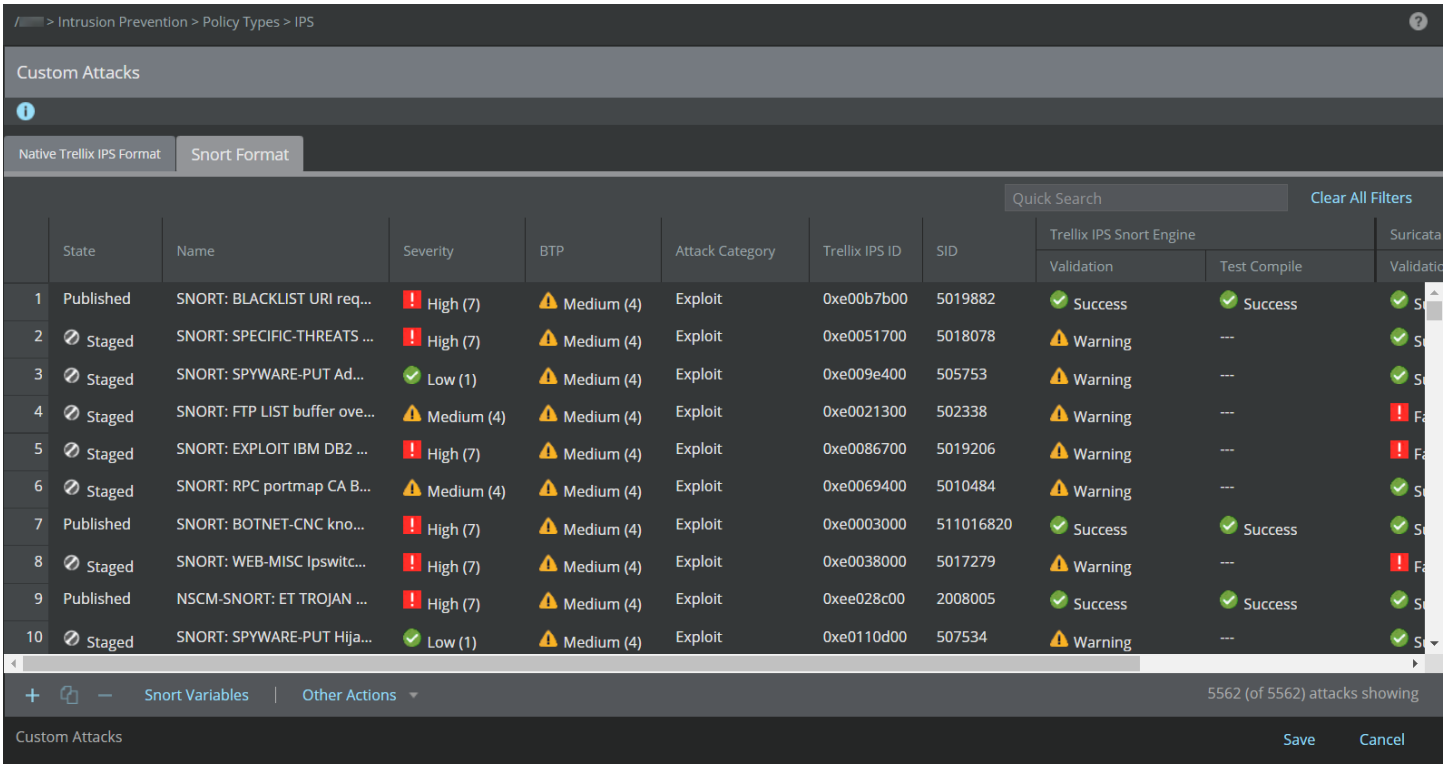


6. Click **Import**.
7. You can refer to the section Managing Snort rules (page 1717) to:
   - View the details of the imported Snort rules
   - Know which rules converted successfully, which converted with warnings, and which failed to convert

Managing Snort rules

All Snort rules are managed on a dedicated tab in the Custom Attack Editor. This section briefly describes the management of Snort rules in the Custom Attack Editor.

Figure 774. Managing Snort rules in the Custom Attack Editor



For description of the columns see Tab regions (page 1687).

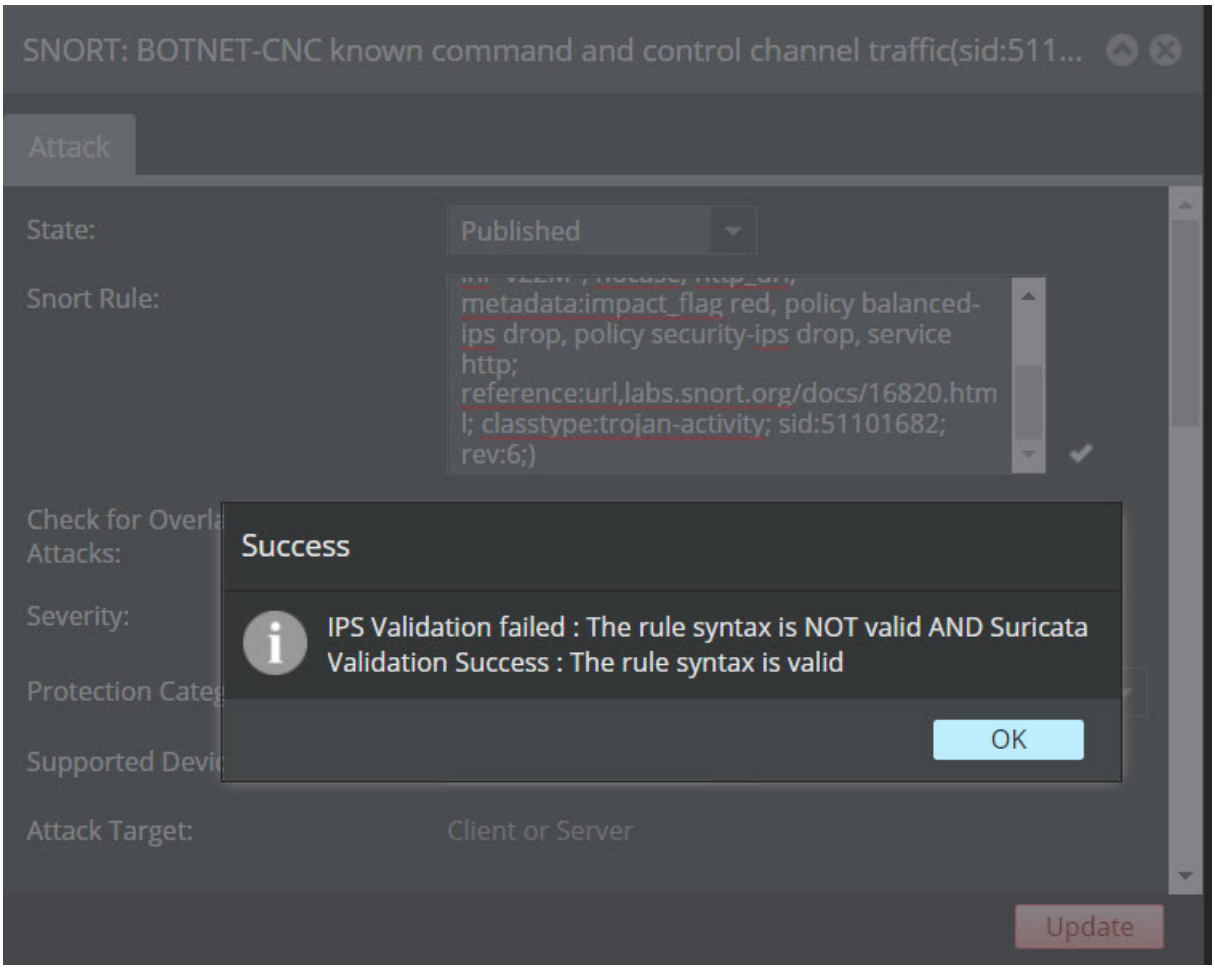
Correct the failed conversions

This sections explains how to fix Snort rules that fail to convert. Rules that fail to convert after import are set to **Failed** in the **Validation Result** column.

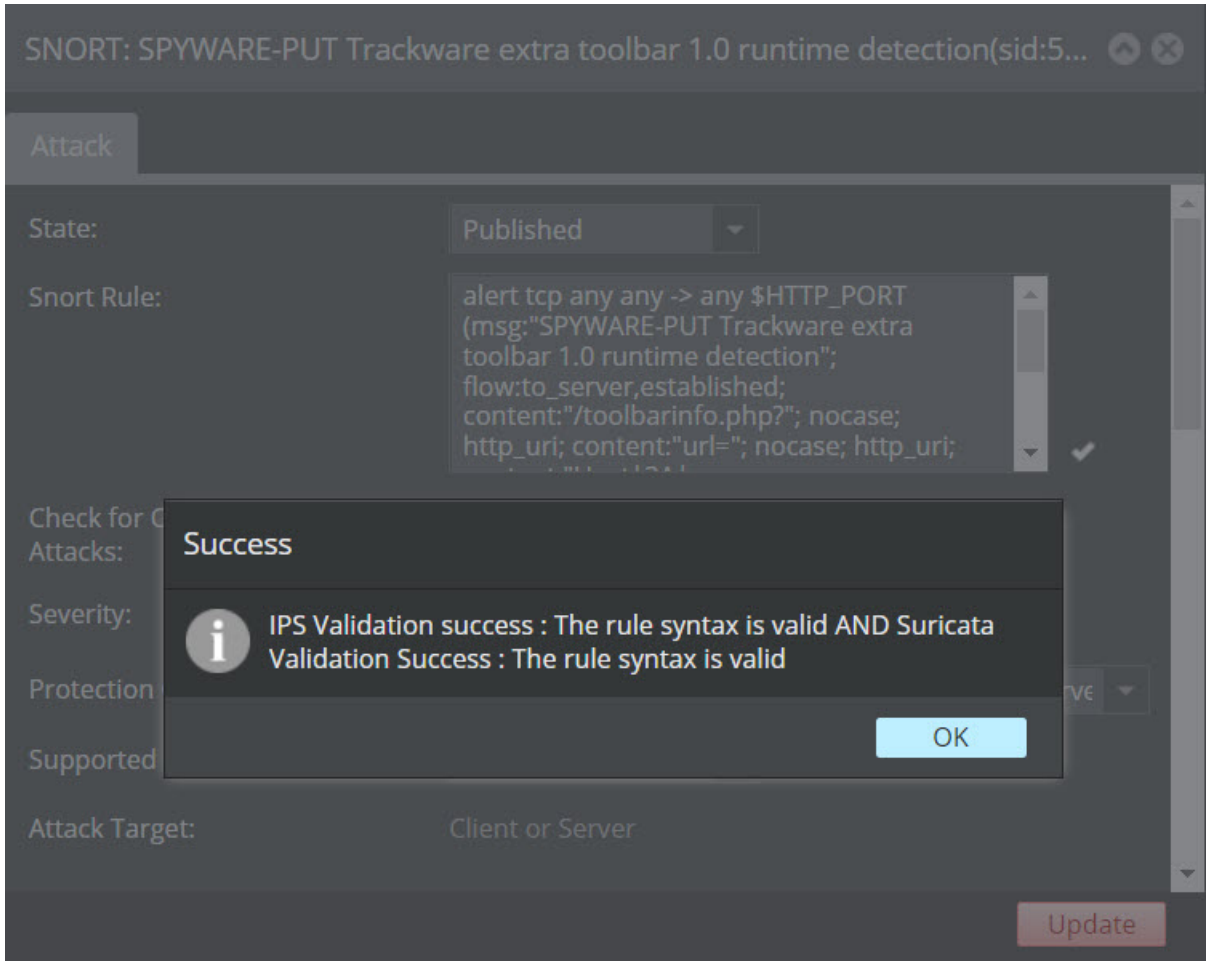
Perform the following steps to troubleshoot a failed rule:

1. Double click on the failed rule in Custom Attack Editor. The Edit Snort Attack window opens.
2. Click ☑ to validate the rule.

   For example, in the image, the validation error is related to an incorrect input type in the rule.



3. Update the rule to resolve the error.
4. Click ☑ to validate the rule.



5. If the rule is validated successfully, a **Success** pop-up appears. Click **OK**.
6. Click **Save** to save the changes you made.

   The rule is now converted to Trellix IPS's format and stored in the Manager database.

> **NOTE**
>
> After the rules are corrected, you can use the **Test Compile** feature to check the validity and compatibility. To validate the attacks, select the required attacks, right-click and select **Test Compile**.

Considerations for rules converted with warnings

Some valid rules may convert with conversion result as **Warning**. The conversion result is displayed in the **Validation Results** column. By default, rules with **Warning** are set to **Staged**. There are two reasons why rules convert with a warning.

- Rules for which there is an equivalent Trellix IPS signature in the Manager are converted with warnings. The Manager identifies such rules based on the CVE ID mentioned in the rule and the signature. You can click on an excluded attack and change its State to **Published**. You can specify your preference in the Custom Attack Editor so that, going forward, the duplicate Snort custom attacks are published in the corresponding policies by default. For information on how to set this preference, see the section Check for overlaps with Trellix IPS attacks (page 1712).

- Rules that do not have certain rule options are converted with a warning. However, based on your requirement, you can set such rules to **Published** state. It is recommended that you investigate such rules to check if they impact Sensor performance. If so, fix the rules before you publish them in the rule sets.

Test compile custom attacks

The Snort rules or User-Defined Signatures (UDS) that you create or import, must be compatible with the Trellix IPS signature set. When you save the custom attacks in the Custom Attack Editor, the Manager validates the rules to check their compatibility. If there are any incompatible custom attacks, a critical system fault message **Incompatible custom attack** is raised as a system fault. You can view the system faults in the Manager → <Admin Domain Name> → Troubleshooting → **Logs** page. After you correct the incompatible custom attacks, you can use **Test Compile** to verify the compatibility of the rules before you save them. For subsequent signature set updates, only attacks that pass compilation are published to the Sensors.

Consider the following when running **Test Compile**:

- Running **Test Compile** does not change the compilation status of attacks. The compilation status of attacks is updated only after you save the attacks. After you save, attacks that fail compilation are marked as **Failed** in the **Test Compile** column and will be in **Staged** state.

  For information on rules that determine the state of the attack, see Rules for determining the value of the State (page 1687).
- You need to select the attacks that should be compiled.
- Attacks only in the **Published** state can be compiled. As an exception, if all the selected attacks are in **Staged** state, the attacks are compiled.
- Attacks that fail the test compilation are not highlighted by the Manager. To identify the specific attacks that fail, you can run **Test Compile** on a subset of attacks and verify if they fail. You can continue this process of elimination until you identify the specific attacks that fail.

  For example, select 10 attacks for test compilation and compilation reports a failure. To identify the specific attacks that failed, select a subset of attacks from the initial 10 attacks and run test compilation. If test compilation still reports failure, repeat the process of elimination until you find the specific attacks that fail.
- Attacks from the Central Manager are not considered for test compile in the Manager.

NOTE

The Manager compiles all the active custom attacks during reboot or startup. The **IPS** page is not available till the Manager finishes compilation. It takes about 7 minutes for the page to load.

Steps:

1. In the Custom Attack Editor, select the custom attacks you want to run a test compilation on.
2. Select Other Actions → **Test Compile.**

   This option is available as part of the right-click menu.

Mechanics of a custom attack

This section explains the elements that make up a Trellix IPS Custom Attack. A good understanding of these elements and how they can impact your IPS setup is required to create effective attack definitions.

Structure of a custom attack

A Trellix IPS Custom Attack is like a top-level container in which you define one or more signatures. Some of the critical values that you need to specify when defining an attack are the attack severity, the impact package, and protocol. Based on these values, the Manager categorizes the attack and includes it in the policies.

NOTE

You must specify at least one impact package or protocol to save a custom attack in the Manager server.

Structure of a signature

Trellix IPS's signature support is very comprehensive. In addition to the normal pattern matching and numeric tests supported by many network IPS systems, Trellix IPS allows signatures to have a complex structure that can order and group the tests necessary for accurate detection.

How tests are logically structured

Trellix IPS provides a simple but powerful set of logical constructs that will allow you to create an attack definition to match the fingerprint of nearly any network activity. The logical constructs provide methods for grouping and ordering the more granular pieces of the signature - numeric tests and pattern matches - in any order you require. The core constructs are:

- AND - Tests are grouped within AND blocks. The tests must all succeed, but may occur in any order inside the context of a given flow. AND blocks cannot be contained within an OR condition.
- OR - The first test to succeed fulfills the condition, and the next AND or OR block is engaged. OR constructs are contained within AND blocks, though at times they may be the only contents.
- ANDTHEN - ANDTHEN is the ordering construct. By placing ANDTHEN statements between AND blocks, you can create a structured order for your tests, if required.

The actual tests of which signatures are composed are placed inside either AND or OR constructs. These are called conditions and are like containers. ANDTHEN is used to link the AND containers (conditions) together to form a larger structure.

Supported test methods

A Trellix IPS Custom Attack supports 2 basic classes of test:

- Pattern Match - Pattern matches can be used to match ASCII or binary strings. Support for common regular expression constructs is available.
- Numeric Comparisons - Numeric comparisons can be used to test for a match with a given value or a range of values, depending on the numeric comparison test chosen.

Other signature components

In addition to the mechanics of the signature itself, Trellix IPS requires a few other pieces of information, as described below, to do its job properly:

- Detection Window - The detection window is the portion of the traffic flow that the Sensor should check against an attack definition for matches. The detection window may be one of the following:
  - Packet - All of the signature tests (and thus all protocol fields) must occur in a single packet on the network.

- Request - All of the signature tests must occur in the request direction of the flow. (Useful if the protocol is bidirectional and might include the same data or commands in either direction.)
- Response - Identical to request, but used to examine only response-direction traffic
- Flow - When the detection window is set to flow, all conditions can be fulfilled by traffic flowing in either direction. Tests are still subject to any ordering imposed by the structure of the signature or flow direction implied by the field being tested.

> **NOTE**
>
> It is possible to create a correct signature that will never trigger if the detection window is set incorrectly. This should be one of the first items you check when troubleshooting a custom attack definition.

- Benign Trigger Probability - This is a measure of the confidence with which you believe the signature can identify a network event. A high benign trigger probability (BTP) implies that a signature may be prone to false positives. When creating the signature, you should set the BTP to "Low" to ensure that your signatures are selected by the Default Policy.

Create more than one signature per attack

The capability of creating more than one signature in an attack definition is part of what allows Trellix IPS to keep its false positive rate so low. You should create multiple signatures for an attack, when possible, so as to be both more inclusive and more specific. You may want to create a generic signature that will catch all attack variants (including those which are unknown to you). You should also create more specific signatures to detect particular pieces of exploit code, if possible. This can be valuable in providing pointers on what to investigate if a machine has been compromised, in addition to keeping your rate of false positives far below that of the average signature-based IPS.

Signature test reference

This section describes each test type available for use in signatures and the required and optional parameters for each.

Numeric comparison tests

- **!=** : Test of numeric inequality
- **==** : Test of numeric equality
- **unsigned <** : True if the unsigned **Value** specified is less than the value obtained from the network traffic
- **signed <** : True if the signed **Value** specified is less than the value obtained from the network traffic
- **unsigned >** : True if the unsigned **Value** specified is greater than the value obtained from the network traffic
- **signed >** : True if the signed **Value** specified is greater than the value obtained from the network traffic
- **unsigned <=** : True if the unsigned **Value** specified is less than the value obtained from the network traffic
- **signed <=** : True if the signed **Value** specified is less than or equal to the value obtained from the network traffic
- **unsigned >=** : True if the unsigned **Value** specified is greater than or equal to the value obtained from the network traffic
- **signed >=** : True if the signed **Value** specified is greater than or equal to the value obtained from the network traffic

Numeric test parameters

Parameter	Description
Protocol Field	The field that will be compared with the supplied value
Value to Match	The value that should be compared against the value retrieved from the network traffic. This field does not support floating point values.

Numeric range tests

- **signed-in-range** — True if the value obtained from the network traffic falls within the specified signed range
- **unsigned-in-range** — True if the value obtained from the network traffic falls within the specified unsigned range

> **TIP**
>
> Trellix recommends using an in-range test as it is more efficient than -gt and --lt tests.

Numeric range test parameters

Parameter	Description
Protocol Field	The field that will be tested for equality with the supplied value
Minimum Value	Minimum value of the comparison range (Inclusive)
Maximum Value	Maximum value of the comparison range (Inclusive) Note that the Minimum Value and Maximum Value fields do not support floating point values.

Numeric enumeration tests

- **unsigned ==** : True if one of the enumerated values matches the value obtained from the network traffic

Numeric enumeration test parameters

Parameter	Description
Protocol Field	The field that will be tested for equality with the supplied value
Integer values	Integer values to be compared against the values derived from network traffic Note that the values cannot be floating point or negative.

Pattern matching

Pattern matching within signatures is always implemented with string-match. String-match accepts a number of optional and required parameters. In the **Text to Match** text box, construct the string that contains the pattern to match. By default, pattern matches are case-sensitive. String-match accepts regular expressions in addition to simple strings.

Pattern match test parameters

Parameter	Description
Protocol Field	The field that will be tested for a match with the supplied pattern
Text to Match	Pattern to be matched
Ignore Case	Select this option to make the expression case insensitive. By default it is case sensitive.
Ignore String Position	Selecting this option enables you to create specific conditions. Offset: Use this to indicate where the Sensor should begin its search for the string. For example, if you set an offset of 5, then the Sensor checks for first byte of the string from the 5th byte of the payload. Depth: Use depth to indicate how far into the traffic should the Sensor look for the string. For example, if you set a depth of 10, the Sensor stops looking for the first byte of the string at the 10th byte from the beginning of the payload. Origin: Select **Packet** if you want the Sensor should apply the offset or depth to a packet. If you want the Sensor to apply the condition to the entire flow, select **Flow.**

Create a fixed field signature

Fixed fields are those protocol fields that are provided by the basic IP protocols ("IPv4"), TCP, UDP and ICMP. They are "fixed" by contrast with the calculated nature of many provided by other protocol specifications. Due to the fact that these fixed fields occur in most packets the Sensor inspects, it is impractical for performance reasons to inspect them in the same fashion as standard protocols. For the same reason, the number of fixed field comparisons is limited to 50.

Two types of tests for fixed fields are available. Both are numeric because the fixed fields are all numeric.

- **fields-eq** — Fields-eq is a special test that is only available for fixed-field testing. It allows you to compare the values in two protocol fields. This is useful if, for example, you want to compare whether the source and destination IP addresses specified by packet headers are the same.
- **All of the numeric tests described for normal signature tests** — This includes both signed and unsigned tests.

> **NOTE**
>
> The **Single Fixed Field Match** in the Custom Attack Editor also provides an "bitmask" function. This is not a normal "bitmask". Instead, starting from the offset you provide (in the selected fixed field), it selects the number of bits you specify, and then uses those bits to create an integer value that is compared against your provided comparison value.

Packet search protocols

Packet search protocols are a form of generic packet inspection capability used by IPS experts when dealing with protocols that are not specifically supported by Trellix IPS. They are generally used for implementing detection on specific ports in an efficient fashion. In these cases, it can be valuable to separate out traffic running on particular ports for processing. This can make detection more efficient because pattern matches and other tests will only examine a limited subset of network traffic. In addition, it is possible to create a packet search protocol to exclude certain traffic from being considered for detection.

Performance issues

- **False positives** — Large numbers of false positives could (in severe cases) overwhelm the Manager. More commonly, they will simply overwhelm the user due to volume and speed of appearance.
- **Too many pattern matches** — If the pattern your signature searches for occurs too often in the network traffic being analyzed, checking each match to determine whether it fulfills a signature condition may degrade Sensor performance.

  NOTE

  The most common cause of overwhelming numbers of pattern matches is making them too short. A pattern to be matched should never be shorter than 3 characters because the likelihood of a chance occurrence of such a pattern in normal traffic is very high.

- **Too many fixed-field tests** — If you configure too many fixed-field tests in your signatures, Sensor performance may be degraded. This is due to the fact that the Sensor will have to inspect this field in every packet of the traffic type being tested. As with pattern matches, checking each test result to see if it fulfills a signature condition may affect Sensor performance.

  NOTE

  The Fixed Field test will have a performance impact as every packet needs to get inspected for all the conditions configured by the admin. Therefore, the Sensor performance degrade due to the Fixed Field Tests is directly proportional to the number of fixed field test instructions configured. **Trellix recommends** to factor in the performance degrade while configuring the Fixed Field Tests in your signatures.

- **Testing overly common fields** — If your signature contains a test of a field that occurs very often in the traffic type being analyzed, it might degrade Sensor performance. This can be due to the number of tests that will be performed, or due to the number of tests that must be checked for fulfilling a signature test condition.

Considerations

Consider the following when you create Trellix IPS Custom Attacks. These should not present an obstacle to most signature writers.

- You can save up to **4500** Trellix IPS Custom Attack definitions in your Manager.
- Each Trellix IPS Custom Attack may not have more than **16** different signatures.
- Each signature may not contain more than **32** different tests, either numeric or pattern-matching.

Creating custom attacks

This section provides the information required to create and maintain Trellix IPS Custom Attacks with one or more signatures.

Create custom attacks

The following is the high-level recommended approach for creating Trellix IPS custom attacks.

Steps:

1. Be clear on what you are trying to achieve through these attacks. Identify the related protocols, applications, hardware and software platforms, and so on for the attack.
2. Understand the mechanics of a Trellix IPS custom attack. You also need to understand the probable impact of your custom attack on the network.
3. Take a quick tour of the Custom Attack Editor and get familiar with it. You can use the Custom Attack Editor to manage the custom attacks.
4. Create a Trellix IPS custom attack with one or more signatures.
5. Verify if the attack is published in the policies.
6. Push the attack with its signatures to the Sensors for attack detection to happen.

Templates for Trellix IPS custom attacks

You can use the predefined templates to create some of the commonly used Trellix IPS custom attacks. By using these templates, you can create effective Trellix IPS custom attacks even if you do not possess detailed knowledge of the related protocol, its header, or the syntax of Trellix IPS custom attacks.

Predefined templates are available to create Trellix IPS custom attacks that:

- Detect a URL
- Detect an email attachment file name
- Detect a DNS query or response
- Detect a string in an application running over a custom port
- Detect a TCP connection attempt from a specific IP address

When you use the templates, a Trellix IPS custom attack with the relevant protocol is automatically created. Also, the corresponding signature is created for the attack. You can add more conditions to the signature or add more signatures to the Trellix IPS custom attack. For example, when you use the template to detect TCP connection attempts from specific IP addresses, the signature for the IP addresses that you specify is automatically created. To specify more IP addresses for this attack, create the corresponding signatures for those IP addresses.

IMPORTANT

By default, the signatures that are created when you use the templates have high value of Benign Trigger Probability (BTP). You can edit this value post-creation. Note that the attacks of BTP value high are not published in the Default Detection and Default Prevention policies.

NOTE

When you save the Trellix IPS custom attacks in the Manager database, an informational fault is displayed in the **Status** page to indicate whether the custom attacks were successfully saved.

Create a Trellix IPS custom attack to detect a URL

You can use the pre-defined template to create a Trellix IPS custom attack to detect a URL.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.

2. Click  .

   The **New Custom Attack** interface opens.

3. In the **Name** field, type a new name for your attack. **UDS** (User-Defined Signature) is appended at the front automatically when you save the attack. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor as well as in the attack database when you save the attack.

   > **NOTE**
   >
   > The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.

5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).

   Severity is set to **Medium (5)** by default.

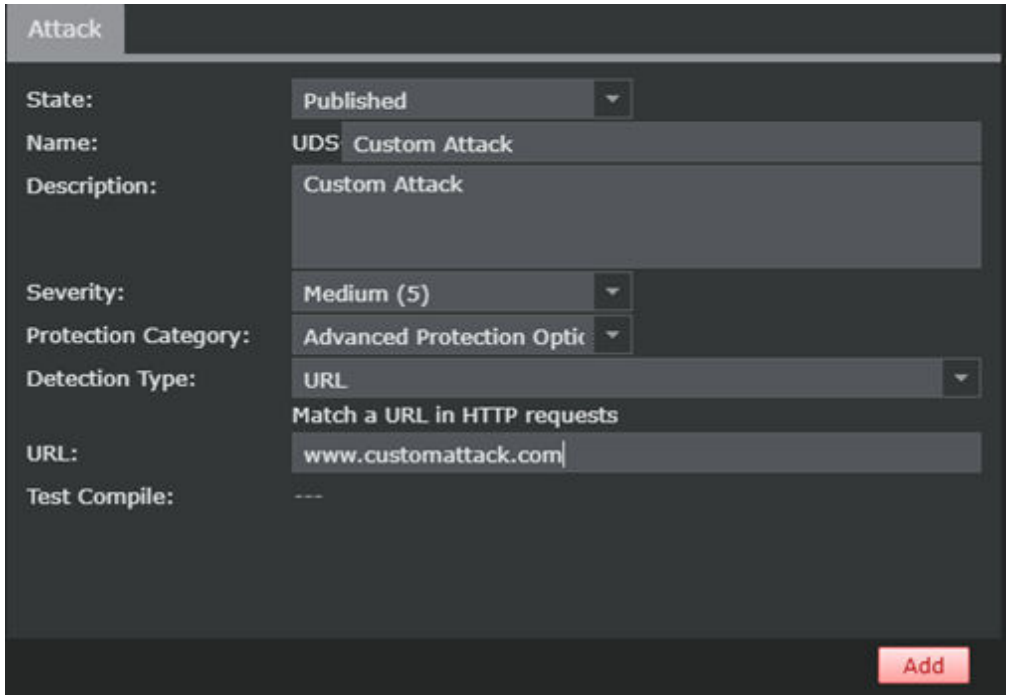
6. Select the most appropriate **Protection Category** for the attack.

7. Select **URL** from the **Detection Type** drop-down menu for the attack.

8. Enter the **URL** that is to be detected, then click **Add**.

   If you are specifying the protocol, you can specify only HTTP or HTTPS in the URL. The attack is listed on the **Native Trellix IPS Format** tab.

Figure 775. Create a Trellix IPS custom attack to detect a URL

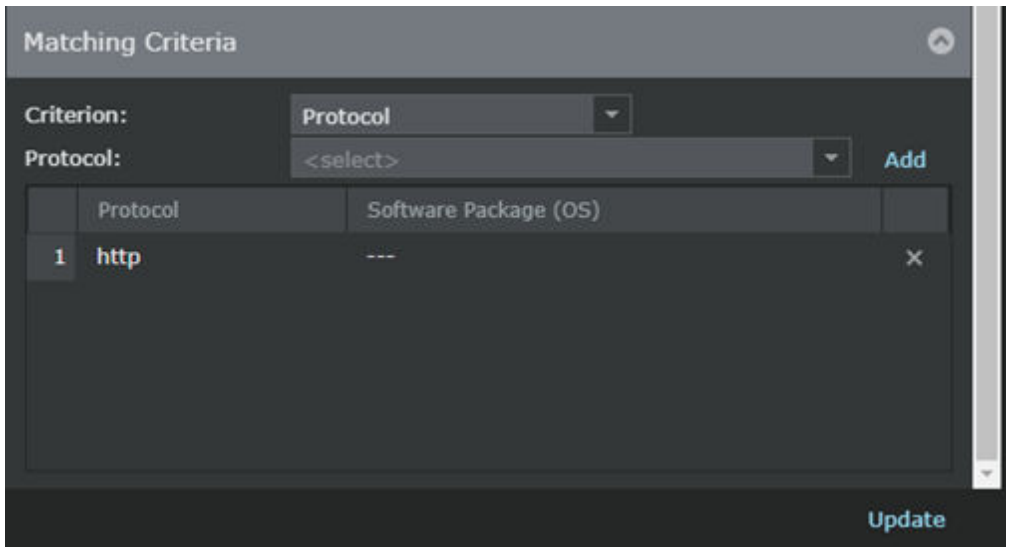


9. Double-click on the attack that you created on the **Native Trellix IPS Format** tab.

   In the **Matching Criteria** section, the protocol is automatically selected as HTTP.

   You can also add more conditions to the signature. From the **Add Custom Attack** window, you can also add more signatures to the attack.

Figure 776. Details of the Trellix IPS custom attack



10. Click **Save** in the **Custom Attack** interface.

Until you save the attack in the database, value for the **Trellix IPS ID** column is not generated. The Sensor detects this attack after you deploy pending changes to the corresponding Sensor (Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab. Then, select the required Sensor from the list and click **Sync**).

Create a Trellix IPS custom attack to detect an email attachment by file name

You can use the predefined template to create a Trellix IPS custom attack to detect an email attachment by the file name.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.

2. Click  .

   The **New Custom Attack** interface opens.

3. In the **Name** field, type a new name for your attack. **UDS** (User-Defined Signature) is appended at the front automatically when you save the attack. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor as well as in the attack database when you save the attack.

   NOTE

   The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.

5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).

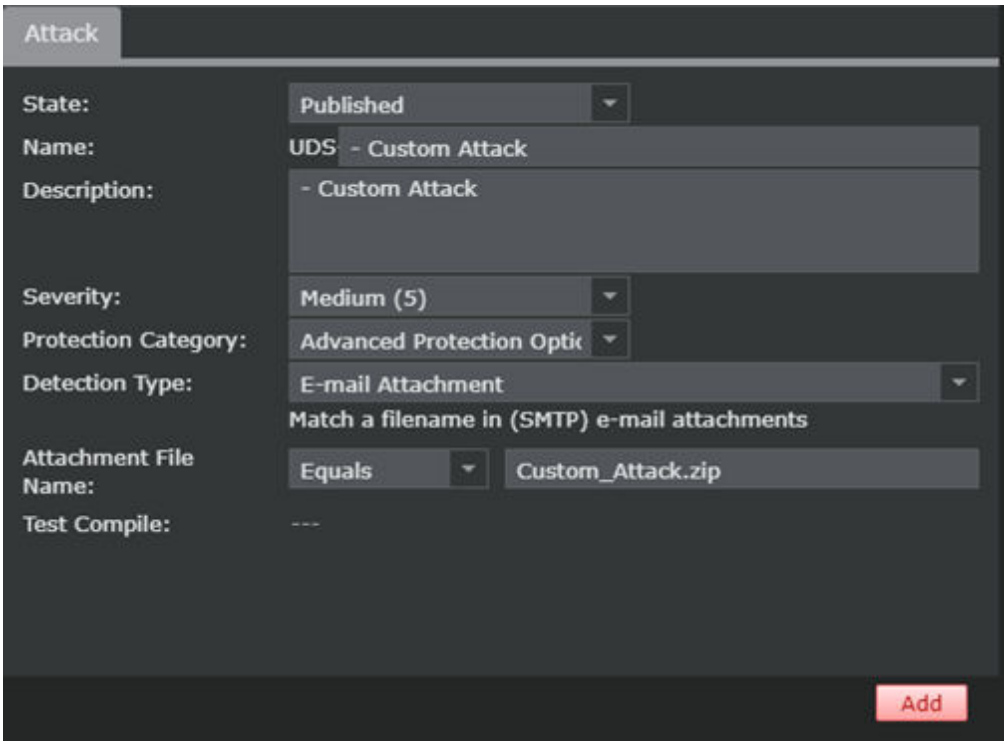
   Severity is set to **Medium (5)** by default.

6. Select the most appropriate **Protection Category** for the attack.

7. Select **E-mail Attachment** from the **Detection Type** drop-down menu for the attack.

8. Select the required parameter for **Attachment File Name** and enter the corresponding value in the text box.

Figure 777. Custom attack to detect an email attachment by its file name

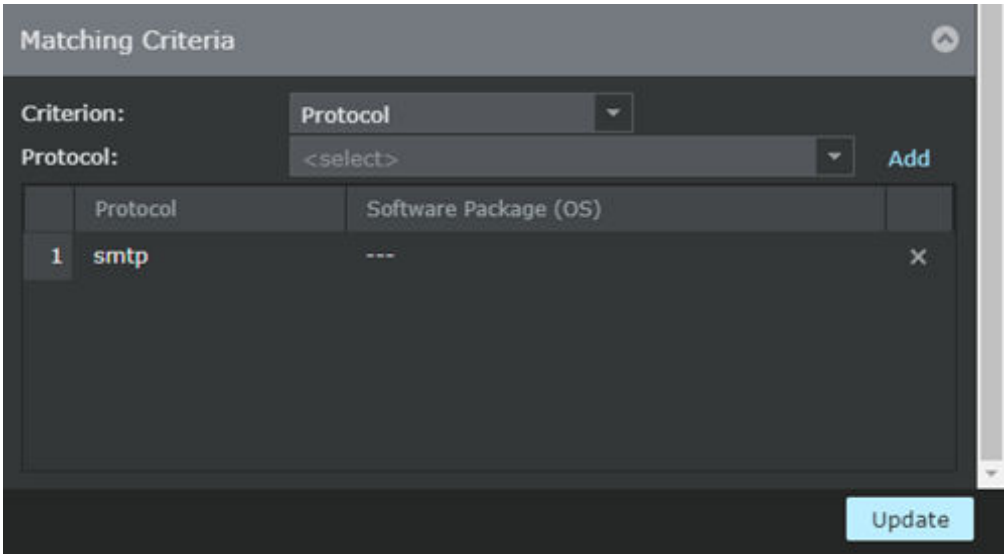


9. Click **Add**.
10. Double-click on the attack that you created on the **Native Trellix IPS Format** tab.

    In the **Matching Criteria** section, the protocol is automatically selected as SMTP.

    To edit these values, select the signature on the **Signature-<signature name>** tab. You can modify the default values. You can also add more conditions to the signature.

Figure 778. Details of the Trellix IPS custom attack



11. Click **Save** in the **Custom Attack** interface.

    Until you save the attack in the database, value for the **Trellix IPS ID** column is not generated. The Sensor detects this attack after you deploy pending changes to the corresponding Sensor (Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab. Then, select the required Sensor from list and click **Sync**).

Create a Trellix IPS custom attack to detect a DNS query or response

You can use the predefined template to create a Trellix IPS custom attack to detect a DNS query or response related to a domain name.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.

2. Click  .

   The **New Custom Attack** interface opens.

3. In the **Name** field, type a new name for your attack. **UDS** (User-Defined Signature) is appended at the front automatically when you save the attack. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor as well as in the attack database when you save the attack.

   > **NOTE**
   >
   > The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.

5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).

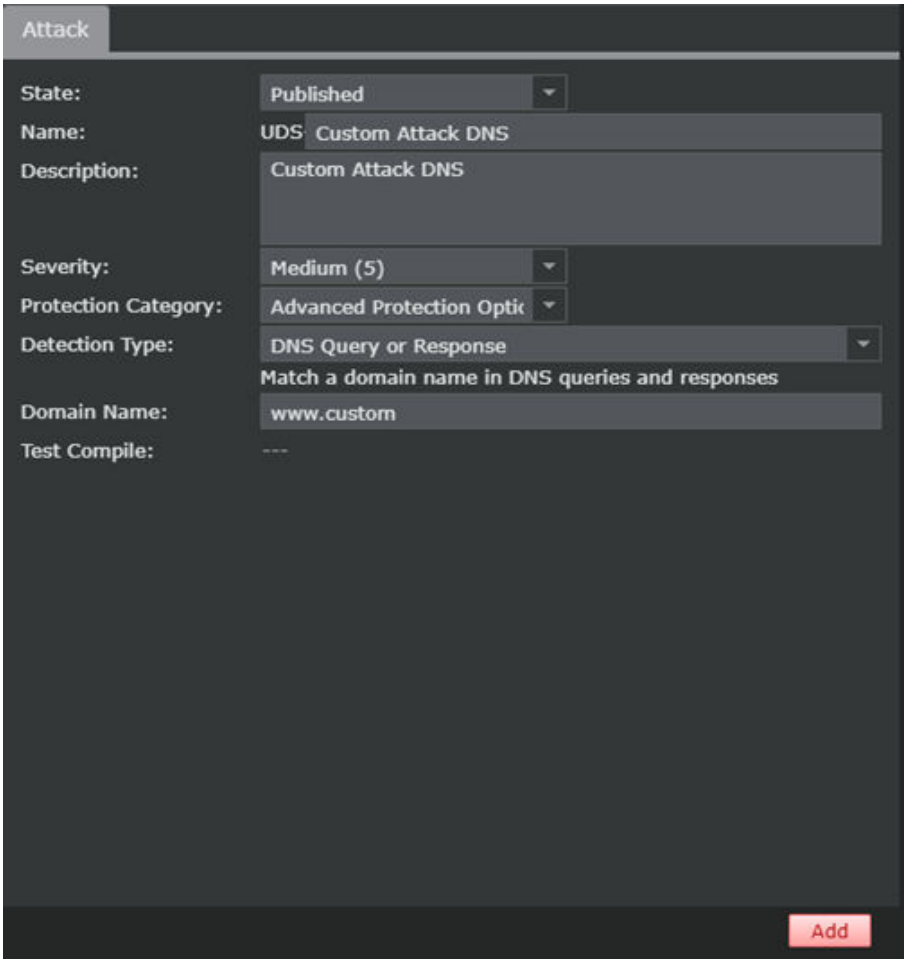
   Severity is set to **Medium (5)** by default.

6. Select the most appropriate **Protection Category** for the attack.

7. Select **DNS Query or Response** from the **Detection Type** drop-down menu for the attack.

8. Enter the full or the partial **Domain Name** that the Sensor should detect in a DNS query or response, and then click **Add**.

Figure 779. Custom attack to detect an DNS query or response

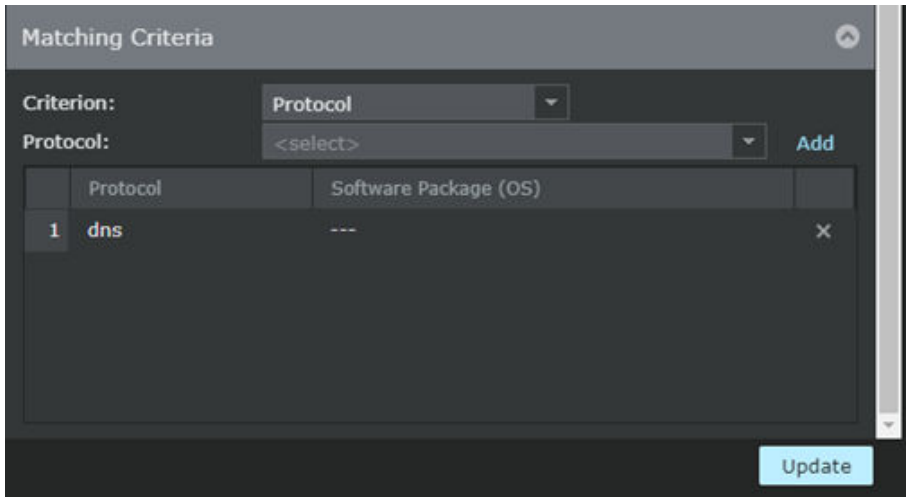


9. Double-click on the attack that you created on the **Native Trellix IPS Format** tab.

   In the **Matching Criteria** section, the protocol is automatically selected as DNS.

   The signature for the URL that you specified is created automatically with the default values. You can modify the default values. You can also add more conditions to the signature.

Figure 780. Details of the Trellix IPS custom attack



10. Click **Save** in the **Custom Attack** interface.

    Until you save the attack in the database, value for the **Trellix IPS ID** column is not generated. The Sensor detects this attack after you deploy pending changes to the corresponding Sensor (Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab. Then, select the required Sensor from list and click **Sync**).

Create a Trellix IPS custom attack to detect a string in an application running over a custom port

You can use the predefined template to create a Trellix IPS custom attack to detect a string in an application that is running over a custom port.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.

2. Click .

   The **New Custom Attack** interface opens.

3. In the **Name** field, type a new name for your attack. **UDS** (User-Defined Signature) is appended at the front automatically when you save the attack. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor as well as in the attack database when you save the attack.

   NOTE

   The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.

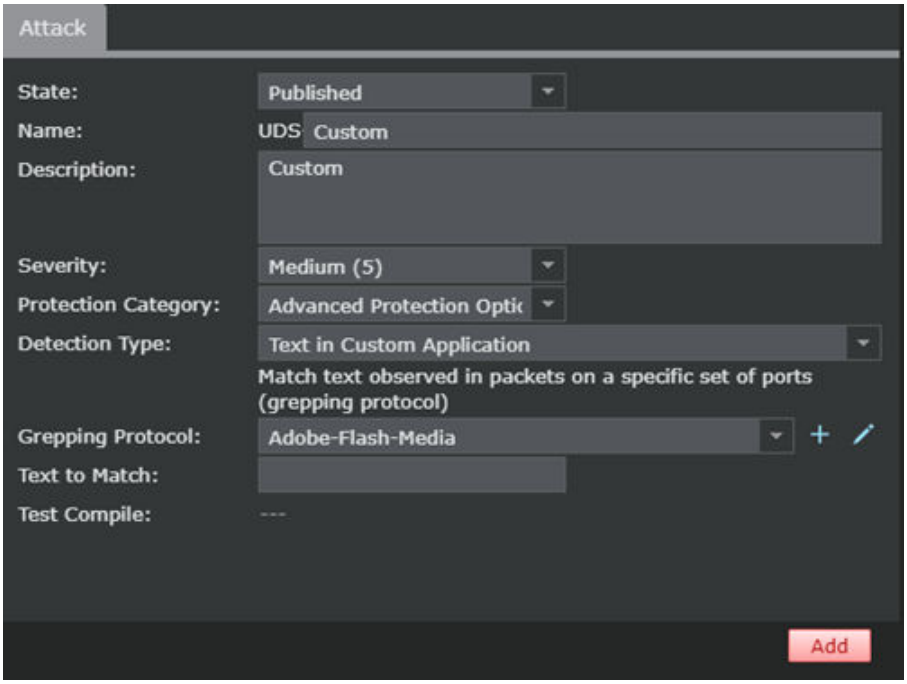
5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).

   Severity is set to **Medium (5)** by default.

6. Select the most appropriate **Protection Category** for the attack.
7. Select **Text in Custom Application** from the **Detection Type** drop-down menu for the attack.
8. Select the appropriate **Grepping Protocol**.
9. Enter the string that you want the Sensor to detect in the **Text to Match** field and click **Add**.

   The **Text to Match** field is case-sensitive. That is, the Sensor matches the case when it detects the string.

Figure 781. Custom attack to detect a string in an application on a custom port



10. Double-click on the attack that you created on the **Native Trellix IPS Format** tab.

    You can modify the values of the signature on the **Signature-<signature name>** tab. You can also add more conditions to the signature.

11. Click **Save** in the **Custom Attack** interface.

    Until you save the attack in the database, value for the **Trellix IPS ID** is not generated. The Sensor detects this attack after you deploy pending changes to the corresponding Sensor (Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab. Then, select the required Sensor from list and click **Sync**).

Create a Trellix IPS custom attack to detect TCP connection attempts

You can use the predefined template to create a Trellix IPS custom attack to detect TCP connection attempts from specific IP addresses.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.

2. Click .

   The **New Custom Attack** interface opens.

3. In the **Name** field, type a new name for your attack. **UDS** (User-Defined Signature) is appended at the front automatically when you save the attack. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor as well as in the attack database when you save the attack.

   NOTE

   The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.

5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).

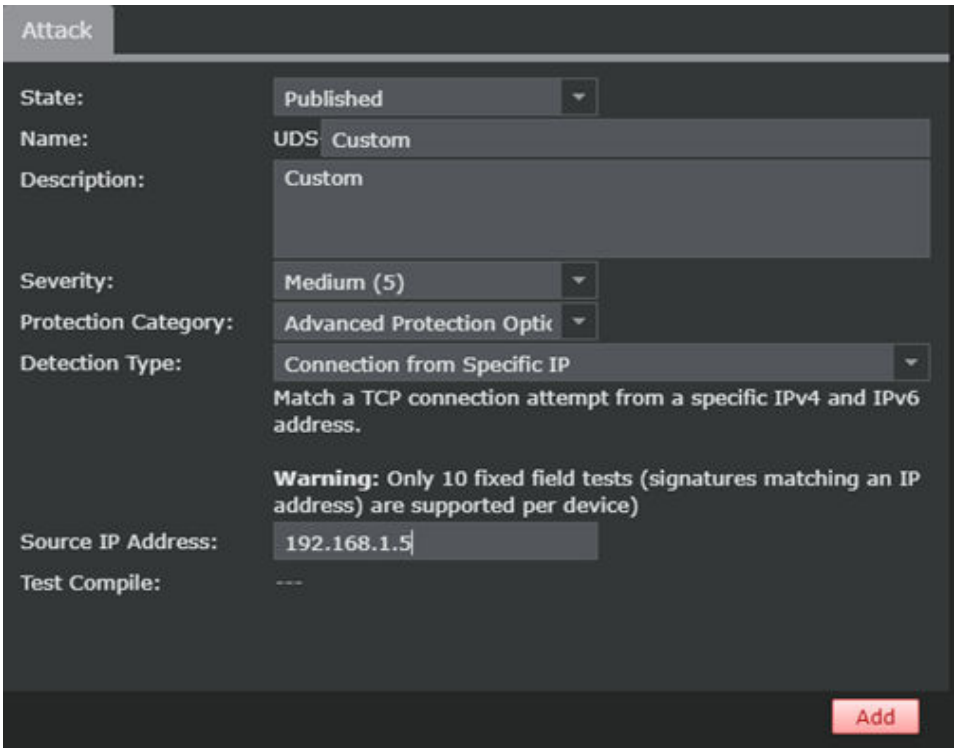
   Severity is set to **Medium (5)** by default.

6. Select the most appropriate **Protection Category** for the attack.

7. Select **Connection from Specific IP** from the **Detection Type** drop-down menu for the attack.

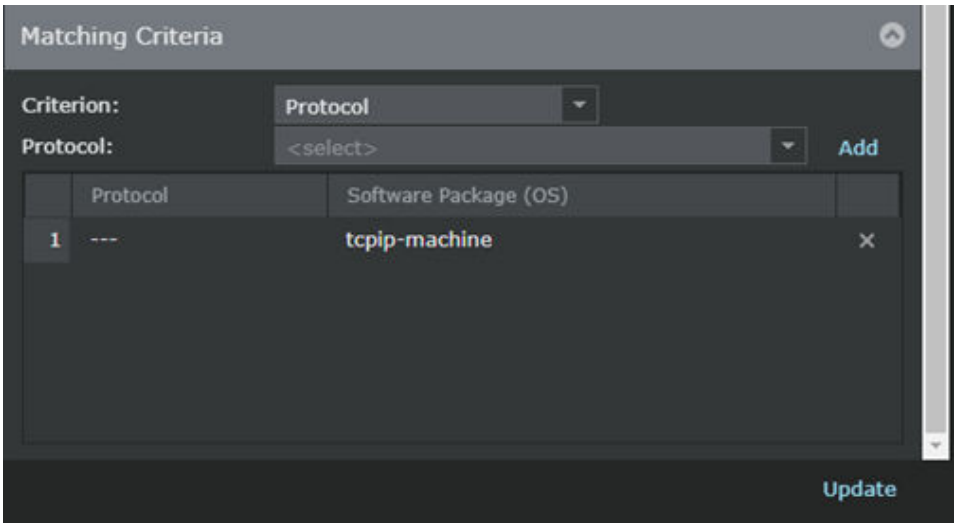
8. Enter the IPv4 or IPv6 **Source IP Address** from which TCP connection attempts are to be detected and click **Add**.

   The attack is listed on the **Native Trellix IPS Format** tab.



9. Double-click on the attack that you created on the **Native Trellix IPS Format** tab.

   In the **Matching Criteria** section, the **Software Package (OS)** is selected as **tcpip-machine**.



You can modify the values of the signature on the **Signature-<signature name>** tab. You can also add more conditions to the signature. For example, do the following to add conditions based on TCP flags:

1. Add a signature or edit a signature.
2. In the corresponding signature, click +.
3. Add a condition by clicking AND or OR.
4. From **Comparison Type** list, select **Single Fixed Field Match**.
5. Select **tcp** from the **Protocol** drop-down menu.
6. Select the required flag from the **Protocol Field.**
7. Select the **Operator**.
8. Enter the value to match in the **Integer or IP to Match** field.
9. Select **Ignore Bitmask** if you want to ignore the bitmask.
10. Click **Save**.

10. Click **Save** in the **Custom Attack** interface.

    Until you save the attack in the database, value for the **Trellix IPS ID** column is not generated. The Sensor detects this attack after you deploy pending changes to the corresponding Sensor (Devices → <Admin Domain Name> → Global → **Device Manager**. Select the **Sensors** tab. Then, select the required Sensor from list and click **Sync**).

Create an exploit attack without template

This section explains how to create Trellix IPS Exploit Attacks and the constituent signatures.

To create a Trellix IPS Exploit Attack instance, you start by first adding a new attack. Attacks are configured first because signatures logically relate to attacks as one particular means of detection.

Attack creation includes impact categorization for proper policy integration and enforcement. Each policy — those provided with Trellix IPS and those you create — consists of rule sets, which contain multiple categories of attacks. Attacks are categorized by the protocols, operating systems, and applications they impact. Within the Custom Attack Editor, you define the impact

categories wherein your attack definition best fits, so that when you save it in the Manager, it will be published in one or more rule sets.

Steps:

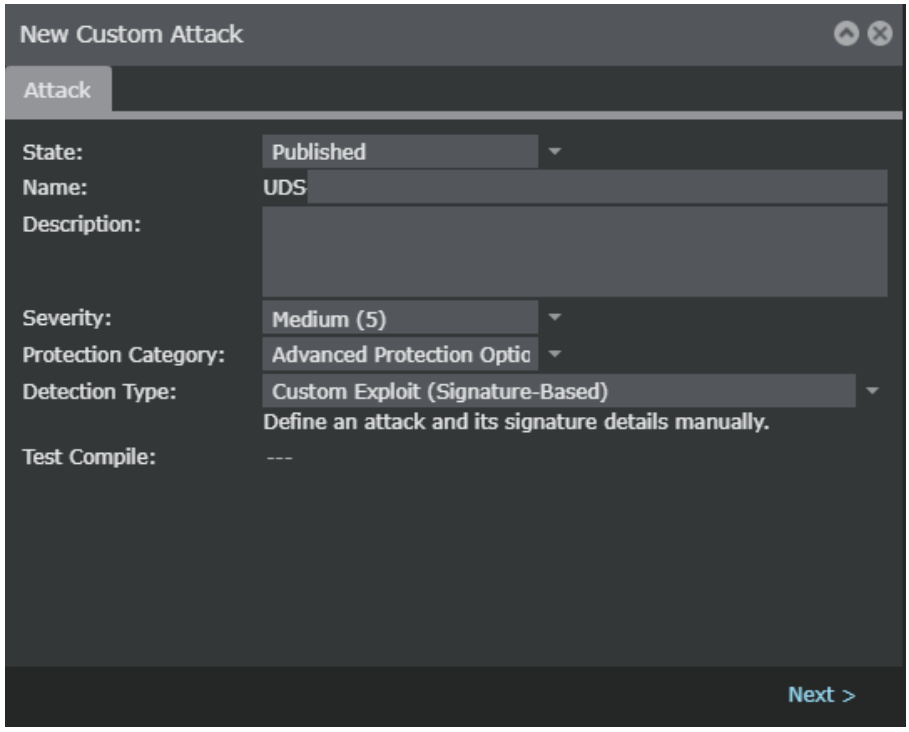
1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.

2. Click .

   The **New Custom Attack** interface opens.

Figure 782. Add Exploit Attack window



3. In the **Name** field, type a new name for your attack. **UDS** (User-Defined Signature) is appended at the front automatically when you save the attack. For example, if you name the new attack "HTTP Attack XYZ", it appears as "UDS-HTTP Attack XYZ" in the Custom Attack Editor as well as in the attack database when you save the attack.

   NOTE

   The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.

5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).

6. Select the most appropriate **Protection Category** for the attack.

7. Select **Custom Exploit (Signature-Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.
9. Select an appropriate **Attack Target**.
10. Select an appropriate **Blocking** type.
11. On the **Matching Criteria** tab:
    a. Complete at least one of the following:
        1. Categorize the attack definition by protocol. For example: HTTP, FTP, DNS. In the **Criterion** dialog box, select **Protocol** and then select a protocol from the **Protocol** list.
        2. Categorize by software package (that is, application and operating system). For example: Internet Explorer on Windows 2003. In the **Criterion** dialog, select **Software Package (OS)** and then select one package from the list. Optionally, select an **Operating System**.
    b. Click **Add**.
    c. Repeat steps to specify more protocols or packages.

> **NOTE**
>
> It is mandatory that you specify at least one impact package or protocol. If you are not sure about the impact package or protocol, select tcpip-machine as the impact package.

> **TIP**
>
> Check the rule sets (Inbound and Outbound) of the policy you plan to enforce to determine whether your attack will be selected. You also have the option of creating a new rule set in order to enforce your Custom Attack.

12. Once your attack configuration is complete, continue to Creating a Signature.

Create a signature

Create one or more signatures to detect an attack. This section assumes that you are adding signatures to the attack that you just created in the previous section. That is, the Add Trellix IPS Attack interface is open and the attack you created is yet to be saved in the Manager server. If you are adding signatures to a previously saved attack, double-click on the attack in a tabbed region to open the Edit Trellix IPS Attack interface.

> **NOTE**
>
> You can create up to 15 signatures per attack definition.

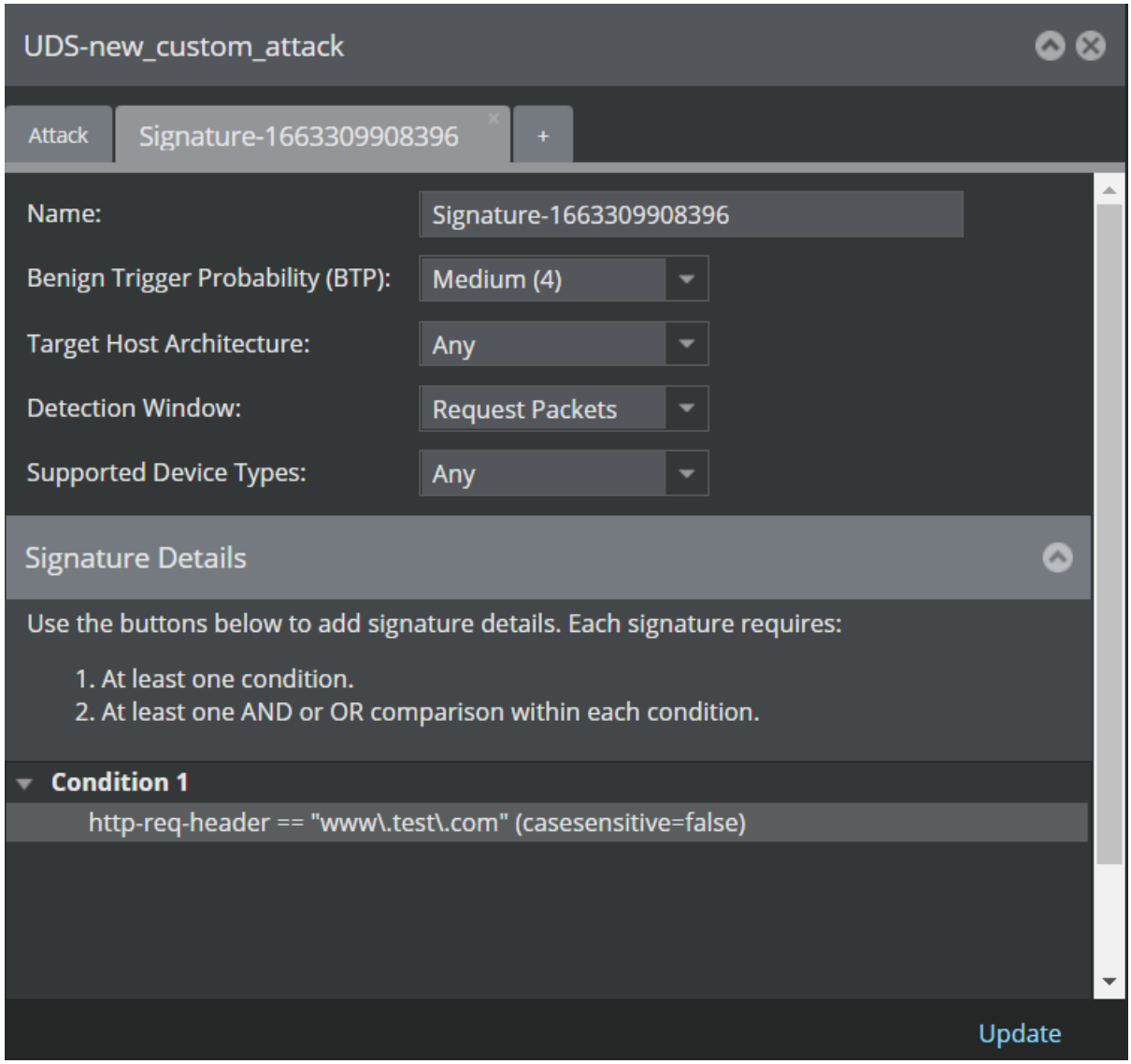
Steps:

1. In the **New Custom Attack** interface, click on the **Signature-<signature name>** tab.

   The signature tab appears.

2. Optionally clear the **Signature Name** and type a new one.
3. Select a **Benign Trigger Probability** value.

Figure 783. New Signature window



4. Select a **Target Host Architecture**. The default is **Any**.
5. Select a **Detection Window**. The choices are as follows:
   - **Single Packet**
   - **Request Packets**
   - **Response Packets**
   - **Entire Flow**
6. Based on the Sensor model that you plan to use you can select any of the following options:
   - **NS-series Only**

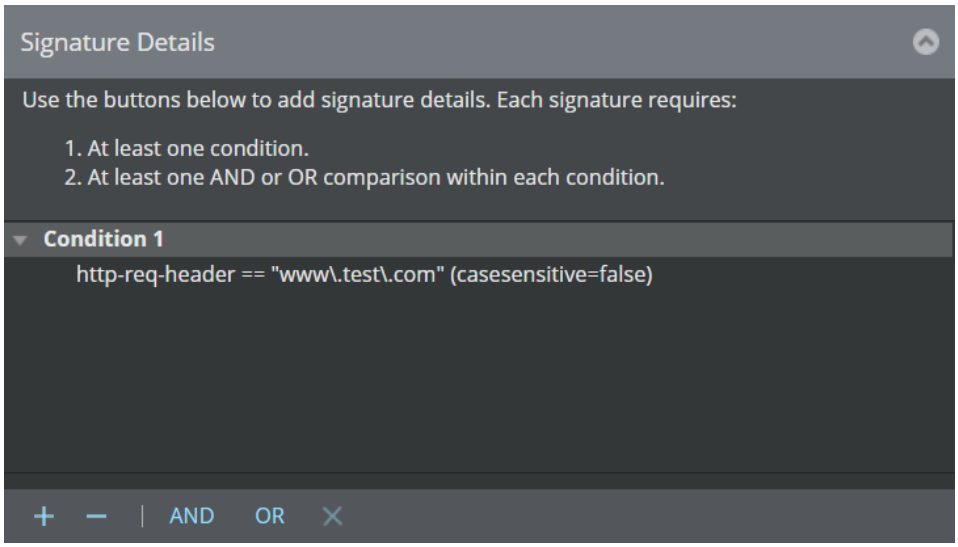
- **VM-series Only**
- **Any**

7. Under **Signature Details** panel, **Condition 1** is added and selected by default.

   To add another condition, do the following:

   a. Click + under **Signature Details**. **[AND THEN] Condition 2** appears in the blank white field.

   b. Click **Condition 1** or **[AND THEN] Condition 2** so that it is highlighted.



   c. Do one of the following:

      1. Click AND under Comparisons to add an AND comparison.
      2. Click OR under Comparison to add OR comparisons.

   d. Select a comparison type from the **Comparison Type** list. The choices are as follows:

      - **String Pattern Match**: The pattern contains a sequence of characters which will be used for detections. It can contain alphanumeric and hexadecimal sequence.
      - **Numeric Value Match**: The pattern contains only numeric values.
      - **Numeric Range Match**: The pattern contains only numeric values. You can configure a minimum and maximum value. These are used to detect numeric values which falls between minimum and maximum value.
      - **Numeric Enumeration Match**: The pattern contains only numeric values. The values may not be in any order but a sequence of numbers against which detection occurs.
      - **Single Fixed Field Match**: This contains mixed values. The input type varies based on the protocol and protocol field selected.
      - **Packet Grep Protocol Match**: This contains alphanumeric or hexadecimal as input and does not contain any regular expression. This will detect patterns in the selected protocol for either request or response. Select this option, only if the protocols are not listed in the **String Pattern Match** or if the requested **Protocol** field is missing from the **String Pattern Match** list.

   Your selection affects what appears in the subsequent dialogs. The **String Pattern Match** option requires knowledge of the Regular Expression Language.

e. From the **Protocol Details** box, select a protocol from the **Protocol** list.

The subsequent options are based on the selected protocol.

> **NOTE**
>
> If you selected **Packet Grep Protocol** from the **Comparison Type** drop-down menu, the available protocols are those packet grep instances created/provided within the **Protocol** drop-down menu.

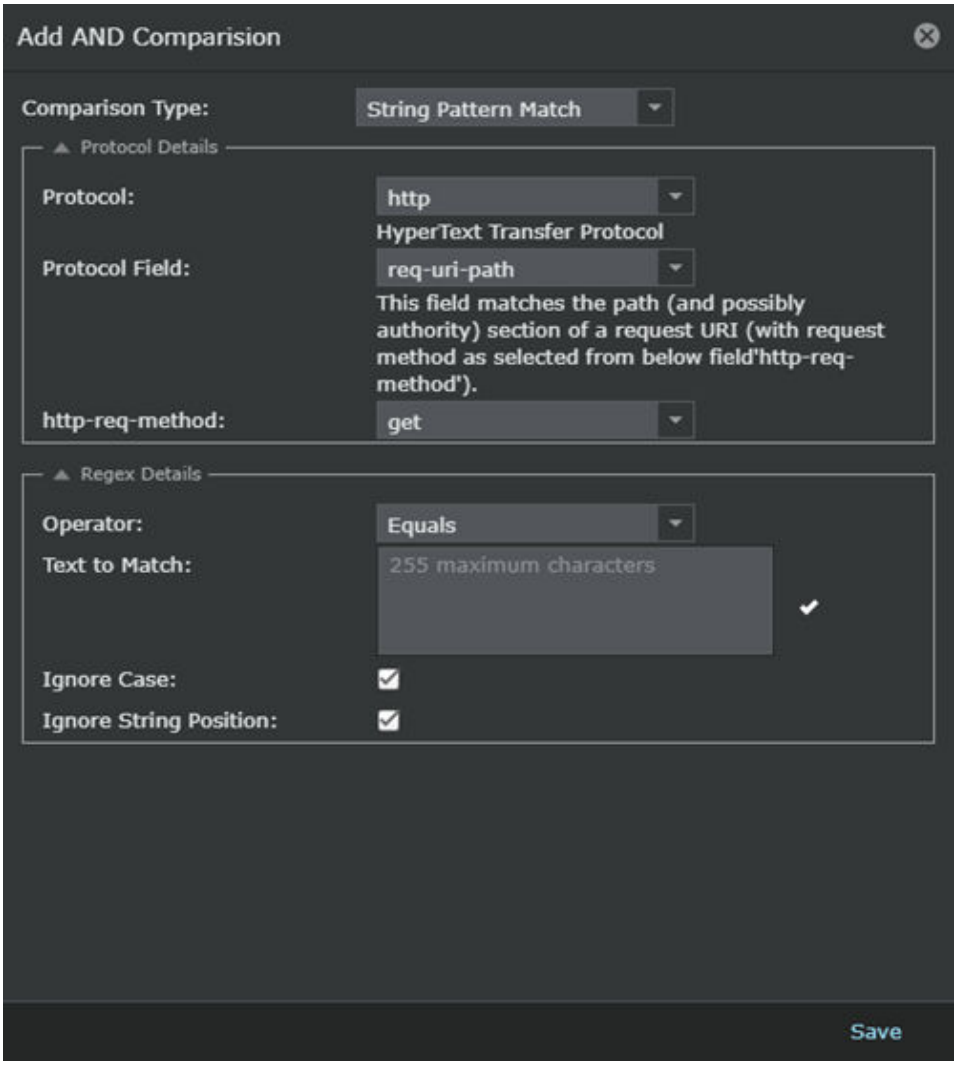
f. Configure the fields for the comparison(s) you have chosen.

> **NOTE**
>
> If selection fields (drop-down menus) are blank, then the protocol and comparison you have chosen cannot be used to create a signature condition; select another protocol and/or comparison combination.

For example, if you want to configure a string match in the URI path of an HTTP GET request:

1. Select **http** for the **Protocol**, **req-uri-path** for the **Protocol Field** and select **get** as the **http-req-method**.

Figure 784. Configure Comparison window



2. From the **Operator** drop-down list in the **Regex Details** section, select the matching criteria as **Equals**.
3. If you are configuring a string pattern match, type your pattern in **Text to Match**.
4. Optionally, click the **Ignore Case** check box if you want the pattern to be matched regardless of [letter] case.
5. Optionally, click the **Ignore String Position** check box if you want the pattern to be matched regardless of string position.
6. Click ✔ to verify that your pattern is valid.

g. Click **Save** when done with the Configure Comparison fields. Your comparison appears under **Condition 1**.

h. Do *one* of the following:

- Click ➕ to add another condition.
- Select **Condition 1** and click **AND** under Comparisons to add another AND comparison.
- Select **Condition 1** and click **OR** under Comparisons to add multiple OR comparisons to your condition. Note that the first of the OR comparison appears under **[AND](One Of)**.

- (Optional) Do *one* of the following if you have created multiple conditions:
- Select a condition and click under to delete a condition, or select a comparison and click to delete a comparison.

8. Optionally, you can add more signatures to your attack by clicking next to the signature tab.
9. Click **Save** in the Custom Attack interface.

   The created Attack and its signatures are saved in the Manager client that you are logged on to.

> **CAUTION**
>
> If you close the Custom Attack Editor without saving the attack, the attack that you created (along with any unsaved changes to other attacks) is lost.

Configure custom reconnaissance attack definition

In the **Custom Attack Editor** (formerly UDS Editor), you create custom recon attacks using both user-defined exploit attacks and Trellix IPS-defined exploit attacks (in sigset) as component attack. You can also define correlated attacks using these individual attack definitions. For example, UDS attacks that check for URI can be further correlated to test for multiple occurrences in a defined time interval to raise a correlated alert.

To configure Custom Reconnaissance Attack Definition:

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.
2. Click .

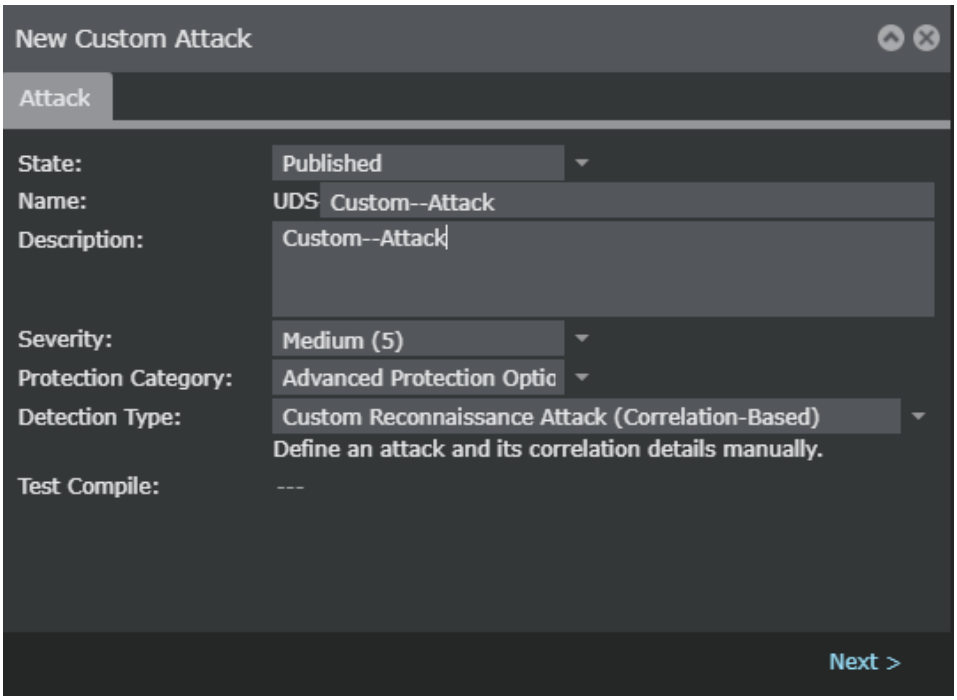
   The New Custom Attack interface opens.
3. In the **Name** field, type the new custom reconnaissance attack.

> **NOTE**
>
> The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

4. Optionally, type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.
5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).
6. Select the most appropriate **Protection Category** for the attack.
7. Select **Custom Reconnaissance Attack (Correlation-Based)** from the **Detection Type** drop-down menu for the attack.

Figure 785. New Custom Attack window



8. Click **Next**.
9. Set the **Benign Trigger Probability (BTP)** for the reconnaissance attack.
10. Set the **Attack Subcategory** from **Correlation Logic** for the attack.

    The following subcategories are available:

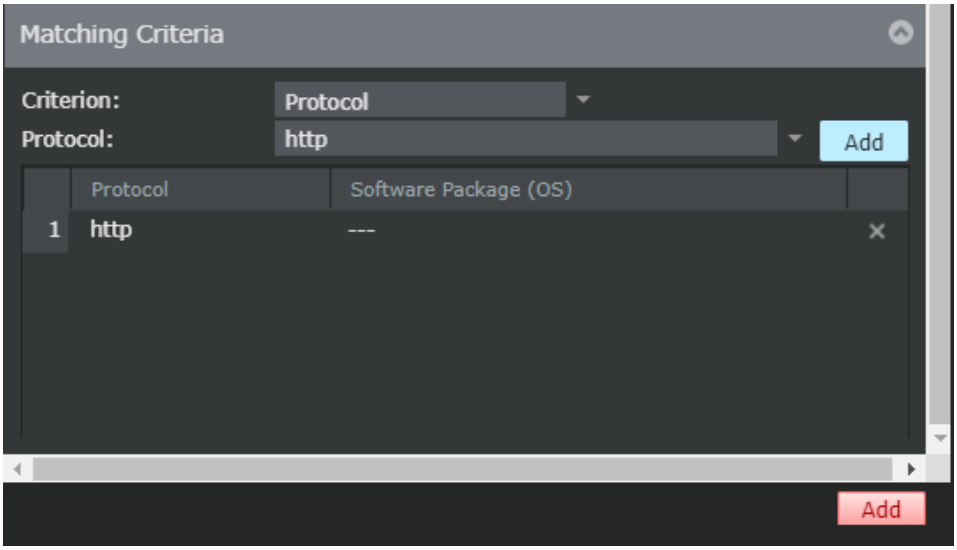
    - **brute-force**
    - **fingerprinting**
    - **host-sweep**
    - **port-scan**
    - **service-sweep**

    You can select the above options using a single component attack for correlation. Select **fingerprinting** option if you wish to use multiple component attacks for correlation.
11. In the **Attack** field, type the attack name and select the relevant attack from the list.

    You can select either a Trellix IPS-defined exploit attack or a user-defined custom attack as a component attack.
12. Set the **Threshold** value between 1 and 255.
13. Set the **Interval** in seconds between 1 and 65535.
14. Select the **Generate Individual Conponent Alerts** check box.
15. Select either **Protocol** or **Software Package (OS)**, and click **Add**.

    You can add more than one matching criteria to your custom reconnaissance attack.

Figure 786. Add Protocols Packages page



16. Click **Add**.
17. Review all the settings, and click **Save**.

    When traffic passing through the Sensor exceeds the threshold count set for the custom reconnaissance attack within a configured Interval, the Sensor raises an alert to the Manager. You can view the alert in the **Attack Log** page. The alerts **Summary** shows the type of attack as either a Trellix IPS Exploit or Trellix IPS Reconnaissance.

> **NOTE**
>
> The custom reconnaissance attacks are staged by the IPS engine when:
>
> - One or more of its component attacks is deleted.
> - One or more of its component attacks is marked as **Staged**.

Configure custom attack definition for multiple attacks correlation

To create custom attack definition for multiple attack correlations perform the following steps:

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.
2. Click .

   The New Custom Attack interface opens.
3. In the **Name** field, type the new custom reconnaissance attack.

> **NOTE**
>
> The Trellix IPS ID is provided by the Manager when you save it in the Manager server.

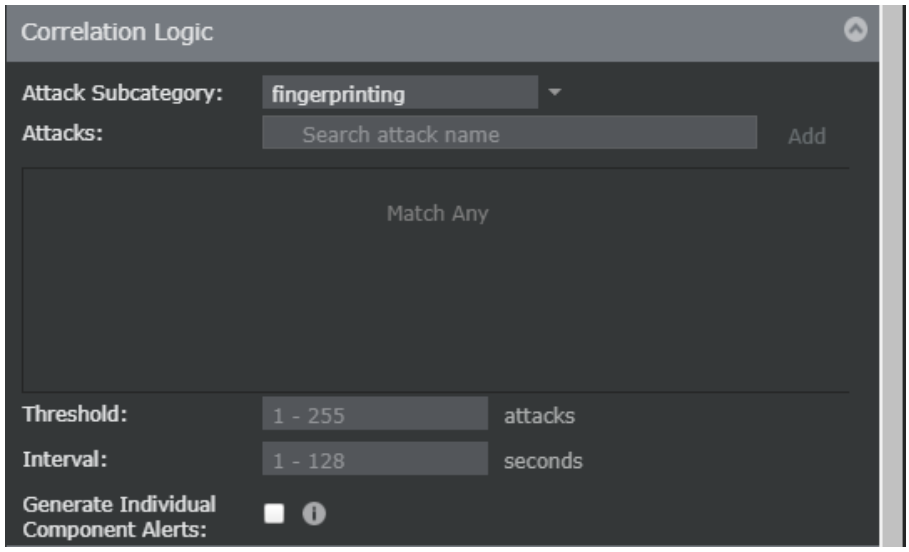
4. Optionally type a **Description** for your attack.

   This area can be used for your notes or other specific information pertinent to your new attack.
5. Select a severity for your attack by toggling the drop-down list. Choices are High (9, 8, 7), Medium (6, 5, 4), Low (3, 2, 1), and Informational (0).
6. Select the most appropriate **Protection Category** for the attack.
7. Select **Custom Reconnaissance Attack (Correlation-Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.
9. If you wish to create a custom reconnaissance attack using multiple attacks correlation, select the **Correlation Method** as **fingerprinting**.
10. Use the **Add** button to add multiple attacks as the component attacks for the custom attack that you are creating.

    You must select a minimum of 2 component attacks for multiple attacks correlation.

> **NOTE**
>
> You can include a component attack in 10 custom reconnaissance attacks.

Figure 787. Custom Attack Definition for Multiple Attacks Correlation



11. Set the **Threshold** value between 1 and 255.
12. Set the **Interval** in seconds between 1 and 65535.
13. Select the **Generate Individual Conponent Alerts** check box.
14. Click **Add**.
15. Review all the settings, and click **Save** in the **Custom Attacks** window.

Regular expression language

This chapter describes the proper method of writing pattern-matching signatures using the Regular Expression Language supported for Trellix IPS Custom Attacks.

NOTE

Signature creation requires a working knowledge of protocols and the data they carry across your network, as well as an ability to write a proper signature using a regular expression language. This information is intended for advanced network security personnel who have experience with Trellix IPS Custom Attack creation.

Signature creation is based on a set of expressions in a defined syntax, also known as regular expressions.

Regular expression syntax

All expressions are generated from the following set of rules for pattern representation, and only from these rules:

Printable characters

You can use any alphanumeric characters for basic string matching purposes.

- lower case 'a' through 'z'
- upper case 'A' through 'Z'
- numerals '0' though '9'

Thus, typing "confidential" and marking the test as Case-Insensitive denotes that either "Confidential" or "confidential" will match. Likewise, the string "007forever" marked as Case-Sensitive denotes a search for the exact phrase "007forever".

Special characters

Special characters are those that are non-alphanumeric/punctuation. They require a special representation so that they are visible and not translated as formatting. A "\r" is a carriage return, part of what makes your cursor go to the next line.

Action or Symbol	ASCII	Type as:
carriage return	CR	\r
newline	NL or LF	\n
horizontal tab	HT	\t
vertical tab	VT	\v
formfeed	FF	\f
backspace	BS	\b
bell char	BS ??	\a
match any single character		.

Pattern	Read as:
first line\nsecond line	first line second line

Hexadecimal values

Hexadecimal values can be represented as two alphanumeric characters (a to f, and A to F, and 0 to 9) preceded by "\x"; thus "\x00" is a proper hex string. The range is from \x00 to \xFF, and matching must be case-insensitive.

Pattern	Description
\x90\x90\x90	Example of hex used to represent binary; often used in shellcode attacks.

Character class

To search for a range of characters, define the range using a hyphen between characters [A - Z].

Pattern	Description
[1-9]	Any digit from 1 to 9 (1, 2, 3, 4, 5, 6, 7, 8, 9)
[a-j]	Any lowercase letter from a to j.
[A-H]	Any capitalized letter from A to H. **NOTE** A search such as [a-F] is not valid.

Optional

To make a character or pattern optional, use parentheses with a trailing question mark: (*string*)?.

Pattern	Description
code red (virus)?	The search for the word "virus" is optional. This pattern matches if either "code red" or "code red virus" is detected.

Alternation

To search using alternation, use the pipe (|) character to separate strings (a|b).

Pattern	Description
(hi|hello)	Either "hi" or "hello" must match.
(su|soo)per	Either "super" or "sooper" must match.

Repeating

To repeat, append a number in brackets to the pattern: for example, (*string*){*n*} means the string must be repeated *n* times for matching purposes.

NOTE

You must enclose the string in parentheses, and the repeating value must be enclosed in brackets.

NOTE

The number in braces must be greater than 0 (n>0).

Pattern	Description
(1){5}=11111	A string of five consecutive 1s without spaces must match.
(text){3}=texttexttext	A string consisting of the word text repeated three times without spaces must match.

To set a minimum and maximum, represent the equation as (*string*){3,5}

Pattern	Description
(1){3,5}=111 or 1111 or 11111	A string of three, four, **OR** five consecutive 1s without spaces must be match.

Anchors

To specify a string that starts or ends a line, use the ^ (carat) or $ (dollar) characters. Using both ^ and $, you can also specify a string that makes up an entire line—start to end.

- Start of line anchor: ^(string)
- End of line anchor: (string)$

Pattern	Description
^Hi	The first word of a line must be "Hi".
bye$	The last word of a line must be "bye".
^Hacked by J03$	"Hacked by J03" forms an entire line.

Reserved characters

The following characters are reserved for regular expression control. They *must* be escaped; that is, prefixed with backslash (\) when they appear as part of a normal matching pattern (that is, not part of an expression), except where noted otherwise.

Name	Symbol	Proper Syntax
backslash	\	\\
dot (period)	.	\.
pipe	|	|
dash (hyphen)	-	\-
carat	^	\^
dollar symbol	$	\$
open paren	(	\(
close paren	)	\)
open bracket	[	\[
close bracket	]	\]

Pattern	Read as:
(text)	text
\(text)	\(text\)
www.trellix.com	www*trellix*com, where * is a single wildcard
www\.trellix\.com	www.trellix.com

Limitations of a custom reconnaissance attack

The limitations of Custom Reconnaissance attack are listed below:

- The maximum threshold count for Custom Reconnaissance attack is 255 for single-AID (type: port scan, host sweep, service sweep, and brute force).
- A component attack can only be included in 10 Custom Reconnaissance attacks.
- A minimum of 2 component attacks need to be added for a multiple-AID (type: fingerprinting) Custom Reconnaissance attack.
- Maximum 5 component attacks can be added in a multiple-AID (type: fingerprinting) Custom Reconnaissance attack.
- Maximum 300 Reconnaissance attacks (Trellix IPS and Custom) can be pushed to the Sensor.
- Maximum 300 component attacks can be pushed to the Sensor.
- Maximum 150 Custom Reconnaissance attacks can be added to the Custom Attack Editor.

Mechanics of a Snort custom attack

This section explains the structure of a Snort Custom Attack. It also provides some information on how to construct valid Snort rules.

Structure of a Snort custom attack

A Snort Custom Attack is made up of one Snort rule. To define a Snort Custom Attack, you either write the Snort rule directly in the Custom Attack Editor or import it into the Editor from a file. The Sensor automatically creates the Snort Custom Attack record for each rule that you write or import.

When the Sensor creates the attack for a Snort rule, it automatically defines the values for fields such as attack name and attack severity. The following section explains how the Sensor defines the attack-level values for a Snort Custom Attack:

For the Attack Name, the format that the Sensor uses for the name is SNORT:<the text specified for the msg rule option in the rule>(<SID>). So, this name is modified accordingly if you modify the msg text or the SID of the rule.

NOTE

msg rule option and a unique SID are mandatory for a Snort Custom Attack.

Blocking is set to attack packet for all Snort Custom Attacks. You cannot modify this.

On the **Impact** tab, the Severity is based on the classtype keyword or the priority tag. Each classtype has a default priority defined. Typically, the classtypes with the default priority values are defined in the classification.config file. If a rule has both classtype keyword and priority tag, the severity is based on the priority tag.

The Sensor assigns the severity for a Snort custom attack based on the following:

- A priority 1 Snort attack definition is assigned a severity of High.
- A priority 2 Snort attack definition is assigned a severity of Medium.
- A priority of 3 or higher is assigned a severity of Low.

When you modify the classtype or the priority tag value of a rule, the Sensor will also modify the severity accordingly. This means when you save the attack to the Sensor server, the rule sets (and policies) in which the attack was published may change.

For the Exploit category, tcpip-machine is selected as the package with any as the OS. You cannot add, delete, or modify any impact package or protocol for Snort Custom Attacks.

Structure of a snort rule

This section discusses the basic structure of a Snort rule and the Snort rule elements that are supported in Trellix IPS. This section contains information on the syntax that you should use in Trellix IPS for each element. You can also find an example rule for each element, wherever applicable.

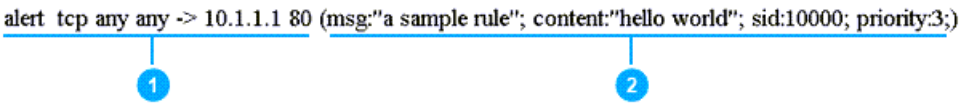
How you combine various Snort rule elements to form a rule depends on your security requirements. This information is out of scope of this document because the requirements can vary from network to network.

NOTE

The Snort rules that you plan to use in Trellix IPS should conform to Snort rules language.

A Snort rule in Trellix IPS can run into multiple lines. A typical Snort rule has two logical sections — rule header and rule options.

The following is an example of a simple but valid Snort rule.



Item	Description
1	Rule header section
2	Rule options section

As shown above, the rule header section starts at the beginning of the rule and ends at the opening parenthesis. This section contains the following:

- Action — In the sample above, it is alert.
- Protocol — In the sample above, it is TCP.
- Source and destination IP addresses — In this case, the source is any and the destination is 10.1.1.1
- Source and destination ports — In this case, the source port is "any" and the destination port is 80.

The rule options section is enclosed within the parentheses. This section contains alert messages and information on which parts of the packet should be inspected to determine if the rule action should be taken. In the rules options section, the words ending in a colon are option keywords.

NOTE

In Trellix IPS, the rule options section should have at least the msg and the sid keywords with values. Rule options enable you accurately define the attack traffic that the Sensor should look for.

All the elements that make up a rule must be true for the Sensor to raise an alert and take the defined response action. You specify the response action for the Snort Custom Attack in the IPS Policy Editor.

Rule header section

In the rule header section, you define the following:

- Action the Sensor needs to take when it sees the attack traffic
- Transport layer protocol of the attack traffic
- Source and destination IP for the attack traffic
- Communication port at both the source and destination of the attack
- Direction of the traffic that the Sensor should inspect

The items listed above are discussed in detail in the subsequent sections.

Rule action

The action specifies how the Sensor should respond when it detects traffic as defined in the rule. In Trellix IPS, the only action that you can specify in a Snort rule is to send an alert to the Manager. The procedure to configure other response actions such

as packet log and packet drop is the same as that of the regular Trellix IPS attacks. That is, use the IPS Policy Editor to configure these actions.

Protocols

In the protocols section you specify the protocol to which the Sensor should apply the rule.

The options are:

- TCP
- UDP
- ICMP
- IP
- HTTP
- FTP
- TLS
- SMB
- DNS

For more information, see http://suricata.readthedocs.io/en/suricata-3.2.3/rules/intro.html#protocol

IP addresses

You need to specify the IP address of the source and target for the attack traffic. The available options are listed below:

- You can use the keyword "any" to specify a wildcard IP address.
- You can use CIDR blocks to specify a range of IP addresses. Example: 172.16.230.0/24
- You can specify a list of IP addresses by specifying them inside square brackets with comma as the separator. Example: [172.16.230.0/24, 172.16.231.0/24]
- You can use variables to specify particular IPs or a range of IPs.

Port numbers

You need to specify the port numbers used at the source and the target for the attack traffic. The available options are listed below:

- You can use the keyword "any" to specify a wildcard port number.
- You can specify a port range using the range operator, colon.

  Example: 1:1024. This indicates that the port must be between 1 and 1024, both inclusive.

  Example: 100: This indicates the port must be equal to 100 or more.

  Example: :500. This indicates that the port must be less than or equal to 500.
- You can use variables to indicate ports.

Direction operator

The direction operator -> indicates the direction of the traffic that the Sensor should apply the rule to. The IP address and port numbers on the left side of the direction operator are that of the source and the ones on the right side are that of the destination of the attack traffic.

Rule options section

The rule options section is the more critical section of a Snort rule. The rule options are to be separated by a semicolon. In a rule option, the keyword and argument are separated by a colon.

Rule options fall into one of the following categories:

- General: These options contain the metadata for the rule but have no effect on attack detection.
- Payload: These options look for data inside the packet payload and can be interrelated.
- Non-payload: These options look for non-payload data.
- Post-detection: These options indicate what happens when an attack is detected. These options are not relevant in Trellix IPS. Instead, you can configure the response actions in the IPS Policy Editor.

General rule options

msg

In the msg rule option, you indicate the alert message. It is a simple text string that utilizes the \ as an escape character to indicate a discrete character such as a semi-colon.

Syntax:

```
msg: "<message text>";
```

When you create a Snort Custom Attack in the Custom Attack Editor, the Manager assigns the attack and rule name, which you cannot edit directly. The format of the name is as below:

Snort: <text entered for msg option> (sid: <sid value>)

The argument of the msg option features in the attack and rule name that the Manager assigns. Changing the msg argument or sid value and saving the rule will change the attack and rule name accordingly.

reference

In a rule, you can use the reference keyword to include references related to the corresponding attack traffic. For example, it could be the bugtraq or CVE id of known vulnerabilities. It could also be the address of a website that provides the details of the attack.

The following are the supported systems that you can specify in the reference option:

- bugtraq
- CVE
- Trellix IPS ID

- Arachnids
- URL

Syntax:

```
reference:<id system>, id;
```

Examples:

reference: bugtraq, 514;

reference: url, www.microsoft.com/technet/security/bulletin/MS99-034.mspx;

You can view the references that are currently available in the Manager.

gid

gid stands for generator id and is not relevant in Trellix IPS. So, do not use them in your rules.

sid

sid stands for Snort rule ID. You must specify a unique sid for each Snort rule in the Manager. For Snort Custom Attacks that failed to import, the Manager assigns -1 as the sid.

Syntax:

```
sid:<sid value>;
```

rev

This enables you to identify any revisions of an existing rule. It is not a mandatory option, but Snort Custom Attacks without the rev option are converted with a warning. When you edit a Snort Custom Attack in the Manager, you can modify the rev value for your reference.

If you want to re-import a Snort Custom Attack with the same sid, then you can change the rev value and import it. The Manager overwrites the existing Snort Custom Attack with the one that you last imported.

Syntax:

```
rev:<revision integer>;
```

classtype

This is one of the options that you can use to categorize a Snort rule. In the Snort rules provided by Snort.org, the classtypes with the default priority are defined in the classification.config file. You can use these classtypes by importing the classification.config file into the Manager. Alternatively, you can define your own in a .config file and import it into the Manager. If you are defining your own classtype, then make sure you also assign a priority to the classtype.

NOTE

A rule must have a classtype or a priority.

NOTE

You can view the classification types that are currently available in the Manager.

Syntax for using a classtype in a rule is as follows. This assumes that the class name is available in the Manager database:

```
classtype: <class name>;
```

Syntax (for defining a classtype in a .conf file):

```
config classification: <class name>,<class description>,<default priority>
```

Example:

config classification: attempted-user,Attempted User Privilege Gain,1

priority

Using the priority option you can assign a severity to the rule. This overrides the default severity defined in the classtype.

The Manager assigns the severity for a Snort custom attack based on the following:

- A priority 1 Snort attack definition is assigned a severity of High.
- A priority 2 Snort attack definition is assigned a severity of Medium.
- A priority of 3 or higher is assigned a severity of Low.

Syntax:

```
priority: <integer value>;
```

Payload rule options

This section describes the options and conditions that you can apply to the payload in TCP, UDP, ICMP, IP, HTTP, FTP, TLS, SMB, or DNS traffic. Note that some of the options work differently in Trellix IPS when compared to Snort. Also, some options are not supported.

The payload rule options discussed in this section include content modifier and preprocessor rule options. You use content modifiers to change the way content option works. These are specifications that the Sensor should apply on the content data before it looks for a match.

Content

This enables you to specify the content that a Sensor should look for in the packet payload. If the Sensor finds traffic matching what you specify in the content, then it raises an alert and also takes the defined response action such as packet log or packet drop.

The option data for the content keyword can contain text, binary (hex values), or mixed text and binary data. The binary data must be enclosed within the pipe (|) character and represented as bytecode.

NOTE

- The following characters must be escaped inside a content rule:
  - : (colon)
  - ; (semi colon)
  - \ (backward slash)
  - " (double quotes)
- Though you can specify even a single-byte token, the longer the content value, the accurate the detection will be. The maximum length of a content or uricontent for NS-series Sensors is 256 bytes.
- Make sure the content option does not contain any generic values identified by Trellix IPS (some examples are listed below). Such rules can severely impact Sensor performance.
  - GET
  - POST
  - Host:
  - User-Agent

Syntax: **`content:"<content string>";`**

Example rules:

- **`alert tcp any any -> 10.1.1.1 80 (msg:"command dot exe attempt"; content:"cmd.exe"; flow:to_server; sid:2001; priority: 1;)`**
- **`alert tcp any any -> 10.1.1.1 80 (msg:"command dot exe attempt"; content:"|63 6D 64 2E 65 78 65|"; flow:to_server; sid:2001; priority: 1;)`**
- **`alert tcp any any -> 10.1.1.1 80 (msg:"command dot exe attempt"; content:"|63| m |64 2E 65 78 65|"; flow:to_server; sid:2001; priority: 1;)`**

This section explains the content modifiers, which you can use to change the way content option works. The content modifiers are specifications that the Sensor should apply on the content data before it looks for a match.

nocase

Use this if you want the Sensor to look for the content data regardless of the case.

Syntax: **`nocase;`**

Example rule:

`alert tcp any any -> 10.1.1.1 80 (msg: "command dot exe attempt"; content: "cMd.eXe"; nocase; flow:to_server; sid:2002; priority: 1;)`

rawbytes

Use this if you want the Sensor to consider the content data as raw data. Then Sensor matches the content data against the non-normalized traffic.

Syntax: **`rawbytes;`**

For example, http://www.example.com/big%20cars/blue%20colored%20cars/pictures.htm

will normalize to http://www.example.com/big cars/blue colored cars/pictures.htm.

If you want the Sensor to find "blue%20color" in the traffic before normalization (that is, as seen in the "wire"), then your rule could be as shown below:

```
alert tcp any any -> 10.1.1.1 80 (msg: "example rule for rawbytes"; content:"blue%20color"; raw-
bytes; flow:to_server; sid:2003;priority:1;)
```

If you do not specify rawbytes for the same rule, the Sensor will look for "blue%20color" in the normalized traffic, which it would never find.

http_client_body

Use this modifier if you want the Sensor to look into only the normalized http client body.

Note the following:

- Content should precede http_client_body, and it applies only to the immediately preceding Content.
- If you use http_client_body with *offset or depth*, then these options are calculated from the beginning of the http payload. Consider the example rule below:

  ```
  alert tcp any any -> any any (msg: "example rule for http_client_body"; content:"red"; http_cli-
  ent_body; depth:30; sid:2007;priority:1;)
  ```

  The Sensor looks for "red" within 30 bytes from the beginning of the http payload and not from the beginning of the http client body.
- Because this modifier works only for the normalized data, you cannot use it with rawbytes for the same content.

Example rule:

```
alert tcp any any -> any any (msg: "example rule for http_client_body"; content:"red"; con-
tent:"blue"; http_client_body;sid:2007;priority:1;)
```

For this rule, the Sensor looks for "red" in the entire payload and for "blue" only in the normalized HTTP request.

http_cookie

The http_cookie modifier is supported in Trellix IPS.

http_header

In this case, the Sensor checks for the content only in the normalized HTTP request.

Note the following:

- Content should precede http_header, and it applies only to the immediately preceding Content.
- If you use http_header with *offset or depth,* then these options are calculated from the beginning of the payload. Consider that you created a rule as shown below:

  ```
  alert tcp any any -> 10.1.1.1 80 (msg: "example rule for http_header"; content:"user";
  http_header; depth:100; sid:2008;priority:1;)
  ```

  The Sensor looks for "user" within 100 bytes from the beginning of the http payload.

- You cannot apply the http_header and rawbytes on the same content.

Syntax: **`http_header;`**

Example rule:

```
alert tcp any any -> any any (msg:"example for http_header"; content:"red"; con-
tent:"user";http_header;sid:2008;priority:1;)
```

In this rule, the Sensor looks for "red" in the entire payload and for "blue" just in the normalized HTTP header part of the payload.

http_method

In this case, the Sensor checks for the content only in the normalized HTTP method section within a HTTP request.

Note the following:

- Content should precede http_method, and it applies only to the immediately preceding content.
- If you use http_method with *offset or depth,* then these options are calculated from the beginning of the http payload and not within a specific http field. Consider that you created a rule as shown below:

  ```
  alert tcp any any -> any any (msg: "example rule for http_method"; content:"post"; http_method;
  depth:5; sid:2009;priority:1;)
  ```

  The Sensor looks for "post" within 5 bytes from the beginning of the http payload.
- You cannot apply the http_method and rawbytes to the same content.

Syntax: **`http_method;`**

Example rule:

```
alert tcp any any -> any any (msg:"example for http_method"; content:"red"; content:"PUT";http_meth-
od;sid:2009;priority:1;)
```

For this rule, the Sensor looks for "red" in the entire payload and whether the HTTP method is PUT.

http_uri

In this case, the Sensor checks for the content only in the normalized request URI section.

Note the following:

- Content should precede http_uri, and it applies only to the immediately preceding Content.
- Functionally, using http_uri is same as using the uricontent option explained later in this section.
- If you use http_uri with *offset or depth,* these options are calculated from the beginning of the http payload. Consider that you created a rule as shown below:

  ```
  alert tcp any any -> any any (msg: "example rule for http_uri"; content:"red"; http_uri;
  depth:50; sid:2009;priority:1;)
  ```

  The Sensor looks for "red" within 50 bytes from the beginning of the http payload.
- You cannot apply http_uri and rawbytes on the same content.

Syntax: **`http_uri;`**

Example rule:

```
alert tcp any any -> any any (msg:"example for http_uri"; content:"red"; content:"blue"; http_uri;
sid:2009; priority:1;)
```

In this rule, the Sensor looks for "red" in the entire payload; "blue" just in the normalized request URI.

http_raw_cookie

This searches the extracted unnormalized cookie header field of a HTTP request or a HTTP response. Since this is a content modifier to the previous content, there must be a content in the rule preceding the http_raw_cookie rule option.

> **NOTE**
>
> In a Snort custom attack, you cannot use http_raw_cookie modifier with rawbytes or http_cookie modifiers for the same content.

Syntax: **`http_raw_cookie;`**

Example rule:

```
alert tcp any any -> any 80 (msg: "example rule for http_raw_cookie"; content:"red"; content:"blue";
http_raw_cookie;sid:2099;priority:1;)
```

This rule searches only for blue in the extracted unnormalized cookie header field of a HTTP request.

http_raw_header

This searches the extracted unnormalized header fields of a HTTP request or a HTTP response. Since this is a content modifier to the previous content, there must be a content in the rule preceding the http_raw_header rule option.

> **NOTE**
>
> In a Snort custom attack, you cannot use http_raw_header modifier with rawbytes or http_cookie modifiers for the same content.

Syntax: **`http_raw_header;`**

Example rule:

```
alert tcp any any -> any 80 (msg: "example rule for http_raw_header"; content:"red"; content:"blue";
http_raw_header;sid:2199;priority:1;)
```

This rule searches only for blue in the extracted unnormalized header fields of a HTTP request or HTTP response.

http_raw_uri

This searches the unnormalized request URI field. Since this is a content modifier to the previous content, there must be a content in the rule preceding the http_raw_uri rule option.

> **NOTE**
>
> In a Snort custom attack, you cannot use http_raw_uri modifier with rawbytes or http_cookie modifiers for the same content.

Syntax: **`http_raw_uri;`**

Example rule:

```
alert tcp any any -> any 80 (msg: "example rule for http_raw_uri"; content:"red"; content:"blue";
http_raw_uri;sid:2499;priority:1;)
```

This rule searches only for blue in the unnormalized URI.

http_stat_code

This searches the extracted status code field from a HTTP response. Since this is a content modifier to the previous content, there must be a content in the rule preceding the http_stat_code rule option.

> **NOTE**
>
> In a Snort custom attack, you cannot use http_stat_code modifier with rawbytes modifier for the same content.

Syntax: **`http_stat_code;`**

Example rule:

```
alert tcp any any -> any 80 (msg: "example rule for http_stat_code"; content:"red"; content:"200";
http_stat_code;sid:7199;priority:1;)
```

This rule searches for status 200 in the extracted status code field of a HTTP response.

uricontent

Use this keyword to search in the normalized request URI field. Note that if the uricontent value has anything that is normalized, then the rule will return negative. For example, if the value contains %20, then the Sensor does not raise an alert because it will check for %20 in the normalized uricontent, which it will never find. To check for non-normalized content, consider using the content option with rawbytes.

Note the following:

- This is same as using content with http_uri.
- If you use uricontent with *offset or depth,* these options are calculated from the beginning of the http payload. Consider that you created a rule as shown below:

  ```
  alert tcp any any -> any any (msg: "example rule for uricontent"; uricontent:red; depth:50;
  sid:2009;priority:1;)
  ```

  The Sensor looks for "red" within 50 bytes from the beginning of the http payload.
- You cannot use rawbytes with uricontent.

Syntax: **`uricontent:[!]<content string>;`**

Example rule:

```
alert tcp any any -> any any (msg:"example for uricontent"; content:"red"; uricontent:"hello+world";
sid:2033; priority:1;)
```

In this rule, the Sensor looks for "red" in the entire payload; "hello+world" just in the normalized request URI.

urilen

This is a condition that enables you to specify the exact, minimum, or maximum lengths, or range of URI lengths to match.

Syntax:

`urilen: int<>int;`

`urilen: [<,>] <int>;`

Examples:

urilen:5

Matches URIs that are 5 bytes in length.

Example rule:

```
alert tcp any any -> any any (msg:"example for urilen"; content:"red"; content:"blue"; urilen:5;
sid:2009; priority:1;)
```

For this rule, the Sensor checks for the strings "red" and "blue" in the entire payload and also sees if the request URI is exactly 5 bytes in length.

urilen: < 5

Matches URIs that are less shorter than 5 bytes.

urilen: 5<>10

Matches URIs that are >= 5 bytes and <= 10 bytes.

PCRE

You can use Perl Compatible Regular Expressions (PCRE) with the related modifiers in the Snort rules. If you use PCRE in a rule, then it should be preceded by a Content. The Content is the triggering token for PCRE options following it. That is, the Sensor checks for the PCRE part of the rule only when the traffic is positive for the preceding Content. Do not use negation operator on the triggering token.

> **IMPORTANT**
>
> PCRE options are resource-intensive on the Sensor. Trellix recommends that you check if there are other options to achieve the same result.

Syntax: **`pcre:[!]"(/<regex>/)[ismxAEGUPHMCOIDKYS]";`**

- / is the only supported delimiter.
- For the PCRE options, by default, the Sensor considers only the first 256 bytes from the beginning of the triggering token.
- When you import or validate the Snort rules in the Manager, you can know the unsupported PCRE options due to which the rules failed to convert successfully.

The following table explains the PCRE-related options supported in Trellix IPS.

Modifier	Description
i	The Sensor ignores the case of the corresponding string.
s	Use this to consider new lines in the dot meta-character.
m	This is used with the anchors (^ and $). Use m with ^ if you want the Sensor to check for the string immediately after a new line as well as at the beginning of the buffer. Use m with $ if you want the Sensor to check for the string immediately before a new line as well as at the end of the buffer.
x	Use this if you want the Sensor to ignore any empty space characters in the buffer unless it is escaped or inside a character class.
A	The Sensor checks if the string is at the beginning of the buffer. This is the same as ^.
E	This is used with $. Without E, $ also matches immediately before the final character if it is a new line but not before any other new lines.
G	This inverts the "greediness" of the quantifiers so that they become greedy only when followed by a question mark.
I	Matches the unnormalized HTTP request URI buffer. This is similar to http_raw_uri in function. Snort does not allow using this modifier along with the HTTP request uri buffer modifier for the same content.
C	Matches normalized HTTP request or HTTP response cookie. This is similar to http_cookie in function. This is not allowed with the unnormalized HTTP request or HTTP response cookie modifier for the same content.
H	Matches normalized HTTP request or HTTP response header. This is similar to http_header. This modifier is not allowed with the unnormalized HTTP request or HTTP response header modifier for the same content. For SIP message, matches SIP header for request or response, similar to how sip_header functions.
P	Matches unnormalized HTTP request body. This is similar to how http_client_body functions. For SIP message, matches SIP body for request or response, similar to how sip_body works.
D	Matches unnormalized HTTP request or HTTP response header, similar to http_raw _header. This modifier is not allowed with the normalized HTTP request or HTTP response header modifier for the same content.
M	Matches normalized HTTP request method, similar to http_method
K	Matches unnormalized HTTP request or HTTP response cookie, similar to http_raw_cookie. This modifier is not allowed with the normalized HTTP request or HTTP response cookie modifier for the same content.
S	Matches HTTP response status code, similar to http_stat_code
Y	Matches HTTP response status message, similar to http_stat_msg

NOTE

\X, \P, \K, \U, \R, and \C escape sequences and back references are not supported.

Example rule:

```
alert tcp any any -> any any (msg: "command dot exe attempt"; content: "user"; pcre:"/cMd.eXe/i";
sid:2030; priority: 1;)
```

This rule first checks for the string, "user". Here, "user" is the triggering token. If "user" is found, the Sensor then checks for the PCRE "cmd.exe" in the first 256 bytes from the beginning of the buffer.

sip_method

This rule option enables you to check for Session Initiation Protocol (SIP) request methods. In the same option, you can specify multiple SIP request methods separated by commas. In this case, it is considered as an OR condition. That is, the rule triggers if there is a match for any of the mentioned request methods.

Syntax:

`sip_method:<method>|<method-list>`

The following request methods are supported:

- invite
- cancel
- ack
- bye
- register
- options
- refer
- subscribe
- update
- join
- info
- message
- notify
- prack

The ! operator is supported. However, if you use !, you can specify only one method in one sip_method option.

Examples:

- **`sip_method:invite`** — This checks for the invite request method.
- **`sip_method:!invite`** — The condition is true if the method is anything other than invite.
- **`sip_method:invite,cancel,bye`** — The condition is true if the method is invite, cancel, or bye.
- **`sip_method:!invite; sip_method:!cancel`** — The condition is true if the method is anything other than invite and cancel.

Example rule:

```
alert udp any any -> 10.1.1.1 5060 (msg:"Example rule"; flow:to_server; sip_method:invite; con-
tent:"SIP/2.0"; nocase; priority:1; sid:20189;rev:1;)
```

sip_stat_code

This rule option enables you to check for SIP response status codes. The condition matches if any of the specified status code is present in the SIP response.

Syntax:

sip_stat_code:<code>|<code>,<code>

The following request methods are supported:

Examples:

- **sip_stat_code:400** — This checks for the status code 400.
- **sip_stat_code:180,182** — The condition matches of the status code is 180 or 182.
- **sip_stat_code:4** — This condition looks for 4xx. That is it is true if the method is anything from 400 to 599. The numbers 1 to 6 are expressed as 1xx, 2xx, 3xx, and so on where, for example, 1xx corresponds to the range 100 - 199.

Example rule:

```
alert udp any any -> 10.1.1.1 5060 (msg:"Example rule"; flow:to_server; sip_stat_code:401; con-
tent:"SIP/2.0"; nocase; priority:1; sid:20289;rev:1;)
```

sip_header

This rule option searches only the extracted header fields of a SIP request or response.

Syntax: **sip_header;**

Example rule:

```
alert udp any any -> 10.1.1.1 5060 (msg:"Example rule"; flow:to_server; sip_header; con-
tent:"SIP/2.0"; nocase; priority:1; sid:20290;rev:1;)
```

sip_body

This rule option points the Sensor to the beginning of the body fields of a SIP message.

Syntax: **sip_body;**

Example rule:

```
alert udp any any -> 10.1.1.1 5060 (msg:"Example rule"; flow:to_server; sip_body; content:"SIP/2.0";
nocase; priority:1; sid:20491;rev:1;)
```

ssl_version

This rule option can check for the SSL version numbers exchanged between the server and the client during the handshake. In the same option, you can check for multiple SSL versions separated by commas. In this case, it is considered as an OR condition. That is, the rule triggers if there is a match for any of the versions. To check for an AND condition involving two or more versions, use separate **ssl_version** rule options.

Syntax:

ssl_version:<version-list>

The ! operator is supported. However, if you use !, you can specify only one method in one sip_method option.

Examples:

- **`ssl_version:sslv2`** — This checks for SSL version 2.
- **`ssl_version:!sslv3`** — The condition is true for any version other than SSL version 3.
- **`ssl_version:tls1.0,tls1.1,tls1.2`** — The condition is true if the SSL version is TLS 1.0, TLS 1.1, or TLS 1.2.
- **`ssl_version:!tls1.0; ssl_version:!tls1.1`** — The condition is true if the SSL version is anything other than TLS 1.0 and TLS 1.1.

Example rule:

```
alert tcp any any -> 10.1.1.2 443 (msg:"Example rule"; flow:to_server; ssl_version:sslv2; content:"|0B|"; priority:1; sid:20389;rev:1;)
```

ssl_state

This option is not relevant for a Snort rule in Trellix IPS, and is not supported. If a rule that you imported contained this option, it is displayed in the Conversion Notes section of the rule. The Sensor ignores this option when it checks the traffic against this rule.

modbus_func

This rule option checks for the specified function code in the in a Modbus header. You can specify either the code number in the decimal format or the equivalent string.

Syntax: **`modbus_func:<code>`**

The following are the supported values for code:

- A number ranging from 0 to 255
- read_coils
- read_discrete_inputs
- read_holding_registers
- read_input_registers
- write_single_coil
- write_single_register
- read_exception_status
- diagnostics
- get_comm_event_counter
- get_comm_event_log
- write_multiple_coils
- write_multiple_registers
- report_slave_id
- read_file_record

- write_file_record
- mask_write_register
- read_write_multiple_registers
- read_fifo_queue
- encapsulated_interface_transport

Examples:

- **modbus_func:1**
- **modbus_func:read_discrete_inputs**

Example rule:

```
alert tcp any any -> 10.1.1.5 502 (msg:"Example rule"; flow:to_server; modbus_func:write_mul-
tiple_coils; byte_test:2,>,1968,10; reference:url,www.modbus.org/docs/Modbus_Application_Proto-
col_V1_1b.pdf; classtype:protocol-command-decode; priority:1; sid:20589;rev:1;)
```

modbus_data

This rule option points the Sensor to the beginning of the data field in a Modbus request or response.

Syntax: **modbus_data;**

Example rule:

```
alert tcp any any -> 10.1.1.7 502 (msg:"Example rule"; flow:to_server; modbus_data; content:"example
content"; nocase; priority:1; sid:20481;rev:1;)
```

dnp3_func

This rule option checks against the function code of a DNP3 request or response header. You can specify either the code number in the decimal format or the equivalent string.

Syntax:

dnp3_func:<code>

The following are the supported values for code:

- A number ranging from 0 to 255
- confirm
- read
- write
- select
- operate
- direct_operate
- direct_operate_nr
- immed_freeze

- immed_freeze_nr
- freeze_clear
- freeze_clear_nr
- freeze_at_time
- freeze_at_time_nr
- cold_restart
- warm_restart
- initialize_data
- initialize_appl
- start_appl
- stop_appl
- save_config
- enable_unsolicited
- disable_unsolicited
- assign_class
- delay_measure
- record_current_time
- open_file
- close_file
- delete_file
- get_file_info
- authenticate_file
- abort_file
- activate_config
- authenticate_req
- authenticate_err
- response
- unsolicited_response
- authenticate_resp

Examples:

- **`dnp3_func:2;`**
- **`dnp3_func:get_file_info;`**

dnp3_data

This rule option points the Sensor to the beginning of the application-layer fragment so that the Sensor can execute the other rule options.

Syntax:

```
dnp3_data;
```

Example:

```
dnp3_data; content:"example content";
```

Non-payload rule options

This section explains Snort non-payload rule options.

flags

Use this if you want the Sensor to check for TCP flags. You can check for the following flags:

- F - FIN (LSB in TCP Flags byte)
- S - SYN
- R - RST
- P - PSH
- A - ACK
- U - URG
- 1 - Reserved bit 1 (MSB in TCP Flags byte)
- 2 - Reserved bit 2
- 0 - No TCP Flags Set

You can apply the following operators on the flags option:

- **+** — Checks if all the specified flags are set
- ***** — Checks if at least one of the specified flags is set
- **!** — Checks if none of the flags are set

Syntax: **`flags:[!|*|+]<FSRPAU120>[,<FSRPAU120>];`**

Example rule:

```
alert tcp 10.1.1.1 any -> any any (msg:"example for flags"; flags:R; sid:2019; priority:3;)
```

This rule raises an alert when the host 10.1.1.1 resets a TCP connection.

flow

This option enables you to write rules specific to a direction of the traffic flow. For example, you can write a rule that the Sensor applies only on the traffic from the clients.

The following table describes the flow options that you can use in Trellix IPS:

Option	Description
`to_client`	Rule is applicable only to the response traffic from the server in a TCP session.
`to_server`	Rule is applicable only to the request traffic from the client in a TCP session.
`from_client`	Same as to_server

Option	Description
`from_server`	Same as to_client

Syntax: **`flow: [,(to_client|to_server|from_client|from_server)];`**

Example rule:

```
alert tcp !$HOME_NET any -> 10.1.1.1 80 (msg:"example for flow"; flow:to_server; content:"cmd.exe";sid:2015; priority:1;)
```

For this rule, the Sensor checks for cmd.exe in the request traffic from outside network to 10.1.1.1.

Notes:

- Make sure you specify the flow option in the Snort custom attacks to avoid false-positives.
- If you do not specify flow for a TCP rule, then it is saved in the Manager with Conversion Result, "warning" and State **Published**.

itype

Use this if the Sensor is to check for a specific ICMP type value.

Syntax: **`itype:[<|>]<number>[<><number>];`**

icode

Use this if the Sensor is to check for a specific ICMP code value.

Syntax: **`icode: [<|>]<number>[<><number>];`**

Example rule:

```
alert icmp !$HOME_NET any -> $HOME_NET any (msg:"example for itype and icode"; itype 8; icode:0; sid:2022; priority:3;)
```

This rule is triggered for inbound traffic where the type is 8 and code is 0.

icmp_seq

This is to check for a specific ICMP sequence value.

Syntax: **`icmp_seq:<number>;`**

Example rule:

```
alert icmp !$HOME_NET any -> $HOME_NET any (msg:"example for icmp_seq"; icmp_seq:0; sid:2041; priority:3;)
```

Post-detection rule options

Post-detection rule options are irrelevant for Snort Custom Attacks. After an attack is saved in the Manager server, you can configure the response actions for the attack just like you would for any other attack definition in Trellix IPS.

Managing Snort custom attacks

The Trellix IPS supports the Trellix IPS Snort and the Suricata Snort. This section provides information on how to create and maintain Trellix IPS Snort and Suricata custom attacks. In Trellix IPS, you can create the custom attacks in one of two ways:

- Construct the Snort rules, one at a time, directly in the Custom Attack Editor.
- Construct multiple Snort rules in a file and import the file into the Manager. You may want to consider this method when you have a large number of attack definitions to create or if you want to use the Snort rules from a source such as the Snort user community.

> **IMPORTANT**
>
> Before you create custom attacks, make sure you have reviewed and understood the considerations and best practices to be followed when using Snort rules in Trellix IPS.

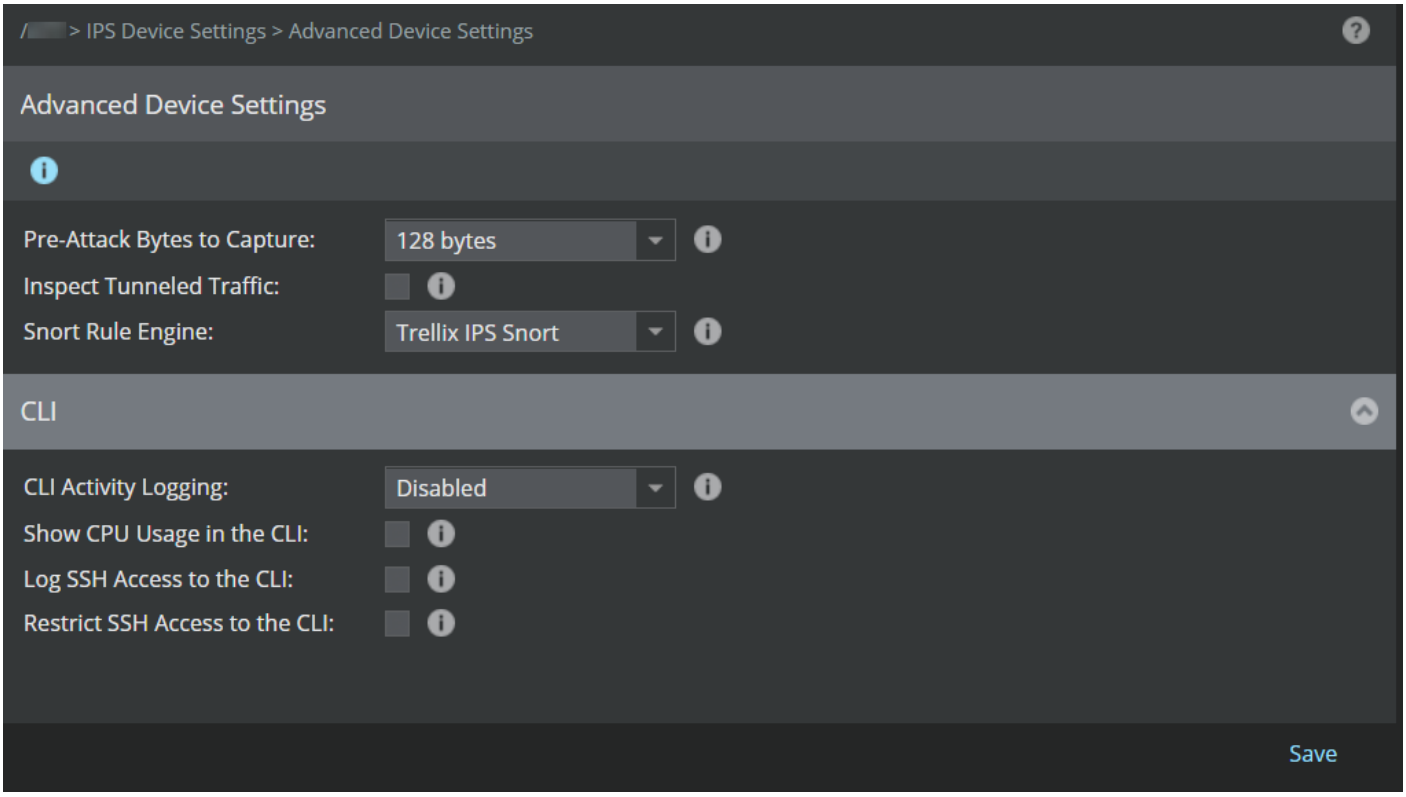
Snort Engines

Trellix IPS NS-series Sensors support either of the following Snort engines:

- Trellix IPS Snort
- Suricata Snort

> **NOTE**
>
> - A Sensor can run only one of the above engines at a time.
> - The Suricata Snort engine is not available on NS7600 and NS3600 Sensors.

You can select a Snort engine at the global level and override the selection per admin domain and/or Sensor, as necessary. The **Advanced Device Settings** page at the global and device levels allows you to select the engine you prefer to use.



NOTE

The default selection is **Trellix IPS Snort**.

Trellix IPS Snort

Consider the following factors when selecting the Trellix IPS Snort engine:

- The NS-series Sensors can support up to 5000 Snort rules. If you require support for more rules, contact Trellix Support.
- \X, \P, \K, \U, \R, and \C escape sequences and backreferences are not supported.
- Isdataat with rawbytes modifier is not supported.
- Norm and raw modifiers are not supported in urilen.
- Snort rules cannot be created on ASN1 decoded content.
- If the length of the content or uricontent (token length) is more than 96 bytes and less than or equal to 256 bytes, the target device type is automatically set to NS-series.
- The following PCRE constructs are not supported:
  - Lookahead and lookbehind assertions.
  - Backreferences and capturing subexpressions.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"WEB-CLIENT Adobe Acrobat
getCosObj file overwrite
```

```
 attempt"; flow:established,to_client; flowbits:isset,http.pdf; file_data; content:".write|
28|"; nocase;
content:".getCosObj|28|"; distance:0; nocase; pcre:"/([A-Z\d_]+)\.write\x28.*?
\1\.getCosObj\x28/smi"; reference:
cve,2011-2442; reference:url,www.adobe.com/support/security/bulletins/apsb11-24.html;
classtype:attempted-user;
sid:20156; rev:1;)
```

In this example rule, \1 is the backreference.

- Subroutine references and recursive patterns.
- Conditional patterns.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS ASP.NET 2.0 cross-
site scripting
attempt"; flow:to_server,established; content:"__LASTFOCUS="; fast_pattern:only; pcre:"/
__LASTFOCUS=(?!([_a-z]\w*|)
([\x26\x3B]|$))/i"; reference:bugtraq,20337; reference:cve,2006-3436;
reference:url,www.microsoft.com/technet/security
/bulletin/MS06-056.mspx; classtype:attempted-user; sid:8700; rev:5;)
```

In this example rule, !([_a-z]\w*|)([\x26\x3B]|$) is the conditional pattern.

- Unicode character properties \p{xx} and \P{xx}.
- Possessive quantifiers.

The following are additional limitations regarding PCRE in Trellix IPS Snort:

- In a Snort custom attack, the maximum value for repetition counter in PCRE is 256. If it exceeds this number, the error message *Pattern too large* is displayed.
- Atomic grouping and possessive quantifiers are not supported.

NOTE

PCRE rules validation is included in the Custom Attack Editor. So, any rule containing invalid or unsupported PCRE options fail to import. You can find the reason in the error message. After you correct these rules, use the **Test Compile** feature to check if the they are valid and compatible. You can select the required attacks and select Other Actions → **Test Compile**.

The following constructs are not supported in Trellix IPS Snort:

- ack
- asn1
- bidirectional operator
- byte_extract
- byte_jump
- byte_test
- cvs
- dce_iface

- dce_opnum
- dce_stub_data
- depth
- distance
- dnp3_ind
- dnp3_obj
- dsize
- fast_pattern
- flowbits
- fragbits
- fragoffset
- ftpbounce
- http_stat_msg
- icmp_id
- id
- ip_proto
- ipopts
- isdataat
- metadata
- modbus_unit
- offset
- port / IP negation
- rpc
- sameip
- seq
- stream_size
- tos
- ttl
- window
- within

The following are not supported in Trellix IPS Snort, but an equivalent option is available in Trellix IPS:

- Rules using ftpbounce keyword are not supported. However, the Trellix IPS signature sets provide adequate protection against FTP bounce attacks.
- Rules to detect CVS attacks are not supported. However, Trellix IPS signature sets can protect your network against most of the CVS attacks.

- Regarding Sensor response actions, you cannot use any post-detection rule options such as Logto, Session, or Tag. Instead, you can configure the required response action after the rule is saved in the Manager database. This is the same as how you would configure the response action for any other attack definition in Trellix IPS.
- Preprocessor plugins are not supported.
- Snort's multi-event logging (event queue) is not supported.
- For event thresholding and alert suppression, you can use only the equivalent features in Trellix IPS and not the options in Snort.

Classification types

It is mandatory that you define the priority for each Snort Custom Attack. Priority is one of the parameters that the Manager uses when it categorizes a Snort Custom Attack. To specify the priority, you can either use the priority keyword directly in the rule or use a classification type in the rule. However, this classification type should either be available in the Manager or declared in a file up front. That is, the Manager must read the classification type declaration before it reads the rule that uses it.

NOTE

You can view the classification types that are currently available in the Manager. You can also re-submit rules for conversion with the currently available values.

Similar to macros, you can define the classification types in a .conf, .config, or .rules file and import it into the Manager.

In the .conf, .config, or .rules file, define the classification type using the syntax as shown below:

```
config classification:<class name>,<class description>,<default priority>
```

Example: config classification: brute-force,attempted brute force,1

Note the following:

- The priority value 1 is mapped to a severity of high in Trellix IPS, 2 to medium, 3 to low, and 4 and above to informational.
- The default priority value that you specify in a classification type can be overridden by using the priority keyword in the rule.

Suricata Snort

The Suricata Snort engine provides a dedicated Snort environment and supports many of the open-source Snort constructs that are available in the public domain. This allows you to import most custom and third-party Snort rules without modification.

Trellix IPS uses Suricata Snort version **3.2.3**. The usage of some of the constructs differs in Suricata Snort when compared to the open-source Snort. See https://docs.suricata.io/en/suricata-3.2.3/rules/http-keywords.html for the list of supported constructs.

The following is the list of considerations when using the Suricata Snort:

- You can import only the Suricata rules having TCP, UDP, IP, and ICMP protocols without modification from the Emerging Threats.
- You cannot push the Suricata Reference config file to the Sensor.
- You cannot import rule variables from the yaml file from the Emerging Threats.
- You cannot exclude a rule for a particular snort engine.

NOTE

The Suricata Snort engine is not available on NS7600 and NS3600 Sensors.

Configuring Snort engine at a global level

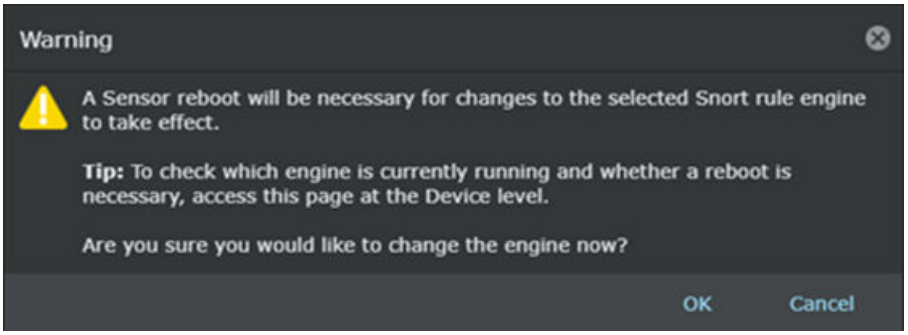
To configure the appropriate snort engine at a global level, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings**.

   The default engine selected is the Trellix IPS Snort engine.

2. To select the snort engine, click the **Snort Rule Engine** dropdown and select the **Suricata Snort**.

   A pop-up appears asking you to confirm your changes and informing you that a reboot will be necessary for the change to take effect.



3. Click **OK** and then click **Save** at the bottom of the page.
4. Reboot the Sensors which require this change.

   After the reboot, the **Advanced Device Settings** page of the Sensor displays Suricata Snort.

Configuring Snort engine at a device level

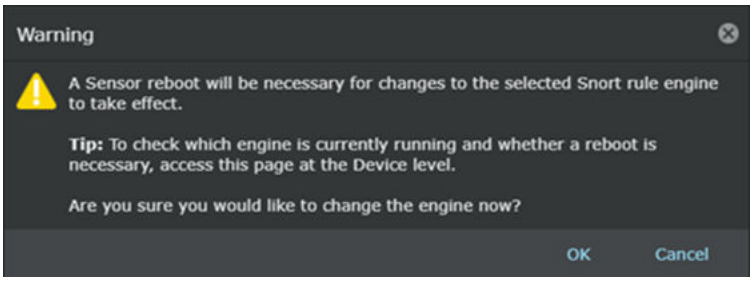
To configure the appropriate snort engine at a device level, perform the following steps:

1. Go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings**.

   The **Advanced Device Settings** page appears.

2. Uncheck the **Inherit Settings?** checkbox to get access to modify settings in this page.
3. Select **Inspected Tunneled Traffic** if you want to inspect GRE, GTP, and tunneled IPv4 and IPv6 traffic.
4. To select the snort engine, click the **Snort Rule Engine** dropdown and select **Suricata Snort**.

   A pop-up appears asking you to confirm your changes and informing you that a reboot will be necessary for the change to take effect.



5. Click **OK** and then click **Save** at the bottom of the page.
6. Reboot the Sensors which require this change.

   After the reboot, the **Advanced Device Settings** page of the Sensor displays Suricata Snort.

CLI commands to monitor Snort

The Sensor CLI provides the following commands to monitor Snort.

- **`show snort config`**
- **`show suricata enginestats`**
- **`show suricata sbstats`**

For more information about the commands, see the *CLI commands* section.

Troubleshooting Tips

This section describes the issues that you might face when working with the Snort rules and the corresponding troubleshooting tips.

Issue: Suricata Snort rules are imported successfully in the Manager but the Sensor does not generate alerts.

Cause: The Snort rules might be failing in the Sensor.

The Sensor does not generate alerts for the failed rules. The Sensor sends the information about the failed rules to the Manager. Information about the failed rules in the Sensor is available in a log file. To view the log file, go to the Manager → <Admin domain> → Troubleshooting → **Logs** page in the Manager.

You can also verify the number of rules processed by a Sensor by using the **`show suricata sbstats`** command. For more information, see the CLI commands to monitor Snort (page 1778) section.

Issue: An alert does not contain the packet information.

Cause: It is possible that the alert might be generated for a buffered packet attack.

The Suricata engine integrated into the Sensor performs packet buffering. When a buffered packet attack is detected and an alert is generated, the Sensor may not have the actual packet information if the alert was raised based on the buffered packet data. In such a scenario, the alert will not have any packet information.

Best practices

This section details the best practices that you **must** follow when you use Snort Custom Attacks:

- Do not use a Snort Custom Attack if there is an equivalent available in the signature set.
- Make sure that the content option value is more than one byte. If you import a rule with a one-byte content, it will fail to import. The longer the content value, the accurate the detection will be. However, the maximum length of a content or uricontent for NS-series Sensors is 256 bytes.
- Make sure the content option does not contain any generic values identified by Trellix IPS (some examples are listed below). Such rules can severely impact Sensor performance.
    - GET
    - POST
    - Host
    - User-Agent
- For better accuracy and performance, Trellix recommends that you use the Custom Attack Editor to create custom attack definitions as opposed to importing Snort rules.
- If you are using byte_test or byte_jump, use them in relation to a content match.
- Specify the classtype or priority to all rules. This enables the Manager to determine the severity for the rule. Understand how the Manager categorizes a Snort Custom Attack to publish it in the rule sets.
- If you are importing the Snort rules, import them from files that are accordingly named. For example, import HTTP rules from a file named http.rules file. In these rules, do not specify the destination port; the Sensor automatically detects protocols running on non-standard ports and applies the rule to the corresponding traffic. If you specify a port number, the Sensor applies the rule only to the traffic destined for that port.
- If you create the Snort rule in the Custom Attack Editor, or if you import it from a generically named file (like myrules.rules), it is very important that you specify the destination port number.
- Specify the revision number for all rules.
- For TCP rules, specify the flow.
- In a rule, do not specify the same value for more than one Content option. For example, do not use a Snort Custom Attack such as the following: alert tcp any any -> 10.1.1.1 80 (msg:"Example rule"; content:"private"; content:"private"; priority:1;sid:20209;rev:1;).

Create snort custom attacks

The following is the high-level approach for creating Snort Custom Attacks.

Steps:

1. Have a clear understanding on what you are trying to achieve through these attacks. See if there are any alternatives or better methods to achieve the same. Identify the related protocols, applications, hardware and software platforms for the attack. Make sure you have all the required information in hand.
2. Understand the mechanics of a Snort Custom Attack. You need to have a strong understanding of network concepts as well as Snort rules language to create effective Snort Custom Attacks.

3. Take a quick tour of the Custom Attack Editor. Get familiar with the Custom Attack Editor - the tool that you will use to manage Custom Attacks. Understand the interfaces related to Snort Custom Attacks.
4. Verify the required variables. Check if the variables that you plan to use are available in the Sensor.
5. Create Snort Custom Attacks. There are two methods:
   - You can import the rules from a file.
   - You can construct the Snort rules directly in the Custom Attack Editor.
6. Check the rules that failed to convert. The Sensor automatically converts all the valid rules, which you imported or wrote, to Trellix IPS's proprietary format. Note that some rules could have failed to convert. Troubleshoot and fix the rules that failed to convert.

   NOTE

   If you are creating or importing Suricata Snort rules, ensure that one of **TCP**, **UDP**, **IP**, and **ICMP** protocols is used in the Snort rules.
7. Save the converted rules in the Manager database.
8. Once saved in the database, the rules are like any other custom attack definition. For example, you may want to customize the response action for the saved Snort rules, or you may want to delete a Snort rule from the database.
9. Update the respective Sensors with the changes.

   The Sensors raise alerts based on the saved Snort rules. You can view these alerts in the Attack Log.

Variables

There can be some values that you may need to mention in all or most of the rules. For example, the target subnet could be the same for many rules. Instead of repeating it in each rule, you can define a variable for the subnet, and then use the variable in the rules. The advantage with using variables is when you want to modify the value. For example, if the target subnet is now different, then instead of modifying each rule, you can just redefine the variable with the new value.

You can use variables for the following:

- Path to a file: When you import Snort rules from a file, you can include other files from within the file that you are importing. Then rules from all these files are automatically imported. When you include a file within another file, you need to provide the absolute or the relative path to the file being referenced. Alternatively, you can use a variable for the path and mention it instead of the mentioning the path to the file.
- IP addresses: You can use variables for the source and target IP addresses or subnets.
- Port numbers: You can use variables for the source and target port numbers.

Define the snort variables

You can define the snort variables in Trellix IPS and then use it in the rules.

Steps:

1. Define the variables with the appropriate values in a file.

2. Import the file into the Sensor.

   To define the variables in a file:

   a. Create a text file and change its file extension to .rules or .conf.

      Assume that you have named it variables.conf

   b. In the text file, define the variables as explained below

      - Use the **var** keyword to define a variable for a file path, IP addresses, and ports.

        For example, var RULE_PATH `../rules`.

        In this example, RULE_PATH is the variable name and its value is the relative path to a folder named "rules".

      - Use the ipvar keyword to define a variable for IP addresses. Some examples are:

        - ipvar INSIDE_NETWORK [10.1.1.0/24, !10.1.1.22, 11.1.1.1, 12.1.1.0/24]
        - ipvar EXAMPLE1 [$INSIDE_NETWORK, !10.1.1.23]
        - ipvar EXAMPLE2 [$EXAMPLE1]
        - ipvar EXAMPLE3 [1.1.1.1, 2.2.2.0/24, ![2.2.2.2, 2.2.2.3]]

      - Use the portvar keyword to define the port numbers

        For example, portvar EXAMPLE_PORTS [100, 102, 150:160, !155]

        In this example, the value of EXAMPLE_PORTS is 100, 102, 150 through 160 except 155.

   c. Save the variables.conf file.

   To import the variables file into Sensor:

   a. In the Custom Attack Editor, from the **Snort Format** tab, click **Snort Variables**. Alternatively, to import select Other Actions → **Import.**

   b. Locate variables.conf and click **Open**.

      If you do not see the conf file at the location where you saved, check the **Files of Type** field in the Open dialog.

   c. Click **Open**.

      The Import Status may show zero for all the fields. Click **OK**.

   d. Select **Snort Format** to make sure the variables are imported with the values you specified in the variables.conf file.

   e. If a variable that you imported is already available in the database, it is assigned the value from the current import.

Viewing the Snort variables

You can use the **Snort Variables** feature to view the names and values of the variables and classification types that are available in the Manager database.

This feature enables you to the following:

- Check if you are using valid macros and classification types when you create or import a Snort Custom Attack. (You cannot create a Snort Custom Attack that contains an undefined macro or classification type. If you import a rule with an undefined macro or classification type, it will fail validation.)
- Verify if a macro or classification type that you want to define is already available.

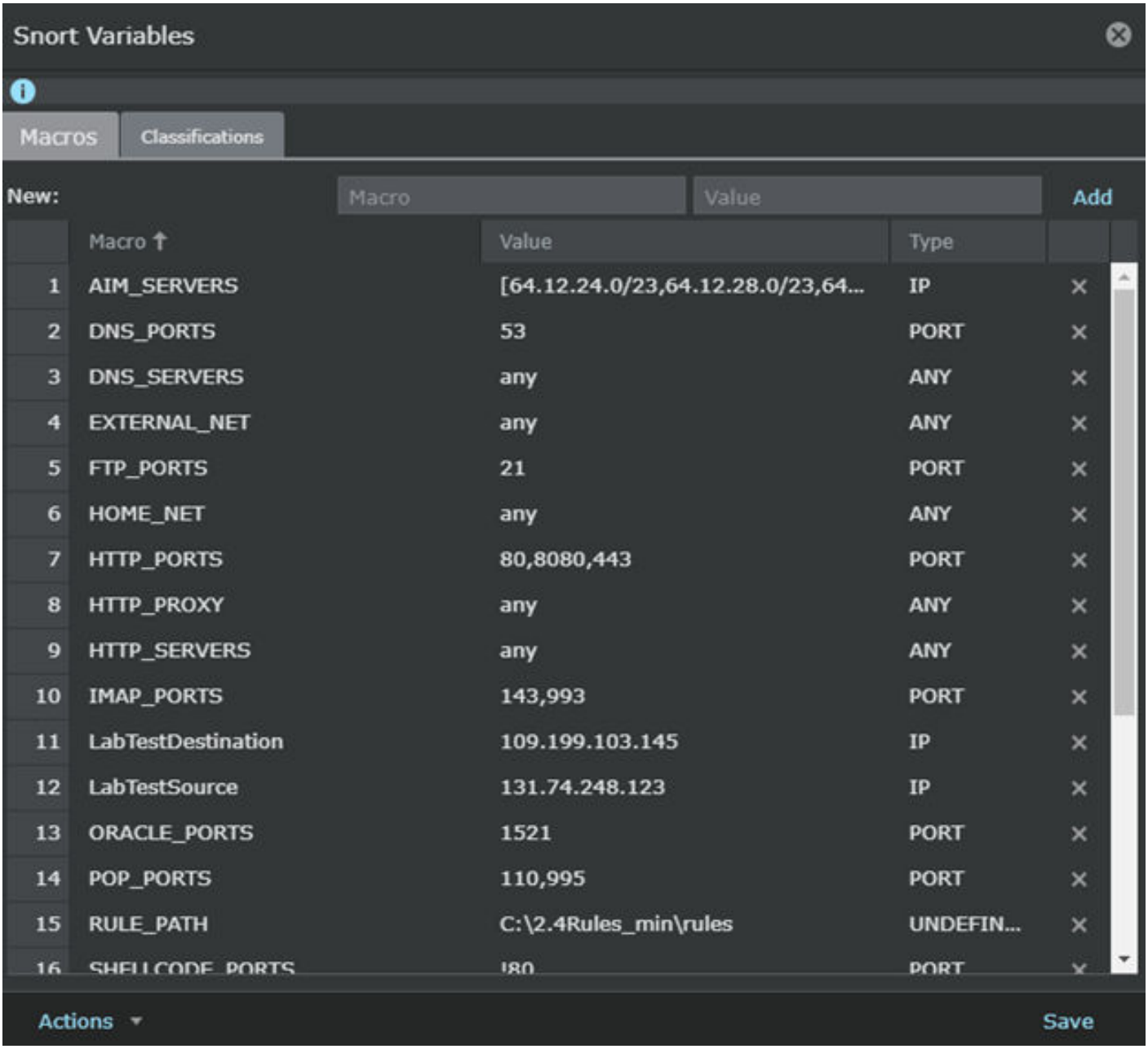
- Verify if an import of macro or classification types was successful.
    - Add or delete macros of a classification type.

To view the names of the macros and classification types in the Manager:

Steps:

- In the Custom Attack Editor from the **Snort Format** tab, click **Snort Variables**.

  The **Snort Variables** dialog opens.



Import variables

To import all the listed variables, classification types, and references:

1. Click Actions → **Import**.

   This imports the variables to the Manager client.

2. Click **Save**.

   This imports the variables to the Manager server. The Manager automatically detects the type of the following types of variable at the time of import:

   - IP address
   - Port
   - Any

NOTE

- If the Manager cannot determine the type of the variable, the variable is listed as **UNDEFINED**.
- You can specify the value of the variable as **any** in which case the variable can be used as an IP address as well as a port number.
- If any of the values of a variable is **any** or **![any]**, the entire value of the variable is considered as **any**.

TIP

As a best practice if you change the value of any variable, always re-evaluate the rules before saving the attack changes.

Modify variables

To modify a variable:

1. Click on **Remove** icon for the variable.
2. Enter the new value in **Value**.
3. Click **Add**.
4. Click **Save**.

After you click **Save**, the updated value of the variable is saved. However, the updated value of the variable is not reflected in the rules that use the variable. To update the value of the variable in all the rules, you should re-evaluate the rules. To re-evaluate the rules:

1. In the **Snort Variables** dialog, click Actions → **Re-Evaluate Rules**.
2. Click **Save** to save the updated Snort rules.

NOTE

When you re-evaluate the rules, all the rules listed in the **Snort Format** tab are submitted for re-evaluation and not just the failed ones.

Re-submitting rules with the current variables and classification types

In the Snort Variables dialog, click Actions → **Re-Evaluate Rules.** if you want the Manager to reevaluate all the rules on the **Snort Format** tab to the currently available variables.

This feature is useful if you had:

- Imported the rules before you had defined the variables. If you resubmit the rules now, the ones that failed to evaluate because of invalid variables get successfully evaluated.
- Modified the values of variables

Restore default variables and classification types

To restore all the listed variables, classification types, and references:

1. Click Actions → **Restore Default Variables**.

   This restores the details to the Manager client.

2. Click **Save**.

   This restores the details from the Manager server.

Deleting variables and classification types from the Manager

To delete all the listed variables, classification types, and references from the Manager:

1. Click Actions → **Delete All Variables**.

   This deletes the details from the Manager client.

2. Click **Save**.

   This deletes the details from the Manager server.

Identification of the protocol of a snort custom attack

When you save a custom attack in the Manager server, the Manager categorizes the attack to include it in the applicable rule sets. One of the criterion that the Manager uses to categorize an attack is the application layer protocol that the attack is intended for. For Native Trellix IPS Format Custom Attacks, you can specify this when creating the attack. For Snort Custom Attacks, the Manager identifies it by itself.

Understand how the Manager identifies the impact protocol for a Snort Custom Attack, to ensure if a Snort Custom Attack is published in the policies it is intended for.

How the Manager identifies the impact protocol is explained below:

1. First, it tries to use the name of the rules file from which you imported the Snort Custom Attack. For example, if you imported it from ftp.rules, the impact protocol for that attack is identified is FTP. Depending on other criteria for classification, the Manager includes the attack definition in the Rule Sets that include FTP.

   If the rules file name starts with web, for example web-attacks.rules or web-client.rules, then the identified protocol is HTTP.

   As a best practice, do not specify the destination port number in the rules if you import rules from files named after the protocol. If you do, the Sensor restricts its search to those port numbers.

2. If the Manager is unable to identify the protocol by the first method, it identifies the protocol based on the destination port number in the rule. This assumes that the destination port number is a standard port number. For example, if you import a rule from a generically named rules file but the destination port is 80, the identified protocol is HTTP.

   The Manager uses this method when you import a rule from a generically named rules file (for example, myrules.rules or when you create the rule in the Custom Attack Editor.

As a best practice, specify the destination port number (standard or otherwise) if you import the rules from a generically named file. This can improve Sensor performance because even if the protocol is not identified, the Sensor looks for the pattern only for the matching destination protocol.

How to use snort rules to detect IP communication between specific hosts

This section explains how to construct Snort rules that can detect TCP, UDP, or ICMP communication between specific hosts or networks based on IP address.

NOTE

To detect TCP, UDP and ICMP communication between a set of IP addresses, you must create 3 separate rules.

TCP communication

To detect TCP communication between hosts specify **`ip_proto:tcp;`** and **`flags:S`** as the attack parameters.

Example:

```
alert tcp 10.1.1.10 any -> [192.168.230.0/24, 192.168.231.0/24] any (msg:”Malicious TCP Traffic”;ip_proto:tcp;flags:S;sid:3121;)
```

Here 10.1.1.10 is an example source IP and [192.168.230.0/24, 192.168.231.0/24] are the example destination subnets.

If you do not specify **`flag:S`** the rule is triggered for all the TCP packets between the specified hosts.

UDP communication

To detect UDP communication between hosts, specify **`ip_proto:udp;`** as the attack parameter.

Example:

```
alert udp 10.1.1.10 any -> [192.168.230.0/24, 192.168.231.0/24] any (msg:”Malicious UDP Traffic”;ip_proto:udp;sid:3122;)
```

Here 10.1.1.10 is an example source IP and [192.168.230.0/24, 192.168.231.0/24] are the example destination subnets. The Sensor sends alerts for any UDP packet detected between the specified hosts.

ICMP communication

To detect ICMP communication between hosts, specify **`ip_proto:icmp;`** as the attack parameter.

Example:

```
alert ip 10.1.1.10 any -> [192.168.230.0/24, 192.168.231.0/24] any (msg:”Malicious ICMP Traffic”;ip_proto:icmp;sid:3123;)
```

Here 10.1.1.10 is an example source IP and [192.168.230.0/24, 192.168.231.0/24] are the example destination subnets.

In the rule, use the following parameters along with icmp for a more specific detection:

itype - Use this to check for a specific ICMP type value

Syntax: **`itype:[<|>]<number>[<><number>];`**

icode - Use this to check for a specific ICMP code value.

Syntax: **`icode: [<|>]<number>[<><number>];`**

Example:

```
alert icmp 10.1.1.10 any -> [192.168.230.0/24, 192.168.231.0/24] any (msg:"example for itype and
icode"; itype 8; icode:0; sid:2022; priority:3;)
```

Here 10.1.1.10 is an example source IP and [192.168.230.0/24, 192.168.231.0/24] are the example destination subnets. This rule is triggered for inbound traffic where the type is 8 and code is 0.

Write snort custom attacks

Prerequisites:

Before you begin to construct the Snort rules, review the following:

- In the rule, you can use only the variables, classtypes, and references that are available in the Manager. For information on how to view the available values, see Viewing the variables and classification types.
- You can write only one rule at a time.

You can construct Snort rules directly in the Manager using the Custom Attack Editor. Note that these rules must conform to the Snort rules language syntax. Structure of a Snort rule provides information how to construct Snort rules within Trellix IPS.

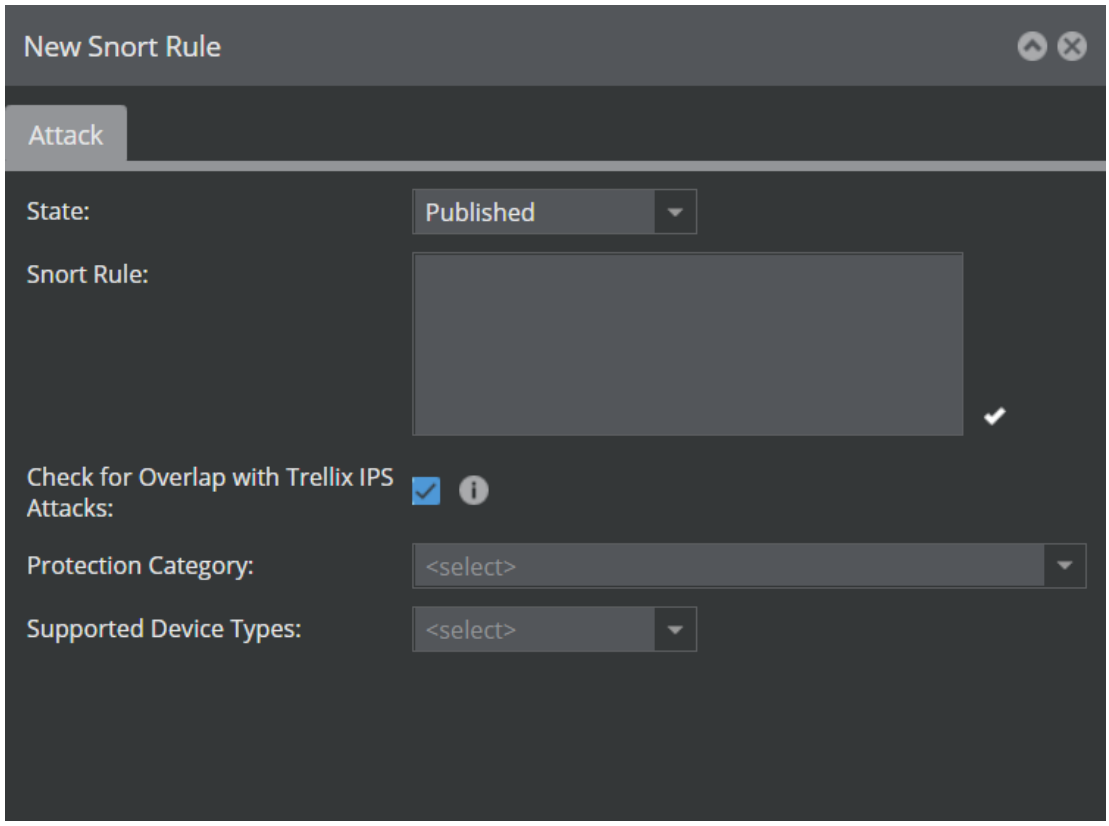
To construct Snort rules in the Manager, perform the following steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

   The Custom Attack Editor opens with the existing Custom Attacks listed on the **Native Trellix IPS Format** tab.
2. Click **Snort Format** tab.
3. Click  .

   The **New Snort Rule** interface opens.

Figure 788. New Snort Rule window



4. Construct the Snort rule in the **Add Snort Rule** dialog.

   Note the following:

   - You cannot define variables in the **Add Snort Rule** dialog, but you can use the variables that are available in the database.
   - You can write only one rule at a time.
   - If you are using the keywords such as classtype or reference, make sure the corresponding values are already defined and available in the database. For example, to import classifications, you can import a file that calls the classification config file and then use these classifications in the rules that you construct.
5. Select **Check for Overlap with Trellix IPS Attacks** to verify if the rule matches an existing Trellix IPS attack definition. If the rule matches then the Snort Rule will be **Staged**.
6. Select the most appropriate **Protection Category** for the attack.
7. Click **Add**.

   The rule is listed in the **All Custom Attacks** tab.
8. Save the rule to the database so that it gets published in the relevant policies.

Saving the Snort custom attacks

After you write or import the rules, you need to save them to the Manager database. Then, the rules for which the State is **Published**, are automatically added to the various exploit policies (both for inbound and outbound). This is similar to how the

Trellix IPS custom rules are **Published** in the policies. Review the following points to understand how the rules are published in the policies.

The newly added or modified attacks are automatically compiled at the time of saving. The attacks that fail compilation are set to:

- **Failed** in the **Test Compile** column
- **Staged** in the **State** column

Only rules that comply with the following conditions qualify to be published in the exploit policies of Trellix IPS:

- The Snort rule has been converted to Trellix IPS format successfully or with warnings.
- The State is set to **Published**.

All the qualified rules are published in the **Default Prevention** policy. In addition, these rules are also published in other policies that meet the following criteria:

- Benign Trigger Probability of medium. By default, all the imported Snort rules are assigned a Benign Trigger Probability value of medium which cannot be modified.
- Severity of the attack. This depends on the default classification based on the classtype of a rule or the priority tag in the rule.
- Protocol

Save the qualified rules

Before you save the Snort Custom Attacks to the database, you can also specify the Sensor type. For example, if you choose NS-series as the Sensor type for an attack, then this attack definition is relevant only to the NS-series Sensors of the corresponding admin domain. So only the NS-series Sensors inspect the traffic for this particular attack definition. Even when you apply the same policy to a Virtual Sensor, it does not check for this attack.

Steps:

1. Go to the corresponding tab in the Custom Attack Editor.
2. Verify that the rules that you want to be published in the rulesets are in the **Published** state. If not, you can click on the attack and select **Published**.
3. Verify the Target Device to which the Snort Custom Attack should be applied to.

   For example, if you select NS-series, only the NS-series Sensors in the current admin domain inspect traffic for this attack.
4. Click **Save**.

   The qualified rules are saved in the database and the corresponding policies are updated with these attacks. You can view the progress in the bottom part of the Custom Attack Editor.
5. You need to update the Sensors for the saved attacks to be detected.

   You can also verify if the attacks are published in the policies.

   1. From the Resource Tree, select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.
   2. Double-click on one of the All Inclusive policies; for example, you can open the **Default Testing** policy.

3. Click **Attack Definitions** tab.
4. Sort the attacks based on Name and verify if the Snort rules have been published.

Customizing the snort rules attack responses

You can use the Policy Editor to customize the Snort attacks like you would customize any other Trellix IPS attack. If you make any configuration changes to an attack, you should update the Sensor of the changes for them to take effect.

NOTE

By default, when you save a Snort attack to the database, Enable Attack and Enable Alert are enabled. All other configurations including blocking and packet logging are disabled.

Delete the snort rules from the database

Whenever required, you can delete the snort rules from the database and stop the Sensors from sending alerts:

Steps:

1. Open the Custom Attack Editor.
2. All the custom rules in the database are listed.
3. Select the required rules, click and select  .
4. Click **Save** to save the changes and update the policies.
5. Update the Sensors of the configuration changes.

Common tasks

This section contains information on tasks that are common to both Trellix IPS as well as Snort Custom Attacks.

How attacks are published in policies

After you create a Custom Attack and the constituent signatures or rules, you need to save the attack in the Manager server for it to be published in every rule set where the attack definition fits one or more categories, rule set categorization that was configured as part of attack creation. When you apply a policy that includes a rule set containing your attack definition, detection of your attack is active.

Consider that when you created a Trellix IPS Custom Attack, you set the Severity to Medium and chose HTTP as the Exploit classification. Once exported, this attack is published in all rule sets that publish Medium-severity, HTTP attacks, such as the Default, Outside Firewall, and Web Server rule sets provided with Trellix IPS. (This also publishes any rule set that you have created which calls for HTTP attacks of Medium severity or higher.) When you apply a policy that publishes one of these rule sets, you are applying your Custom Attack for active searching and alerting upon detection.

When you save the custom attacks to the Manager server, only those attacks with State as **Published** are published in the rule sets. If you want to change the State of a custom attack, right click on it and select **Published** or **Staged**.

When you create a Trellix IPS Custom Attack, the State is set to **Published** by default. In case of Snort Custom Attacks, there are instances where the state is set to **Staged**. For example, if there is a Trellix IPS attack signature with the same CVE ID, the Manager sets the State to staged when you save the attack. The State is also set to staged if the Conversion Result is failed or warning.

NOTE

If after saving the Custom Attack to the Manager server, you import the attack back to the Custom Attack Editor, edit the file and make a name change to either the attack or a signature in the attack, then save it again in the Manager server, the name change will not take affect in any open Attack Log views. You must close all Attack Log windows and restart the Attack Log to see the name change upon attack detection.

Viewing a policy to verify inclusion of the attack

After you save the custom attacks in the Manager server, verify if the attacks in **Published** State have actually been published in the policies. The attacks are categorized based on the following and then published in the corresponding rule sets.

When you have finished creating a custom attack, you need to save it. Saving the attack in the Manager server, publishes your attack definition in every rule set where your attack fits one or more categories, provided the State of the attack is **Published**. When you apply a policy that publishes a rule set containing your attack, detection of your attack is active.

The Manager categorizes attacks based on:

- Impact application
- Impact operating system
- Impact application layer protocol
- Severity of the attack
- Benign Trigger Probability (BTP)

For example, when you created a Trellix IPS Custom Attack, you set the Severity to Medium and chose HTTP as the Exploit classification. Once saved in the Manager server, the attack is published in all rule sets that include Medium-severity, HTTP attacks, such as the **Default**, **Outside Firewall**, and **Web Server** rule sets provided with Trellix IPS. (This also publishes any rule set that you have created which calls for HTTP attacks of Medium severity or higher.) When you apply a policy that publishes one of these rule sets to a port or VIDS, you are publishing your attack for IPS.

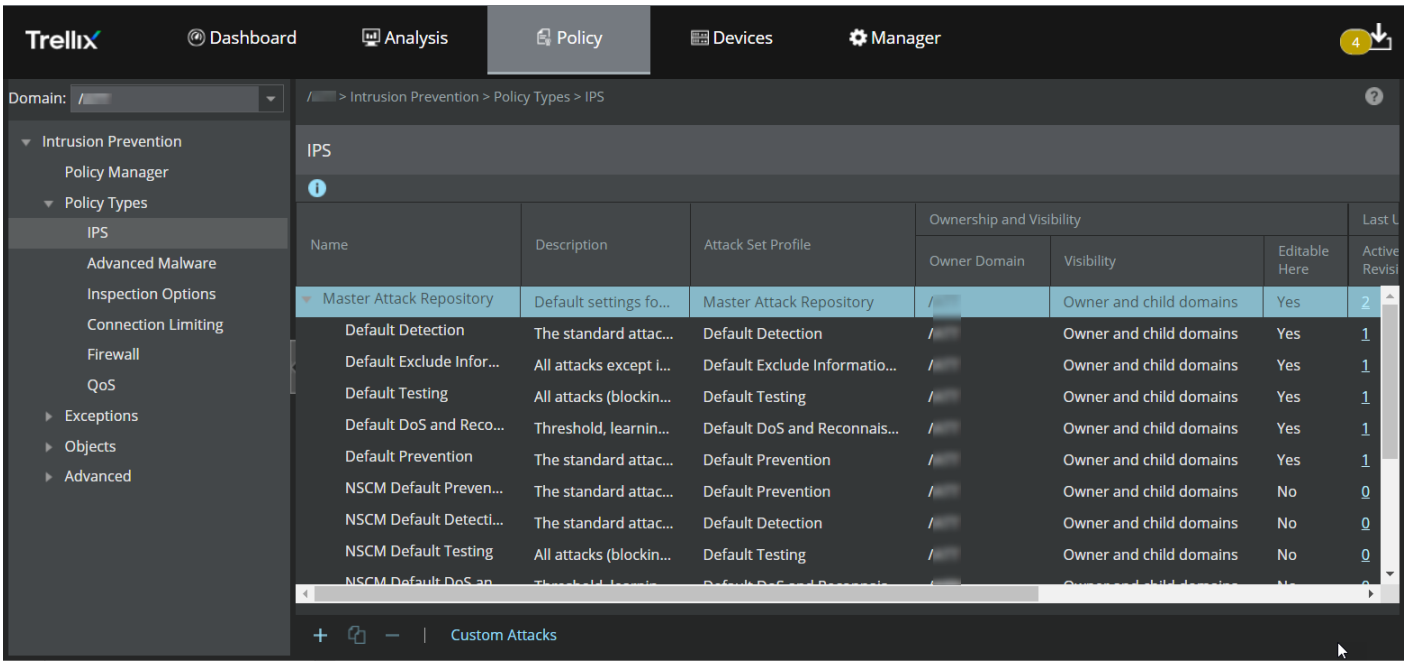
NOTE

If you make a name change to either the attack or a signature within the attack, then save it back into the Manager, the name change will not take affect in any open Attack Log views. You must close all Attack Log windows and restart the Attack Log to see the name change upon attack detection.

Verify the inclusion of custom attack in IPS policies

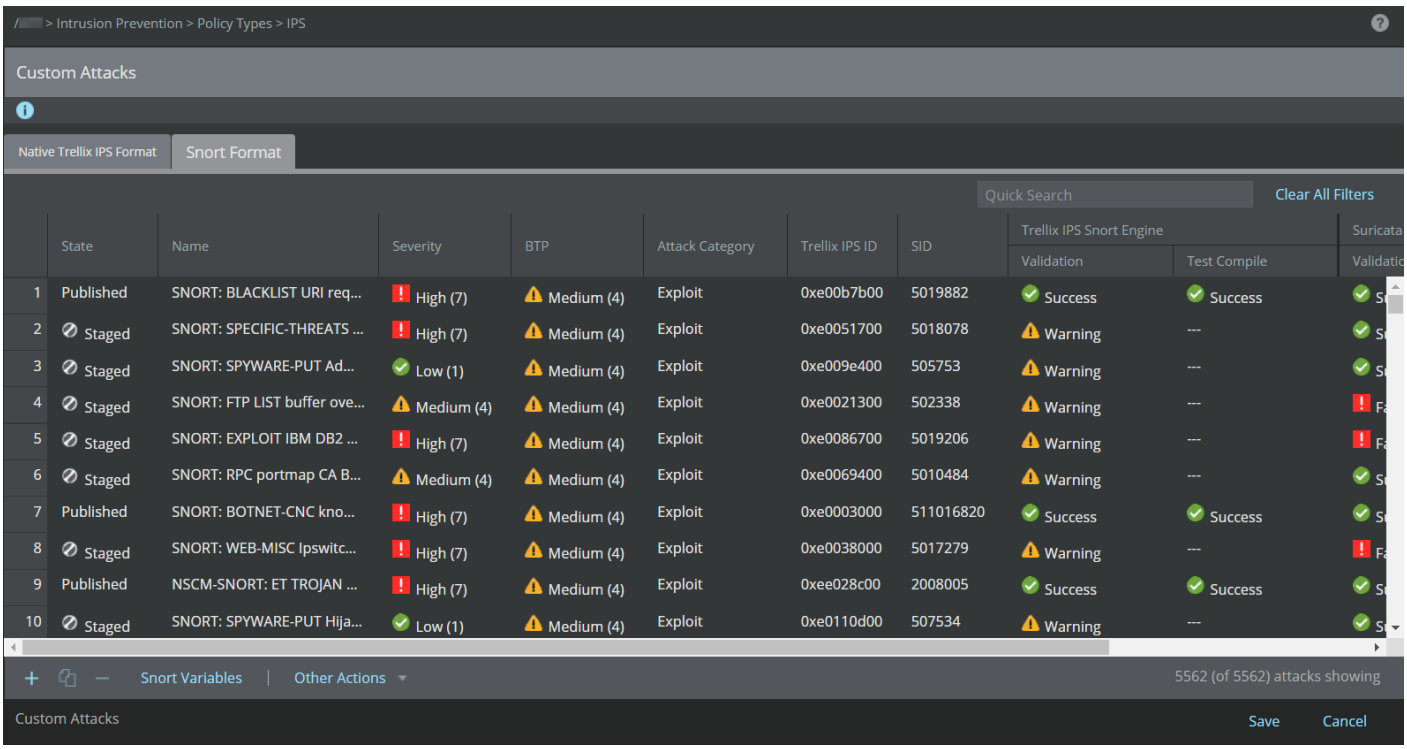
Steps to verify if a custom attack has been published in a rule set:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.
2. Double-click the "Default Testing " attack set to view the selected attacks.



3. Scroll down the list (sorted alphabetically) to find your attack file.

   Trellix IPS Custom Attacks have "UDS-" appended to the beginning of the name, while Snort Custom Attacks have "SNORT-" appended to the beginning.



Add attack descriptions to the Attack Encyclopedia

You can enter Attack Descriptions and comments in the Attack Encyclopedia for custom attacks. Attack Description can be added at the time of creating a custom attack. Comments can be added after creating the custom attack. When an alert is raised for a custom attack, these details can be viewed from the Attack Log as well

This procedure on adding comments assumes that you have a Trellix IPS or a Snort Custom Attack published.

Steps:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**.

   The **IPS** page is displayed. The **Default Testing** policy listed in the **IPS** page contains all the custom attacks (both Trellix IPS and Snort) that have been published.

2. Double-click on the **Default Testing** policy.

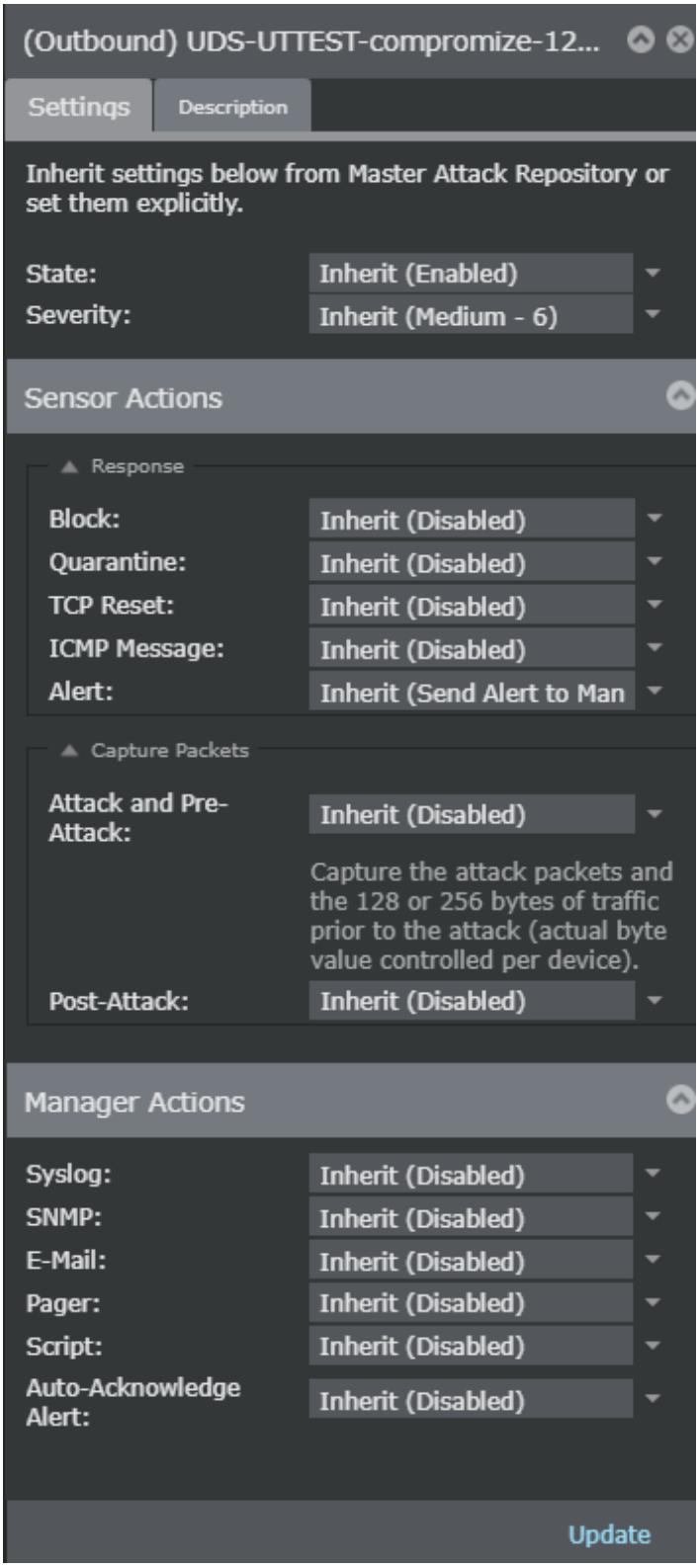
   All the Attacks Definitions under the **Default Testing** policy are listed under the **Attacks Definitions** tab.

3. Search for the custom attack for which you want to add attack descriptions by entering the name of the attack in the **Quick Search** box

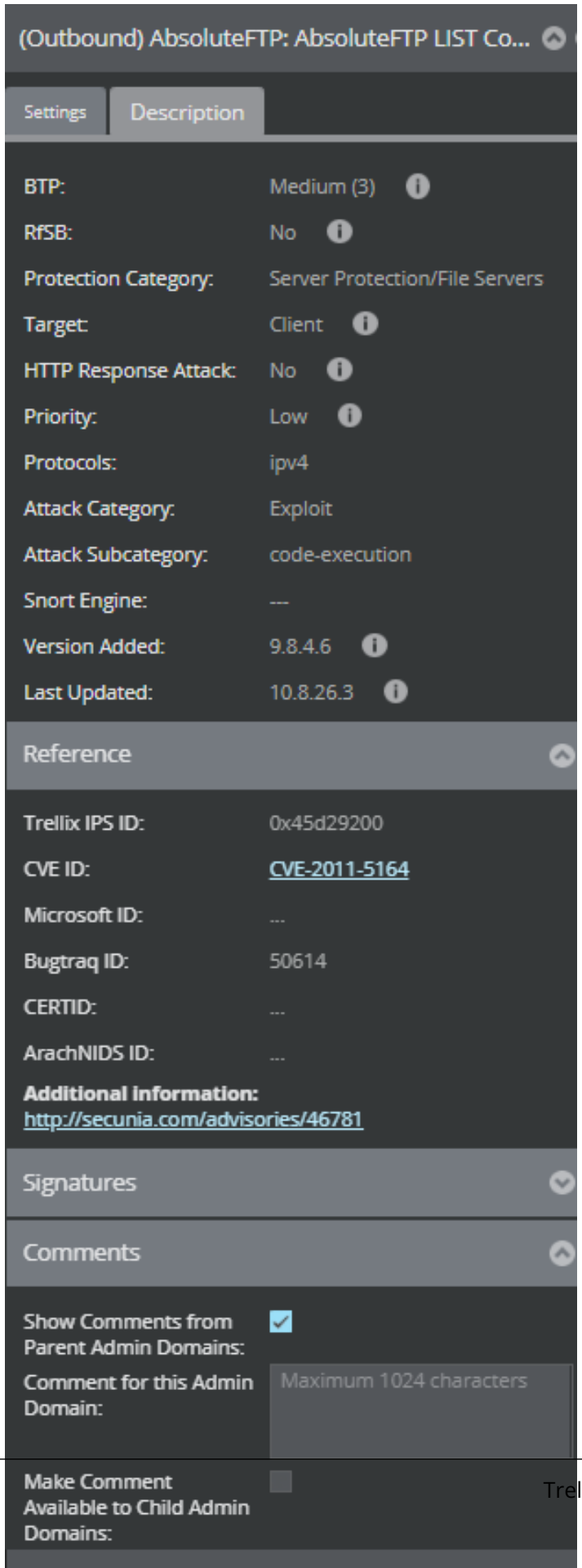
   > **NOTE**
   >
   > All Trellix IPS custom attacks are prefixed "UDS" and all Snort attacks are prefixed "Snort".

4. Double-click on the custom attack that you have located.

   The attack details pane for the selected attack is displayed.



5. Click **Description** to view the details of the custom attack from the attack encyclopedia.


(Outbound) AbsoluteFTP: AbsoluteFTP LIST Co...
Settings
Description
BTP: Medium (3)
RfSB: No
Protection Category: Server Protection/File Servers
Target: Client
HTTP Response Attack: No
Priority: Low
Protocols: ipv4
Attack Category: Exploit
Attack Subcategory: code-execution
Snort Engine: ---
Version Added: 9.8.4.6
Last Updated: 10.8.26.3
Reference
Trellix IPS ID: 0x45d29200
CVE ID: CVE-2011-5164
Microsoft ID: ---
Bugtraq ID: 50614
CERTID: ---
ArachNIDS ID: ---
Additional information:
http://secunia.com/advisories/46781
Signatures
Comments
Show Comments from Parent Admin Domains:
Comment for this Admin Domain:
Maximum 1024 characters
Make Comment Available to Child Admin Domains:

6. Enter the comment for the Attack in the **Comment for this Admin Domain** field.
7. Click **Save Comment**.

Compile the attack definitions

In the policies, you can use the attack definitions from the following types:

- Trellix IPS-supplied Attack definitions (signature set)
- Trellix IPS Custom Attack
- Snort Custom Attack

There can be instances where you may want to publish only specific types of attack definitions for a specific Sensor. For example, you may want to configure a Sensor to monitor traffic for specific attacks. You can also use this feature to troubleshoot and isolate the attack definitions that may cause an adverse effect on a Sensor's performance.

Steps to specify the attack definition type for a Sensor:

1. Select Devices → <Admin domain> → Devices → <Device Name> → Setup → **Attack Compilation**.
2. Select the attack definition type:
   - **Signature Set Attacks** - These are the attacks from Trellix IPS signature set.

     When the **Signature Set Attacks** option is selected, the Manager allows you to choose **Signature Set Attack Priorities** for the Sensor. This allows the Manager to dynamically compile only critical attacks from the standard signature set for Sensors that do not have enough resources to support all attacks.

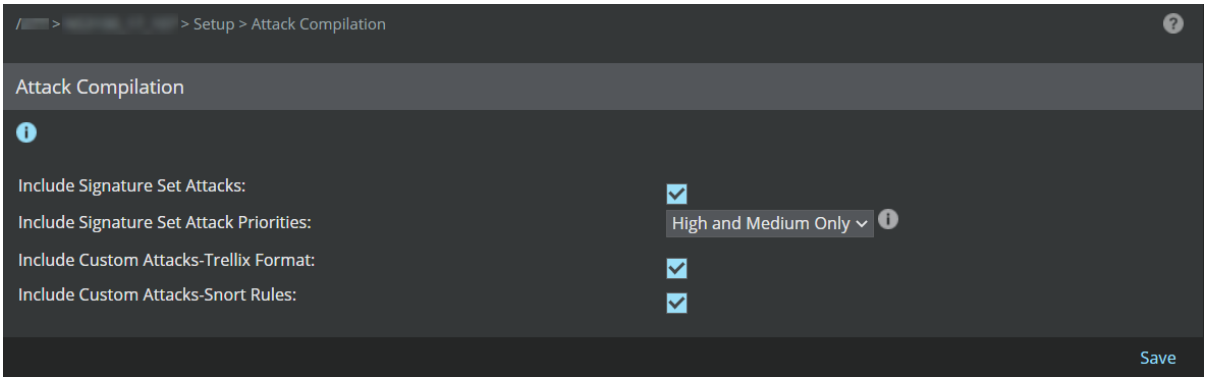
     The signature set attack priorities available are as follows:

     - **All**: Includes all attack definitions in the signature set. This is the default signature set attack priority selected for NS-series and Virtual IPS Sensors and provides complete attack coverage.
     - **High and Medium only**: It comprises of high and medium priority attacks in the signature set. This option provides partial attack coverage.
     - **High only**: It comprises of high priority signature set attacks. You can use this option to optimize Sensor resources on Sensor models running older Sensor software versions to support the latest signatures against most critical attacks.

     > **WARNING**
     >
     > The **High Only** signature set attack priority provides an attack coverage only against the most critical attacks.

   - **Custom Attacks - Trellix IPS Format**: Select this if you want to use the definitions that you created in the Trellix IPS format. This also includes the Trellix IPS-supplied custom attacks (emergency UDS).
   - **Custom Attacks-Imported Snort Rules**: Select this if you want to use the Snort Custom Attack definitions that you created or imported.
3. Click **Save**.

   When you update a Sensor with the configuration changes, only the attack definitions from the type specified here are pushed to the Sensor.



Update the Sensor configuration to apply a policy

Once you have verified that a custom attack is published in a rule set, you need to update the Sensors of the changes for the Sensors to look for traffic matching the attack definition. Since addition of a custom attack affects one or more rule sets, which in turn affects one or more policies, your policies may require updating across all of your Sensors in order for effective detection of your attack definition.

The **Device Configuration Changes** action sends configuration changes, signature updates, and policy changes to all of the devices under the **Devices** node.

> **NOTE**
>
> The **Device Configuration Changes** action updates multiple Sensors, but only transmits the update to one device at a time.

To update the configurations of multiple devices, perform the following steps:

1. Select Devices → <Admin Domain Name> → Global → **Device Manager**.

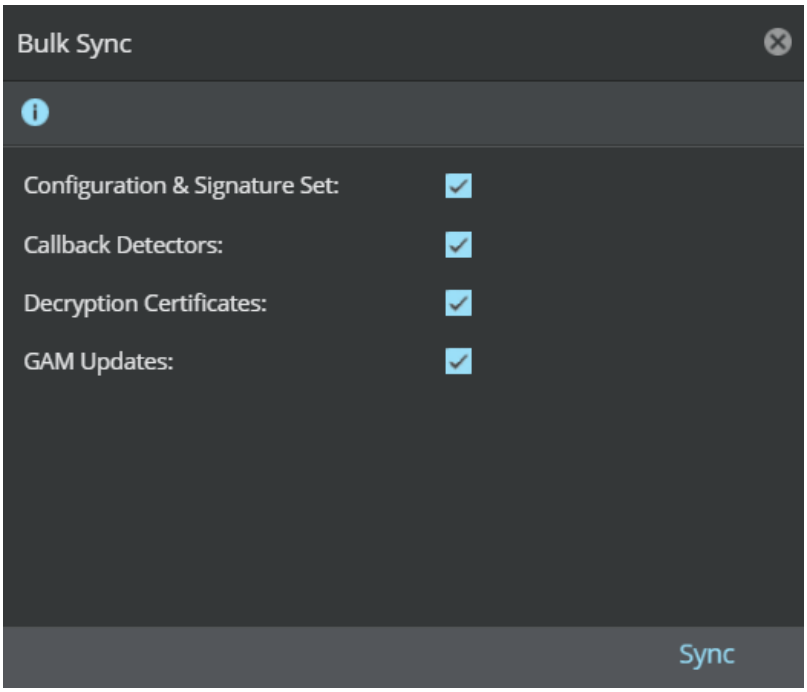
   The **Device Manager** page is displayed.

2. Select the **Sensors** tab. Then, select the Sensor(s) to be updated from the list.

   > **NOTE**
   >
   > You can also do it at the device level by selecting Devices → <Admin Domain Name> → Devices → <Device Name> → **Deploy Pending Changes**.

3. Click **Sync**. The **Bulk Sync** window is displayed. Select the required configurations and click **Sync**.

Figure 789. Bulk Sync



A Snort Custom Attack definition being applied to a Sensor port depends on the following:

- The attack definition should be published in the corresponding policy.
- The attack definition type that you have specified.
- You should have specified the corresponding Target Device for the attack definition. That is, if it is an NS-series Sensor port, you should have selected NS-series as the Target Device for the attack definition.

Custom attacks export

You can export all the Trellix IPS Custom Attacks, Snort Custom Attacks, and custom-defined grep protocols in the Manager to a ZIP file. The export feature enables you to use the custom attacks on a different Manager without having to recreate them. Trellix strongly recommends that you do not try to modify the exported attack files and then re-import them.

In the exported ZIP file:

- The Trellix IPS Custom Attacks are stored in the attacks.xml file.
- The packet grep protocols are stored in the pktgrepprotocol.xml file.
- The Snort Custom Attacks are exported in the Snort format.
- The Snort Custom Attacks Rules and the related data such as variables that you imported are stored in correspondingly named files. For example, assume that you had imported rules from ftp.rules file. When you export, these rules are stored in ftp.rules file within the ZIP.
- The rules that you directly created in the Editor are contained in unknown.rules file.

NOTE

There is no option to export just the Trellix IPS Custom Attacks or just the Snort Custom Attacks. When you export, all custom attacks listed in the All Custom Attacks tab and the custom-defined packet grep protocols are exported.

Export the custom attacks

To export the custom attacks to your client or other reachable location, do the following:

1. In the Custom Attack Editor, click **Native Trellix IPS Format** tab and select Other Actions → **Export** to export Native Trellix IPS Format custom attacks.

   Click **Snort Format** tab, and then select Other Actions → **Export** to export Snort Format custom attacks.
2. Select the folder where you want to save the ZIP file.

   The ZIP file is downloaded automatically to your set download folder, if your system is configured for automatic download to a specific folder.
3. Type a name for the zip file. Do not add an extension.
4. Click **Save**.

Examples

This section contains examples that describe how to create various types of custom attack definitions and import Snort rules for the Suricata Snort Engine.

Use case scenarios

This section describes the following user scenarios:

- Select the Suricata Snort engine and import the Snort rules.
- Create an attack by using String Pattern Match to detect a specific string in the HTTP GET requests.
- Create an attack by using Numeric Pattern Match to detect a specific numeric value in the FTP protocol.
- Create an attack by using Numeric Range Match to detect if the ports are in the specified range in the signature for HTTP protocol.
- Create an attack by using Numeric Enumeration Match to detect if the response code matches the ones specified in the signature for HTTP protocol.
- Create an attack by using Single Fixed Field Match to detect if the IP address and the protocol matches the ones specified in the signature.
- Create an attack by using Packet Grep Protocol to detect if the packets contain a specific string sequence.

To open the Custom Attack Editor, select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

Importing Snort rules for the Suricata Snort engine

This sample user scenario describes the steps for the following activities:

- Selecting the Suricata Snort engine
- Rebooting the Sensor
- Importing Snort variables and rules from a file
- Viewing the status of the imported Snort rules
- Viewing the imported Snort variables
- Pushing changes from the Manager to the Sensor

NOTE

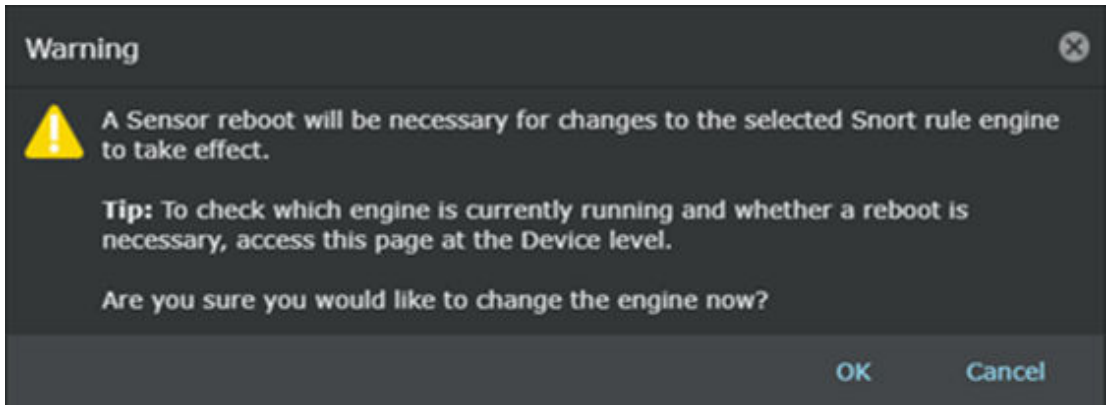
You can configure the Snort engine at a global level but can override the setting per Sensor and select a different engine at a Sensor level. In this scenario, you will be configuring the Snort engine at a global level.

Importing Snort rules for the Suricata Snort engine

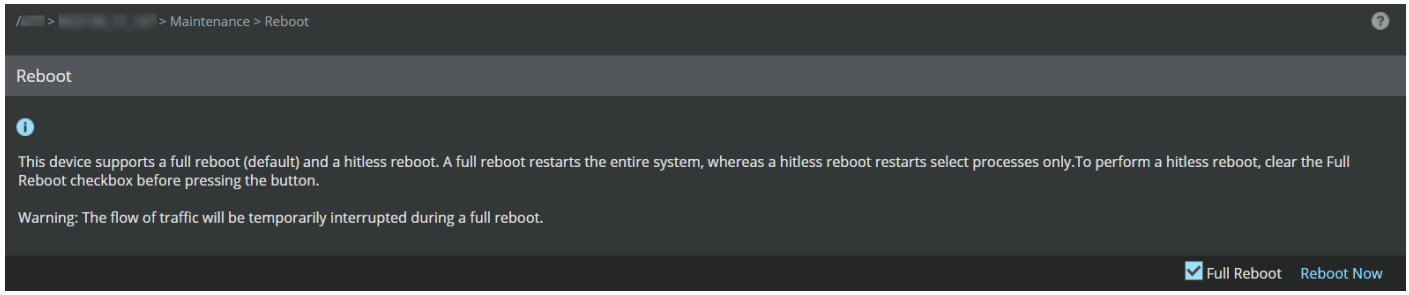
Steps:

1. Go to Devices → <Admin Domain Name> → Global → IPS Device Settings → **Advanced Device Settings**. The default engine selected is **Trellix IPS Snort**.
2. To select the snort engine, click the **Snort Rule Engine** drop-down and select the **Suricata Snort**.

   A pop-up appears asking you to confirm your changes and informing you that a reboot will be necessary for the change to take effect.

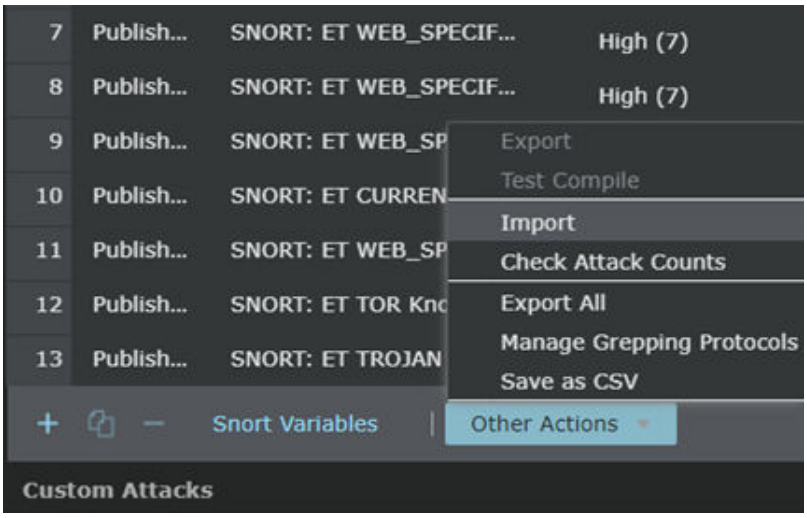


3. Click **OK** and then click **Save** at the bottom of the page.
4. Reboot the Sensors which require this change. Go to Devices → <Admin Domain Name> → **Devices**. Select the device to reboot. Go to Maintenance → **Reboot**. Click **Reboot Now**

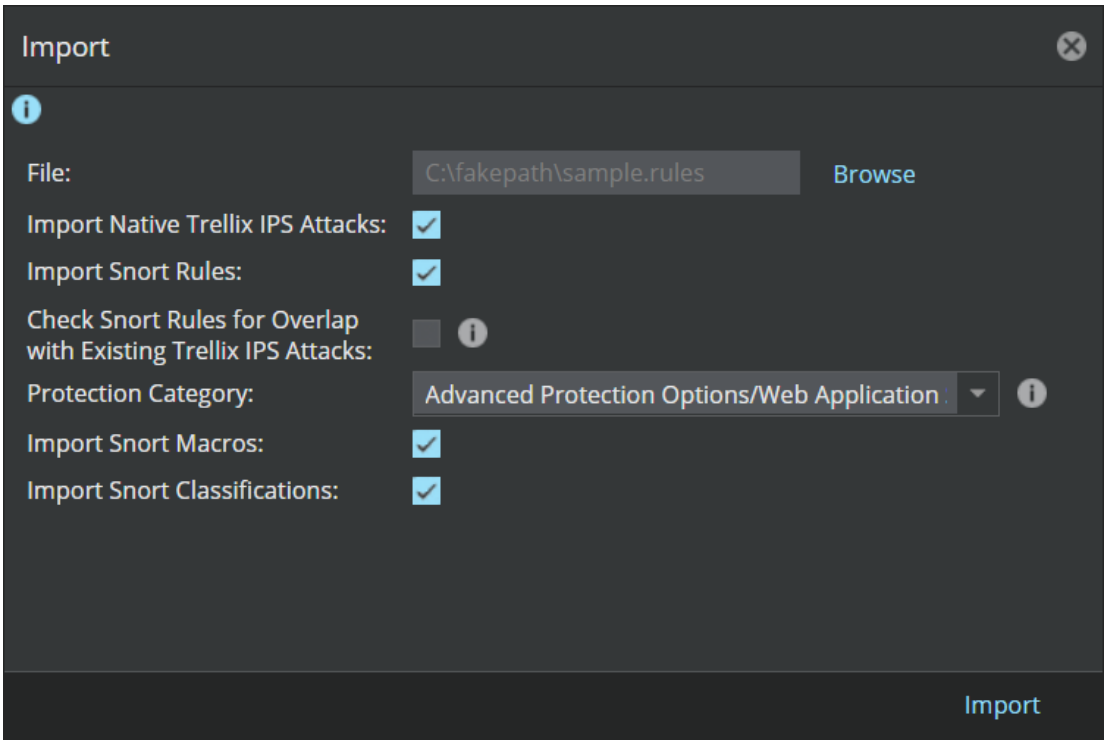


After the reboot, the **Advanced Device Settings** page of the Sensor displays **Suricata Snort**.

5. Go to Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click the **Custom Attacks** button (bottom left corner).
6. In the **Custom Attack Editor**, from the **Snort Format** tab, click Other Actions → **Import**



7. Browse to the location of the rules file to be imported and select the rules file.

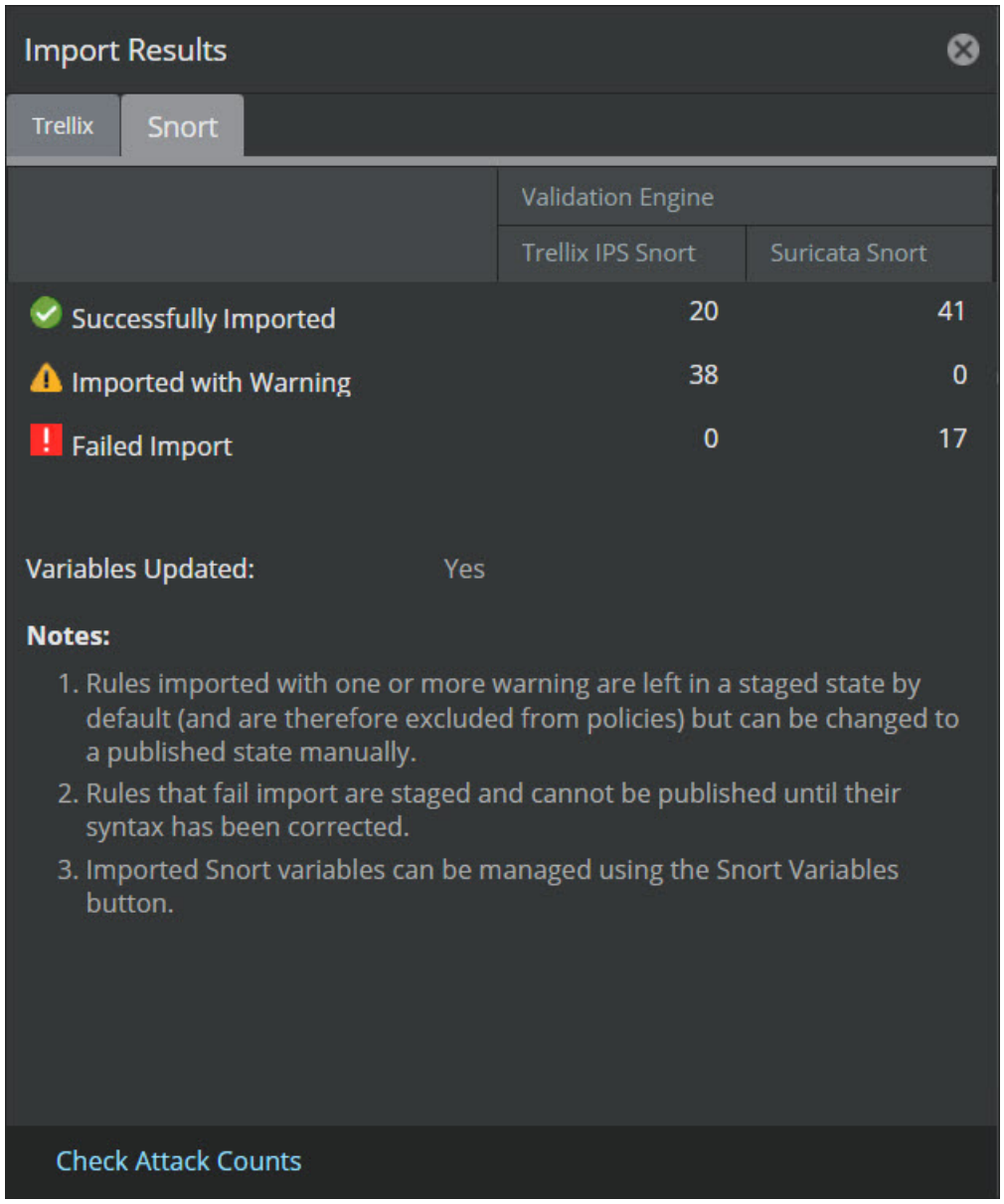


8. Select a Protection Category value.

   The Protection Category indicates the intent of the attack and the intended target. The list of Protection Categories is pre-defined and is provided by Trellix Advanced Research Center. In this scenario, the selected value is **Advanced Protection Option/File Reputation**

9. Click **Import**

   After the import, the **Import Results** screen is displayed.



10. Close the **Import Results** screen.
11. View the imported Snort rules.

    Know which rules converted successfully, which converted with warnings, and which failed to convert. For more information, see Viewing the imported Snort rules (page 1717).

12. View the imported Snort variables.

    Know which variables were imported and their classification type. For more information, see Viewing the Snort variables (page 1781).

13. Verify if the attacks in **Published** state are actually published in the policies.

a. From the Resource Tree, select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS** .

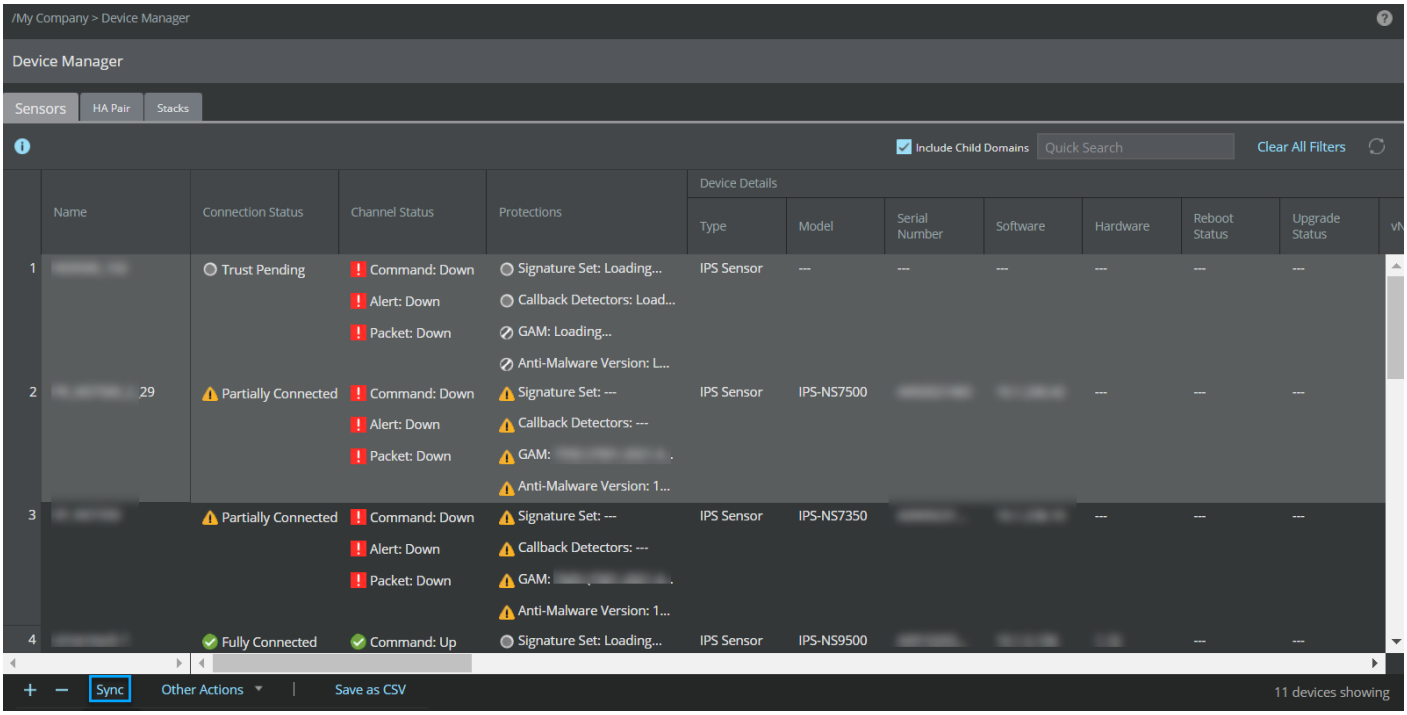
b. Double-click one of the All Inclusive policies; for example, you can open the **Default Testing policy**.

c. Click **Attack Definitions** tab.

d. Sort the attacks based on Name and verify if the Snort rules are published.

> **NOTE**
>
> You can also create your own attack set profiles to define the exact environment resources you want to protect. For more information, see the *Trellix Intrusion Prevention System Product Guide*.

14. Go to Devices → <Admin Domain Name> → Global → **Device Manager**.
15. Select the devices on which you want to deploy the imported rules by selecting the check boxes. Click **Sync**.



The **Bulk Sync** window is displayed.

16. Select **Configuration & Signature Set** from the window, and click **Sync**.

This deploys the IPS policies that contain the new Snort rules to the selected Sensors.

Sample Snort rules file

The following is a sample Snort rules file.

```
var HTTP_PORTS [80,443,8080]
var HOME_NET [10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,169.254.0.0/16,1.0.0.0/8,2.0.0.0/8]
var EXTERNAL_NET !
[$HOME_NET,198.80.42.0/23,198.217.128.0/17,198.241.128.0/17,64.94.118.0/23,66.185.176.0/20]
```

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN TeleBots BCS-
server CnC Beacon_NIDS779"; flow:established,to_server; urilen:1; content:"POST"; http_method;
content:"value="; depth:6; http_client_body; fast_pattern; content:!"Content-Type|3a|";
http_header; content:!"Referer|3a|"; http_header; reference:url,www.welivesecurity.com/2016/12/13/
rise-telebots-analyzing-disruptive-killdisk-attacks/; classtype:trojan-activity; sid:2023652;
rev:1;)
```

NOTE

- The variables and rules can be in separate files. If you are using separate files for variables and rules, ensure that you load the variables before loading the rules.

Create an attack definition for string pattern match

This scenario is about creating a Custom Attack Definition that uses string pattern match to detect any HTTP GET requests in the request URL for a specific string.

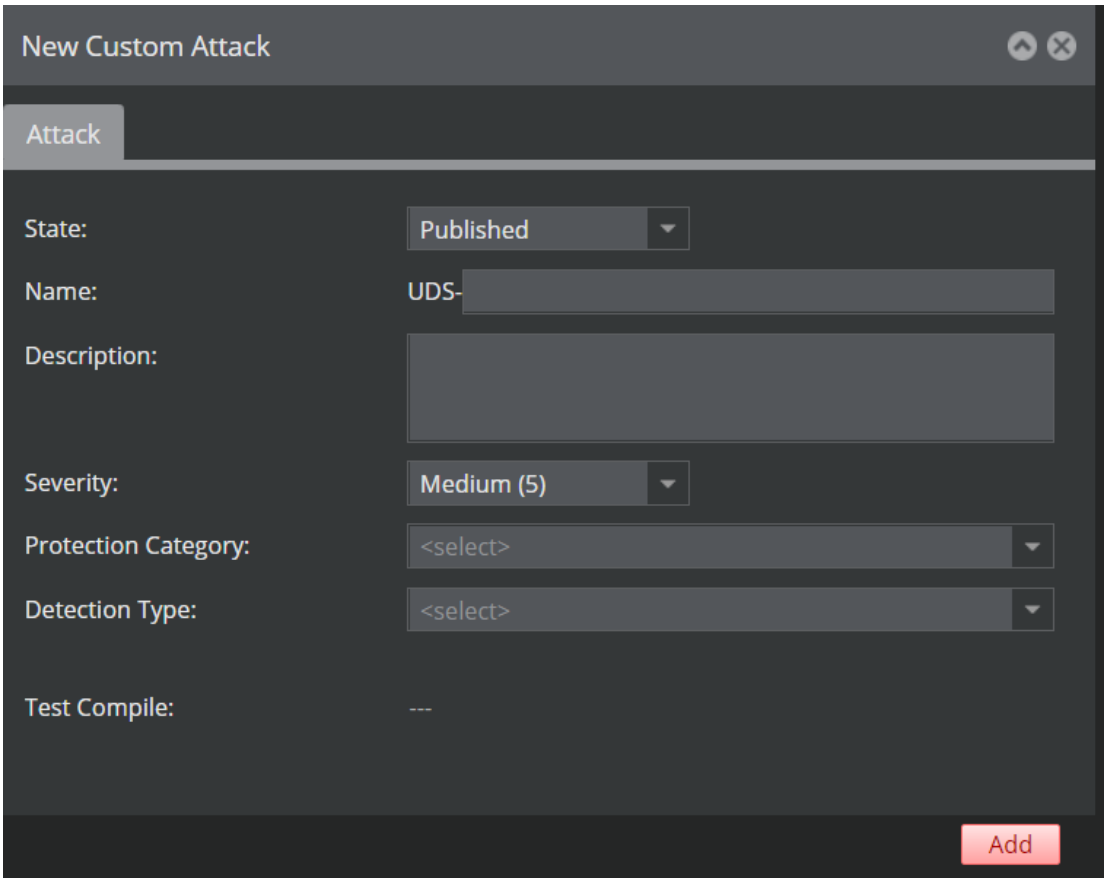
In order to write a proper Native Trellix IPS Format Custom Attack for this example, you must identify several key elements:

- Application protocol: HTTP
- Where to look: URL
- Detection window: request
- Request method: get
- String to match: LpEhZWWuLc0AwAAeHB3DAAAABA

To create the attack definition for this example:

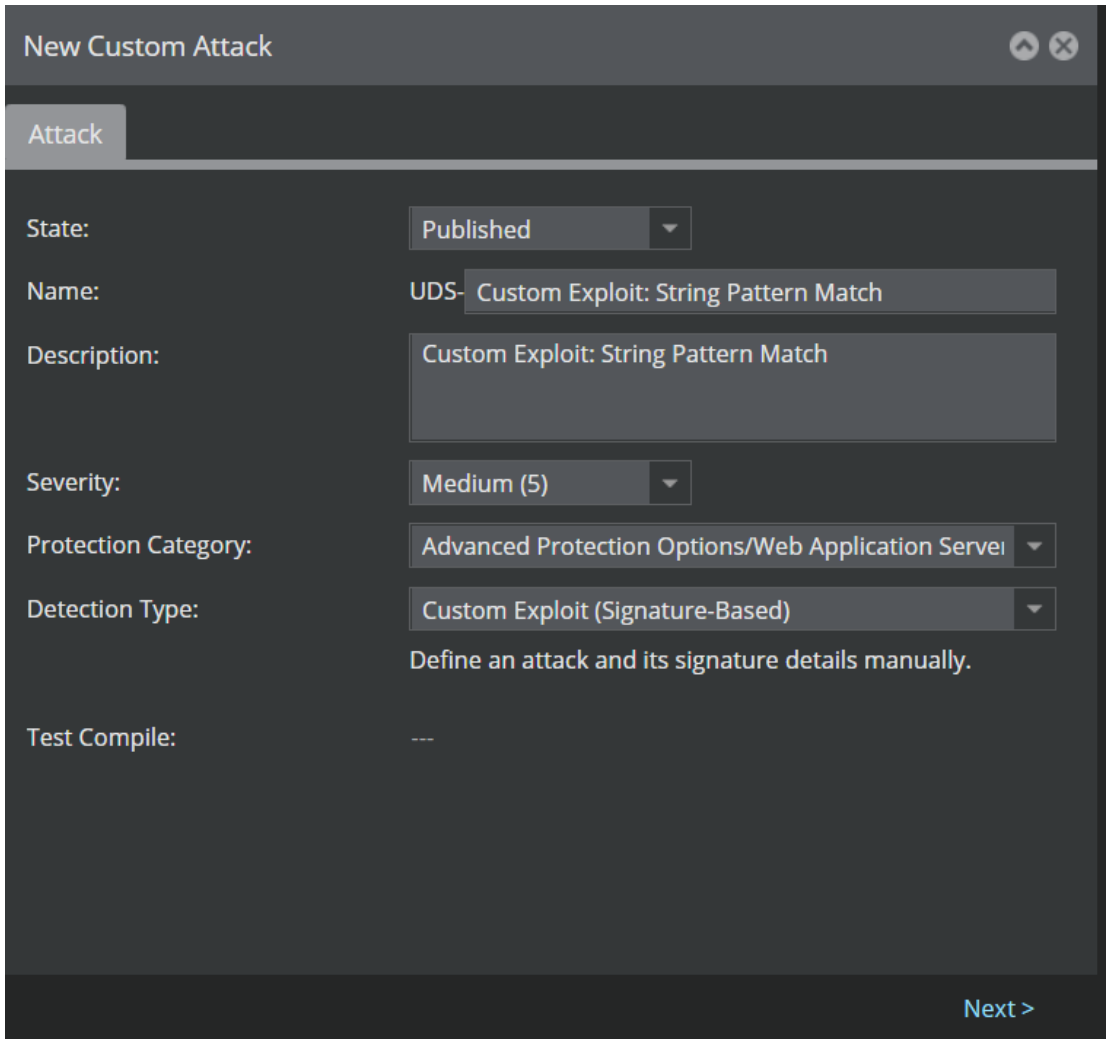
1. In the Custom Attack Editor, click .

   The **New Custom Attack** interface opens.



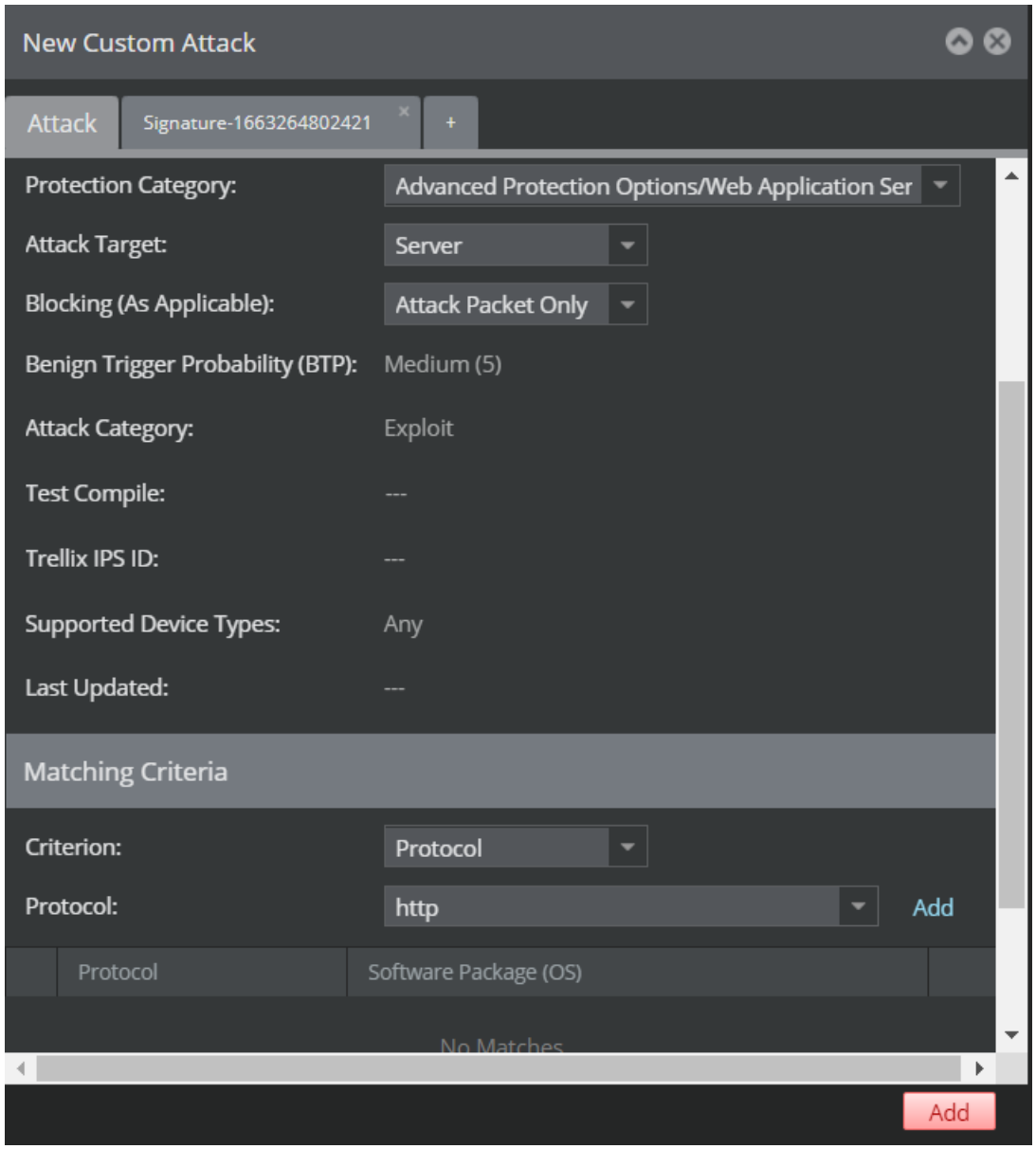
2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as " Custom Exploit: String Pattern Match" as the **Name**.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-Custom Exploit: String Pattern Match" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium (5)** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server** as the **Protection Category**.
7. Select **Custom Exploit (Signature-Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.



9. In the **Matching Criteria** section, select **Protocol** as the **Criterion** and select **http** as the protocol.

   When you subsequently save this attack definition in the Manager server, it will be part of every rule set which includes Medium-severity, HTTP attacks (must match both severity and protocol).



10. Attack details configuration is complete. Continue to create signature.

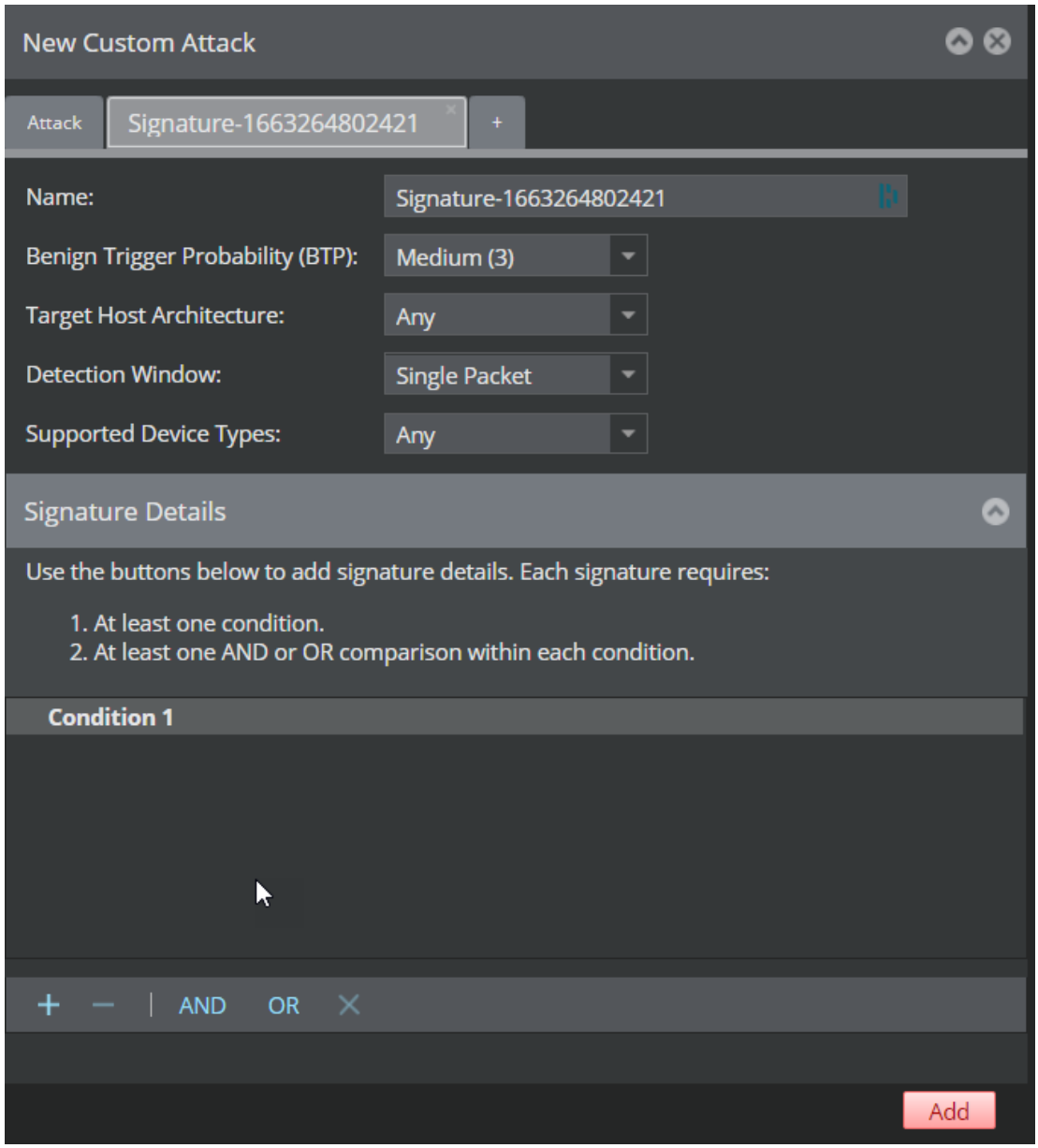
Create the signature for string pattern match

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** window, click **Signature-<signature name>** tab.

Figure 790. New Signature window



2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)**, **Target Host Architecture**, and **Detection Window** with the default values.
4. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.
5. Add the condition to the signature.

   It is in the conditions that you specify the following details:

   - The string that the Sensor should look for
   - Which section of the HTTP request should it look for the string
6. Proceed to add the condition.

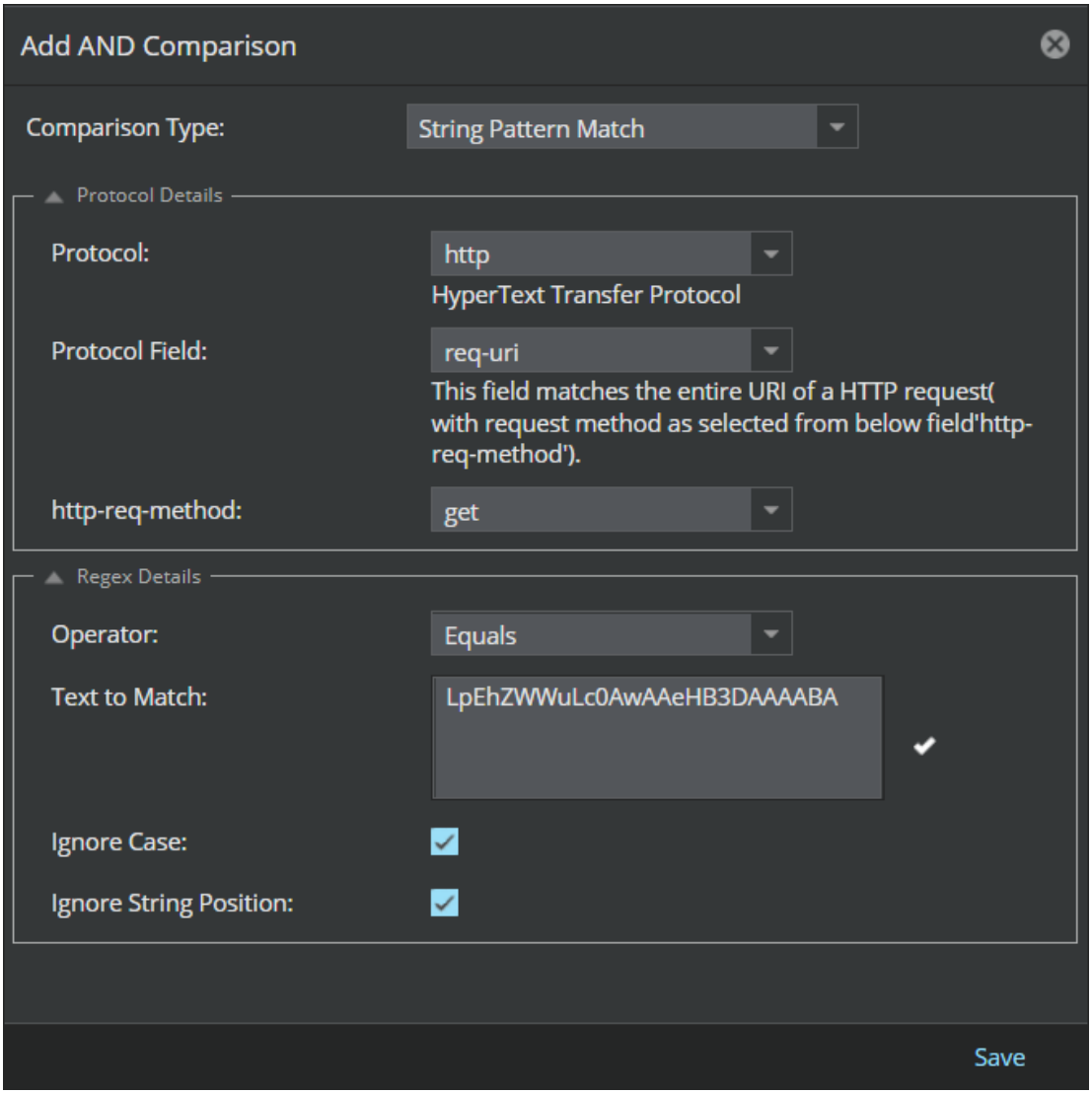
Add the condition for string pattern match

Steps to add the condition to the example signature:

1. **Condition 1** is added automatically according the URL you provided.
2. Click **Condition 1** so that it is highlighted.
3. Click **AND** in the Comparisons section.

   The **Add AND Comparision** dialog opens.

Figure 791. String Pattern Match



4. For this example, select **String Pattern Match** in the **Comparison Type** drop-down menu.
5. Select **http** from the **Protocol** drop-down menu.

   Because you selected HTTP, the Custom Attack Editor displays the HTTP-specific protocol fields on the following screen.

6. Configure the fields for the comparison you have chosen.

   For this example, specify **req-uri** for the **Protocol Field**. This specifies that the Sensor should search in the URI of the request packet.

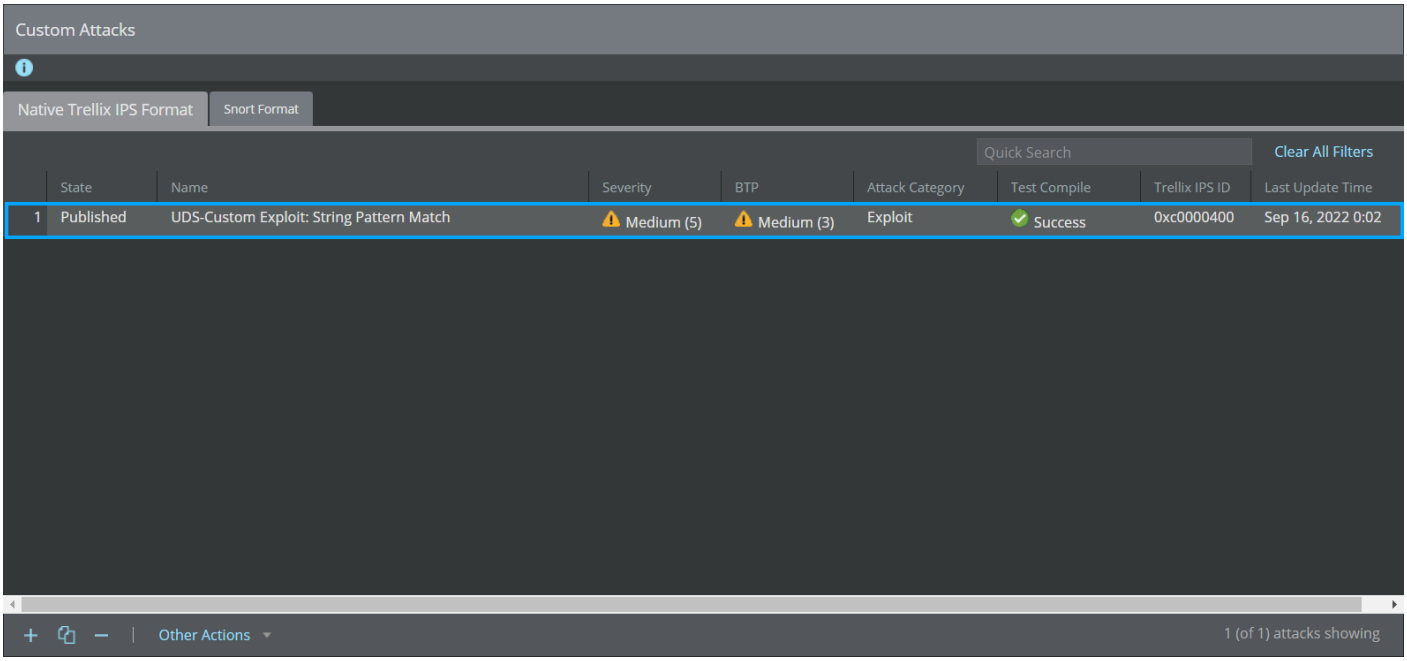
7. Select **get** as the http request method.
8. From the drop-down list in the Regular Expression **Operator** section, select the matching criteria as **Equals** which means that the comparison criteria must be equal to the regular expression entered.
9. Type the pattern to match in the **Text to Match** text box.

   For this example, the pattern to match is "LpEhZWWuLc0AwAAeHB3DAAAABA".

10. Click ☑ to verify that your expression is a valid string, and all required options are represented. Click **OK** to close the validation message window.
11. (Optional) Deselect **Ignore Case** and **Ignore String Position** check boxes.
12. Click **Save**.

    Your comparison appears under **Condition 1**.

13. Click **Add** in the **New Custom Attack** window.
14. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.



15. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
16. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Create an attack definition for numeric value match

This scenario is about creating a Custom Attack Definition that uses numeric value match to detect if the command line parameter length in make directory operation is greater than 50.

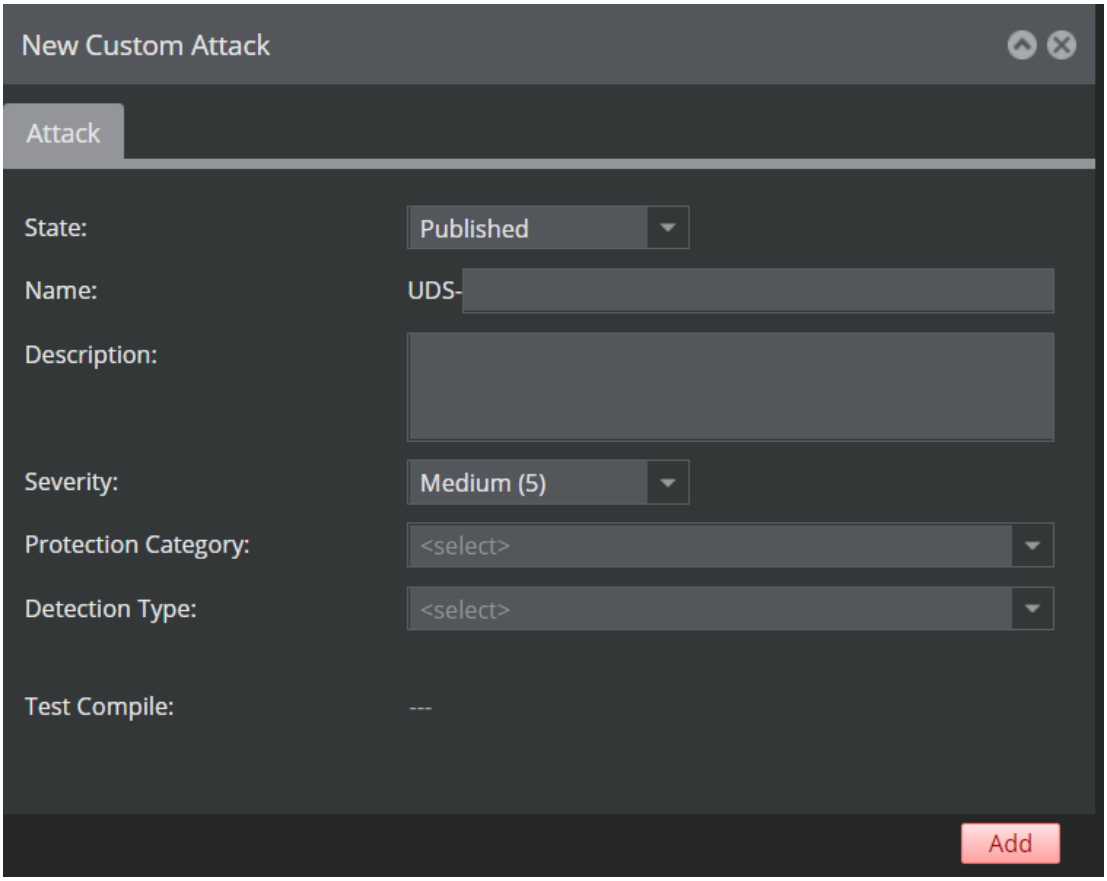
In order to write a proper Native Trellix IPS Format Custom Attack for this example, you must identify several key elements:

- Application protocol: FTP
- Protocol field: cmd-param-length
- Cmd qualifier: mkd
- Value to match: 50

Steps to create the attack definition for this example:

1. In the Custom Attack Editor, click +.

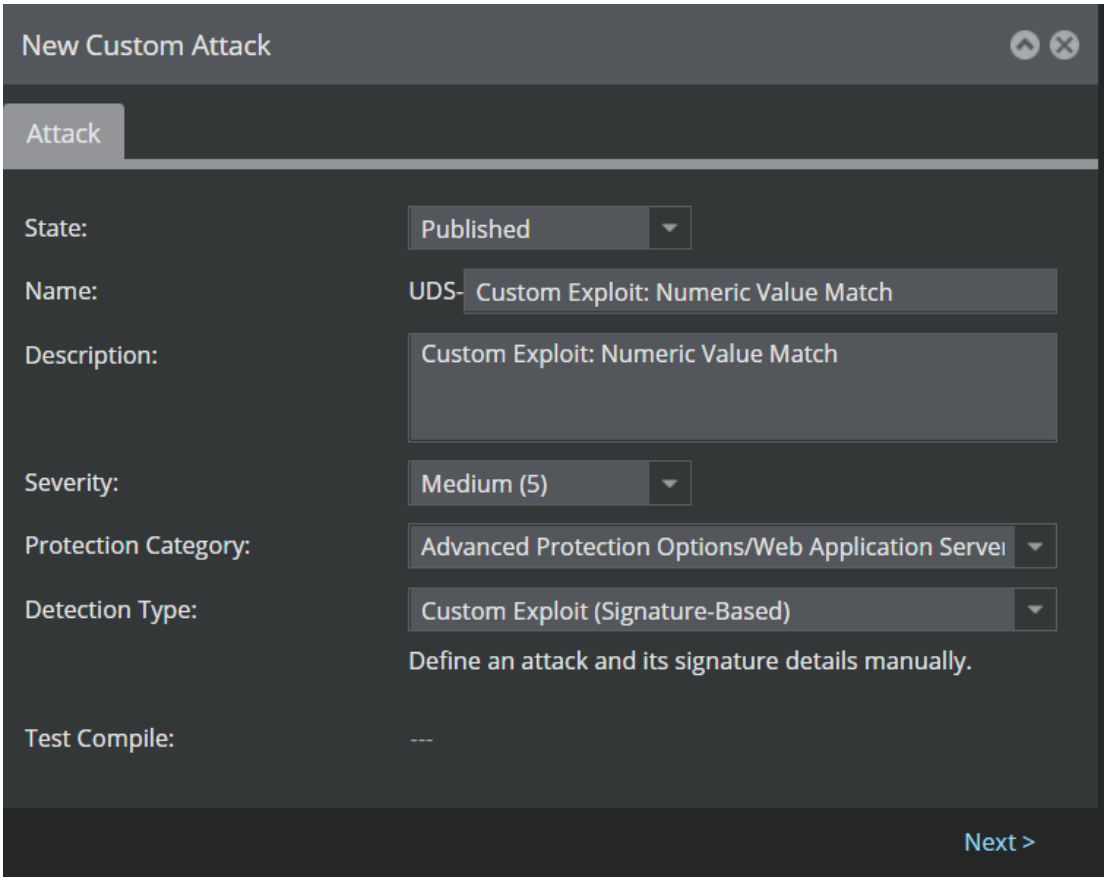
   The **New Custom Attack** interface opens.



2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as "Custom Exploit: Numeric Value Match" as the **Name**.

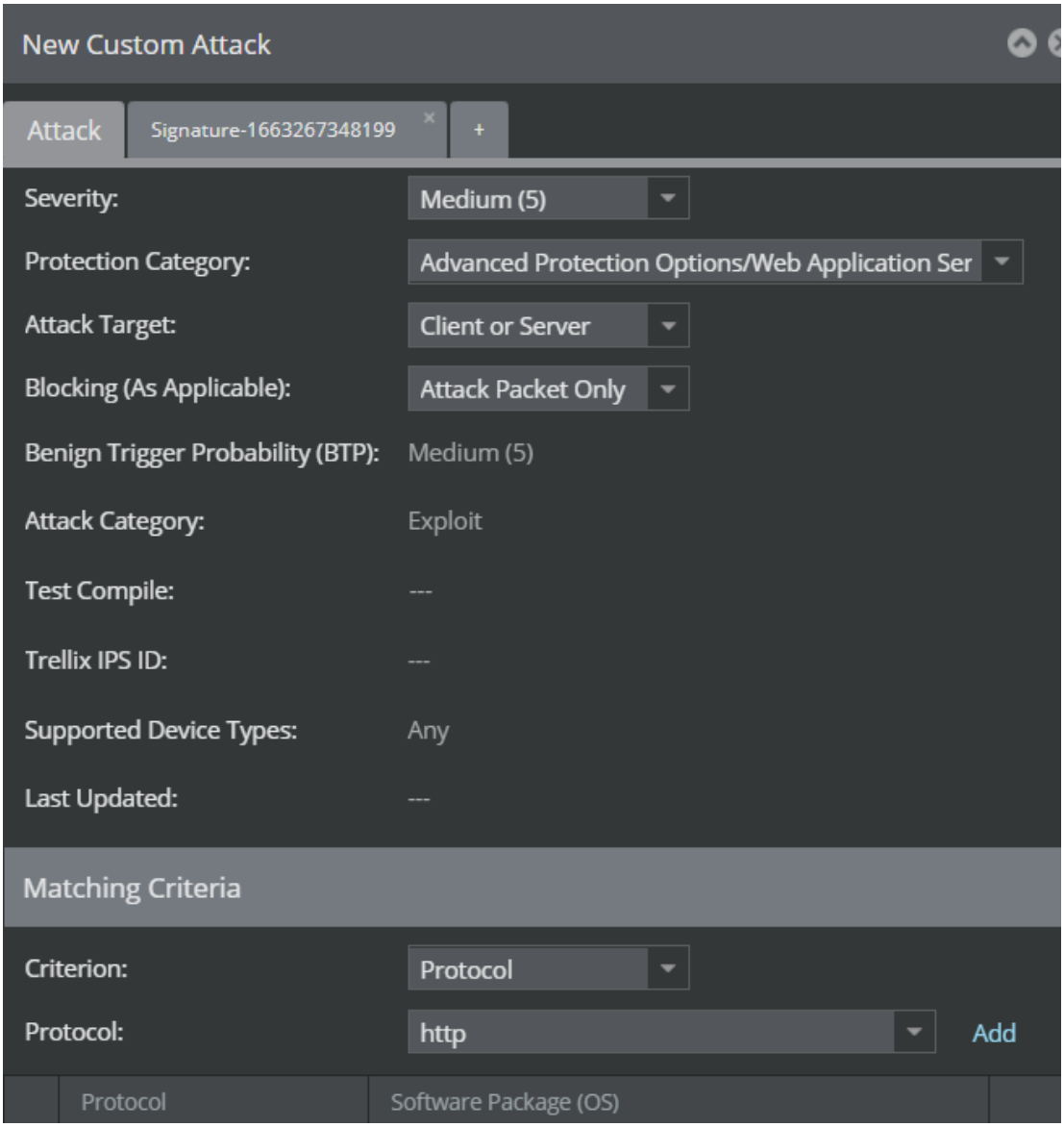
   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-Custom Exploit: Numeric Value Match" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium (5)** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server** as the **Protection Category**.
7. Select **Custom Exploit (Signature Based)** from the **Detection Type** drop-down menu for the attack.

8. Click **Next**.



9. Select **Client or Server** as **Attack Target**.
10. Select **Attack Packet Only** as **Blocking (As Applicable)**.
11. In the **Matching Criteria** section, select **Protocol** as the **Criterion** and select **HTTP** as protocol.

    When you subsequently save this attack definition in the Manager server, it will be part of every rule set which includes Medium-severity, HTTP attacks (must match both severity and protocol).



12. Attack details configuration is complete. Continue to create signature.

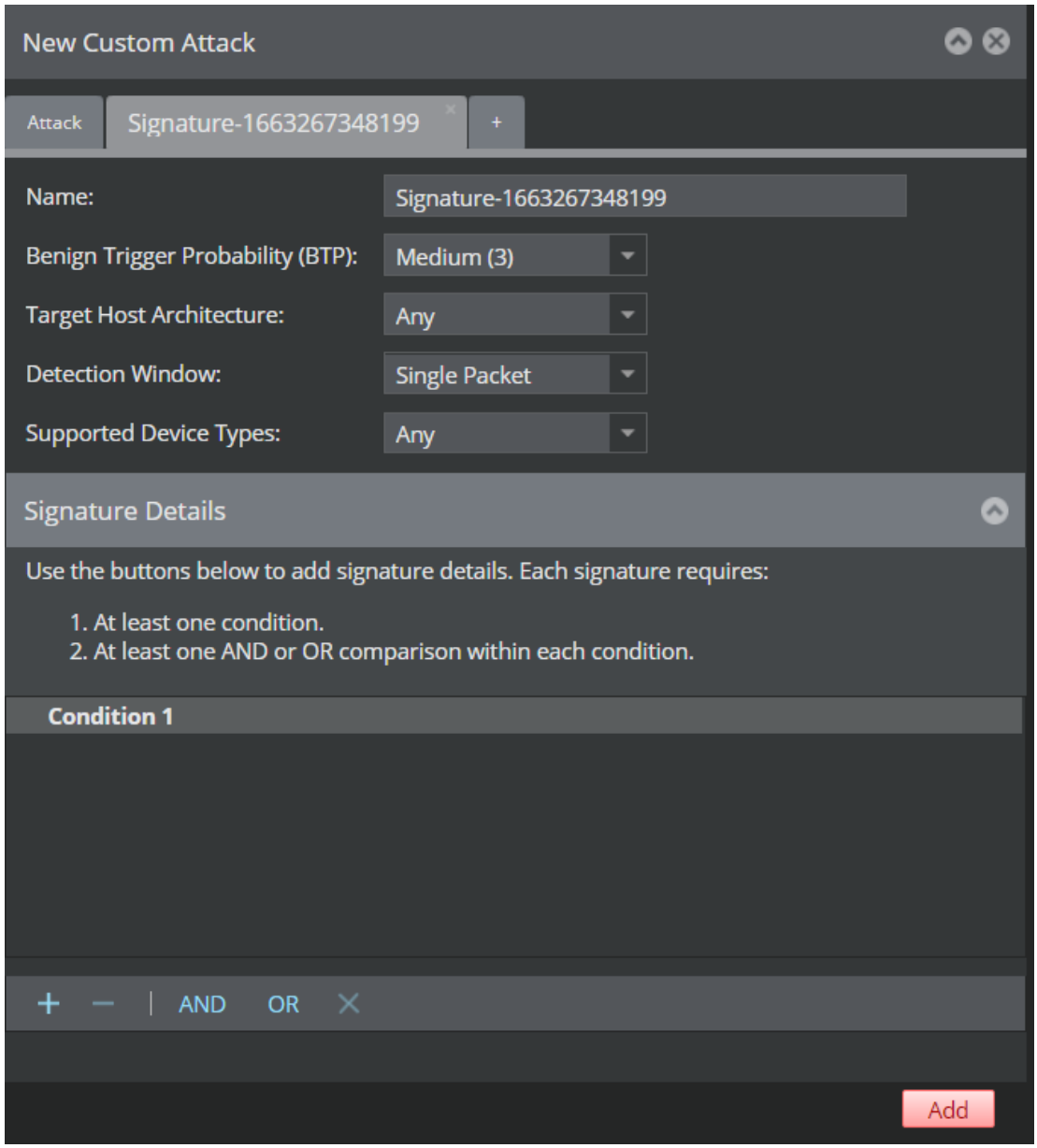
Create the signature for numeric value match

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** window, click **Signature-<signature name>** tab.

Figure 792. New Signature window



2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)**, **Target Host Architecture**, and **Detection Window** with the default values.
4. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.
5. Add the condition to the signature.

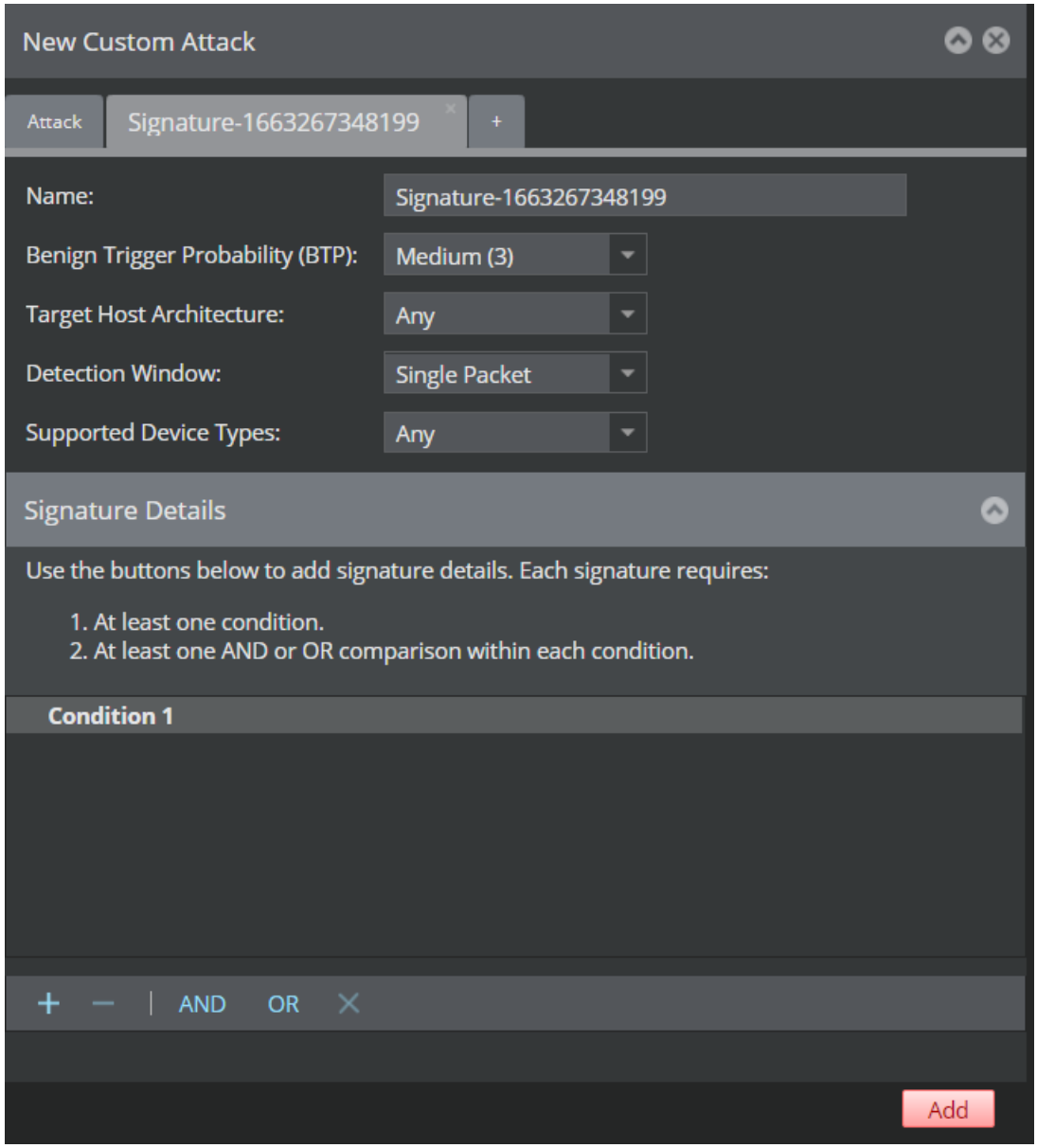
   It is in the conditions that you specify the following details:

   - The string that the Sensor should look for
   - Which section of the HTTP request should it look for the string
6. Proceed to add the condition.

Add the condition for numeric value match

To add the condition to the example signature:

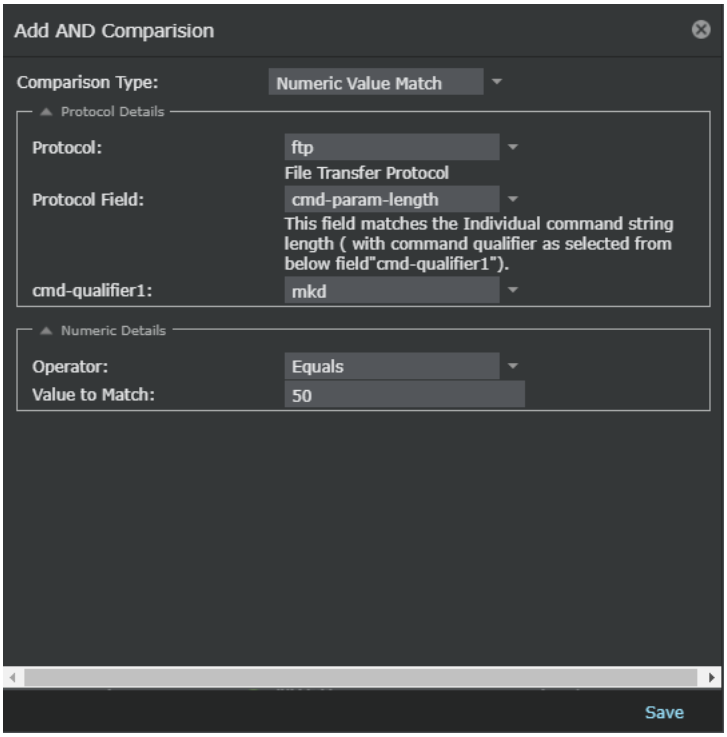
1. Click **Condition 1** so that it is highlighted.



2. Click **AND** in the Comparisons section.

   The **Add AND Comparision** window opens.

Figure 793. Numeric Value Match



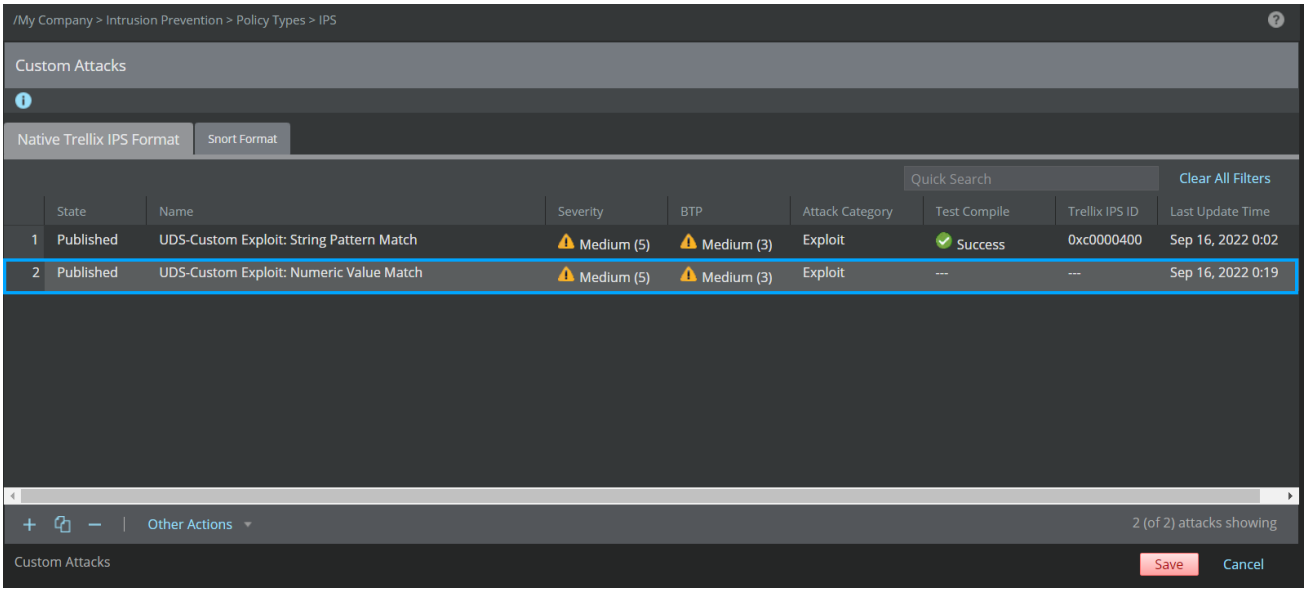
3. For this example, select **Numeric Value Match** in the **Comparison Type** drop-down menu.
4. Select **FTP** from the **Protocol** list.

   Because you selected FTP, the Custom Attack Editor displays the FTP-specific protocol fields on the following screen.
5. Configure the fields for the comparison you have chosen.

   For this example, specify **cmd-param-length** for the Protocol Field. This specifies that the Sensor should search in the URI of the request packet.
6. Select **mkd** as the qualifier.
7. From the **Operator** drop-down list, select the matching criteria as **Equals** which means that the comparison criteria must be equal to the regular expression entered.
8. Type the value to match using the **Value to Match**.

   For this example, the value to match is "50".
9. Click **Save**.

   Your comparison appears under **Condition 1**.
10. Click **Add** in the **New Custom Attack** window.
11. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.



12. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
13. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Create an attack definition for numeric range match

This scenario is about creating a Custom Attack Definition that uses numeric range match to detect if the destination port range is between 100 and 2000 for HTTP protocol.

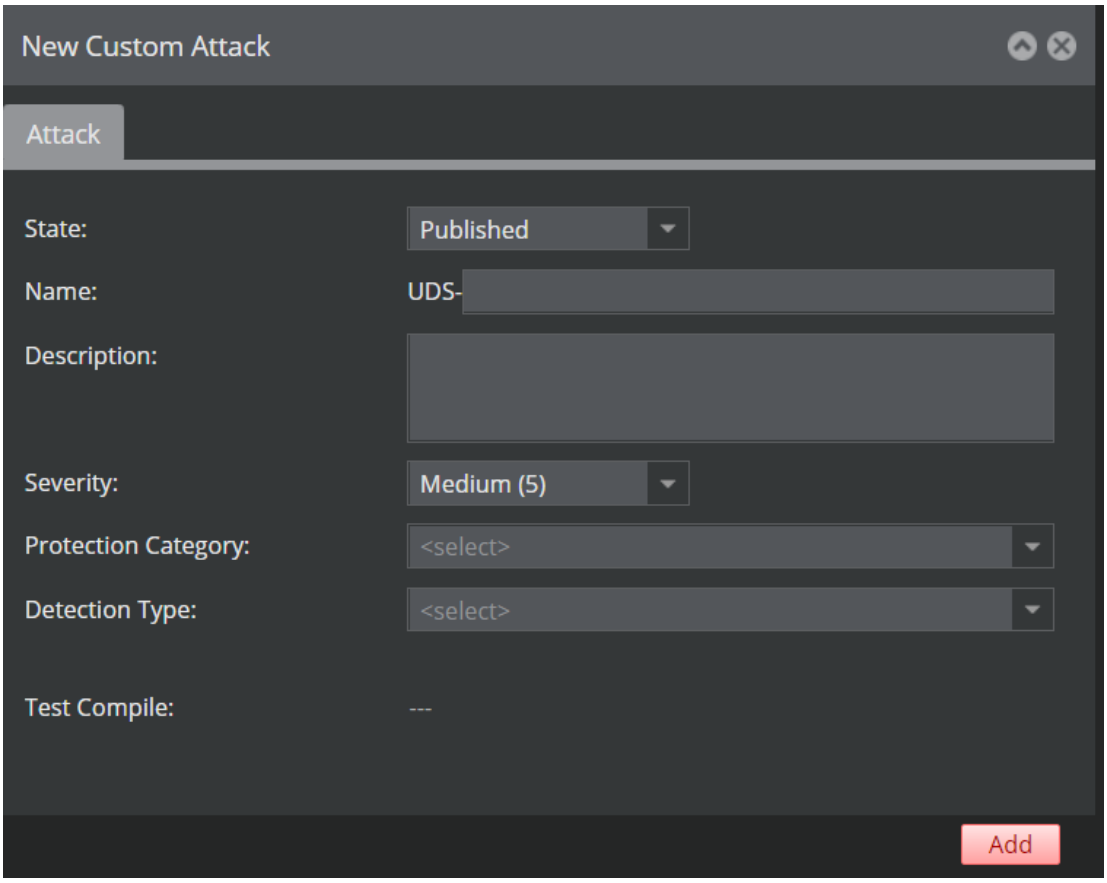
In order to write a proper Native Trellix IPS Format Custom Attack for this example, you must identify several key elements:

- Application protocol: HTTP
- Protocol field: dst-port
- Minimum value: 100
- Maximum value: 2000

Steps to create the attack definition for this example:

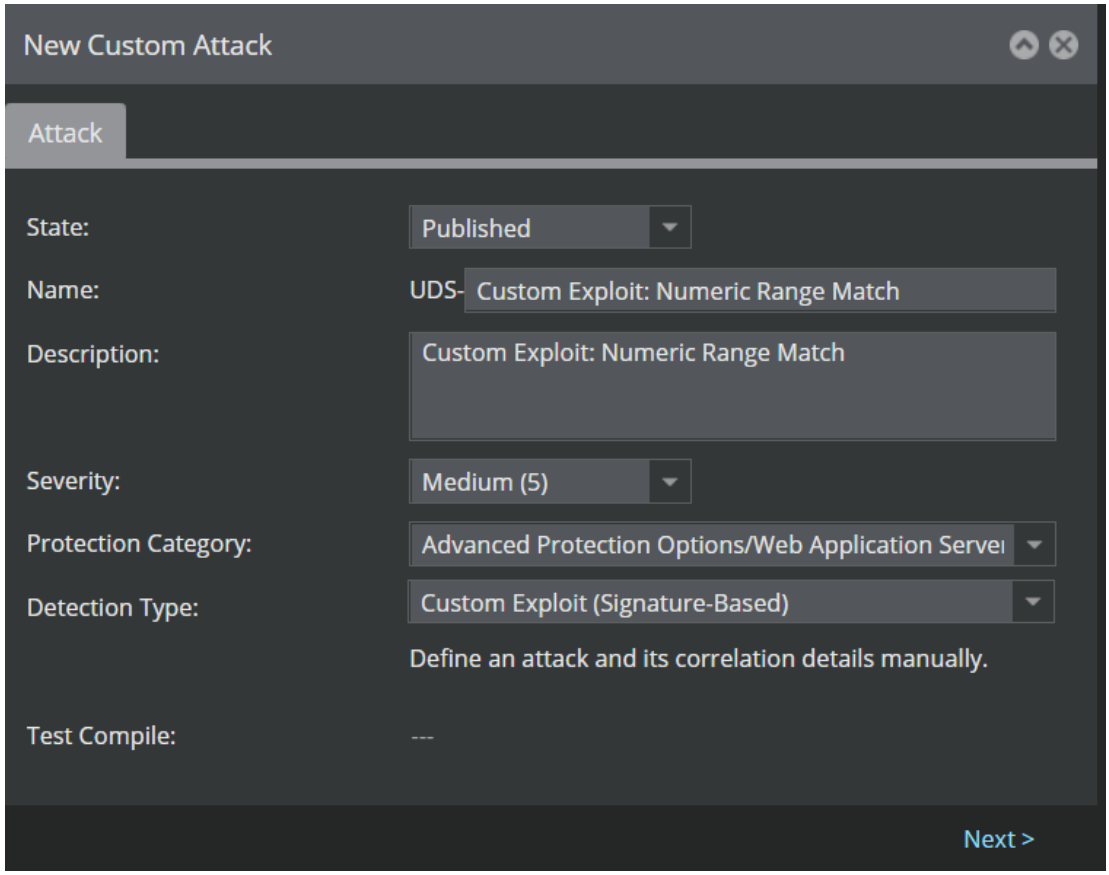
1. In the Custom Attack Editor, click .

   The **New Custom Attack** interface opens.



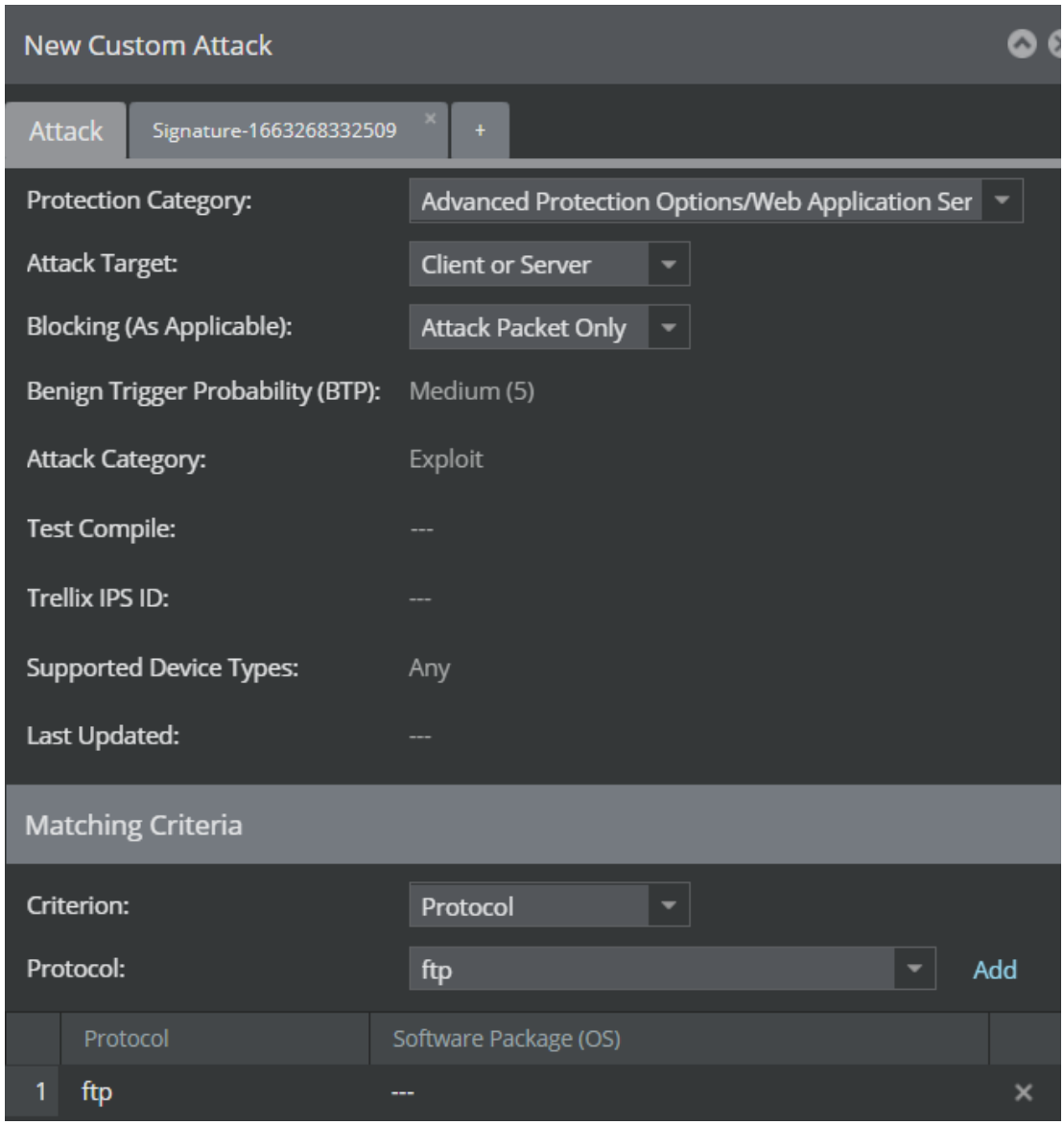
2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as "Custom Exploit: Numeric Range Match" as the **Name**.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-Custom Exploit: Numeric Range Match" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium (5)** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server** as the **Protection Category**.
7. Select **Custom Exploit (Signature Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.



9. Select **Client or Server** as **Attack Target**.
10. Select **Attack Packet Only** as **Blocking (As Applicable)**.
11. In the **Matching Criteria** section, select **Protocol** as the **Criterion** and select **ftp** as the protocol.

    When you subsequently save this attack definition in the Manager server, it will be part of every rule set which includes Medium-severity, HTTP attacks (must match both severity and protocol).



12. Attack details configuration is complete. Continue to create signature.

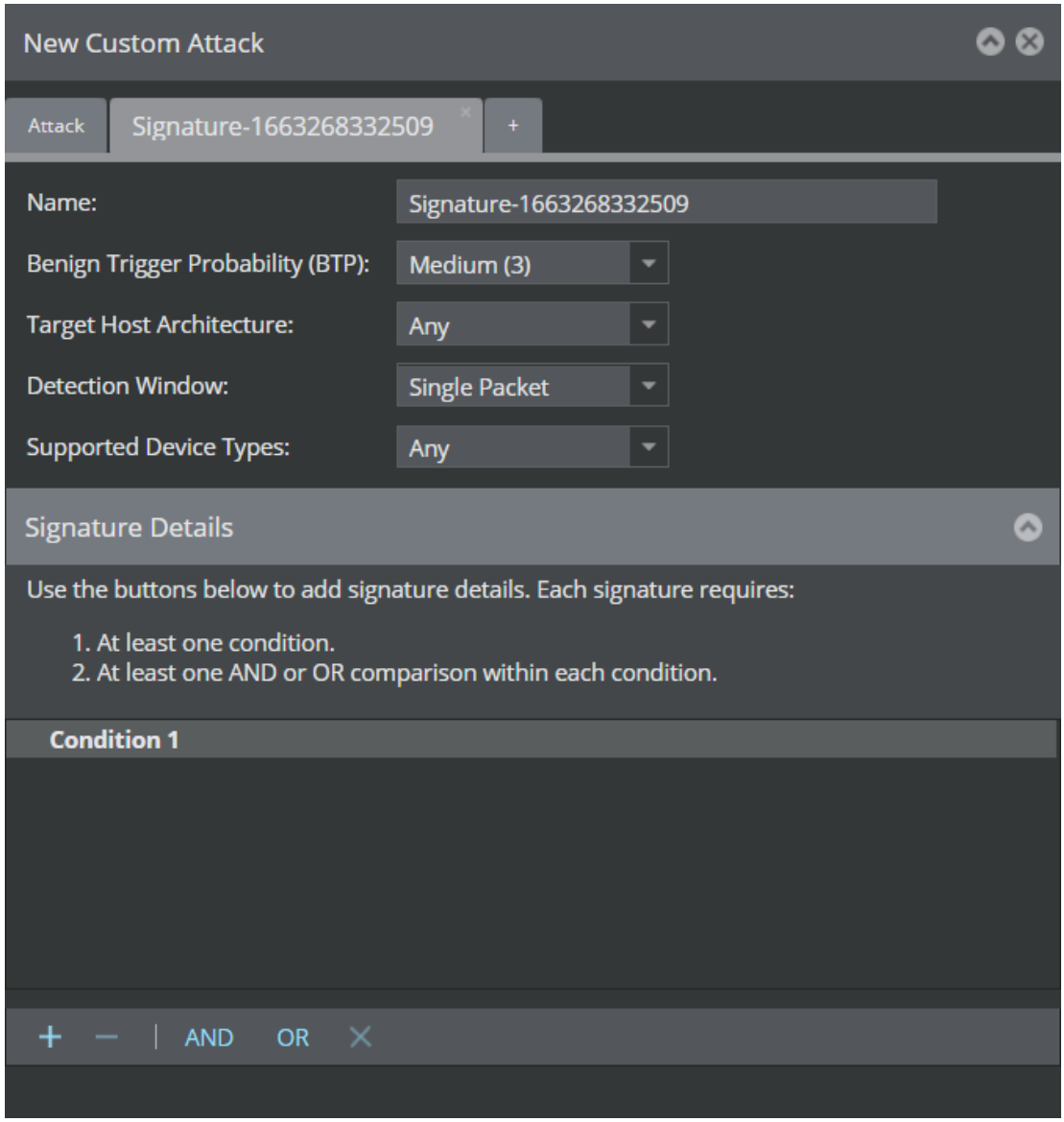
Create the signature for numeric range match

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** window, click **Signature-<signature name>** tab.

Figure 794. New Signature window



2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)**, **Target Host Architecture**, and **Detection Window** with the default values.
4. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.
5. Add the condition to the signature.

   It is in the conditions that you specify the following details:

   - The string that the Sensor should look for.
   - Which section of the http request should it look for the string.
6. Proceed to add the condition.

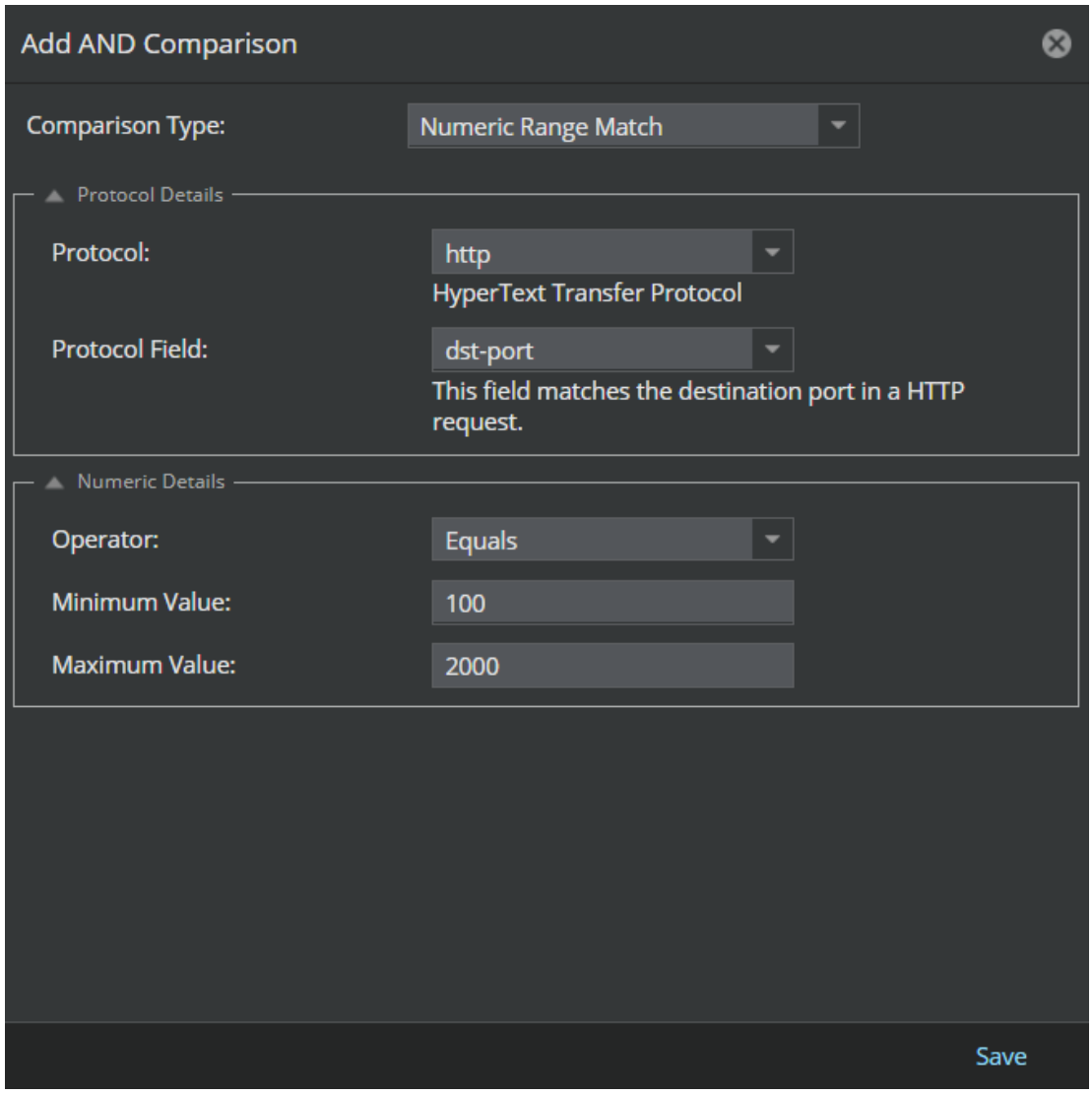
Add the condition for numeric range match

Steps to add the condition to the example signature:

1. Click **Condition 1** so that it is highlighted.
2. Click **AND** in the Comparisons section.

   The **Add AND Comparision** dialog opens.

Figure 795. Numeric Range Match



3. For this example, select **Numeric Range Match** in the **Comparison Type** drop-down menu.
4. Select **http** from the **Protocol** list.

   Because you selected HTTP, the Custom Attack Editor displays the http specific protocol fields on the screen.
5. Configure the fields for the comparison you have chosen.

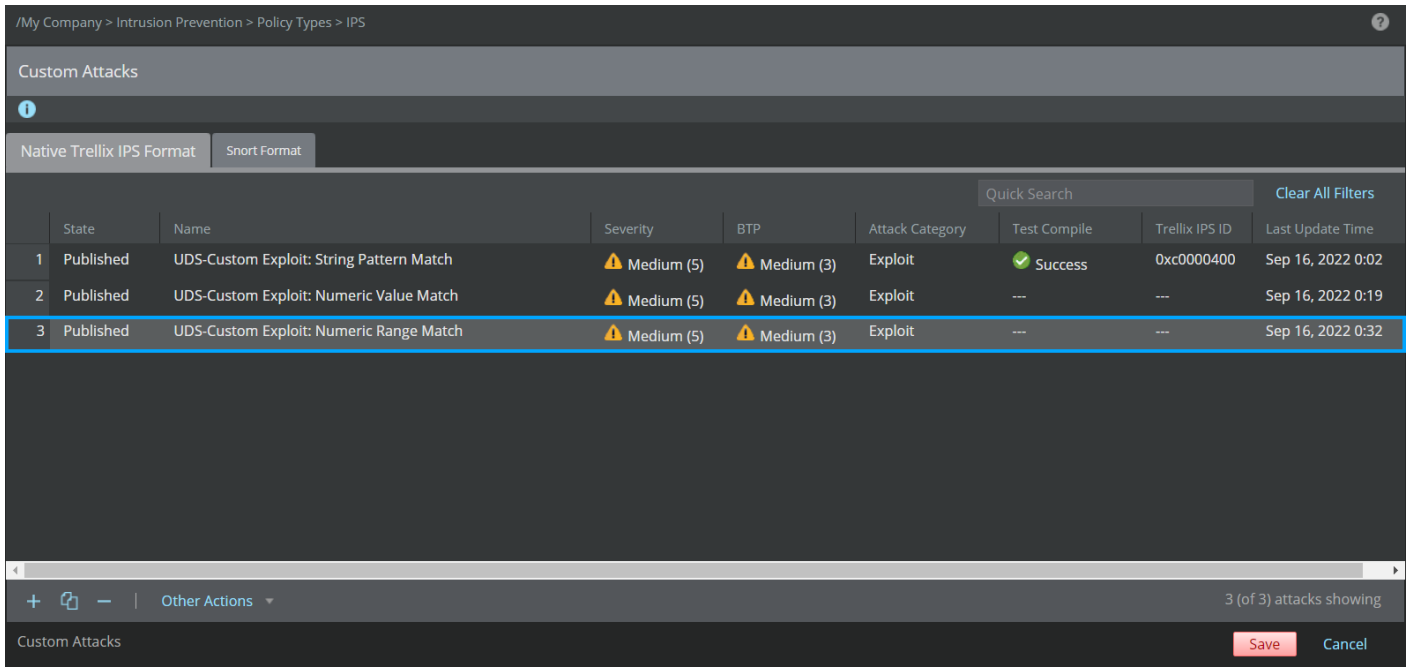
For this example, specify **dst-port** for the Protocol Field. This specifies that the Sensor should search in the URI of the request packet.

6. From the drop-down list in the **Operator**, select the matching criteria as **Equals** which means that the comparison criteria must be between to the minimum and maximum values entered.
7. Type the minimum value in the **Mininum Value** field.

   For this example, the minimum value is "100".
8. Type the maximum value in the **Maximum Value** field.

   For this example, the value to match is "2000".
9. Click **Save**.

   Your comparison appears under **Condition 1**.
10. Click **Add** in the **New Custom Attack** window.
11. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.



12. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
13. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Create an attack definition for numeric enumeration match

This scenario is about creating a Custom Attack Definition that uses numeric enumeration match to detect if the HTTP response code is either 302 or 404.

In order to write a proper Native Trellix IPS Format Custom Attack for this example, you must identify several key elements:

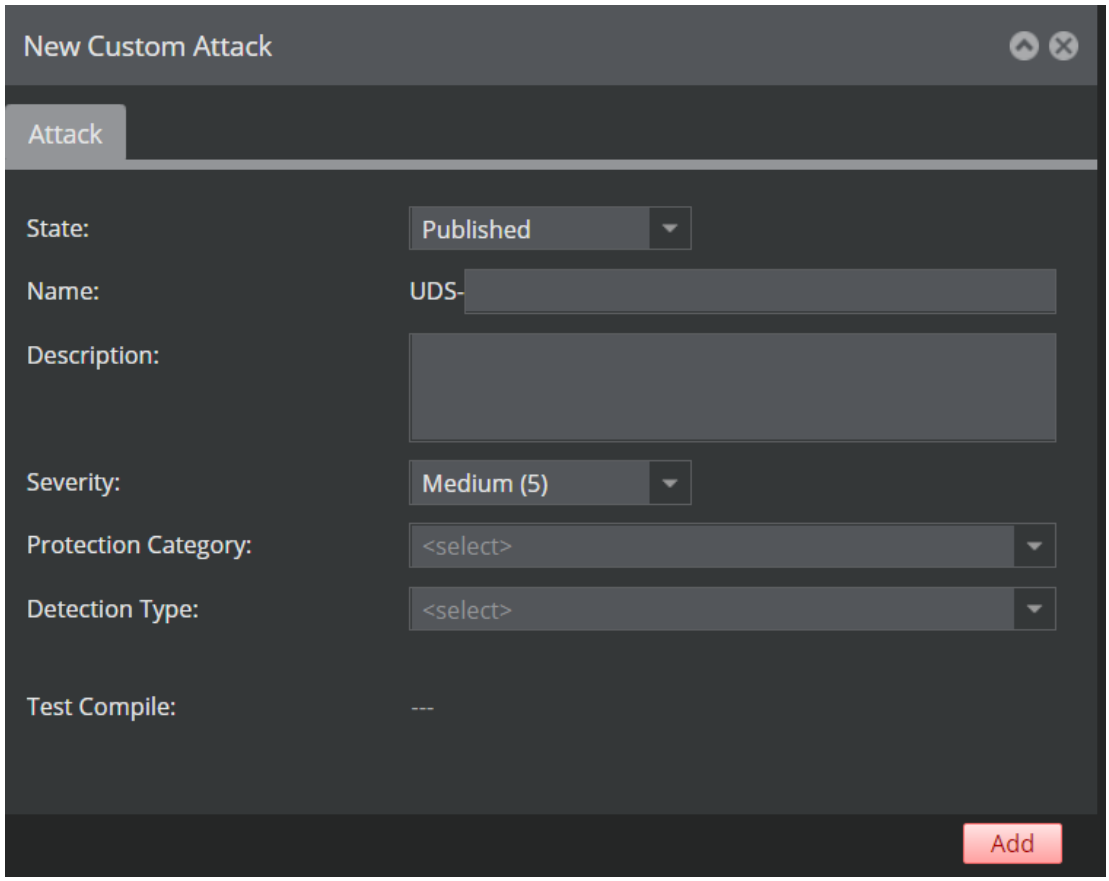
- Application protocol: HTTP
- Protocol field: rsp-code

- Enumeration value (integer): 302 and 404

Steps to create the attack definition for this example:

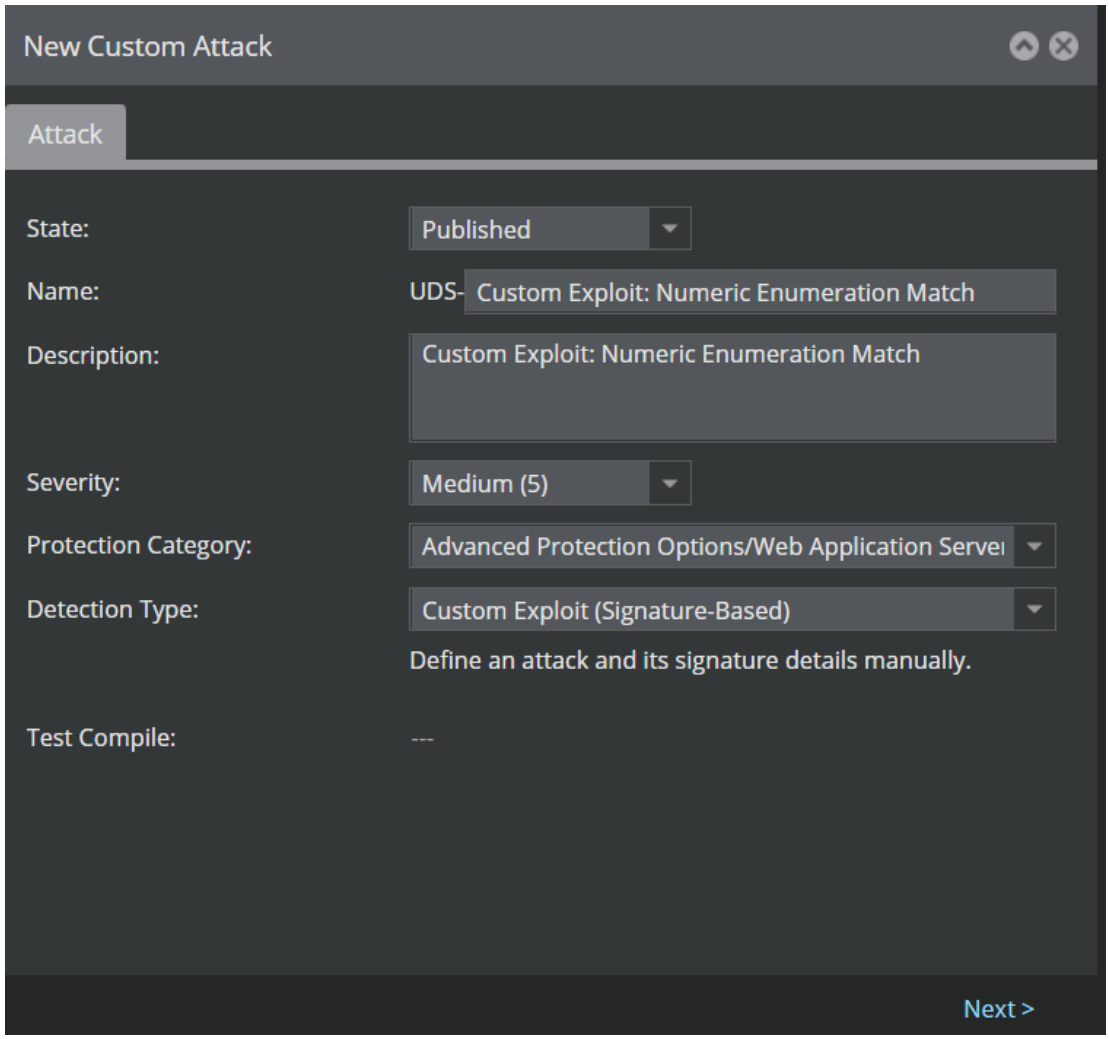
1. In the Custom Attack Editor, click +.

   The **New Custom Attack** interface opens.



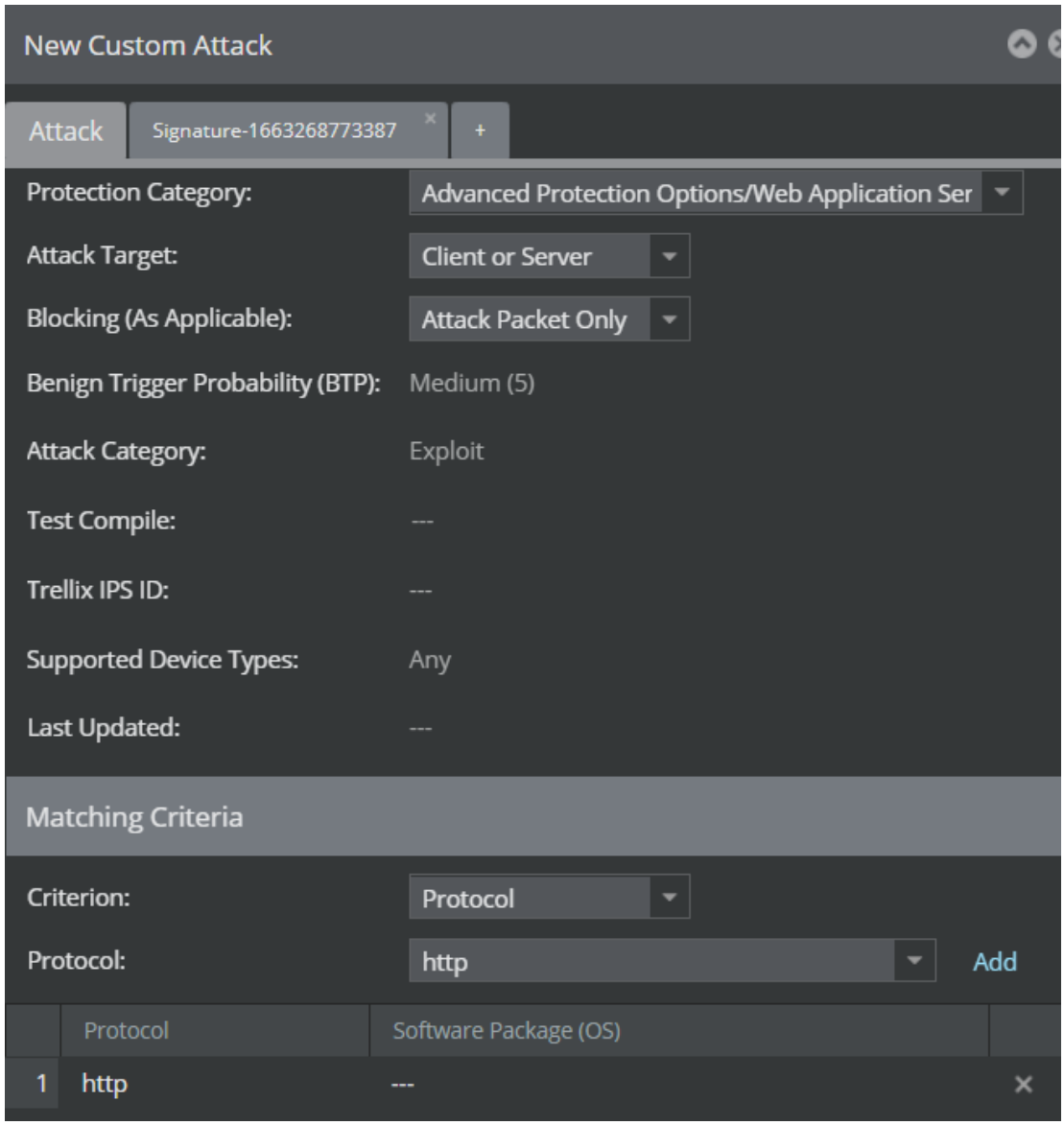
2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as "Custom Exploit: Numeric Enumeration Match" as the **Name**.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-Custom Exploit: Numeric Enumeration Match" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium (5)** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server** as the **Protection Category**.
7. Select **Custom Exploit (Signature Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.



9. Select **Client or Server** as **Attack Target**.
10. Select **Attack Packet Only** as **Blocking (As Applicable)**.
11. In the **Matching Criteria** section, select **Protocol** as the **Criterion** and select **http** as the protocol.

    When you subsequently save this attack definition in the Manager server, it will be part of every rule set which includes Medium-severity, HTTP attacks (must match both severity and protocol).



12. Attack details configuration is complete. Continue to create signature.

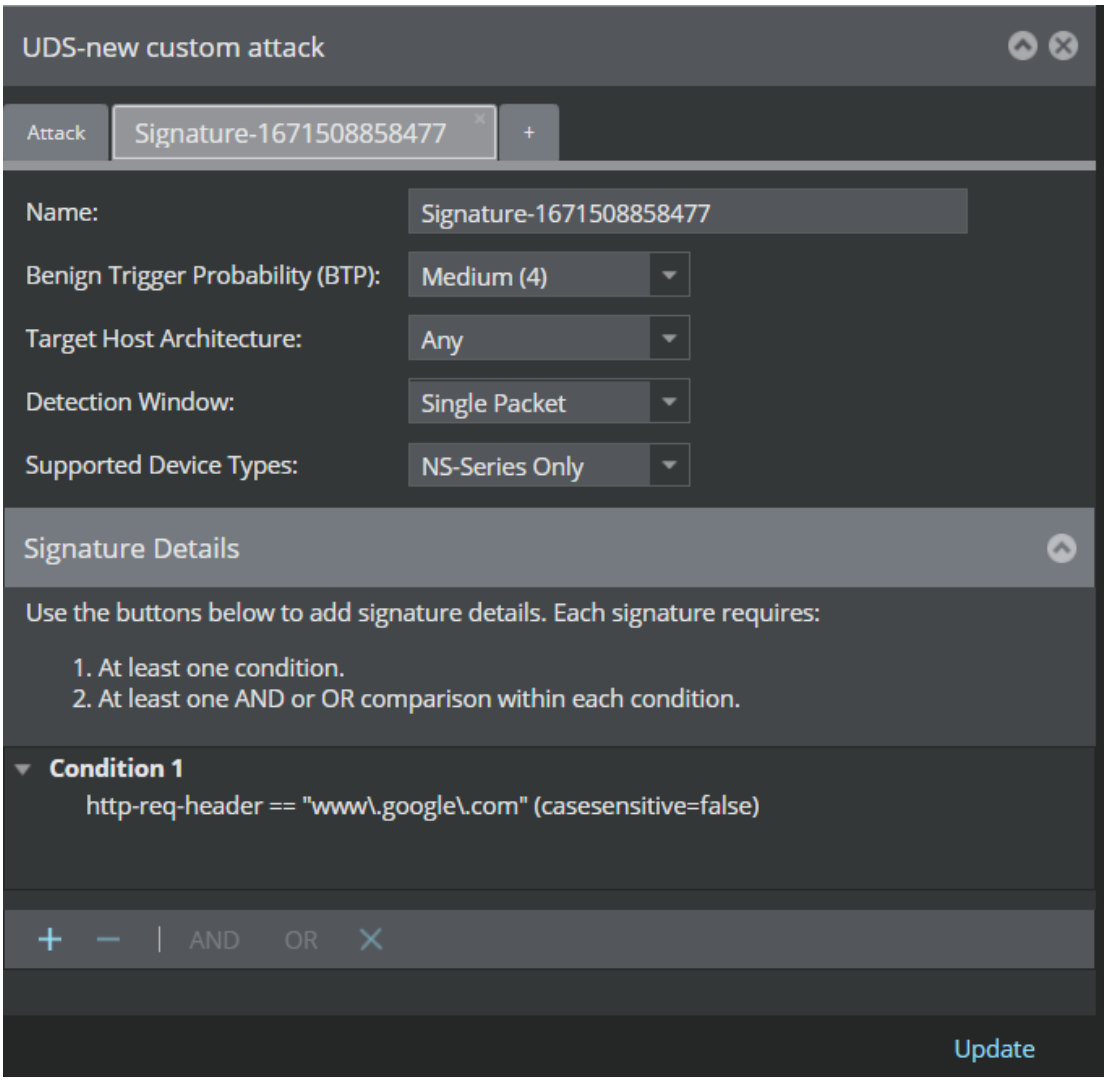
Create the signature for numeric enumeration match5

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** window, click **Signature-<signature name>** tab.

Figure 796. New Signature window



2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)**, **Target Host Architecture**, and **Detection Window** with the default values.
4. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.
5. Add the condition to the signature.

   It is in the conditions that you specify the following details:

   - The string that the Sensor should look for
   - Which section of the HTTP request should it look for the string
6. Proceed to add the condition.

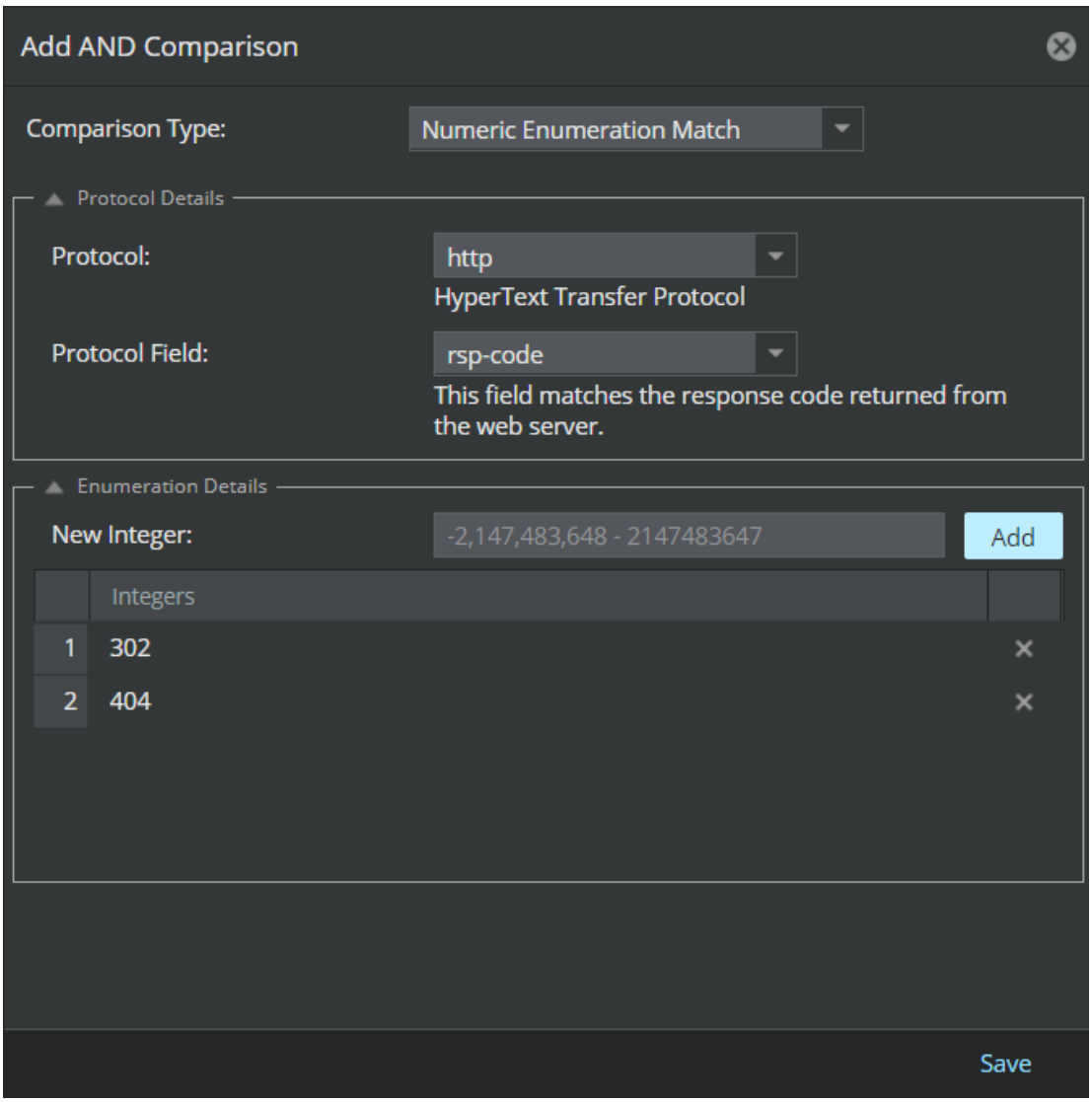
Add the condition for numeric enumeration match

Steps to add the condition to the example signature:

1. Click **Condition 1** so that it is highlighted.
2. Click **AND**.

   The **Add AND Comparision** dialog opens.

Figure 797. Numeric Enumeration Match



3. For this example, select **Numeric Enumeration Match** in the **Comparison Type** drop-down menu.
4. Select **http** from the **Protocol** list.

   Because you selected HTTP, the Custom Attack Editor displays the HTTP-specific protocol fields on the following screen.
5. Configure the fields for the comparison you have chosen.

   For this example, specify **rsp-code** for the Protocol Field. This specifies that the Sensor should search in the URI of the request packet.
6. In the **New Integer** field, enter the in the numeric value.
7. Click **Add**.

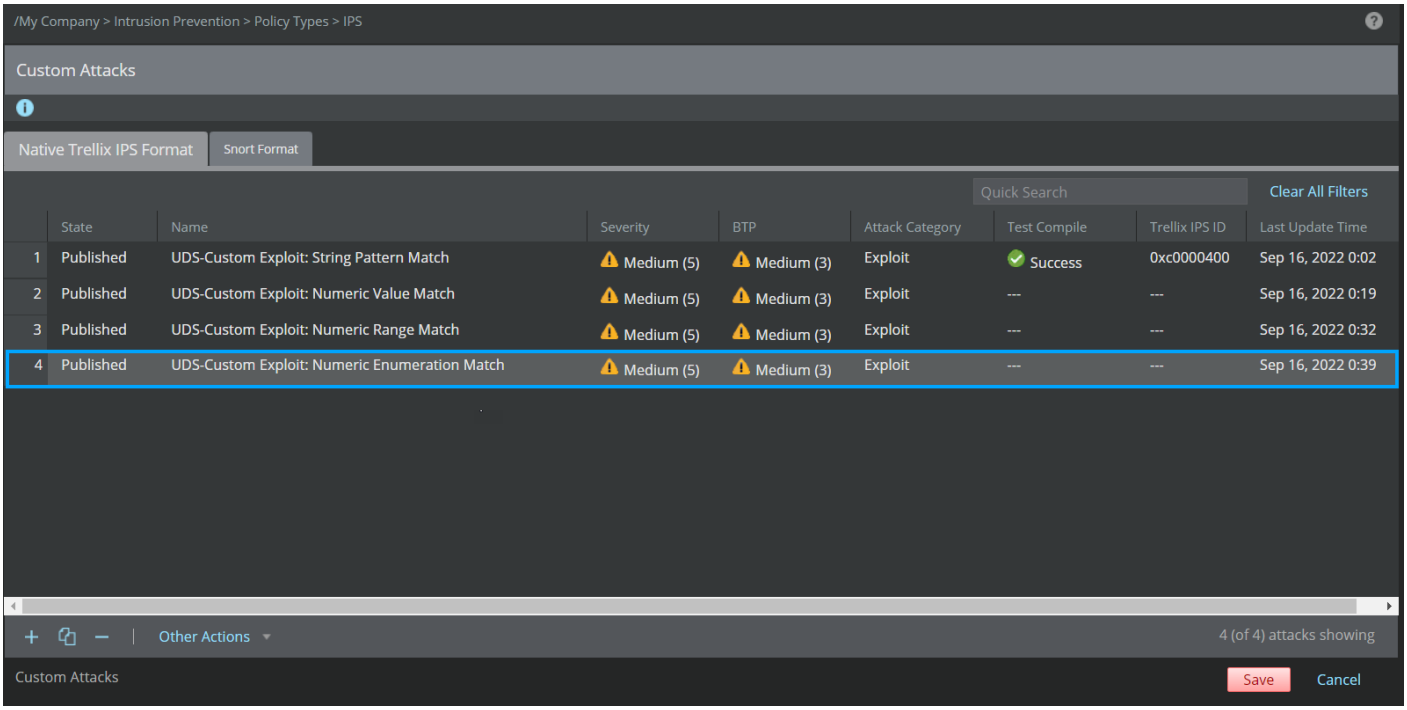
You can add multiple values in the **New Integer** field. For this example enter 302 and 404.

8. Click **Save**.

   Your comparison appears under **Condition 1**.

9. Click **Add** in the **New Custom Attack** window.

10. Verify that the attack definition is listed on the **All Custom Attacks** tab.



11. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.

12. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Create an attack definition for single fixed field match

This scenario is about creating a Custom Attack Definition that uses single fixed field match to detect if the IPv4 address matches 103.17.47.20 in HTTP protocol.

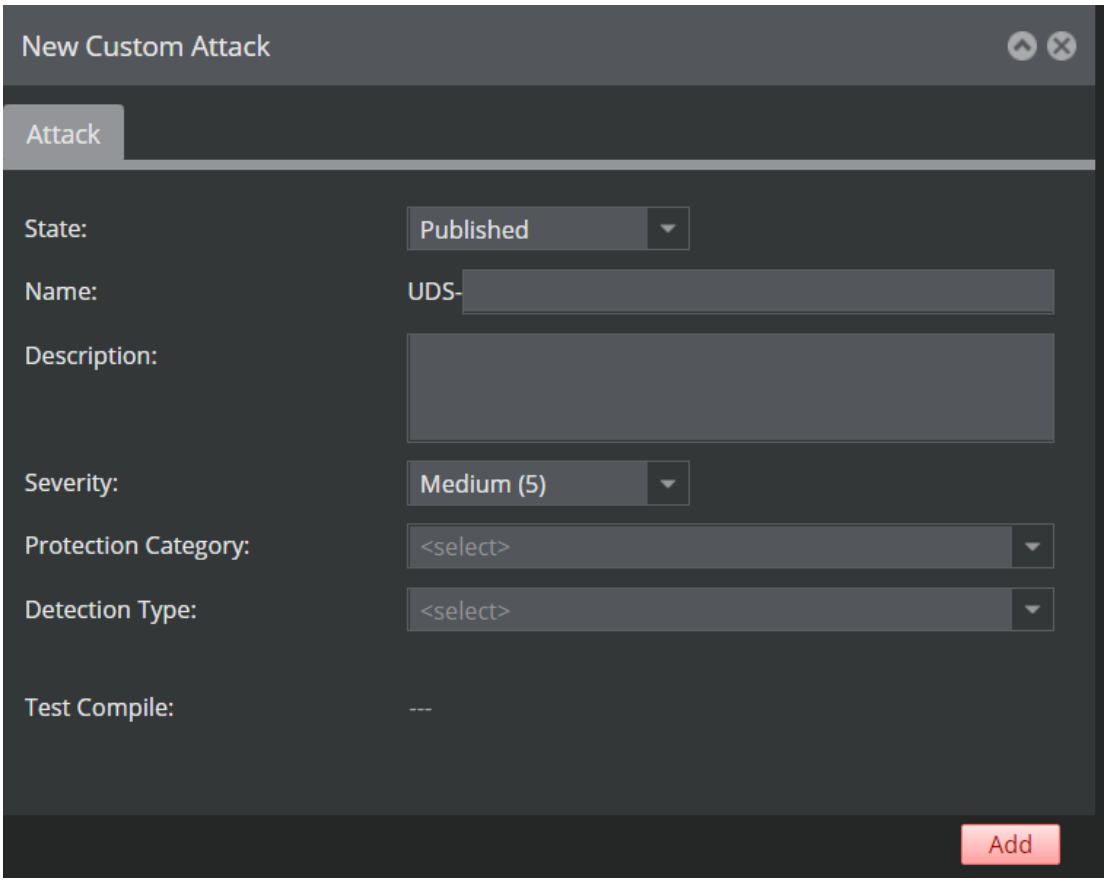
In order to write a proper Native Trellix IPS Format Custom Attack for this example, you must identify several key elements:

- Application protocol: IPv4
- Protocol field: ipv4-destination-ip
- IP address to match: 103.17.47.20

Steps to create the attack definition for this example:

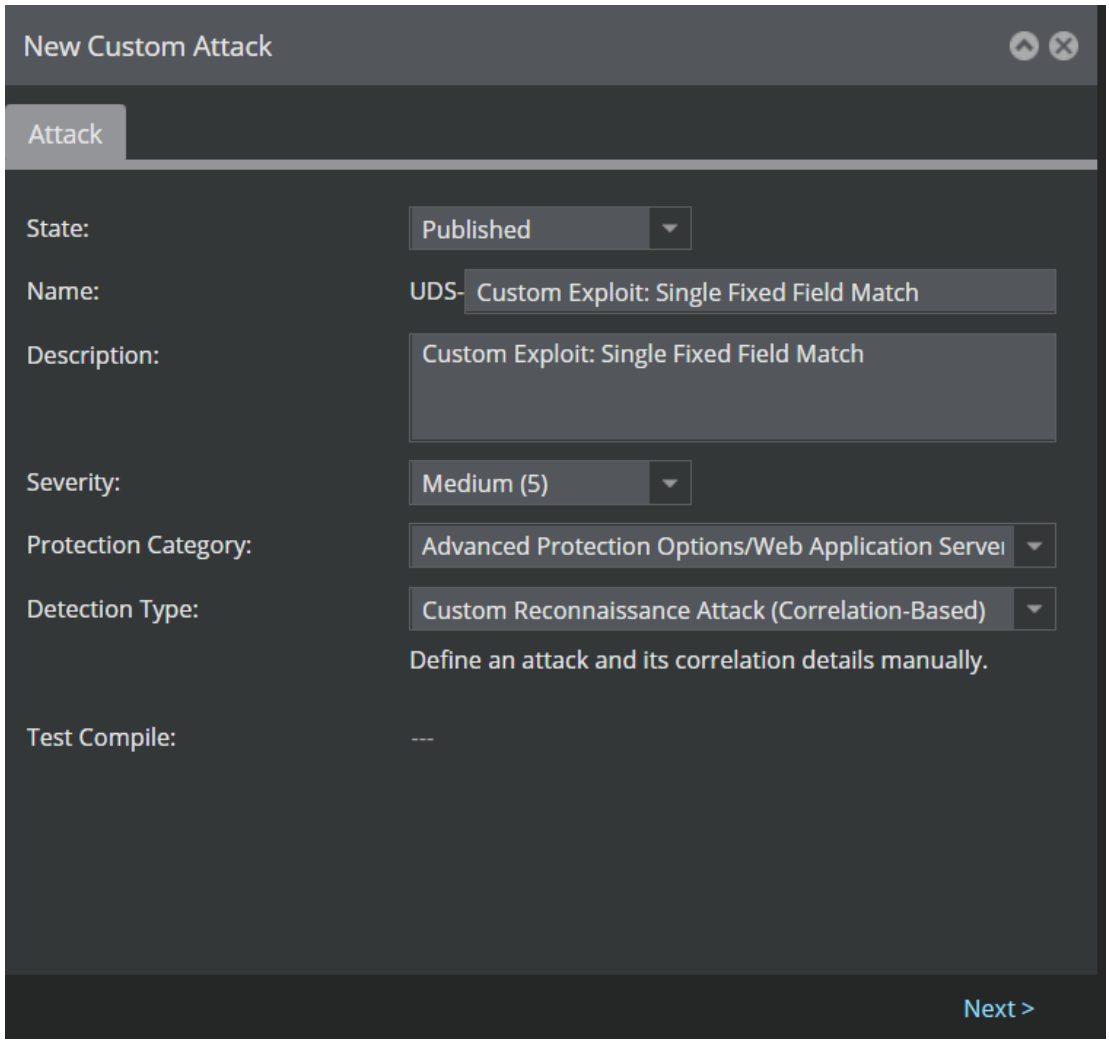
1. In the Custom Attack Editor, click +.

   The **New Custom Attack** interface opens.



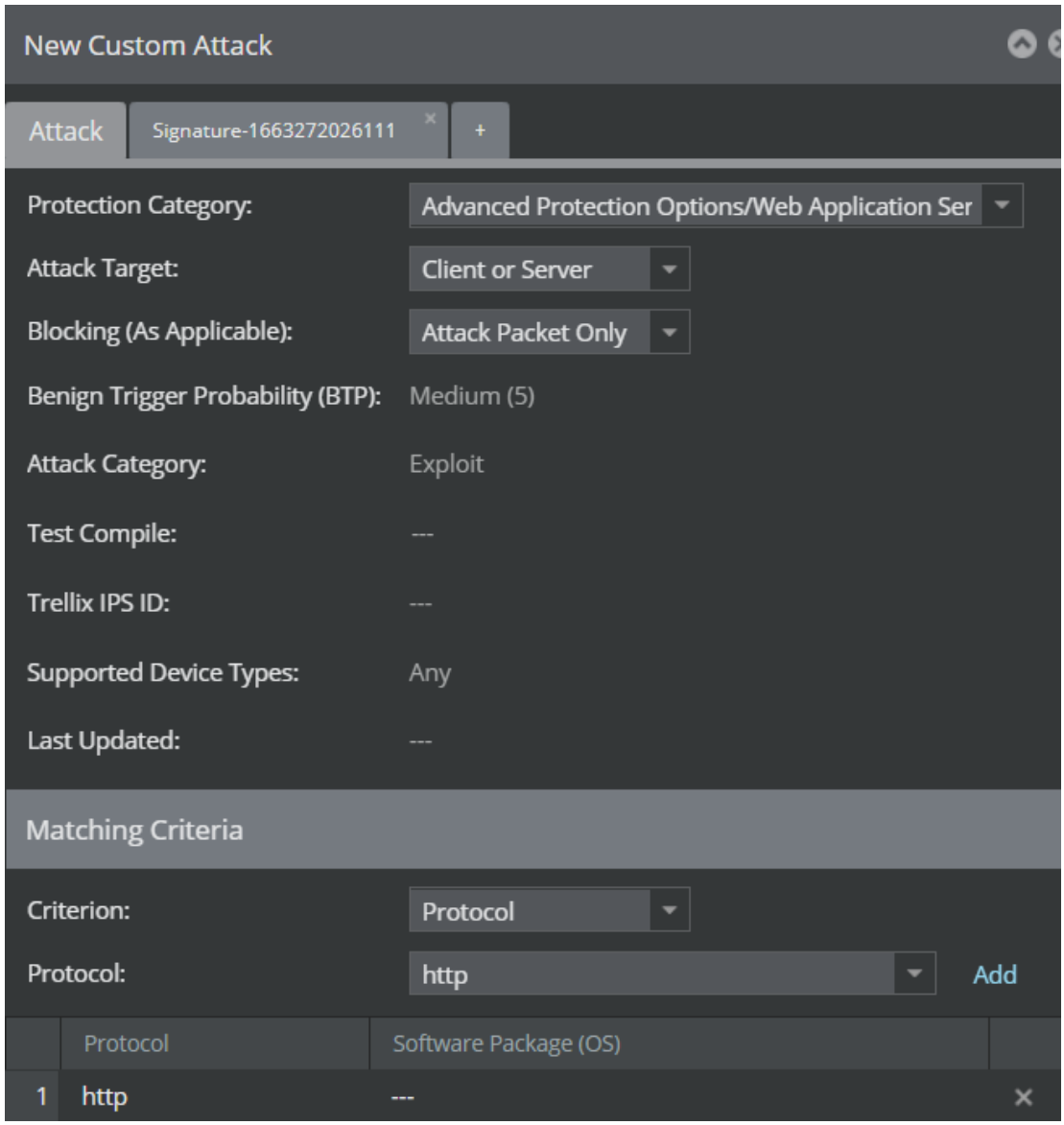
2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as "Custom Exploit: Single Fixed Field Match" as the **Name**.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-Custom Exploit: Single Fixed Field Match" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium (5)** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server** as the **Protection Category**.
7. Select **Custom Exploit (Signature Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.



9. Select **Client or Server** as **Attack Target**.
10. Select **Attack Packet Only** as **Blocking (As Applicable)**.
11. In the **Matching Criteria** section, select **Protocol** from the **Criterion** and select **http** as the protocol.

    When you subsequently save this attack definition in the Manager server, it will be part of every rule set which includes Medium-severity, HTTP attacks (must match both severity and protocol).



12. Attack details configuration is complete. Continue to create signature.

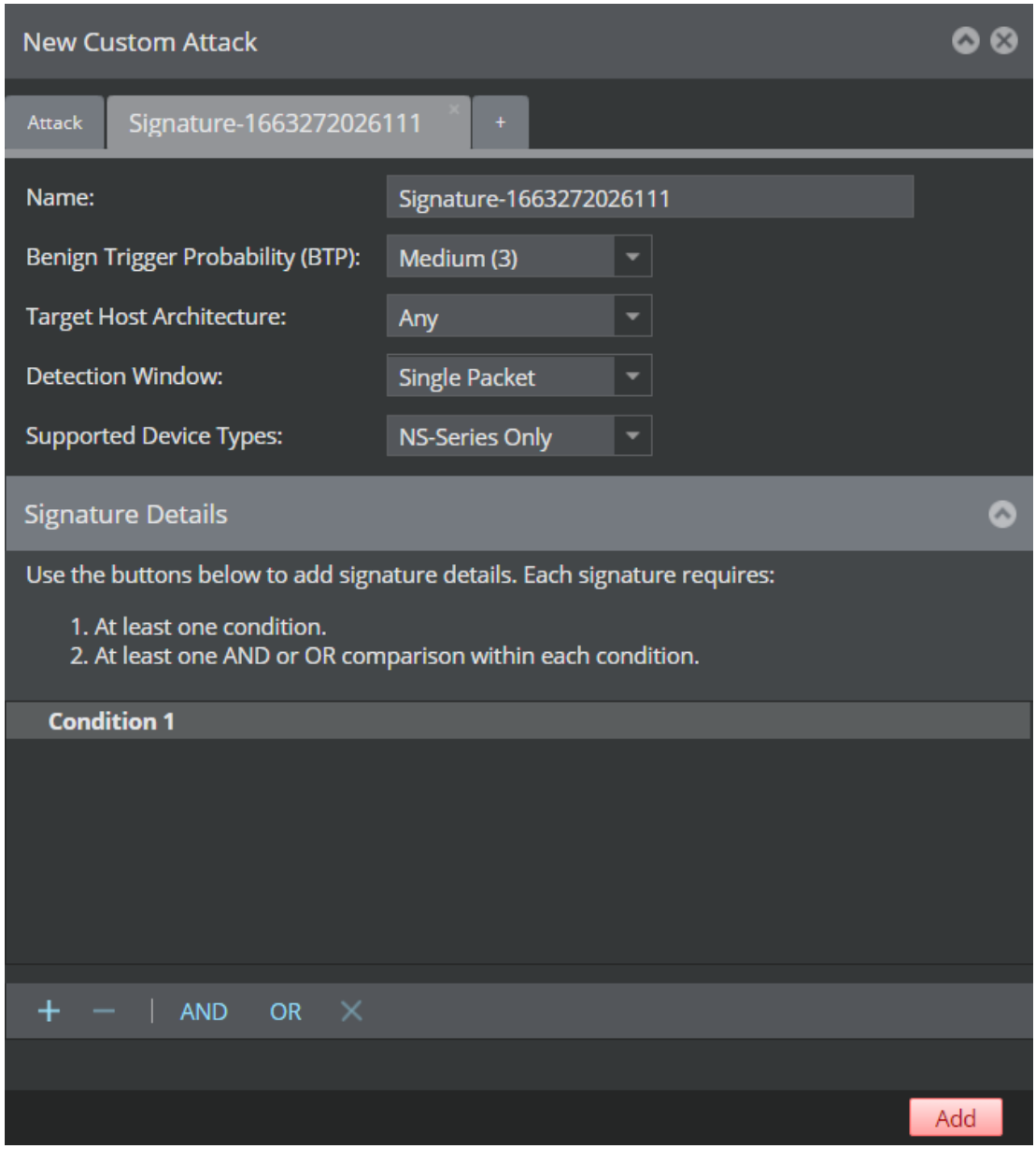
Create the signature for single fixed field match

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** window, click **Signature-<signature name>** tab.

Figure 798. New Signature window



2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)**, **Target Host Architecture**, and **Detection Window** with the default values.
4. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.
5. Add the condition to the signature.

   It is in the conditions that you specify the following details:

   - The string that the Sensor should look for
   - Which section of the HTTP request should it look for the string
6. Proceed to add the condition.

Add the condition for single fixed field match

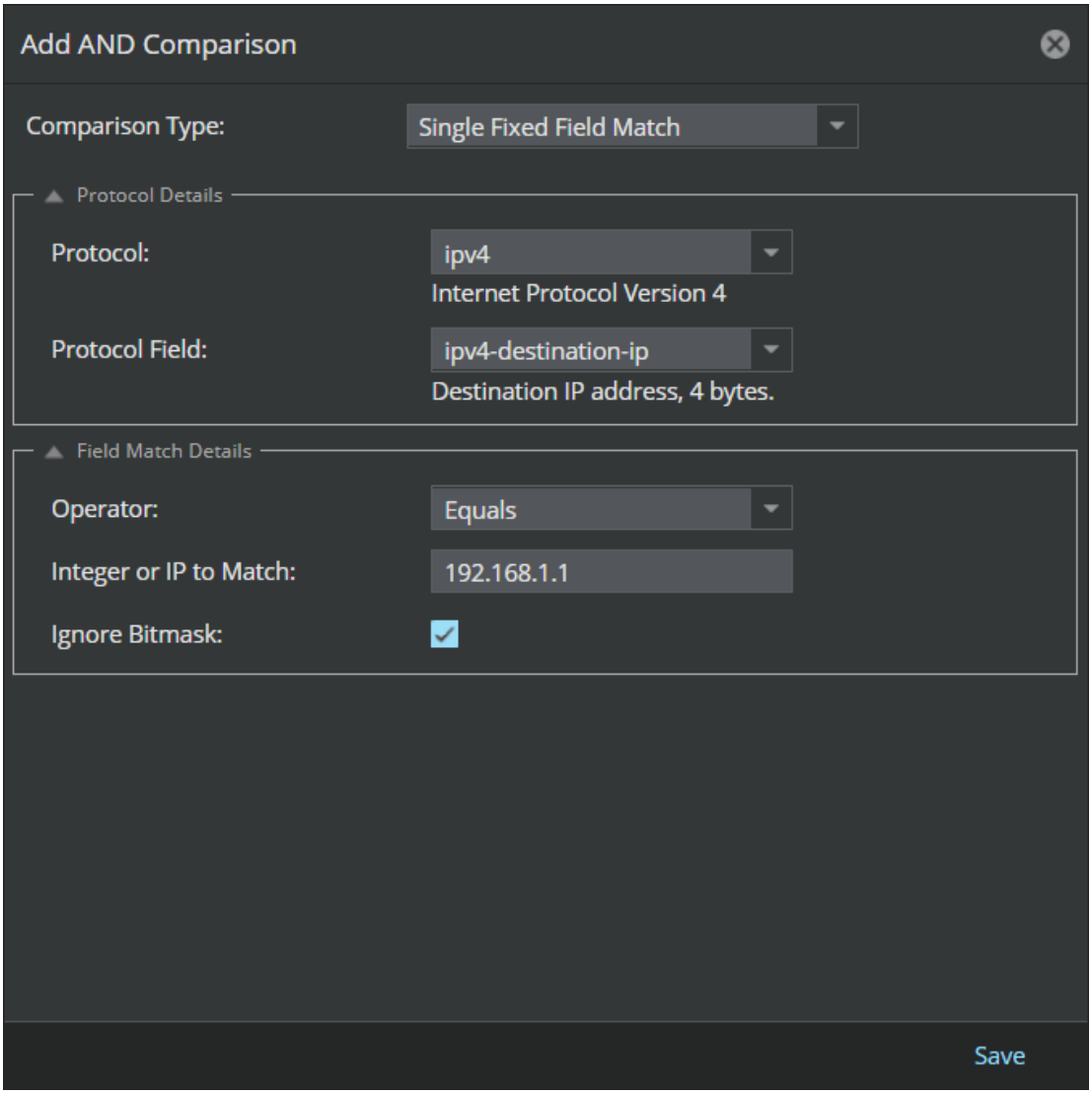
To add the condition to the example signature:

Steps:

1. Click **Condition 1** so that it is highlighted.
2. Click **AND** in the Comparisons section.

   The **Add AND Comparison** dialog opens.

Figure 799. Single Fixed Field Match



3. For this example, select **Single Fixed Field Match** in the **Comparison Type** drop-down menu.
4. Select **ipv4** from the **Protocol** list.

   Because you selected IPv4, the Custom Attack Editor displays the IPv4-specific protocol fields on the following screen.

5. Configure the fields for the comparison you have chosen.

   For this example, specify **ipv4-destination-ip** for the Protocol Field.

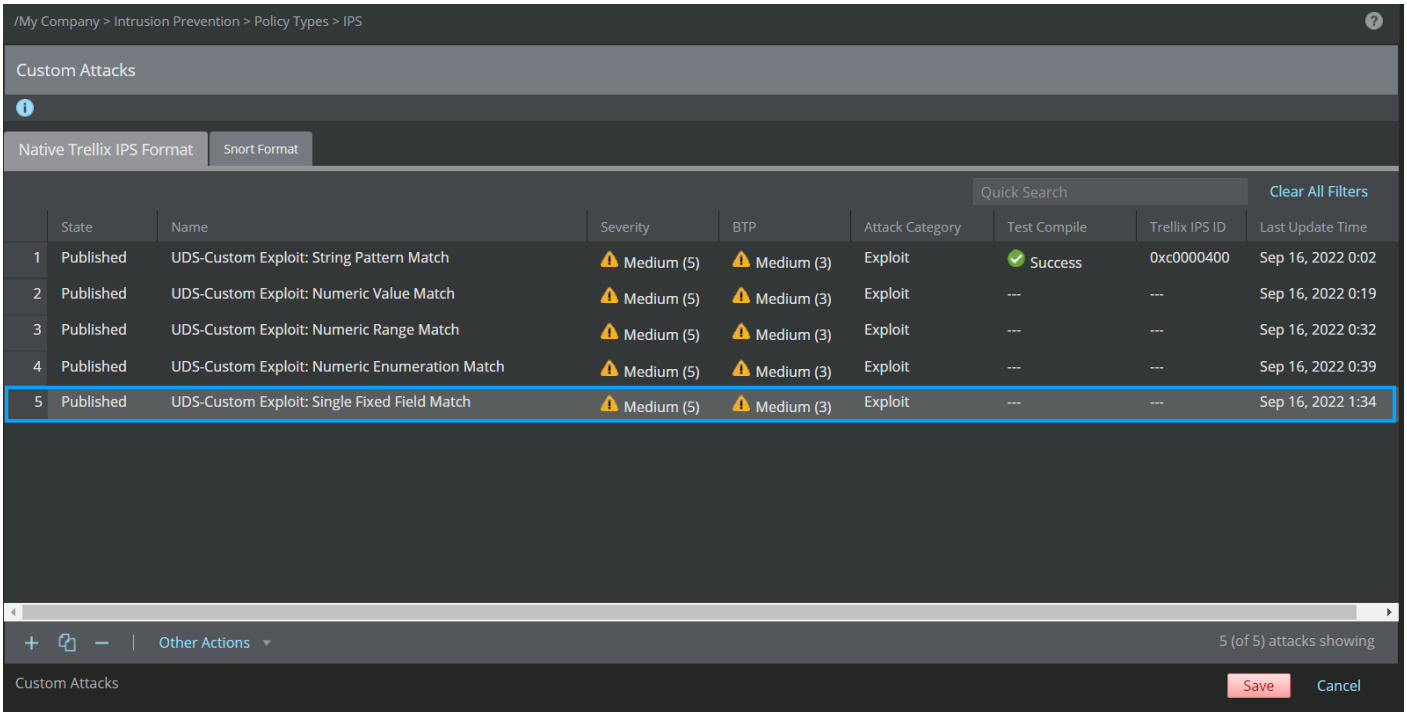
6. From the **Operator** drop-down list, select the matching criteria as **Equals** which means that the comparison criteria must be equal to the IP address entered.
7. Type the IP address in the **Integer or IP to Match**.

   For this example, the value to match is "192.168.1.1".

8. (Optional) Uncheck **Ignore Bitmask** if you want to process the bitmask of the IP address.
9. Click **Save**.

   Your comparison appears under **Condition 1**.

10. Click **Add** in the **New Custom Attack** window.
11. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.



12. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
13. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Create an attack definition for packet grep protocol match

This scenario is about creating a Custom Attack Definition that uses packet grep protocol match to detect if the DNP3 protocol contains a specific character sequence.

In order to write a proper Native Trellix IPS Format Custom Attack for this example, you must identify several key elements:

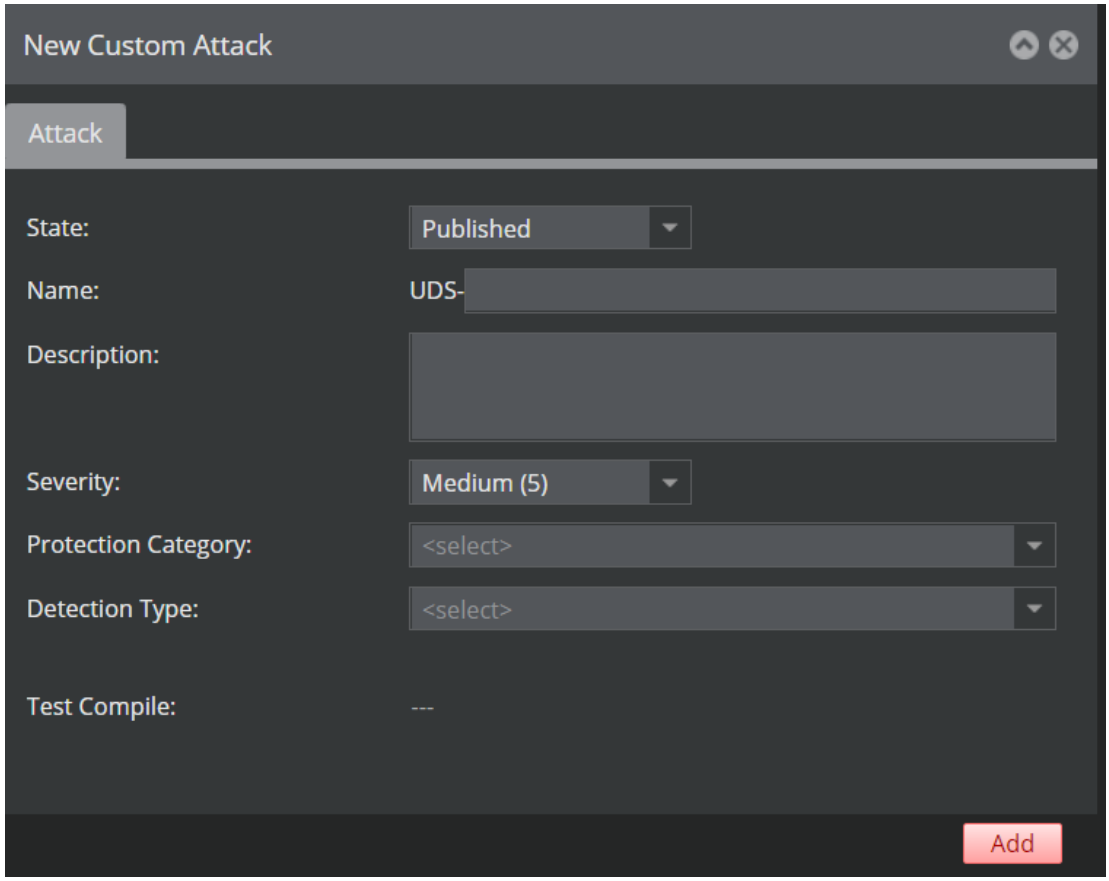
- Application protocol: dnp3

- Packets to parse: Request Packets Only
- Text to match: \x00\x00\x00\x3a\x20\x45\x56\x00\x0a

Steps to create the attack definition for this example:

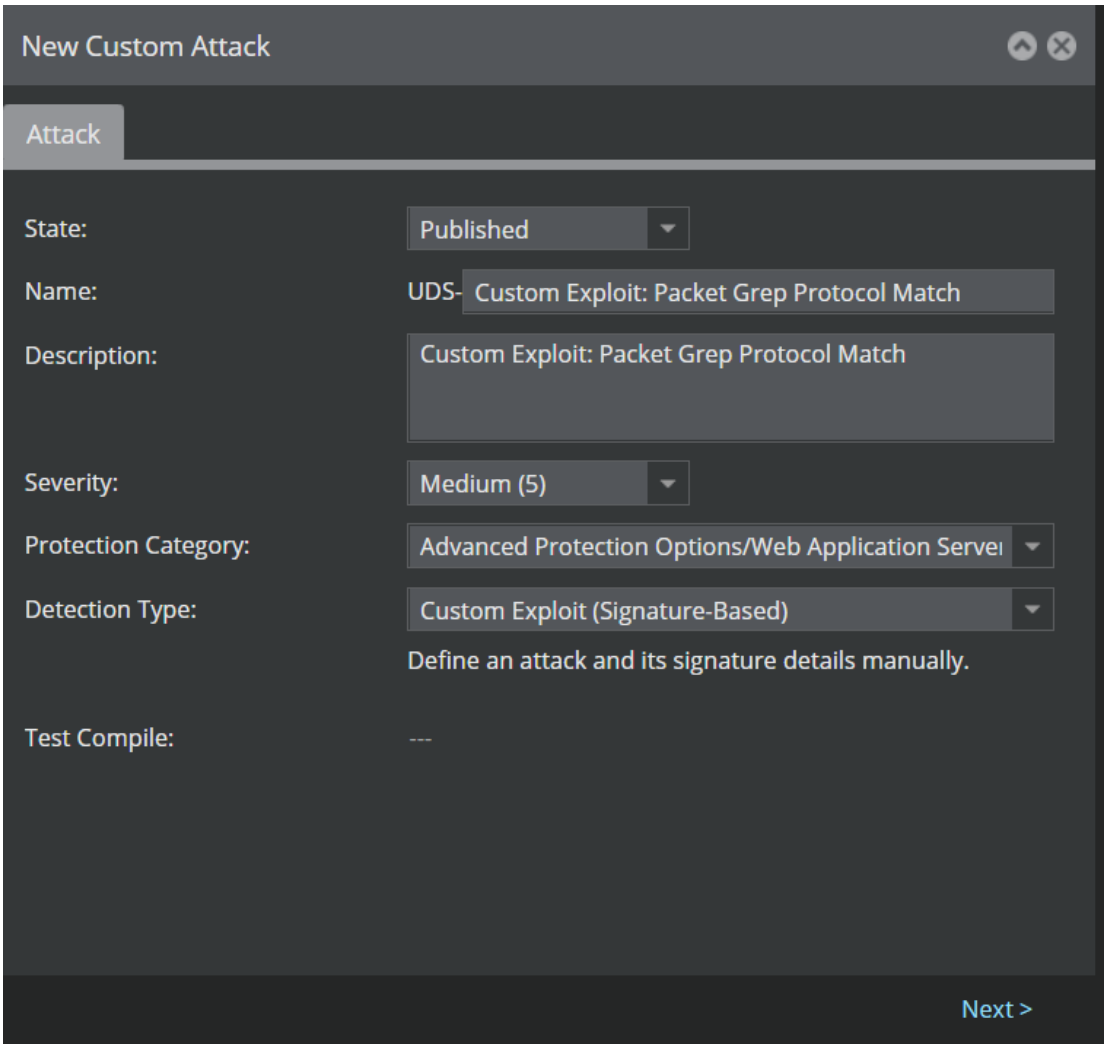
1. In the Custom Attack Editor, click +.

   The **New Custom Attack** interface opens.

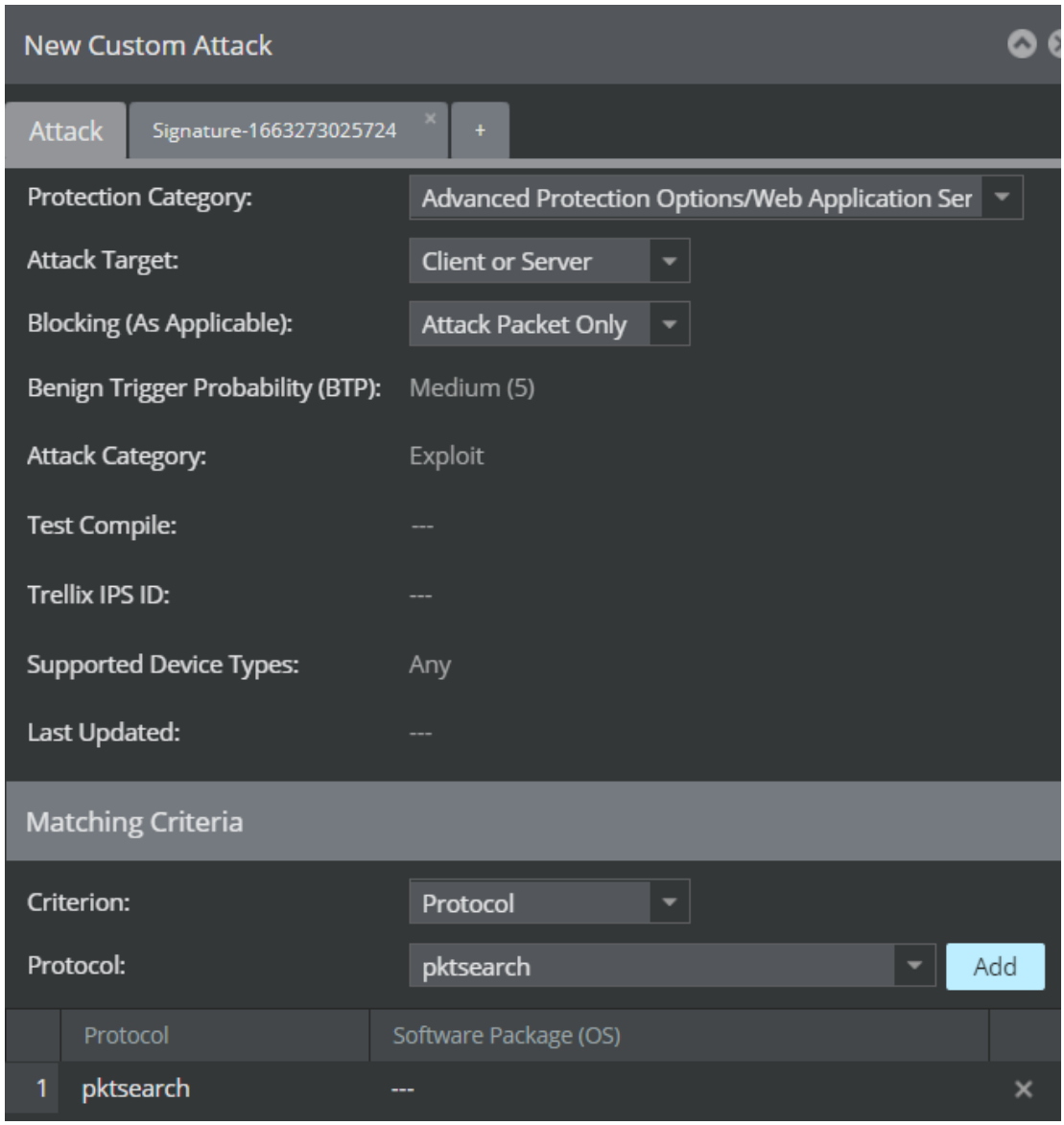


2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as "Custom Exploit: Packet Grep Protocol Match" as the **Name**.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-Custom Exploit: Packet Grep Protocol Match" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium (5)** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server** as the **Protection Category**.
7. Select **Custom Exploit (Signature Based)** from the **Detection Type** drop-down menu for the attack.
8. Click **Next**.



9. Select **Client or Server** as **Attack Target**.
10. Select **Attack Packet Only** as **Blocking (As Applicable)**.
11. In the **Matching Criteria** section, select **Protocol** as the **Criterion** and select **pktsearch** as the protocol.



12. Attack details configuration is complete. Continue to create signature.

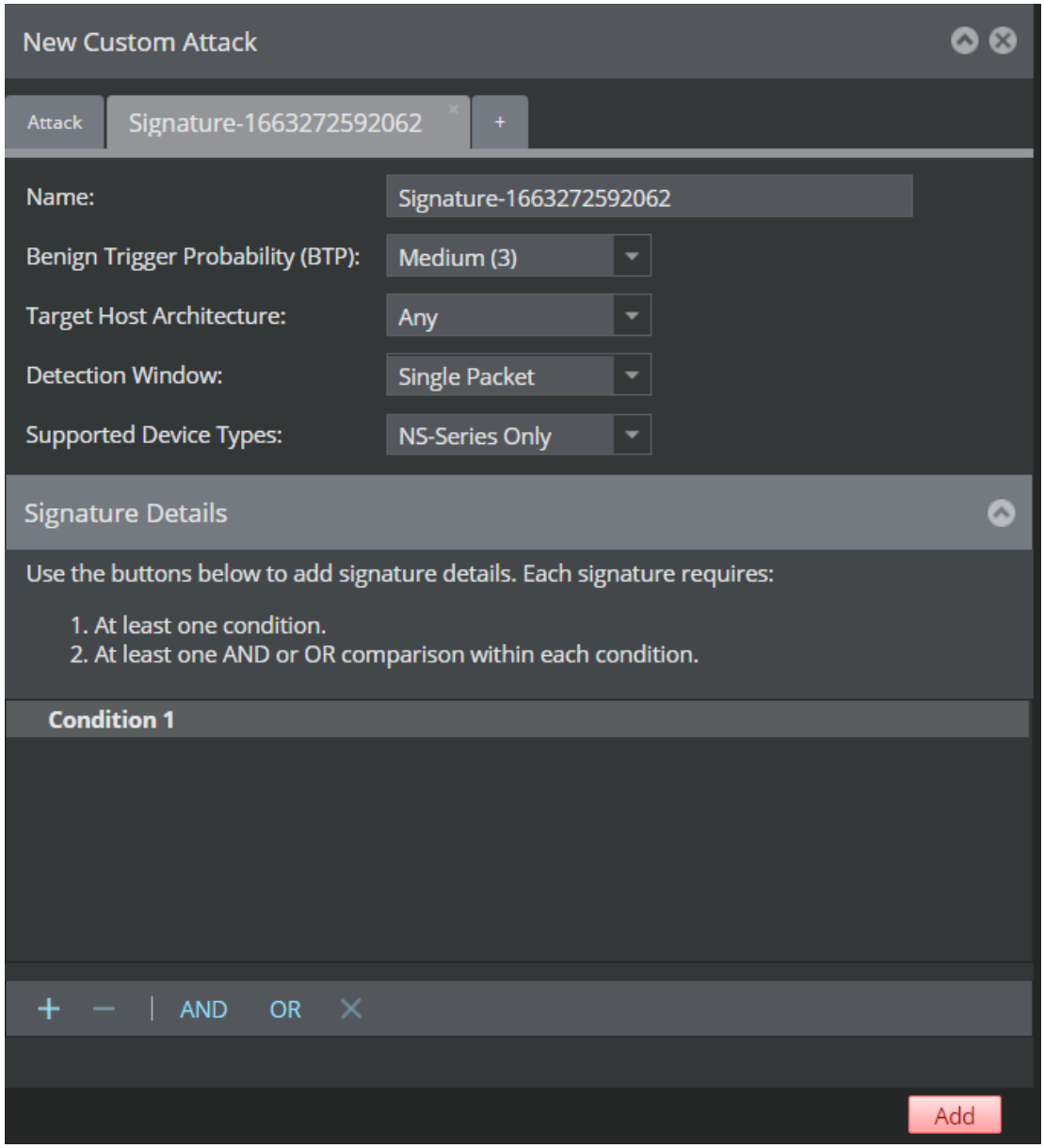
Create the signature for packet grep protocol match

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** window, click **Signature-<signature name>** tab.

Figure 800. New Signature window



2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)**, **Target Host Architecture**, and **Detection Window** with the default values.
4. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.
5. Add the condition to the signature.

   It is in the conditions that you specify the following details:

   - The string that the Sensor should look for
   - Which section of the HTTP request should it look for the string
6. Proceed to add the condition.

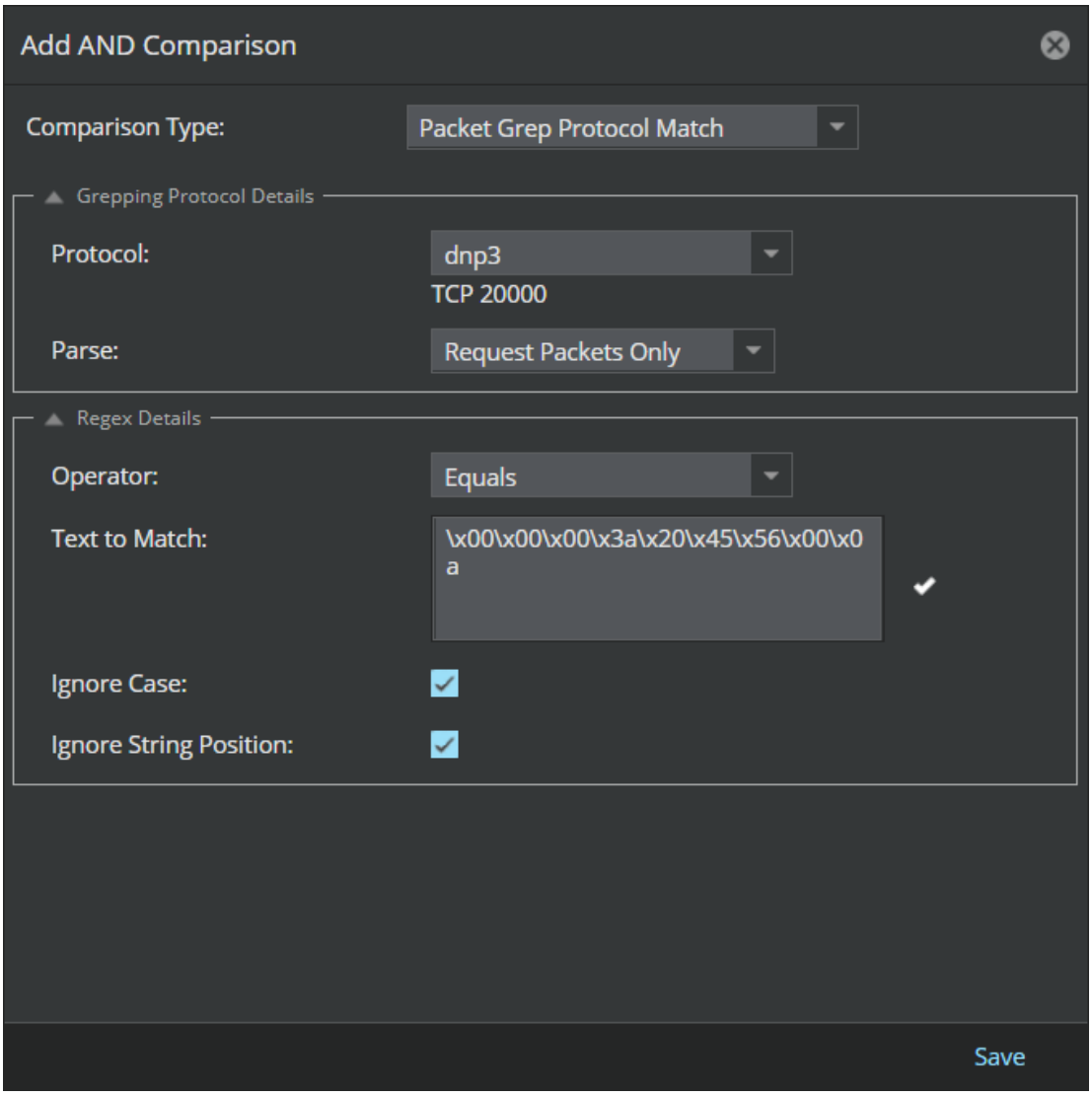
Add the condition for packet grep protocol match

Steps to add the condition to the example signature:

1. Click **Condition 1** so that it is highlighted.
2. Click **AND** in the Comparisons section.

   The **Add AND Comparison** dialog opens.

Figure 801. Packet Grep Protocol Match



3. For this example, select **Packet Grep Protocol Match** in the **Comparison Type** drop-down menu.
4. Select **dnp3** from the **Protocol** list.

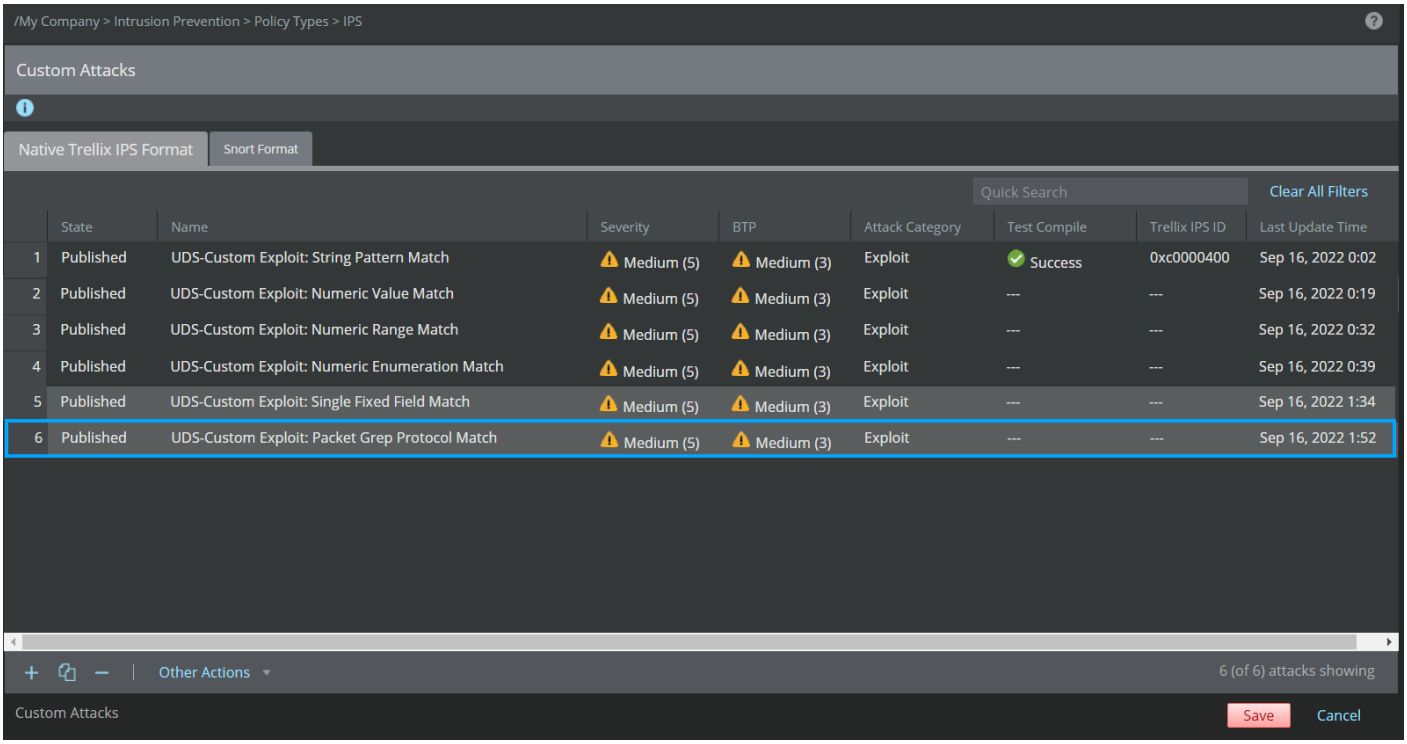
   Because you selected IPv4, the Custom Attack Editor displays the IPv4-specific protocol fields on the following screen.
5. Configure the packets you want to parse.

   For this example, specify **Request Packets Only** for the **Parse** field.

6. From the **Operator** drop-down list, select the matching criteria as **Equals**.
7. Type the text you are searching for in the packets in the **Text to Match**.

   For this example, the text to match is " \x00\x00\x00\x3a\x20\x45\x56\x00\x0a".
8. (Optional) Deselect **Ignore Case** and **Ignore String Position**.
9. Click **Save**.

   Your comparison appears under **Condition 1**.
10. Click **Add** in the **New Custom Attack** window.
11. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.



12. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
13. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Custom attack with a pattern-match signature

Scenario

This is about creating a Custom Attack Definition that uses pattern matching to detect any HTTP GET requests in the URI patch for a specific CGI script. This scenario is useful because it illustrates the simplest method of configuring a custom attack definition with proper syntax, defined options, and case sensitivity.

Creation of such an attack definition is also a good example of activity that may not be a malicious attack; rather, you could create such an instance and use it to track requests for sensitive information.

In order to write a proper Native Trellix IPS Format Custom Attack or a Snort Custom Attack for this example, you must identify several key elements:

- Application protocol: HTTP
- Where to look: URI path
- Detection window: request
- Request method: get
- String to match: cgi.bin/trillion.pl or cgi.bin/trilliant.pl, where only "pl" is case insensitive

When you have all of the required elements to properly identify the activity, attack definition can be successful.

To create a custom attack definition:

- Open the Custom Attack Editor.

  Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

Create a custom attack

This section explains how to create a Native Trellix IPS Format Custom Attack definition for the scenario explained in the previous section.

Create an attack definition

Steps to create the attack definition for this example:

1. In the Custom Attack Editor, click  .

   The **New Custom Attack** interface opens.
2. Select one of the options from the **State** drop-down menu.
3. You can specify a name such as "CGI: Trillion or Trilliant" as the **Name**.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion; thus, this attack appears as "UDS-CGI: Trillion or Trilliant" in the Custom Attack Editor, as well as the attack database when you save in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. You can select **Medium** as the **Severity** because this example scenario does not necessarily involve malicious activity.
6. Select **Advanced Protection Options/Web Application Server Protection** as the **Protection Category**.
7. Select **URL** from the **Detection Type** drop-down menu for the attack.
8. Enter the **URL** that is to be detected, then click **Add**.
9. In the **Matching Criteria** section, the protocol is automatically selected as **http**.

   When you subsequently save this attack definition in the Manager server, it will be part of every rule set which includes Medium-severity, HTTP attacks (must match both severity and protocol).
10. Attack details configuration is complete. Continue to create signature.

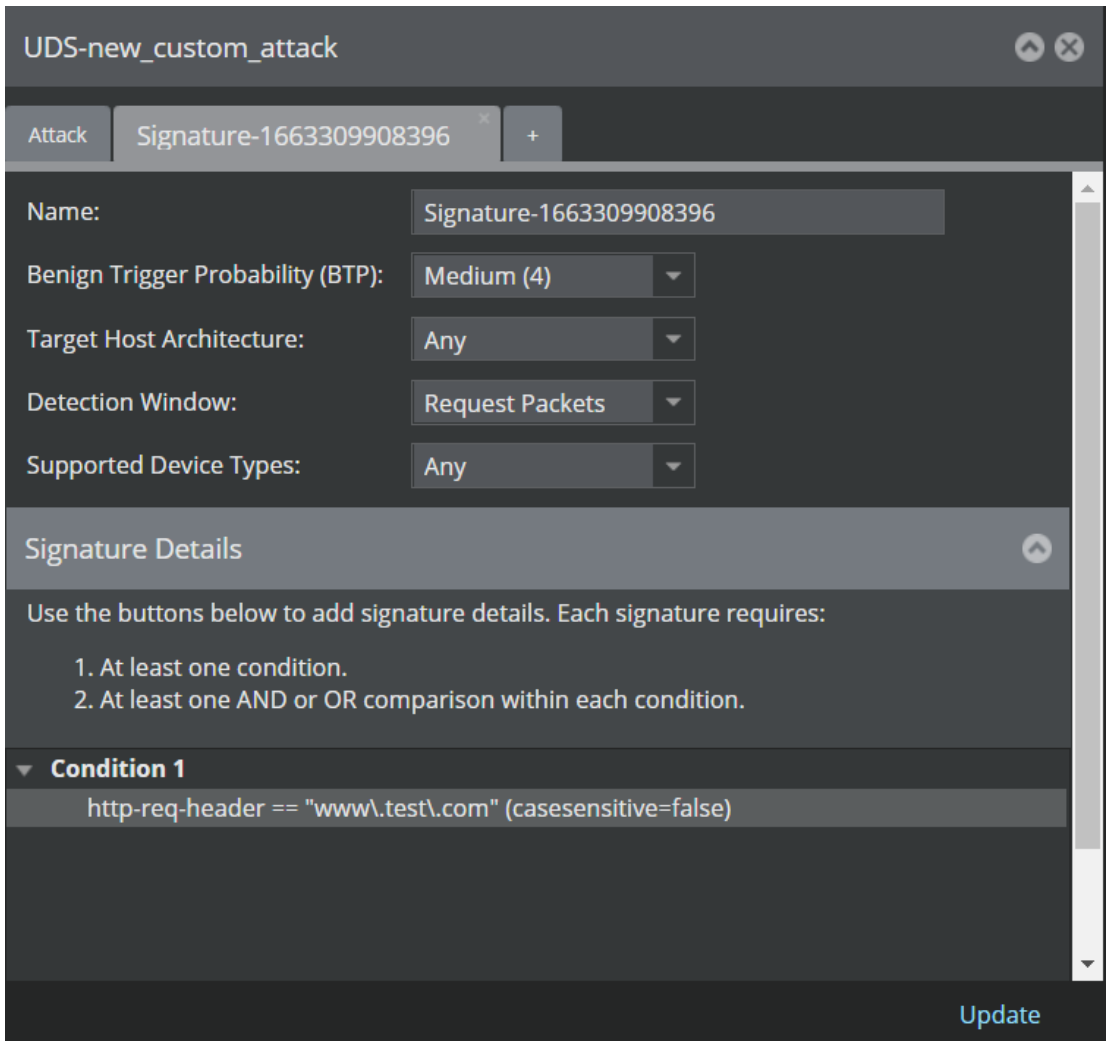
Create the signature

After you create the attack definition, you create the signature for the attack.

Steps:

1. Click **Signature-<signature name>** tab.
2. (Optional) Clear the **Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability (BTP)** and **Target Host Architecture** with the default values.
4. This example is to search for a string in the HTTP URI. So, select **Request Packets** as the **Detection Window**.
5. Based on the Sensor model that you plan to use for this example, select the **Supported Device Types**.

Figure 802. New Signature window



6. Add the condition to the signature.

   It is in the conditions that you specify the following details:

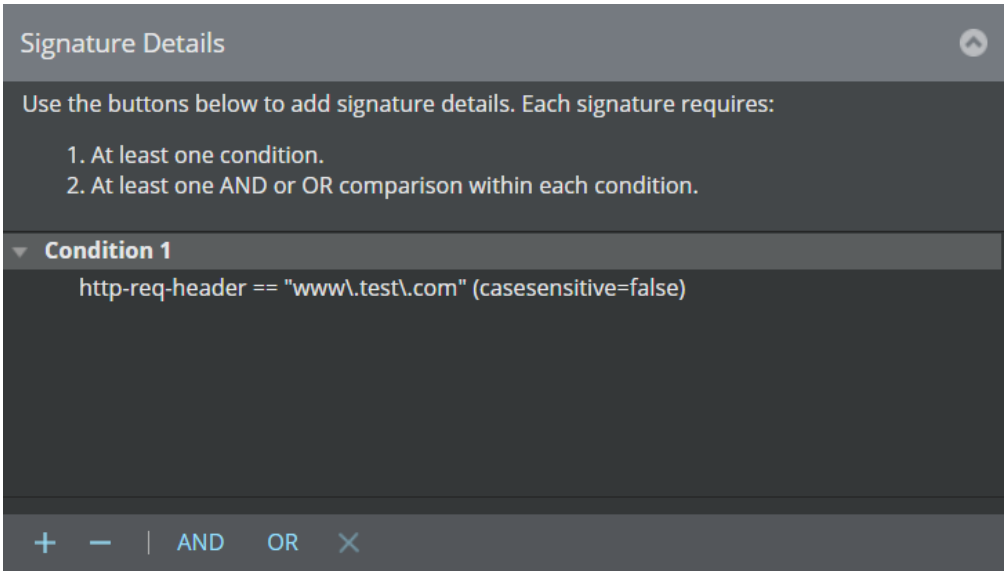
   - The string that the Sensor should look for
   - Which section of the HTTP request should it look for the string

7. Proceed to add the condition.

Add the condition

Steps to add the condition to the example signature:

1. **Condition 1** is added automatically according to the URL you provided.
2. Click **Condition 1** so that it is highlighted.



3. Click **AND** in the Comparisons section.

   The **Add AND Comparison** dialog opens.
4. For this example, select **String Pattern Match** in the **Comparison Type** drop-down menu.
5. Select **http** from the **Protocol** list.

   Because you selected HTTP, the Custom Attack Editor displays the HTTP-specific protocol fields on the following screen.
6. Configure the fields for the comparison you have chosen.

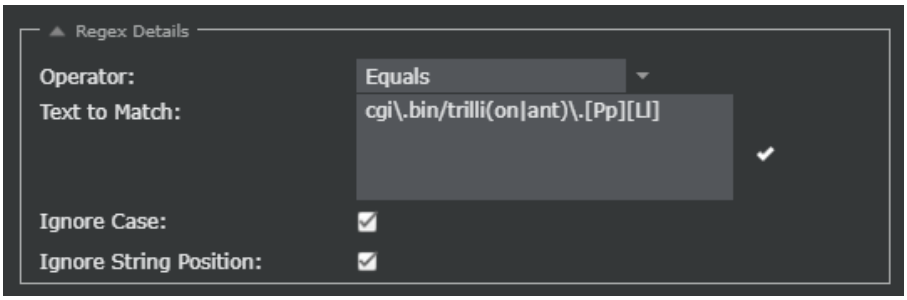
   For this example, specify **req-uri-path** for the Protocol Field. This specifies that the Sensor should search in the URI of the request packet.
7. Select **get** as the http request method.
8. From the **Operator** drop-down list, select the matching criteria as **Equals** which means that the comparison criteria must be equal to the regular expression entered.
9. Type the pattern to match using the **Text to Match**.

   For this example, the pattern to match is either "cgi.bin/trillion.pl" or "cgi.bin/trilliant.pl", where "pl" is case-insensitive. To properly write this expression, use the following rules:

   - Add a backward slash (\) before every dot (.) to escape: cgi.bin = cgi\.bin
   - Use alternatives where possible. For this example, trillion and trilliant can be written as: trilli(on|ant).
   - Use character classes to denote case insensitivity for "pl": [Pp][Ll]

The final string should appear as: cgi\.bin/trilli(on|ant)\.[Pp][Ll]

Figure 803. Regular Expression details



10. Click ✔ to verify that your expression is a valid string, and all required options are represented. Click **OK** to close the validation message window.
11. Click **Save**.

    Your comparison appears under **Condition 1**.
12. Click **Save** in the **Add Exploit Attack** window.
13. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.
14. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
15. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Create a snort custom attack — an example

To write a Snort Custom Attack definition for the scenario explained in the previous section:

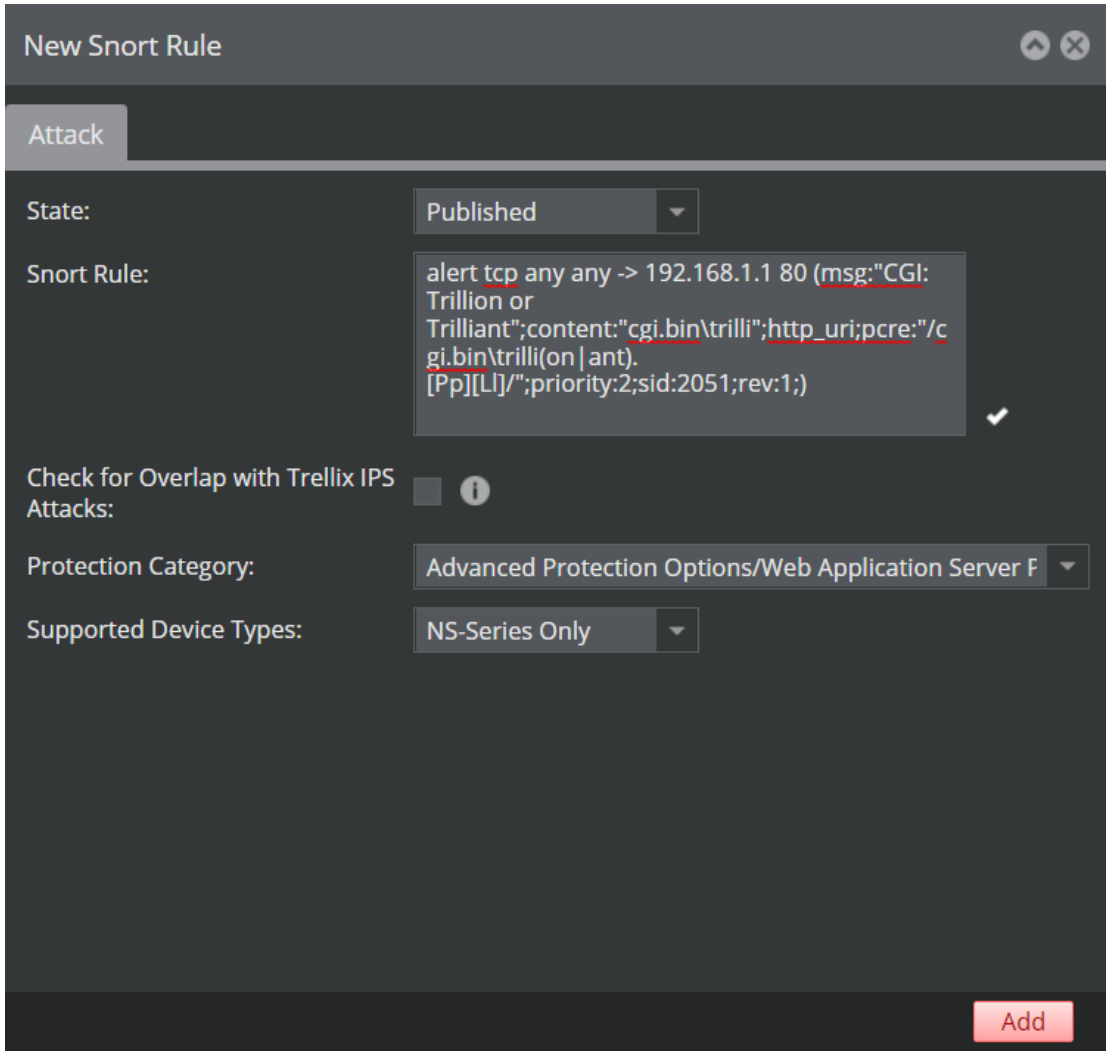
Steps:

1. In the Custom Attack Editor, click **Snort Format** tab.
2. Click +.

   The **New Snort Rule** text box opens.
3. Select one of the options from the **State** drop-down menu.
4. Construct the Snort rule for the scenario, which is the following:

   alert tcp any any -> 192.168.1.1 80 (msg:"CGI: Trillion or Trilliant";content:"cgi.bin\trilli";http_uri;pcre:"/cgi.bin\trilli(on|ant).[Pp][Ll]/";priority:2;sid:2051;rev:1;)

Figure 804. Add Snort Rule window



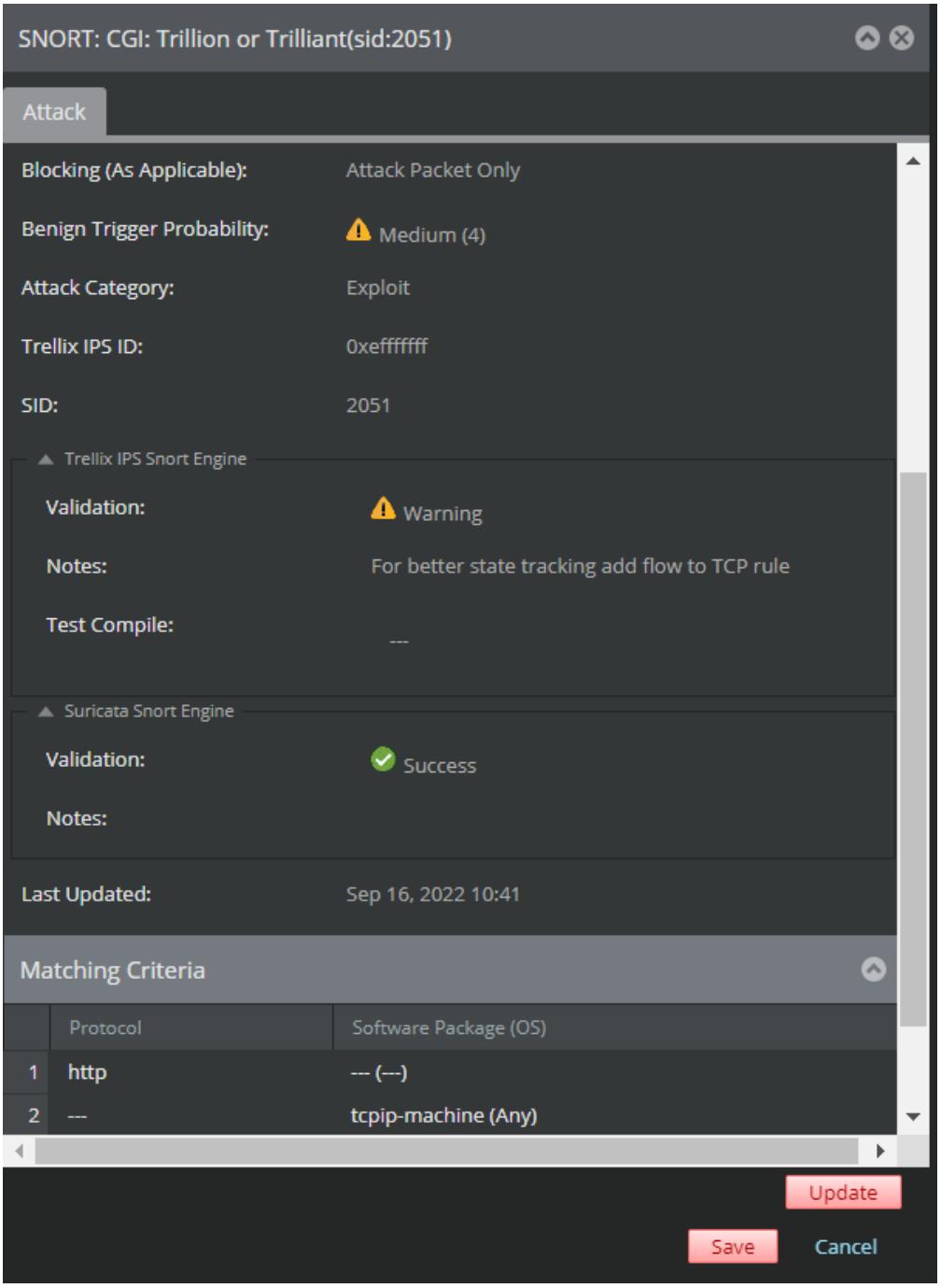
Some points to note regarding the rule:

- Specifying the destination IP address improves the performance of the Sensor.
- As you are adding the Snort rule directly in the Custom Attack Editor, as a best practice, you need to specify the destination port number. The Sensor then checks only the HTTP request packet for this rule.
- You need to specify the msg, priority, SID, and the revision number.

5. Select **Check for Overlap with Trellix IPS Attacks** to verify if the rule matches an existing Trellix IPS attack definition.
6. Select **Advanced Protection Options/Web Application Server Protection** as the **Protection Category**.
7. Click **Add**.

   The **Attack** window opens.

Figure 805. Edit Snort Attack window



8. Note that the Manager assigns the Attack Name based on the msg option and SID of the rule.
9. Set the severity to Medium. This is because the priority of the rule is 2.
10. Note that the Protocol is set to **http**. This is because the destination port number is 80.
11. Note that the **Benign Trigger Probability** is set to the default value.
12. Close the Attack window.

13. In the **Custom Attacks** window, click **Save** to save the Snort Custom Attack in the Manager server database.
14. Make sure the Snort Custom Attack is saved in the database and also published in the policies.

Custom attacks with multiple comparisons

In case of Trellix IPS Custom Attacks, you can use multiple conditions and/or comparisons within a single attack definition to increase your confidence in detecting an unknown attack. There are many configuration possibilities; the procedure that follows details the following scenario:

- One signature with two conditions. Both conditions must be met before an alert is generated.
- The first condition has a single comparison.
- The second condition employs an OR comparison; that is, either of the two comparisons in the condition signifies a positive match.

You can use various comparison methods within a condition. For example, if you employ two comparisons within a condition, one comparison can be a string match, while the second can be a fixed field check.

To create the Trellix IPS Custom Attack definition:

- Open the Custom Attack Editor.

Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**

Create an attack definition for the example

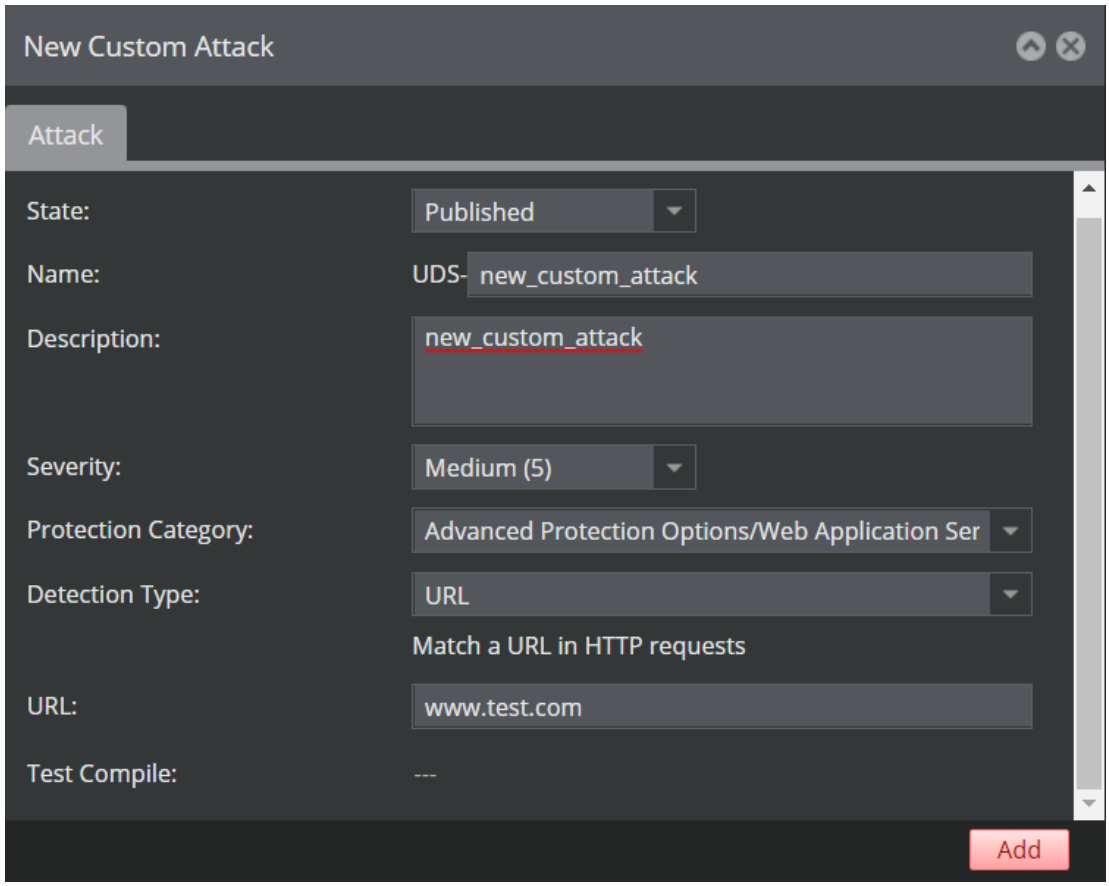
Steps to create the attack definition for this example:

1. Select Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **IPS**. Click **Custom Attacks**.

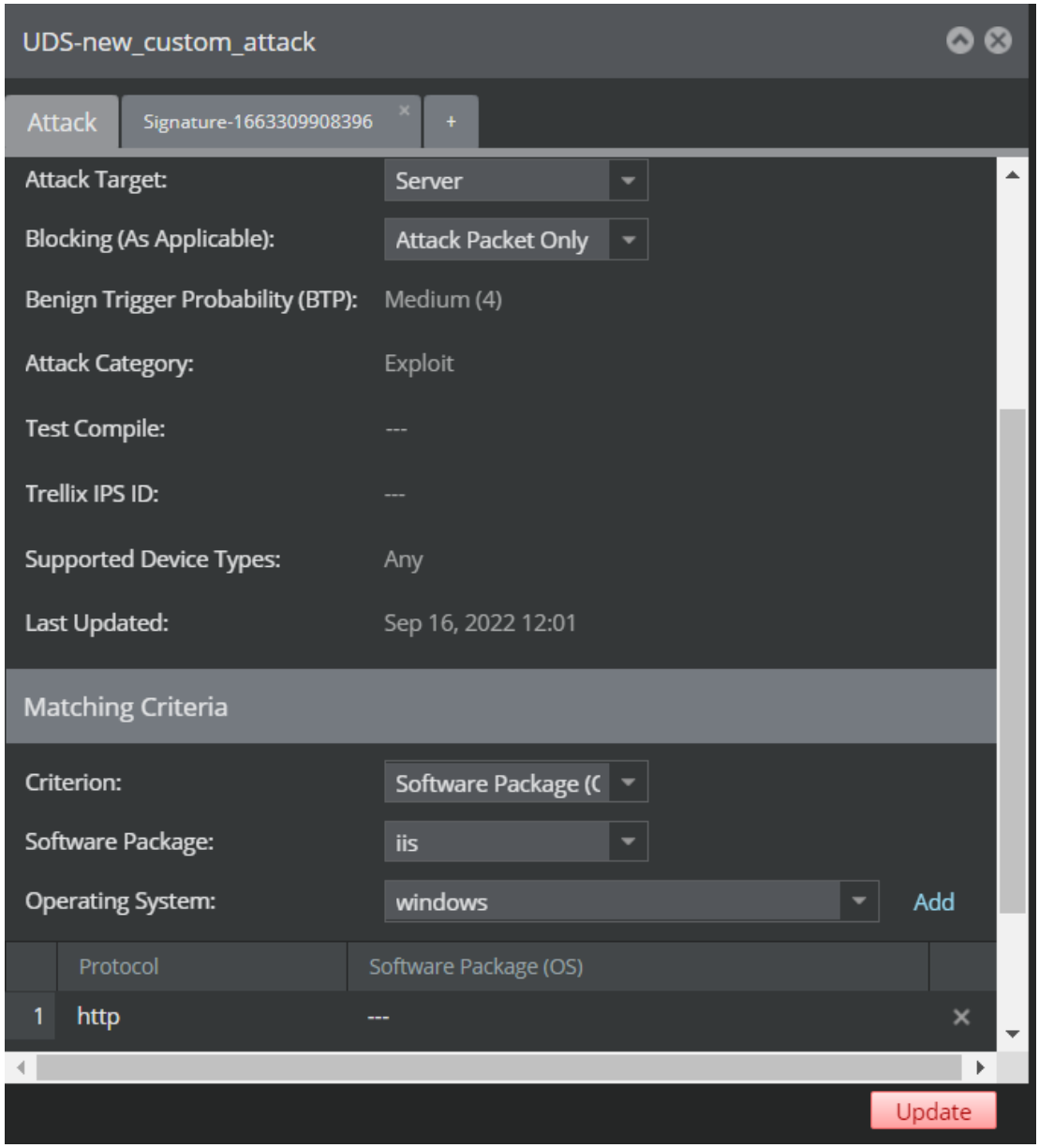
   The Custom Attack Editor opens with the existing Custom Attacks listed on the Native Trellix IPS Format tab.
2. Click  .

   The **New Custom Attack** interface opens.
3. In the **Name** field, type a new name for your attack.

   The letters "UDS" (user-defined signature) are appended to the front of the name upon completion when you save it in the Manager server.
4. Type a description for your attack. This area can be used for your notes or other specific information pertinent to your new attack.
5. Select **Advanced Protection Options/Web Application Server Protection** as the **Protection Category**.
6. Select **URL** from the **Detection Type** list.
7. Enter the **URL** that is to be detected, then click **Add**.



8. In the **Matching Criteria** section, the protocol is automatically selected as HTTP.
9. Select **Software Package (OS)** as the **Criterion**.
10. Select **iis** from the **Software Package** list .
11. Select **windows** from the **Operating System** list and then click **Add**.
12. Verify that both HTTP and IIS appear in the Matching Criteria table.



13. Click **Update**.
14. Attack details configuration is complete. Continue to create signature.

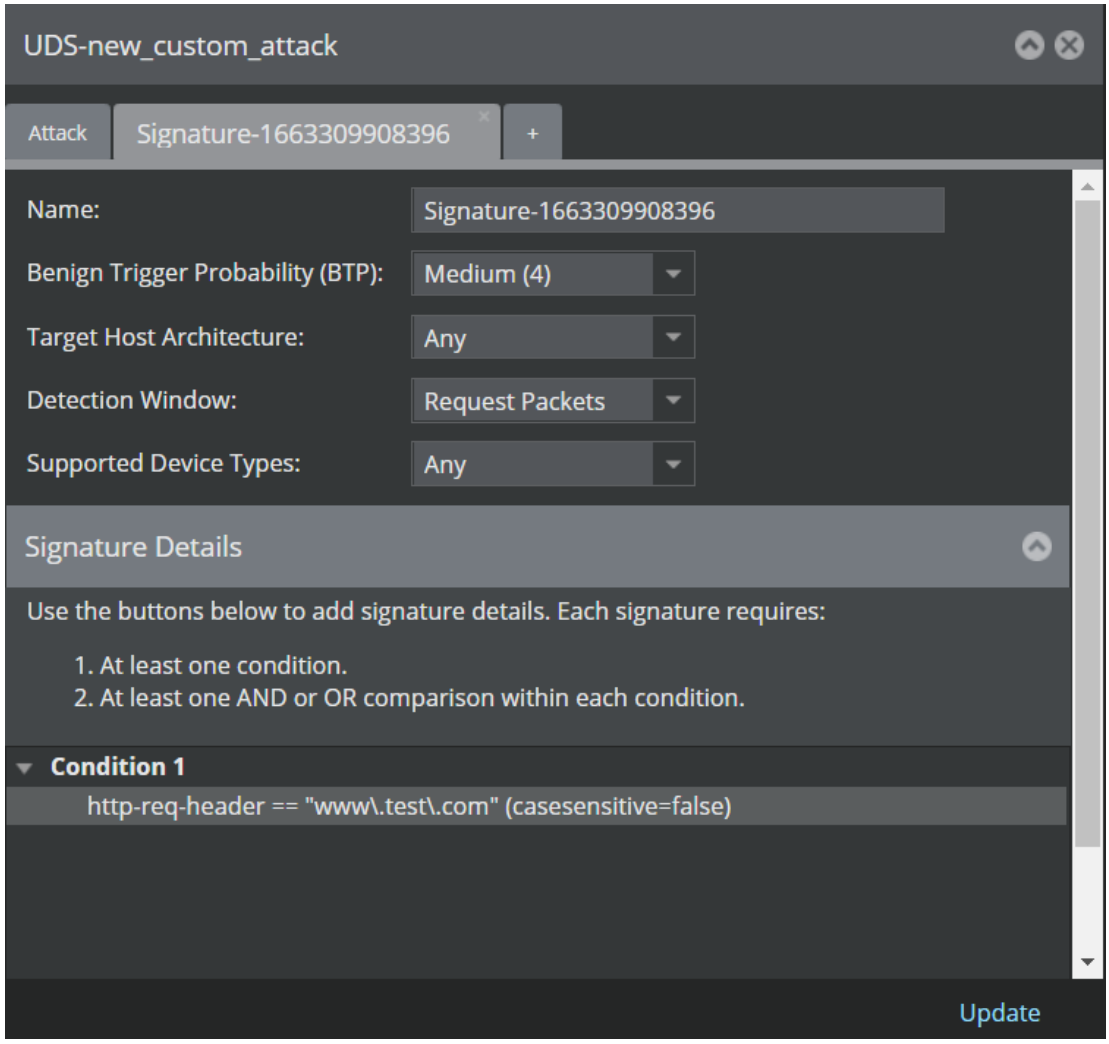
Create the signature for the example

After you create the attack definition, you create the signature for the attack.

Steps:

1. In the **New Custom Attack** interface, click on the **Signature-<signature name>** tab.

Figure 806. New Signature



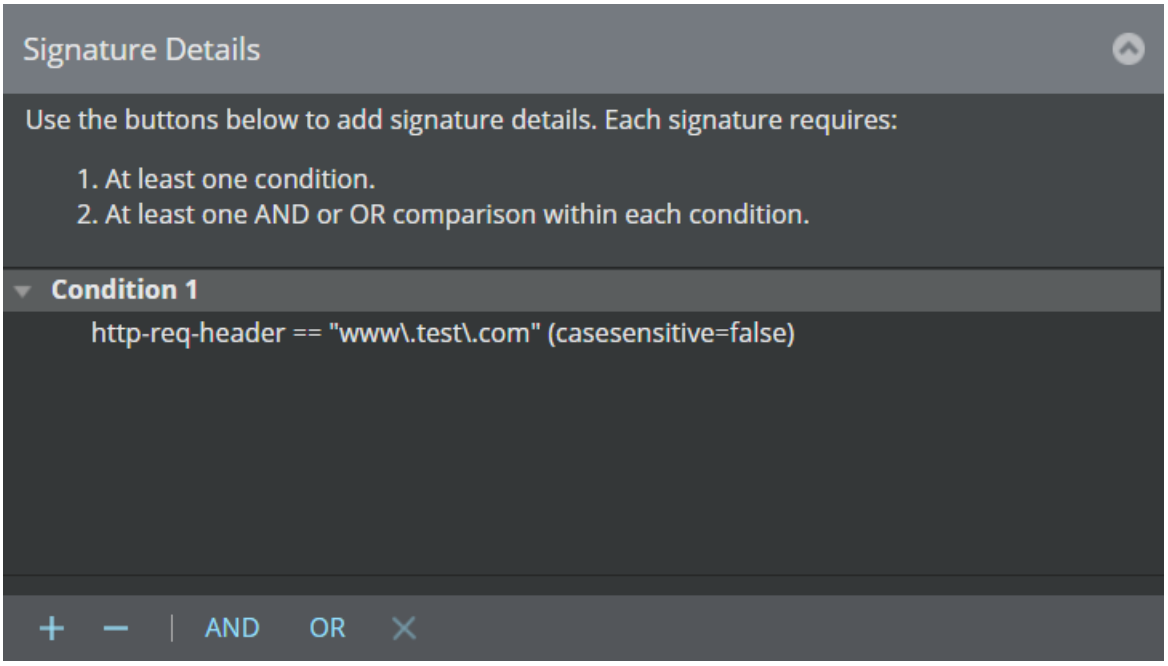
2. (Optional) Clear the **Signature Name** and type a new name for your signature.
3. For this example, you can leave the **Benign Trigger Probability** and **Target Host Architecture** with the default values.
4. For this example select **Request Packets** as the **Detection Window**.
5. Based on the Sensor model that you plan to use for this example, select the **Target Device Type**.
6. Proceed to add the condition for your signature.

Add the first condition and comparison for your signature

Steps to add the condition to the example signature:

1. **Condition 1** is added automatically with the URL.
2. Click **Condition 1** so that it is highlighted.

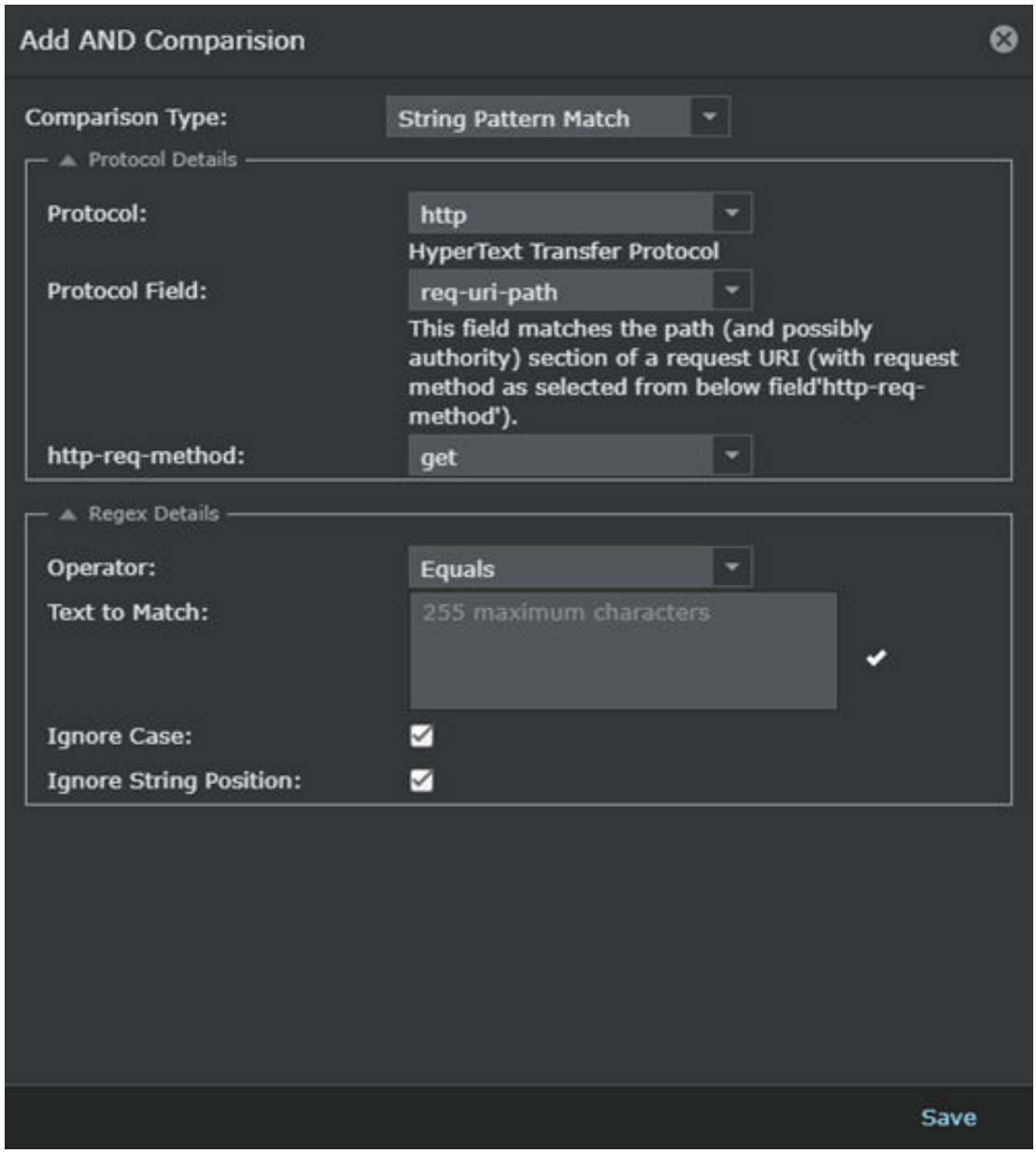
Figure 807. Adding Conditions



3. Click AND in the Signature Details section.

   The **Add AND Comparison** dialog opens.

Figure 808. Configure Comparison window



4. For this example, select **String Pattern Match** from the **Comparison Type** drop-down list.
5. Select **http** from the Protocol List.

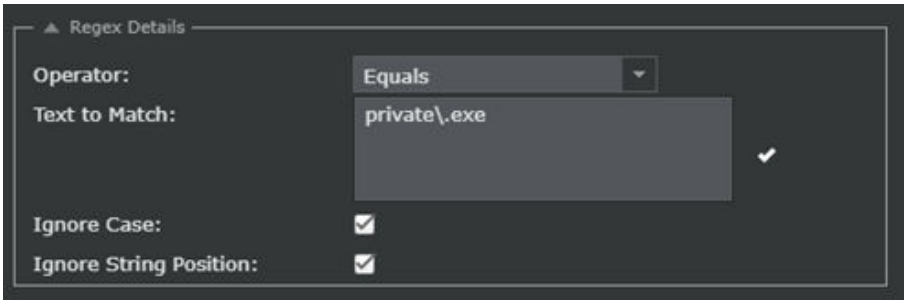
   Because you selected HTTP, the Custom Attack Editor displays the HTTP-specific protocol fields on the following screen.
6. Configure the fields for the comparison you have chosen.

   For this example, specify **req-uri-path** for the Protocol Field. This specifies that the Sensor should search in the URI of the request packet.
7. Select **get** as the http-request-method.
8. From the drop-down list in the **Regex Details** section, select the Operator as **Equals** which means that the comparison criteria has to be equal to the string pattern entered.

9. In the **Text to Match** text box, type the pattern to match using the Regular Expression Language rules.

   The pattern to match is "private.exe". You must add a backward slash (\) before the dot (.) to escape the dot character so that it is properly interpreted. The final string should appear as private\.exe.

Figure 809. Adding the string pattern to match



10. Click ✔ to verify that your expression is valid, and that the appropriate pattern is represented.
11. Click **Save**.

    Your comparison appears under **Condition1**.

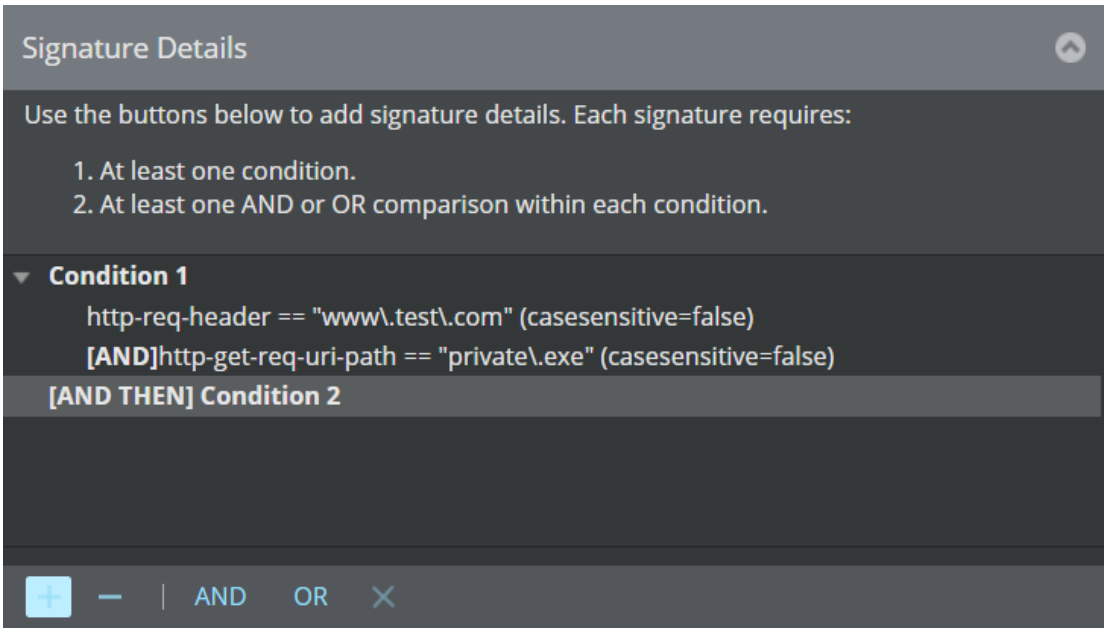
Add the second condition with OR comparisons

Steps to add the second condition to the example signature:

1. In the **Signature Details** section, click + to add the condition.

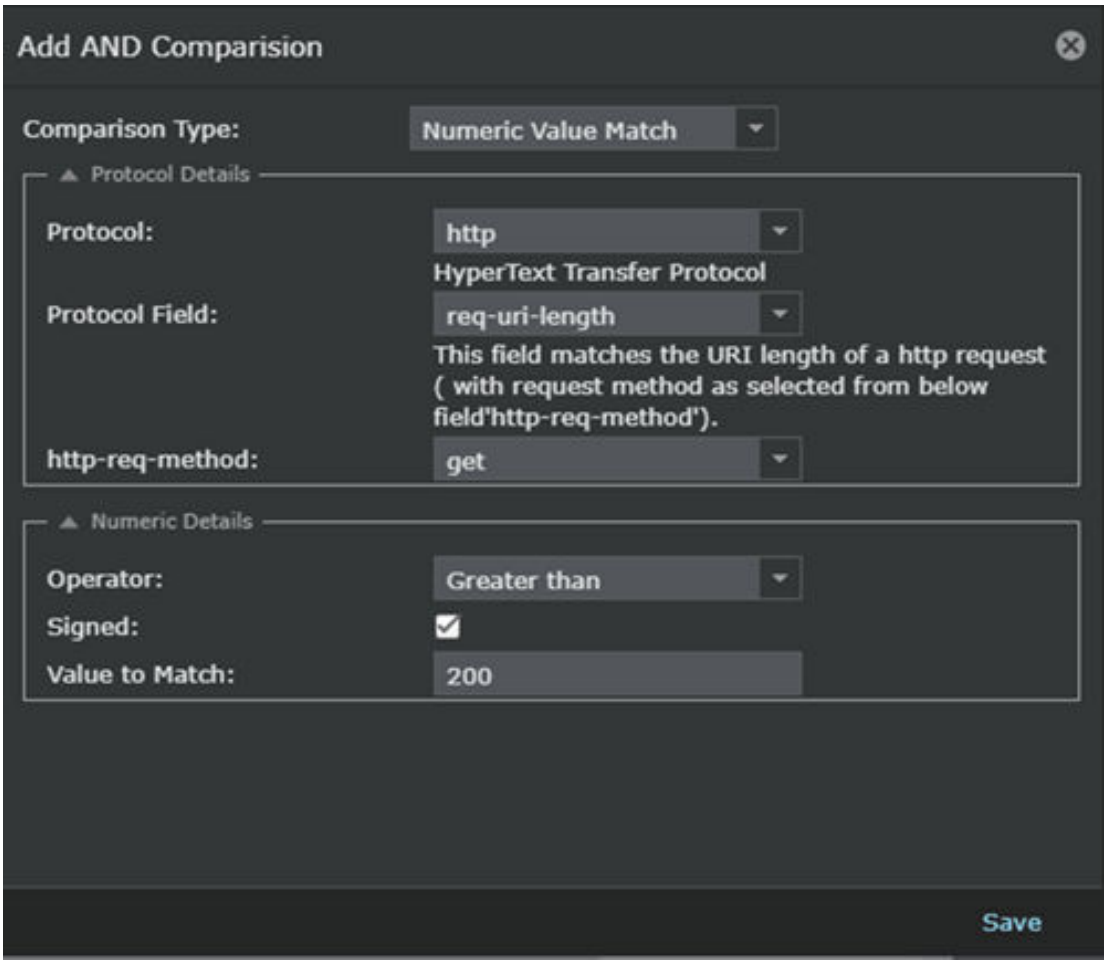
   The first condition is minimized and the second condition reads as **[AND THEN] Condition 2**, thus signifying the first condition must match before the second condition can be tested.

Figure 810. Adding conditions



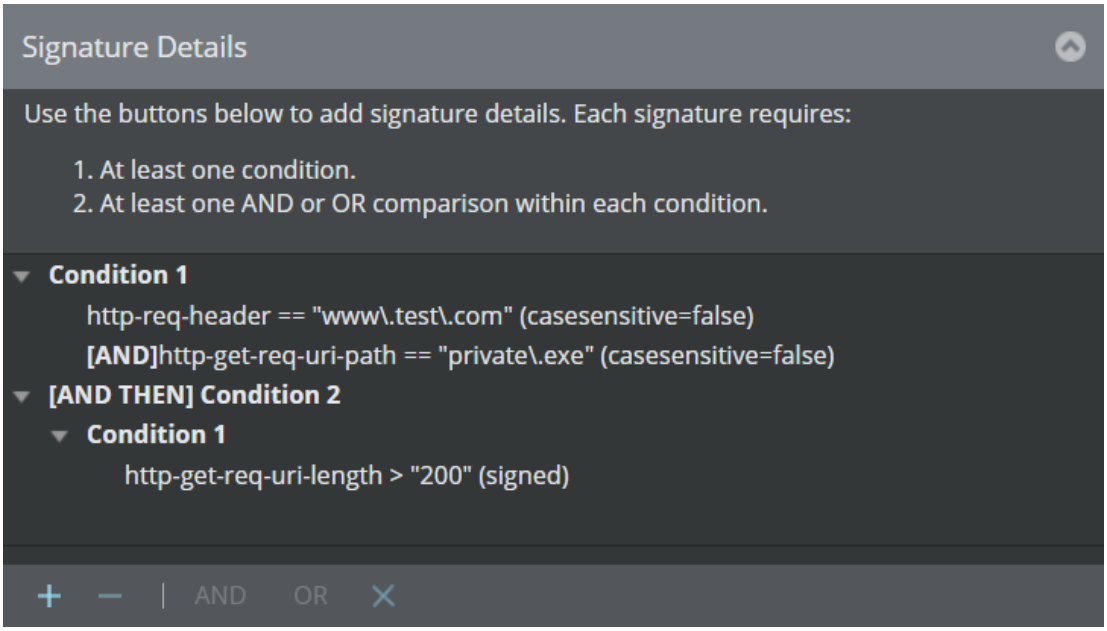
2. Select the text of the second condition, click OR.
3. Select **Numeric Value Match** from the **Comparison Type** drop-down list.
4. Select **http** from the Protocol list.
5. Select **req-uri-length** for the Protocol Field, then **get** as the request method.
6. Select **Greater than** from the Operator drop-down list.

Figure 811. Configure Comparison window to select the comparator



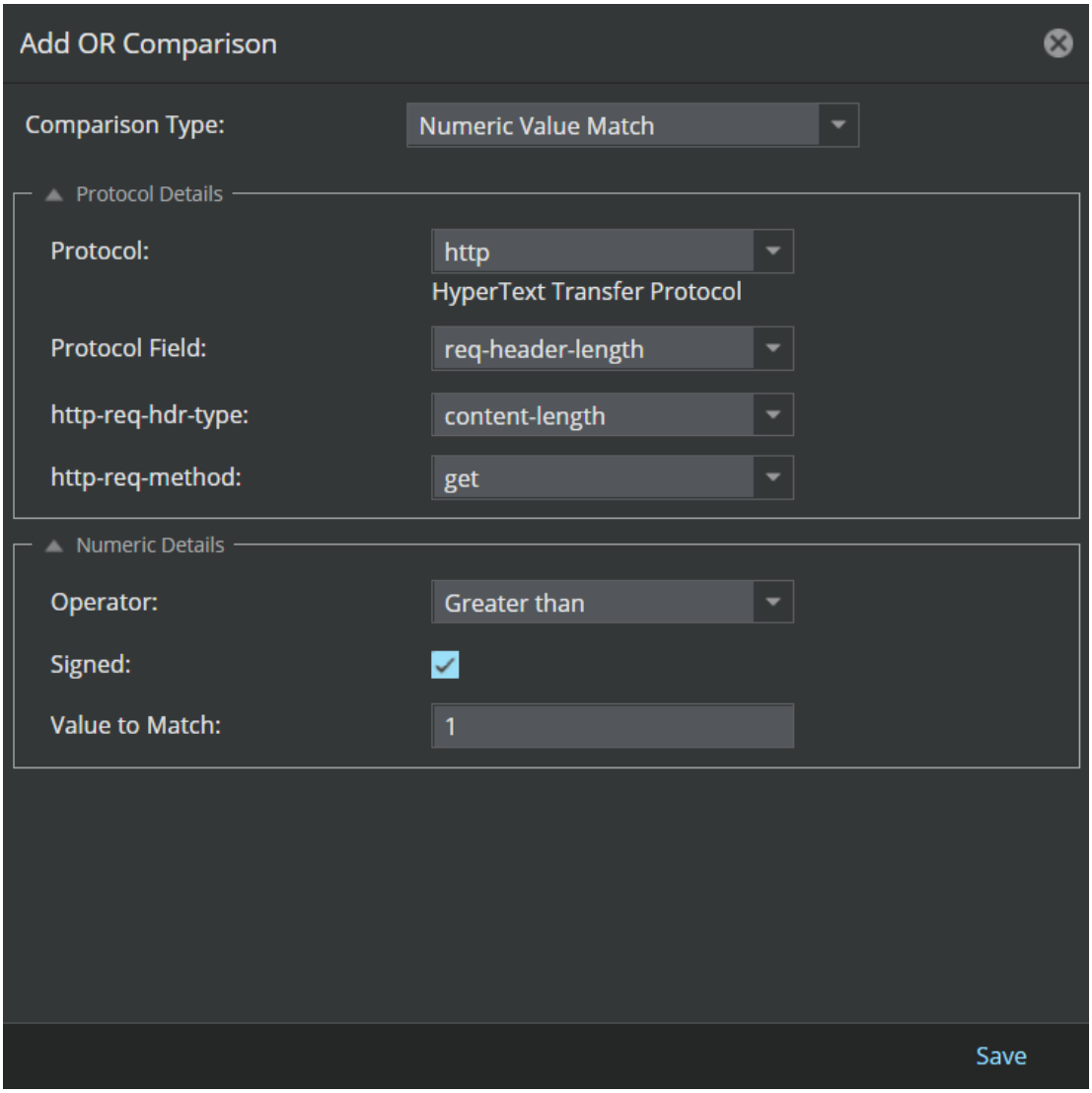
7. (Optional) Check the **Signed** check box if you want the value to be signed.
8. Type a length value in the **Value to Match** field. For this example, type **200** (bytes) as the length over which this comparison will match.
9. Click **Save**; you are returned to the **New Signature** window.
10. Verify that your newly added comparison appears under **Condition 2** under the heading **[AND Then]**.

Figure 812. View the new condition defined

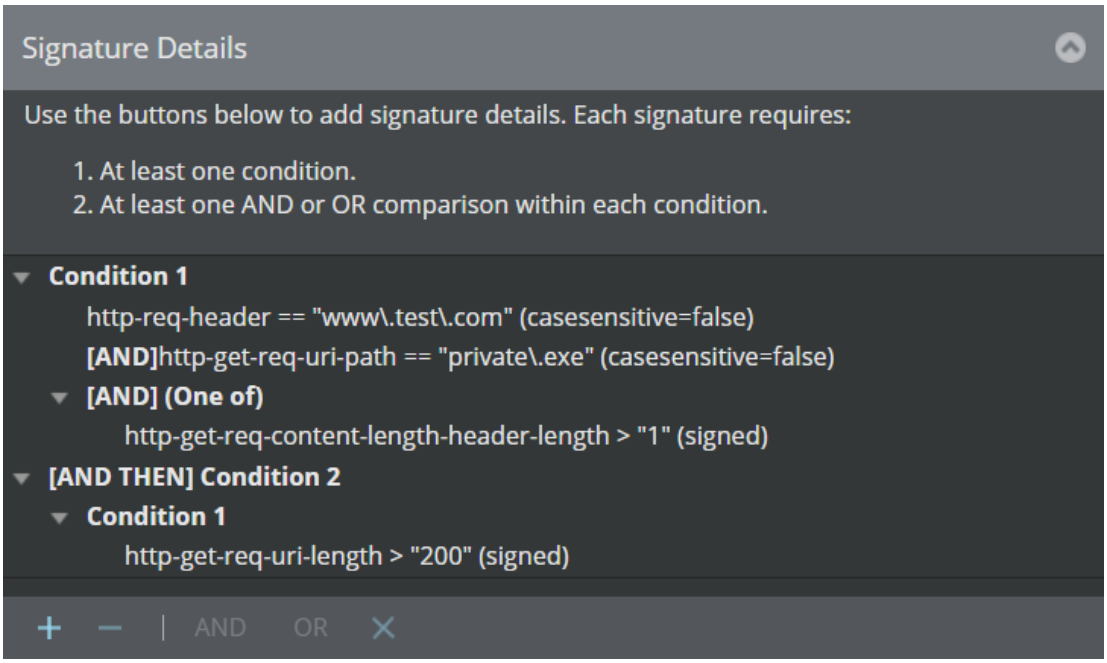


11. Click on **Condition 1**, then click OR under **Comparisons**.
12. Select **Numeric Value Match** from the **Comparison List**.
13. Select **http** from the **Protocol**.
14. Select **req-header-length** for the **Protocol Field**, select **content-length** as the http-req-hdr-type, then select **get** as the http-req-method.
15. Select **Greater than** from the Operator drop-down list.
16. Type a length value in the **Value** field. For this example, type **1** (byte) as the length over which this comparison will match.

> **NOTE**
>
> As stated in the **Description** field, a value of 1 byte is significant for this comparison as the normal header length of a request should be zero.



17. Click **Save**; you are returned to the **New Signature** window.
18. Verify that your newly added comparison appears beneath the first comparison you configured for **Condition 2**. The second comparison line is preceded by **[OR]** to signify the either-or relationship between the two comparisons.



19. Click **Update** in the signature details window.

> **NOTE**
>
> Though there are multiple conditions and comparisons, only one signature was created; so only one signature is uploaded to the Manager.

20. Verify that the attack definition is listed on the **Native Trellix IPS Format** tab.
21. Click **Save** to save the Trellix IPS Custom Attack in the Manager server database.
22. Make sure the Trellix IPS Custom Attack is saved in the database and also published in the policies.

Equivalent snort custom attack

It is not possible to create an equivalent Snort Custom Attack for all the conditions used in this example, because Snort does not support http-get-req-header-length option.

Management of custom attacks from the Central Manager

Using the Trellix IPS Central Manager, you can manage custom attacks for the corresponding Managers. Functionally, the Custom Attack Editor of a Central Manager is the same as that of a Manager. So, see the earlier sections in this document for information on how to use the Editor for Trellix IPS Custom Attacks and Snort Custom Attacks.

The summary of managing custom attacks from the Central Manager is as follows:

1. Create the custom attack definitions using the Custom Attack Editor in the Central Manager.
2. Save the custom attacks in the Central Manager server database.

3. Synchronize the policies of the constituent Managers.
    a. From the Resource Tree of the Central Manager, select Manager List → **Policy Synchronization**.
    b. Select the Synchronization Type for the required Managers and then click **Synchronize**.
4. View the status of the synchronization. Check the **Status of Activities** section on the Home page of the Central Manager.
5. Update the Sensors with the configuration change.
    a. Log on to the required Manager.
    b. Update the relevant Sensors with the policy change.
    c. Repeat this process for the other Managers.

Important notes

This section lists some important notes related to managing custom attacks in the Central Manager.

- You can create custom attack definitions for a Manager in the Central Manager. When you configure the Manager in the Central Manager the custom attack definitions are published to the Manager.
- You can create or edit custom attack definitions in a Manager.
- All custom attacks sent from the Central Manager to the Manager as part of synchronization are automatically saved in the Manager database and also published in the relevant policies.
- In a Manager, when an attack matching the custom attack definition is detected, you can view the alert in the **Attack Log** page of the Manager and Central Manager.
- In the Custom Attack Editor of the Manager, you cannot modify or delete any custom attack that was sent from the Central Manager. You cannot change the State of the Central Manager attack definitions in the Manager.
- When you synchronize the Central Manager with the constituent Managers, only the custom attacks with State as **Published** are sent to the Managers.
- If you remove a Manager from the Central Manager, all custom attacks sent from the Central Manager to the Manager are removed from the Manager database. To remove these attacks from the corresponding Sensors as well, you need to do a configuration update.
- Recall the custom attack capacity per Sensor type:
    - You can use up to 4500 Trellix IPS Custom Attacks and 5000 Snort Custom Attacks per NS-series Sensor.

  Factor this in when you send custom attacks from the Central Manager to the corresponding Managers.

CLI commands

Introduction

This section gives a basic overview of Trellix Intrusion Prevention System Sensor and Network Threat Behavior Analysis Appliance.

About Trellix Intrusion Prevention System Sensor

Trellix Intrusion Prevention System Sensor is a content-processing appliance built for accurate detection and prevention of intrusions, misuse, and distributed denial of service (DDoS) attacks. Trellix IPS Sensor is specifically designed to handle traffic at wire speed, inspect and detect intrusions with a high degree of accuracy, and flexible enough to adapt to the security needs of any enterprise environment.

When deployed at key network access points, a Sesnor provides real-time traffic monitoring to detect malicious activity and respond to the malicious activity as configured by the administrator.

Sensors are configured and managed using Trellix IPS Manager. The process of configuring a Sensor and establishing communication with the Manager is described in later chapters of this guide.

Issuing CLI commands

You can issue CLI commands locally from the Sensor Console, or remotely via **ssh**.

Issuing a command via the console

NOTE

When the documentation indicates that you must perform an operation "on the Sensor," it signifies that you must perform the operation from the command line of a console host connecting to the Sensor. For example, when you first configure a Sensor, you must do so from the console.

For more information on setting up a console, refer to the respective Sensor Guide.

When you are successfully connected to the Sensor, you will see the login prompt.

factorydefaults

You can use this command to wipe all settings, certificates, and signatures from the Sensor, restoring it to blank settings. This command does not appear when you type ? or commands, nor does the auto-complete function apply to this command. You must type the command in full to execute it.

This command has no parameters.

NOTE

Upon execution of this command, you are warned that the operation will clear the Sensor and you must confirm the action. The warning occurs since the Sensor returns to its clean, pre-configured state, thus losing all current configuration settings.

Syntax:

```
factorydefaults
```

On executing the command, the following messages are displayed for an NTBA Appliance:

```
Are you sure you want to reset NTBA to factory defaults?

WARNING: All existing configuration and data will be lost.

Please enter Y to confirm: y

Step 1 of 3: Removing trust with Network Security Manager

Network Security Manager trust is removed.

Step 2 of 3: Resetting the NTBA database to factory defaults. This will take few minutes.

Stopping all services.

Formatting NTBA database partitions. This will take several minutes depending on the disk size.

Creating fresh databases.

Resetting NTBA configurations.

The NTBA configuration and signature files are reset to default.

Step 3 of 3: Rebooting the NTBA appliance. After the reboot, log in to complete the NTBA setup.

Broadcast message from root (Thu Feb 27 11:57:26 2014):

The system is going down for reboot NOW!
```

Applicable to:

NS-series Sensors

Errors while running factorydefaults

The following errors might occur while you run this command:

- **An error occurred while stopping the database events. Restart the appliance or VM and rerun factorydefaults.**
- **An error occurred while trying to disable database events. Restart the appliance or VM and rerun factorydefaults.**
- **An error occurred while stopping the database processes. Restart the appliance or VM and rerun factorydefaults.**

- **An error occurred while disabling the database processes. Restart the appliance or VM and rerun factorydefaults.**
- **The NTBA database service is still up. Sending a termination signal.**
- **The NTBA database service is still up. Sending a kill signal.**
- **The NTBA database service can't be stopped. Restart the appliance or VM and rerun factorydefaults.**
- **Formatting the NTBA database partitions. This will take several minutes depending on the disk size.**
- **Dropping NTBA databases failed. Restart the appliance or VM and rerun factorydefaults.**
- **Formatting NTBA database partitions failed. Restart the appliance or VM and rerun factorydefaults.**
- **Creating fresh databases**
- **Mounting NTBA database partitions failed. Restart the appliance or VM and rerun factorydefaults.**
- **Installing the NTBA database engine failed. Restart the appliance or VM and rerun factorydefaults.**
- **Installing the NTBA databases failed. Restart the appliance or VM and rerun factorydefaults.**
- **Resetting NTBA configurations**
- **Verifying software image on the appliance or VM failed. Load the correct NTBA software image and rerun factorydefaults.**
- **Extracting the tar file failed. Load the correct NTBA software image and rerun factorydefaults.**
- **Checking consistency of software image on the appliance or VM failed. Load the correct NTBA software image and rerun factorydefaults.**
- **Retrieving package from the software image failed. Load the correct NTBA software image and rerun factorydefaults.**
- **NTBA configuration and signature files are reset to default.**

Issuing a command via ssh

You can administer a Sensor remotely from a command prompt via **ssh**. To do so, you must ensure the **ssh daemon** on the Sensor is started (the default). If it is stopped, you can start it from the console using the CLI command **sshd enable**.

NOTE

Only 5 sshd sessions can be open concurrently on a Sensor.

Logging onto the Sensor via an SSH client

Steps:

1. Open an **ssh** client session to logon to the Sensor.

2. At the login prompt, enter the default username **admin** and password **admin123**. The number of login attempts to the Sensor from a client, on a single connection, is set to 3, after which the connection is closed.

> **NOTE**
>
> The number of login attempts to the Sensor can differ based on the ssh client that you are using. You can get 3 login attempts with certain clients (for example, Putty release 0.54, Putty release 0.56, etc.), or you can get 4 login attempts with other clients (for example, Putty release 0.58, Linux ssh clients, etc.).

Auto-complete

The CLI provides an auto-complete feature. To auto-complete a command, press **TAB** after typing a few characters of a valid command and then press **ENTER**. For example, typing **expo** and pressing **TAB** would result in the CLI auto-completing the entry with the command **exportsensorcerts**.

If the partially-entered text matches multiple options, the CLI displays all available matching commands.

CLI syntax

You issue commands at the command prompt as shown below:

<command> <value>

- Values that you must enter are enclosed in angle brackets (< >).
- Optional keywords or values are enclosed in square brackets ([ ]).
- Options are shown separated by a line (|).
- Variables are indicated by *italics*.

> **NOTE**
>
> Do not type the < or [ ] symbols.

Command sequence

Some operations require that you first specify a network value before you issue a command. For example, you must specify a TFTP server IP address before you issue a **loadimage** command. See the instructions on performing the operation for the correct sequence.

Mandatory commands

There are certain commands that must be executed on the Sensor before the Sensor is fully operational. The remaining commands in this chapter are optional and will assume default values for their parameters unless they are executed with other specific parameter values.

The following are the required commands:

- **`set sensor name`**
- **`set sensor ip/ipv6`**
- **`set manager ip`**
- **`set sensor sharedsecretkey`**
- If the Sensor is on a different network than the Manager, you will need to use the **`set sensor gateway`** (or **`set sensor gateway-ipv6`**) command.

Granular access control for CLI commands

Trellix Intrusion Prevention System supports creation of multiple user accounts for the Sensor. Each of these user accounts is created for various functions, that is, different roles are associated with these user accounts. The role of a user determines the CLI commands he or she is able to access.

The following Sensor user roles are supported:

- **`Admin`** – Access to all commands
- **`Read and Write`** – Access to all commands, except the ones available only to the administrator
- **`Read Only`** – Access to all show commands
- **`Updater`** – Access to update Sensor images and signature files
- **`Maintainer`** – Access to update Sensor images, signature files, and also adding a Sensor to a specific Manager

> **NOTE**
>
> The debug commands can be accessed by admins or users with read and write access.

You can authenticate users by using either TACACS+ or RADIUS servers. For a TACACS+ user to obtain granular access control, authorization should be enabled at the Sensor. If not, **`Admin`** access is given to the user. The role should be assigned in the TACACS+ server configuration. If no role is configured in the TACACS+ server, **`Admin`** access is given. If a role other than the allowed roles is assigned, **`Read-Only`** access is given. Users authenticated by RADIUS server are assigned the **`Admin`** role by default. Role based user logins cannot be created through the RADIUS server.

The following is an example of the TACACS+ server configuration file:

```
user=user1 {

.................

.................

service = intrushell {

role= “RO-Access”

}
```

}

NOTE

In case of RADIUS configuration, the role is assigned as **`Admin`** by default.

The allowed strings to be given in the TACACS+ configuration file are the following:

- “Updater”
- “Maintainer”
- “RO-Access”
- “RW-Access”
- “Admin-Access”

NOTE

Trellix recommends either TACACS+/RADIUS users or local users on the Sensor are configured. If both are required, ensure that users with the same name are not present in the Sensor and the TACACS+/RADIUS servers.

adduser WORD

Use this command to add a new user in the default role (Read Only). The admin can later choose to override the user’s role using the **`userrole`** command.

A maximum of 100 users can be added.

Syntax:

`adduser WORD`

where **`WORD`** stands for the user name. Consider the following when specifying a user name:

- The length of a user name can be 1-25 characters.
- The user name can be created using alphabets, numbers, and few special characters.
- The special characters that you can use are dot (.), hyphen (-) and underscore (_).
- The user name must begin with an alphabet, and is case-sensitive.
- The user can log on using the password assigned by the admin. The admin can assign passwords with no restrictions.

Applicable to:

NS-series Sensors

commands

It displays all CLI commands supported for the current user role.

This command has no parameters.

Syntax:

commands

Applicable to:

NS-series Sensors

deleteuser WORD

This command deletes existing users.

If the user is currently logged in, you cannot delete the account until the user logs off.

Syntax:

deleteuser WORD

where **WORD** stands for the user name to be deleted.

Applicable to:

NS-series Sensors

deleteallusers

This command deletes all existing users.

If the user is currently logged in, you cannot delete the account until the user logs off.

Syntax:

deleteallusers

Applicable to:

NS-series Sensors

lockuser WORD

This command locks out any user created by the admin.

Syntax:

lockuser WORD

where **WORD** stands for the user name.

Note the following:

- The user **admin** cannot be locked using this command.
- When locked, the users using this command will not be able to login until they are unlocked using the **unlockuser** command.

Applicable to:

NS-series Sensors

passwd

This command changes the password of the currently logged in user. A password must contain at least 8 characters and can consist of any alphanumeric character or symbol. This command is applicable for changing the password for admin as well non-admin users.

The user will be asked to enter the current password before changing to a new password.

Syntax:

`passwd`

Applicable to:

NS-series Sensors

userpasswd WORD

Use this command to assign/reset the password for existing users.

Syntax:

`userpasswd WORD`

where **`WORD`** stands for the username for whom the password needs to be assigned or reset.

Once the password is reset, the admin must inform the user about the new password.

The password supplied by the admin is not validated for password strength and minimum length.

Applicable to:

NS-series Sensors

userlist

This command displays the list of existing users created by admin and the roles assigned to them. The currently locked users are also displayed.

The locked users, when displayed, are marked with an asterisk (*).

Syntax:

`userlist`

> **NOTE**
>
> If a user account gets locked due to login failure, the locked status is displayed after the next login attempt.

Applicable to:

NS-series Sensors

userrole WORD

This command changes the role of an existing user.

Syntax:

`userrole WORD <admin|readwrite|readonly|updater|maintainer>`

where **`WORD`** stands for the user name for whom the role is to be changed.

Applicable to:

NS-series Sensors

unlockuser WORD

This command unlocks a user account that is locked due to multiple authentication failures.

Syntax:

`unlockuser WORD`

where **`WORD`** stands for the user name to be unlocked.

Three successive logon failures result in locking of a user account. The admin can then unlock the user account using this command. Once unlocked, the user can continue to use the same password.

NOTE

- The local administrator cannot be locked out to ensure that administrative access is always maintained.
- The **`userpasswd`** command can also be used to unlock a user account. However, in case of **`userpasswd`**, the user will receive a new password.

Applicable to:

NS-series Sensors

whoami

This command displays the name of the user who is currently logged in.

Syntax:

`whoami`

Applicable to:

NS-series Sensors

Role and CLI command matrix

The following table shows the different CLI commands and their availability for different roles.

Table 96. Role and CLI command matrix

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
adduser	N	N	N	N	Y
accelerate-ftp	N	N	N	N	Y
accelerate-ftp status	N	N	N	N	Y
appidlog <enable | disable>	N	N	N	N	Y
appidlog status	N	N	N	N	Y
appidstat	N	N	N	Y	Y
arp delete	N	N	N	Y	Y
arp dump	N	N	Y	Y	Y
arp flush	N	N	N	Y	Y
arp spoof	N	N	N	Y	Y
auditlogupload	N	N	Y	Y	Y
clearmalwarecache <all | tis | flash | gam | gti | ivx | office | pdf>	N	N	N	N	Y
clearnistats	N	N	N	Y	Y
checkmanagerconnectivity	N	N	N	N	Y
clrdnseliststats	N	N	N	N	Y
clrdpdstats	N	N	N	N	Y
clrstat	N	N	N	Y	Y
clrtscache	N	N	N	Y	Y
clrtsstats	N	N	N	N	Y
clear ssl outbound urlcache	N	N	Y	Y	Y
commands	Y	Y	Y	Y	Y
console eventlog (on|off| status)	N	N	N	N	Y
debug	N	N	N	Y	Y
deinstall	N	Y	N	Y	Y
deleteallusers	N	N	N	N	Y
deletemgrsecintf	N	Y	N	Y	Y
deletesignatures	N	N	N	Y	Y
deleteuser	N	N	N	N	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
disconnectalertandpktlog-channels	N	Y	N	Y	Y
dnsprotect	N	N	N	Y	Y
dnsprotect (add|delete|resetlist)	N	N	N	Y	Y
dnsprotect resetlist	N	N	N	Y	Y
downloadstatus	Y	Y	Y	Y	Y
dumpappidlog <1-100>|running	N	N	N	N	Y
dumpdnseliststats	N	N	N	N	Y
dumpdnsexcplistentries	N	N	N	N	Y
dumpmalwarecache	N	N	N	Y	Y
exit	Y	Y	Y	Y	Y
exportsensorcerts	N	N	Y	Y	Y
factorydefaults	N	N	N	Y	Y
failovermode forward-peer-stp (enable|disable)	N	N	N	Y	Y
filerep gti md5 <md5_hash>	N	N	N	Y	Y
fwdump acl	N	N	N	N	Y
getnistats	N	N	Y	N	Y
guest-portal	N	N	N	Y	Y
help	Y	Y	Y	Y	Y
Importsensorcerts	N	N	N	Y	Y
ipreassembly timeout forward	N	N	N	Y	Y
ivx lookup sha256 <sha256>	N	N	N	Y	Y
latency-monitor	N	N	N	Y	Y
latency-monitor enable action <alert-only | put-in-layer2>	N	N	N	Y	Y
latency-monitor restore-inline enable <10-60>	N	N	N	N	Y
latency-monitor restore-inline disable	N	N	N	N	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
latency-monitor sensitivity-level <high | medium | low>	N	N	N	N	Y
logstat (all|datapath|mgmt|dos)	N	N	N	N	Y
layer2 mode	N	N	N	Y	Y
loadconfiguration	N	Y	N	Y	Y
loadimage	Y	Y	N	Y	Y
loadsavedimage	N	N	N	Y	Y
lockuser	N	N	N	N	Y
logstat	N	N	Y	Y	Y
niantic_stats	N	N	N	N	Y
ninetflowstat	N	N	Y	N	Y
ntbastat	N	N	Y	Y	Y
passwd	Y	Y	Y	Y	Y
ping	Y	Y	Y	Y	Y
quit	Y	Y	Y	Y	Y
raidrepair	N	N	Y	Y	Y
reboot	Y	Y	N	Y	Y
reconnectalertandpktlog-channels	N	Y	N	Y	Y
rescuedisk	N	N	N	Y	Y
resetconfig	N	N	N	Y	Y
secureerase	N	N	N	Y	Y
sensor perf-debug<time in minutes>	N	N	N	Y	Y
sensor perf-debug off	N	N	N	Y	Y
sensor perf-debug status	N	N	Y	Y	Y
sensor-datapath-stat-analysis log	N	N	N	N	Y
sensor-datapath-stat-analysis show	N	N	N	N	Y
sensordroppktevent	N	N	N	Y	Y
set attackId list logging	N	N	N	N	Y
set autorecovery	N	N	N	Y	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
set auxport (enable|disable)	N	N	N	Y	Y
set console timeout	N	N	N	Y	Y
set debugmode passwd	N	N	N	N	Y
set dnsprotect	N	N	N	Y	Y
set dospreventionseverity <dos-measure-name> <inbound | outbound> <0-200>	N	N	N	Y	Y
set dpimonitor <enable | disable>	N	N	N	N	Y
set dpimonitor-action <enable|disable>	N	N	N	N	Y
set flowvolumelimit disable	N	N	N	Y	Y
set flowvolumelimit enable <threshold>	N	N	N	Y	Y
set gam-airgap-network <enable | disable>	N	N	N	Y	Y
set gam-behavioral-scan config <enable | disable>	N	N	N	Y	Y
set gigfailopen disable	N	N	N	Y	Y
set gigfailopendelay	N	N	N	Y	Y
set hypervisor server ip	N	Y	N	Y	Y
set inactiveuserslock <enable | disable>	N	N	N	N	Y
set intfport id flowcontrol	N	N	N	Y	Y
set manager alertport	N	N	N	Y	Y
set manager alertport_RSA-2048-bit	N	N	N	Y	Y
set manager installsensorport	N	N	N	Y	Y
set manager installsensorport_RSA-2048-bit	N	N	N	Y	Y
set manager ip	N	Y	N	Y	Y
set manager logport	N	N	N	Y	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
set manager log-port_RSA-2048-bit	N	N	N	Y	Y
set manager secondary ip	N	Y	N	Y	Y
set mgmtport auto	N	N	N	Y	Y
set mgmtport mtu	N	N	N	Y	Y
set mgmtport speed	N	N	N	Y	Y
set mnsconfig	N	N	N	N	Y
set mnsconfig radiusLB	N	N	N	N	Y
set nmsuserwriteaccess	N	N	N	Y	Y
set outofcontext acllook-up <enable|disable>	N	N	N	N	Y
set portsettletime <sec-onds>	N	N	N	Y	Y
set scpserver ip	Y	Y	N	Y	Y
set sensor gateway	N	Y	N	Y	Y
set sensor gateway-ipv6	N	Y	N	Y	Y
set sensor ip/ipv6	N	Y	N	Y	Y
set sensor name	N	N	N	Y	Y
set sensor sharedsecret-key	N	Y	N	Y	Y
set sessionlimit timeout	N	N	N	N	Y
set sshinactivetimeout	N	N	N	Y	Y
set syncookietcpreset (on|off)	N	N	N	Y	Y
set ta wakeup port [<1-65536>]	N	N	N	N	Y
set tacacsauthorization	N	N	N	Y	Y
set tcpudpchecksumerror drop	N	N	N	Y	Y
set tcpudpchecksumerror forward	N	N	N	Y	Y
set tftpserver ip	Y	Y	N	Y	Y
set tiscachepurge inter-val hours <1-192>	N	N	N	N	Y
set userconfigvolumedos-threshold	N	N	N	Y	Y
set vlanbasedrecon	N	N	N	N	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
setfailopencfg restore-inline	N	N	N	N	Y
setfailopencfg restore-inline-interval < 5-60 minutes >	N	N	N	N	Y
setfailopencfg internal/external-failopen bypass/inline	N	N	N	N	Y
setup	N	N	N	Y	Y
show	Y	Y	Y	Y	Y
show ab stats	N	N	N	Y	Y
show acl stats	N	N	Y	Y	Y
show arp spoof status	N	N	Y	Y	Y
show attackIdList logging status	N	N	N	N	Y
show auditlog	N	N	Y	Y	Y
show auditlog status	N	N	Y	Y	Y
show auditlogtomgr status	N	N	N	Y	Y
show autorecovery status	N	N	Y	Y	Y
show auxport status	N	N	Y	Y	Y
show botnet-alertstats	N	N	N	Y	Y
show console timeout	N	N	Y	Y	Y
show coppersfpserialnumbers	N	N	Y	Y	Y
show dnsprotect	N	N	Y	Y	Y
show dnsprotectstat	N	N	Y	Y	Y
show dospreventionprofile	N	N	Y	Y	Y
show dospreventionseverity	N	N	Y	Y	Y
show dpimonitor status	N	N	N	N	Y
show dpimonitor-action status	N	N	N	N	Y
show dxl status	N	N	N	N	Y
show eventlog	N	N	Y	Y	Y
show failover-status	N	N	Y	Y	Y
show festats	N	N	Y	Y	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
show flows	N	N	Y	Y	Y
show flowvolumelimit config	N	N	Y	Y	Y
show gam-airgap-network status	N	N	Y	Y	Y
show gam-behavioral-scan status	N	N	Y	Y	Y
show gam engine stats	N	N	N	N	Y
show gigfailopendelay	N	N	Y	Y	Y
show gti config	N	N	Y	Y	Y
show gti stats ip	N	N	N	N	Y
show inactiveuserslock status	N	N	N	N	Y
show inlinepktdropstat	N	N	Y	Y	Y
show ingress-egress stat	N	N	Y	Y	Y
show intfport	N	N	Y	Y	Y
show l7ae status	N	N	N	N	Y
show l7ddosstat	N	N	N	N	Y
show layer2 forward all	N	N	Y	Y	Y
show layer2 forward intfport <port>	N	N	N	Y	Y
show layer2 mode	N	N	Y	Y	Y
show malwareenginestats	N	N	N	N	Y
show malwarefilestats	N	N	N	N	Y
show mem-usage	N	N	Y	Y	Y
show mgmtport	N	N	Y	Y	Y
show mnsconfig	N	N	N	N	Y
show msoffice-fdi stats	N	N	N	N	Y
show ni status	N	N	Y	N	Y
show ivx config	N	N	Y	Y	Y
show ivx stats brokerid (1|2|3|4|5|all)	N	N	N	N	Y
show ivx status brokerid (1|2|3|4|5|all)	N	N	N	N	Y
show ivxcloud config	N	N	Y	Y	Y
show ivxcloud stats	N	N	N	N	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
show ivxcloud status	N	N	N	N	Y
show netstat	N	N	Y	Y	Y
show nmsuserwriteaccess status	N	N	N	N	Y
show outofcontext acl-lookup	N	N	N	N	Y
show parsetunneledtraffic status	N	N	Y	Y	Y
show pktcapture status	N	N	N	Y	Y
show pluggable– module	N	N	Y	Y	Y
show portsettletime	N	N	Y	Y	Y
show previous256byteslogging status	N	N	Y	Y	Y
show raid status	N	N	N	Y	Y
show rescueimages	N	N	Y	Y	Y
show respport r1	N	N	N	N	Y
show savedalertinfo	N	N	Y	Y	Y
show savedimages	N	N	N	Y	Y
show sensordroppktevent status	N	N	Y	Y	Y
show sensor-load	N	N	Y	Y	Y
show sessionlimit timeout	N	N	N	N	Y
show snort config	N	N	N	N	Y
show ssh config	N	N	Y	Y	Y
show sshaccesscontrol status	N	N	Y	Y	Y
show sshinactivetimeout	N	N	Y	Y	Y
show sshlog status	N	N	N	N	Y
show ssl config	N	N	Y	Y	Y
show ssl stats	N	N	Y	Y	Y
show ssl stats inbound agents	N	N	N	Y	Y
show sslagentaccesscontrol satus	N	N	N	Y	Y
show suricata sbstats	N	N	N	N	Y
show suricata enginestats	N	N	N	N	Y

Command Name	Updater	Maintainer	ReadOnly	ReadWrite	Admin
show syncookietcpreset	N	N	Y	Y	Y
show syslog statistics	N	N	Y	Y	Y
show tacacs	N	N	Y	Y	Y
show tcpipstats	N	N	Y	Y	Y
show tcpudpchecksumerror	N	N	Y	Y	Y
show tiestats	N	N	N	N	Y
show userconfigvolumedos-threshold	N	N	Y	Y	Y
show userInfo stats	Y	Y	Y	Y	Y
show vlanbasedrecon status	N	N	N	N	Y
showfailopencfg	N	N	N	N	Y
shutdown	N	N	N	Y	Y
snmpv2support	N	N	N	N	Y
sshd disable	N	N	N	Y	Y
sshd enable	N	N	N	Y	Y
sshlogupload WORD	N	N	N	N	Y
sshaccesscontrol resetlist	N	N	N	Y	Y
sslagentaccesscontrol resetlist	N	N	N	Y	Y
status	Y	Y	Y	Y	Y
Suricata <on|off>	N	N	N	N	Y
tiscache autopurge <enable|disable>	N	N	N	N	Y
tiscache autopurge status	N	N	N	N	Y
traceupload	N	N	Y	Y	Y
unlockuser	N	N	N	N	Y
userlist	N	N	N	N	Y
userpasswd	N	N	N	N	Y
userrole	N	N	N	N	Y
vlanbridestp	N	N	N	Y	Y
watchdog	N	N	N	Y	Y
whoami	Y	Y	Y	Y	Y

Logon to the CLI

Before you can enter CLI commands, you must first log on to the Sensor with a valid user name (username is **admin**) and password (default is **admin123**).

> ⚠ **CAUTION**
>
> Trellix strongly recommends you change this password using the **passwd** command within your first interaction with the Sensor.

Type **exit** to log off.

Debug mode

Log on to the Sensor with a valid user name (username is **admin**) and password (default is **admin123**). At the command prompt, type **debug** to log on to debug mode. You can now run the debug mode commands.

Type **exit** to log off.

Displaying next possible strings with "?"

? displays the next possible command string that you can enter.

Syntax

?

> **NOTE**
>
> **?** shows the next word you can type. If you execute the ? command in conjunction with the set command, for example, Trellix IPS displays a list of all options available with the **set** command.

IPS CLI Commands - Normal Mode

This section details the commands that can be run in Normal mode. In this mode, you can't run the Debug mode commands.

accelerate-ftp

This command configures the fast forward FTP data flows feature.

Syntax:

```
accelerate-ftp (inbound | outbound) (enable | disable)
```

Default Value:

It is disabled by default.

Example:

```
intruShell@john-3050> accelerate-ftp inbound enable
```

```
intruShell@john-3050> accelerate-ftp outbound enable

intruShell@john-3050> accelerate-ftp inbound disable

intruShell@john-3050> accelerate-ftp outbound disable
```

Applicable to:

NS-series Sensors

accelerate-ftp status

This command displays the fast forward FTP data flows feature status.

Syntax:

```
accelerate-ftp status
```

Sample output:

```
intruShell@john> accelerate-ftp status

FTP acceleration inbound : ENABLED

FTP acceleration outbound : DISABLED
```

Applicable to:

NS-series Sensors

appidlog

This command dumps applications detected in the sensor to sensor.dbg. By default, the command is disabled.

Syntax:

```
appidlog <enable | disable>
```

Applicable to:

NS-series Sensors

appidlog status

It displays whether appidlog feature is enabled or disabled. This command has no parameter.

Syntax:

```
appidlog status
```

Sample Output:

```
intruShell@chand-9100-2> appidlog status

intruShell@chand-9100-2> appidlog status
```

`appidlog = Disabled`

Applicable to:

NS-series Sensors

arp delete

This command removes a single MAC or IP address association from the ARP table. It is used in conjunction with Trellix IPS ARP spoofing detection feature. This command might also be used in situations where a machine on the network is replaced with new hardware.

Syntax:

`arp delete <IP address>`

Parameter	Description
IP address	This is a 32-bit IP address number indicated by four numbers separated by periods (X.X.X.X), where X indicates a number between 0-255.

Example:

The following example shows that the IP address 209.165.202.255 is removed from the ARP table.

`arp delete 209.165.202.255`

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

arp dump

This command dumps the contents of the current MAC/IP address mapping table in the database to a debug file. It is used for debugging purposes. Use it with the **`logstat`** command to provide a diagnostic trace to supply to Technical Support. It is used in conjunction with the Trellix IPS ARP spoofing detection feature.

This command has no parameters.

Syntax:

`arp dump`

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

arp flush

This command deletes the contents of the MAC/IP addresses mapping table. It is used in conjunction with the Trellix IPS ARP spoofing detection feature.

This command has no parameters.

Syntax:

arp flush

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

arp spoof

This command enables or disables the ARP spoofing detection. It is used in conjunction with the Trellix IPS ARP spoofing detection feature.

Syntax:

arp spoof <enable><disable>

Parameter	Description
enable	Enables ARP spoofing detection
disable	Disables ARP spoofing detection

Default Value:

It is disabled by default.

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

auditlogupload

This command uploads the audit log file to the configured TFTP/SCP server. This file can contain a maximum of 5000 recent audit events.

Syntax:

auditupload WORD

auditlogupload tftp WORD

auditlogupload scp WORD

where **WORD** stands for the name of the audit log file to be uploaded.

Note the following:

- When loading an audit log file on the SCP server, you are prompted for the SCP server credentials (username and password). The command succeeds only on providing the correct SCP server credentials.
- When loading an audit log file on the SCP server, the pathname of the file should be absolute. When loading from the TFTP server, the pathname of the file should be relative to /tftpboot.
- If no filename is specified, the default filename is created in the specified path on the SCP server. The default file name for the audit log is audit_<sensor_timestamp>_<sensor_name>.log.
- Before executing this command (uploading on the TFTP server), make sure that the file is created on the TFTP server with write permissions for everyone.

- The functionality of **`auditlogupload tftp WORD`** is the same as **`auditupload WORD`**.

Applicable to:

NS-series Sensors

checkmanagerconnectivity

This command checks the connectivity between the Sensor and the Manager and displays the following status information:

- Alert channel
- Packet log channel
- Authentication channel

For any of the above, if the status is displayed as `down`, it additionally displays the steps for troubleshooting the connectivity.

Syntax:

`checkmanagerconnectivity`

Sample Output:

```
intruShell@john> checkmanagerconnectivity

[Manager Trust]

Trust Established : Yes

[Manager Communications]

IP Connection : Pass

Alert Channel : down

Log Channel : up

Authentication Channel : up

[Manager Port Reachability]

Install TCP Port 8501 : OPEN

Alert TCP Port 8502 : OPEN

Logging TCP Port 8503 : OPEN
```

NOTE

The **`[Manager Port Reachability]`** section in the **`checkmanagerconnectivity`** command output lists the port status related to the Manager and Sensor communication. The **`[Manager Port Reachability]`** section lists **CA Signed cert** ports' status when the Manager and Sensor communication is using a CA-signed certificate; or else it will have **Self Signed cert** ports' status.

Applicable to:

NS-series Sensors

Troubleshooting tips:

- Reinitialize both the alert and log channels by executing the commands **`disconnectalertandpktlogchannels`** and **`reconnectalertandpktlogchannels`** at the CLI.
- If the issue persists, capture the packets on the Sensor's management port and also in the Manager for further analysis.

clear afo dst-mac

This command clears the previously configured destination MAC address on the specified port-pairs.

> **NOTE**
>
> Upon clearing the configuration, when you execute the command *show afo status* (page 1959), the **AFO Destination MAC** column in the output will display the status of IFO-ACTIVE port-pair(s) as **Auto Detected**. If you plan to reconfigure the destination MAC address in the heartbeat packets sent by the Active Fail-Open (AFO) kit, you can use the command *set afo port-pair and dst-mac* (page 1923).

Syntax:

`clear afo <port-pair | all> dst-mac`

Parameter	Description
<port-pair>	Set the port-pair for which the status is to be displayed. Valid port-pairs for NS9500, NS7600, NS7500 Sensors are: g0/1-g0/2 | g0/3-g0/4 | g1/1-g1/2 | g1/3-g1/4 | g1/5-g1/6 | g1/7-g1/8 | g2/1-g2/2 | g2/3-g2/4 | g2/5-g2/6 | g2/7-g2/8 | g3/1-g3/2 | g3/3-g3/4 | g3/5-g3/6 | g3/7-g3/8 Valid port-pairs for NS3600 Sensor are: 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 | 13-14
<all>	Display the status of all the IFO-ACTIVE port-pairs.

Example 1:

`intruShell@NS7500> clear afo g0/1-g0/2 dst-mac`

The above command clears the destination MAC address configuration on port-pair g0/1-g0/2.

Example 2:

`intruShell@NS7500> clear afo all dst-mac`

The above command clears the destination MAC address configuration on all the IFO-ACTIVE port-pairs.

Applicable to:

NS-series Sensors NS9500, NS7600, NS7500, and NS3600.

clear ssl proxy applog

This command clears virtual appliance applogs that contain session data specific to proxy based SSL traffic decryption.

This command has no parameters.

Syntax:`clear ssl proxy applog`

Applicable to:

NS-series Sensors (except NS7600 and NS3600)

clear ssl proxy stats

This command clears all the statistics generated for both inbound and outbound proxy SSL traffic.

Syntax:

```
clear ssl proxy stats
```

Applicable to:

NS-series Sensors (except NS7600 and NS3600)

clearmalwarecache

This command deletes the cache entries made in the Sensor for all the malware engines or specific malware engine based on user input.

Syntax:

```
clearmalwarecache <all | flash | gam | gti | ivx | office | pdf | tis>
```

Example:

```
intruShell@IPS-NS9500> clearmalwarecache ivx

Sent Cache delete request
```

Applicable to:

NS-series Sensors

clrstat

This command clears all the statistics counters in the Sensor.

Syntax:

```
clrstat
```

> **NOTE**
>
> Upon clearing the counters, the **Pending list free nodes** counter which is a part of the **`show ivx stats brokerid`** and **`show ivxcloud stats`** output also gets cleared. But, when you issue these commands after some time, the **Pending list free nodes** counter displays the total count i.e., **200** in case of IVX Cloud deployments and **200** - **1000** (depending on the number of broker nodes you have configured) in case of IVX appliance deployments. Please note that the counter value starts decrementing when you start fetching reports form the IVX engine.

Applicable to:

NS-series Sensors

clrtsstats

This command clears all the trusted source counters in the Sensor.

Syntax:

```
clrtsstats
```

Applicable to:

NS-series Sensors

clear ssl proxy outbound urlcache

This command clears the URL cache generated for outbound SSL traffic where exceptions are set for specific URLs.

Syntax:

```
clear ssl proxy outbound urlcache
```

Applicable to:

NS9500, NS9200, NS9100, NS7500, NS7300, and NS7200 Sensors

commands

It displays all CLI commands supported for the current user role.

This command has no parameters.

Syntax:

```
commands
```

Applicable to:

NS-series Sensors

console eventlog

This command enables or disables logging for console events. The status option displays whether logging is on or off.

Syntax:

```
console eventlog on
```

```
console eventlog off
```

```
console eventlog status
```

Sample output:

```
intruShell@john-3050> console eventlog status

console logging = off
```

Applicable to:

NS-series Sensors

debug

This command enables you to log on to debug mode.

Syntax:

```
debug
```

Applicable to:

NS-series Sensors

deinstall

This command clears the Manager-Sensor trust data (the certificate and the shared key value). Every time you delete a Sensor from the Manager, you must issue this command on the Sensor to clear the established trust relationship before reconfiguring the Sensor.

This command has no parameters.

Syntax:

```
deinstall
```

On executing the command, the following messages are displayed:

```
deinstall the sensor and remove the trust with the manager ?

Please enter Y to confirm: Y
```

> **NOTE**
>
> If you enter **Y**, the Manager/Sensor trust is removed. By pressing **N**, the Manager/Sensor trust remains intact and you come out of the deinstall prompt.

Pressing **Y** displays the following message:

```
deinstall in progress ...

this will take a couple of seconds, please check status on CLI
```

Applicable to:

NS-series Sensors

deletemgrsecintf

This command clears the IP address of a Manager's secondary NIC.

This command has no parameters.

Syntax:

```
deletemgrsecintf
```

On executing the command, the following messages are displayed:

```
Please enter Y to confirm: y

Managers secondary intf IPaddr doesn't exist.

Deleting managers secondary interface had some Warnings/Errors.
```

Applicable to:

NS-series Sensors

deletesignatures

This command deletes signatures on the Sensor and reboots the Sensor. When you execute this command, the signatures are deleted and the Sensor is restarted automatically. Before executing the command, you are asked whether both the tasks should be performed.

This command has no parameters.

Syntax:

```
deletesignatures
```

On executing the command, the following messages are displayed:

```
Delete the signatures and reboot the sensor ?

Please enter Y to confirm: y

deleting the signatures and rebooting the sensor

signatures deleted

Broadcast message from root (Fri Mar 28 05:15:54 2014):

The system is going down for reboot NOW!
```

Applicable to:

NS-series Sensors

disconnectalertandpktlogchannels

This command removes the alert and log channels between the Sensor and the Manager without deleting the trust keys. It breaks the communication with the Manager without disturbing the configured trust information.

This command has no parameters.

Syntax:

`disconnectalertandpktlogchannels`

On executing the command, the following message is displayed:

`this will take a couple of seconds , please check status on CLI`

Applicable to:

NS-series Sensors

dnsprotect

This command performs the following tasks:

- Adds a new DNS Spoof protection IP address
- Deletes an existing DNS Spoof protection IP addresses (IPv4, IPv6, or both) from the Protected Server List (PSL)
- Relists the DNS spoofing protection IP address

This command does not perform when the IPv6 packets have a routing header.

Syntax:

Use the following syntax for adding or deleting a DNS spoof protection IP address:

`dnsprotect <add/delete/> <ipv4/ipv6> <IP address>`

While using the <resetlist> parameter, use the following syntax:

`dnsprotect <resetlist> <ipv4/ipv6/all>`

Parameter	Description
add	Adds a new DNS spoofing protection IP address
delete	Deletes an existing DNS spoofing protection IP address
resetlist	Resets the list the DNS spoofing protection IP address
ipv4	Indicates that the IP address is for IPv4 packet
ipv6	Indicates that the IP address is for IPv6 packet
all	Indicates that the resetlist of the existing DNS spoofing protection IP address is for both IPv4 and IPv6
IP address	This is a 32-bit IP address number indicated by four numbers separated by periods (X.X.X.X), where X indicates a number between 0-255.

Example:

The following example shows the **`dnsprotect`** command used for adding the DNS spoof protection IP address for IPv4:

`dnsprotect add ipv4 157.125.202.255.`

The following example shows the **dnsprotect** command used for reset listing of DNS spoof protection IP address for all the IP addresses(IPv4 and IPv6):

dnsprotect resetlist all

Applicable to:

NS-series Sensors

downloadstatus

The command displays the status of various download and upload operations from the Manager to Sensor and from the Sensor to Manager. It also lists the number of times you performed the operation, and status of your previous attempt to perform the operation. The time of the command execution is also listed.

This command has no parameters.

Syntax:

downloadstatus

Sample Output:

```
intruShell@john> downloadstatus

[Download Status]

--------------------

Signatures Downloaded : 1

Last Signature Download Status : good

Last Signature Download Time (UTC) : 7:12:28, 7/30/2021

Last Signature Download Type : SIGSET + POLICY

Certificates Downloaded : 0

DAT Files Downloaded : 0

Software Upgrades : 0

DoS Profile Downloads from Manager : 0

DoS Profile Uploads to Manager : 0

Diagnostic Trace Requests : 0

Guest Portal SSL Cert Downloads from Manager : 0

Guest Portal SSL CSR Uploads to Manager : 0

CA Signed Sensor Cert Downloads from Manager : 0

CA Signed Sensor CSR Uploads to Manager : 0
```

```
IBAC AD file Downloads from Manager : 0

IBAC AD file Uploads to Manager : 0

Offline downloads to sensor : 0

Suricata failed rules file Uploads to Manager : 0

Device Profile update count : 0

User Id Acl Bulk File download count : 0

CA store download from Manager : 1

Last CA store downloaded status : good

Last CA store downloaded time (UTC) : 12:58:35, 7/30/2021
```

Applicable to:

NS-series and Virtual IPS Sensors

dumpappidlog

This command prints the following information on the CLI about the application making a request for the same:

Application name, source IP, destination IP, source port, destination port, and the timestamp.

By default, it is disabled.

Syntax:

```
dumpappidlog <1-100>|running
```

Sample Output:

```
intruShell@chand-9100-2> dumpappidlog running

DATE AND TIME APPNAME SRCIP DESTIP SRCPORT DESTPORT
```

Applicable to:

NS-series Sensors

exit

When executed, this command enables you to exit the CLI.

This command has no parameters.

Syntax:

```
exit
```

Applicable to:

NS-series Sensors

exportsensorcerts

This command writes the Sensor certificates to an external flash. It exports the certificates which establish trust between the Sensor and the Manager. These certificates include the Manager public key, Sensor private key, and Sensor public key.

> **NOTE**
>
> Before executing this command, ensure that trust is established between the Sensor and the Manager.

This command has no parameters.

Syntax:

```
exportsensorcerts
```

On executing the command, the following messages are displayed:

```
This will delete all the data from Flash and reformat. Proceed?.

Please enter Y to confirm:
```

Applicable to:

NS-series Sensors

exportsshpublickey

This command exports the Sensor public key from the Sensor to your remote machine for file transfers.

Syntax:

```
exportsshpublickey <path for public key>
```

Option	Definition
`<path for the public key>`	The file path of the public key

Applicable to:

NS-series Sensors

factorydefaults

You can use this command to wipe all settings, certificates, and signatures from the Sensor, restoring it to blank settings. This command does not appear when you type ? or commands, nor does the auto-complete function apply to this command. You must type the command in full to execute it.

This command has no parameters.

> **NOTE**
>
> Upon execution of this command, you are warned that the operation will clear the Sensor and you must confirm the action. The warning occurs since the Sensor returns to its clean, pre-configured state, thus losing all current configuration settings.

Syntax:

```
factorydefaults
```

On executing the command, the following messages are displayed for an NTBA Appliance:

```
Are you sure you want to reset NTBA to factory defaults?

WARNING: All existing configuration and data will be lost.

Please enter Y to confirm: y

Step 1 of 3: Removing trust with Network Security Manager

Network Security Manager trust is removed.

Step 2 of 3: Resetting the NTBA database to factory defaults. This will take few minutes.

Stopping all services.

Formatting NTBA database partitions. This will take several minutes depending on the disk size.

Creating fresh databases.

Resetting NTBA configurations.

The NTBA configuration and signature files are reset to default.

Step 3 of 3: Rebooting the NTBA appliance. After the reboot, log in to complete the NTBA setup.

Broadcast message from root (Thu Feb 27 11:57:26 2014):

The system is going down for reboot NOW!
```

Applicable to:

NS-series Sensors

Errors while running factorydefaults

The following errors might occur while you run this command:

- **An error occurred while stopping the database events. Restart the appliance or VM and rerun factorydefaults.**
- **An error occurred while trying to disable database events. Restart the appliance or VM and rerun factorydefaults.**
- **An error occurred while stopping the database processes. Restart the appliance or VM and rerun factorydefaults.**
- **An error occurred while disabling the database processes. Restart the appliance or VM and rerun factorydefaults.**
- **The NTBA database service is still up. Sending a termination signal.**
- **The NTBA database service is still up. Sending a kill signal.**
- **The NTBA database service can't be stopped. Restart the appliance or VM and rerun factorydefaults.**

- **Formatting the NTBA database partitions. This will take several minutes depending on the disk size.**
- **Dropping NTBA databases failed. Restart the appliance or VM and rerun factorydefaults.**
- **Formatting NTBA database partitions failed. Restart the appliance or VM and rerun factorydefaults.**
- **Creating fresh databases**
- **Mounting NTBA database partitions failed. Restart the appliance or VM and rerun factorydefaults.**
- **Installing the NTBA database engine failed. Restart the appliance or VM and rerun factorydefaults.**
- **Installing the NTBA databases failed. Restart the appliance or VM and rerun factorydefaults.**
- **Resetting NTBA configurations**
- **Verifying software image on the appliance or VM failed. Load the correct NTBA software image and rerun factorydefaults.**
- **Extracting the tar file failed. Load the correct NTBA software image and rerun factorydefaults.**
- **Checking consistency of software image on the appliance or VM failed. Load the correct NTBA software image and rerun factorydefaults.**
- **Retrieving package from the software image failed. Load the correct NTBA software image and rerun factorydefaults.**
- **NTBA configuration and signature files are reset to default.**

failovermode forward-peer-stp

This command configures the forwarding of the STP packets to the remote standby Sensor during a Sensor failover. When the active Sensor fails or is temporarily shut down, the STP packets get forwarded to the standby Sensor via the failover link.

Syntax:

`failovermode forward-peer-stp<enable|disable>`

Parameter	Description
enable	Enables the forwarding of STP packets to the remote standby Sensor
disable	Disables the forwarding of STP packets to the remote standby Sensor

Applicable to:

NS-series Sensors

fwdump acl

This command displays the configured firewall rules.

Syntax:

`fwdump acl (0 | 1) (fileName | NULL)`

Example:

```
intruShell@john-3050> fwdump acl 0 NULL

Dumping FW Table @ Index 0 into (null)

intruShell@john-3050> fwdump acl 1 NULL

Dumping FW Table @ Index 1 into (null)

intruShell@john-3050> fwdump acl 1 test

Dumping FW Table @ Index 1 into test
```

Applicable to:

NS-series Sensors

guest-portal

This command installs, de-installs, starts, stops, or shows the status of the guest portal on the Sensor.

Syntax:

```
guest-portal <install ><de-install><start><stop><status>
```

Parameter	Description
install	Installs the guest portal web server on the Sensor
de-install	De-installs the guest portal web server on the Sensor
start	Starts the guest portal web server on the Sensor
stop	Stops the guest portal web server on the Sensor
status	Displays the status of the guest portal web server on the Sensor

Example:

The following example shows the **guest-portal** command used for stopping the web server on the Sensor.

```
guest-portal stop
```

Applicable to:

NS-series Sensors

help

This command provides a description of the interactive help system.

This command has no parameters.

Syntax:

```
help
```

Sample Output:

```
intruShell@john> help

If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'set ?') and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'set em?'.)
```

Applicable to:

NS-series Sensors

importsensorcerts

This command imports Sensor certificates from an external flash. It imports the certificates which establish trust between the Sensor and the Manager. These certificates include the Manager public key, Sensor private key, and Sensor public key.

> **NOTE**
>
> Before executing this command, ensure that trust is not established between the Sensor and the Manager.

> **NOTE**
>
> After executing this command, ensure that you reboot the Sensor to establish trust between the Sensor and the Manager.

This command has no parameters.

Syntax:

```
importsensorcerts
```

On executing the command, the following message is displayed:

```
Imported certificates from flash, please reboot the sensor.
```

Applicable to:

NS-series Sensors

importsshpublickey

This command imports the public key to the Sensor so that the user can access the Sensor.

Syntax:

```
importsshpublickey <username> <path of public key>
```

This command takes two parameters:

Option	Definition
<username>	The user name of the user who has access to the Sensor
<path of public key>	The file path of the public key

Applicable to:

NS-series Sensors

ipreassembly timeout forward

Sensors receive the fragmented packets and hold them until all the fragments arrive or the fragment timer expires. After the fragment timer expires (the default value is set to 2 minutes), the fragments are dropped.

This command allows you to configure the Sensor to forward such fragments instead of dropping them.

Syntax

ipreassembly timeout forward <enable|disable>

> **NOTE**
> This configuration is persisted across Sensor reboots.

Parameter	Description
enable	Enables the packet fragments to be forwarded
disable	Disables the packet fragments to be forwarded

ipreassembly timeout forward status

It displays the status of the **ipreassembly timeout forward** (enabled or disabled).

Sample Output:

```
intruShell@john> ipreassembly timeout forward enable

IP Reassembly timeout forward : ENABLED

IPv4 Reassembly timeout frag forward count : 0

IPv6 Reassembly timeout frag forward count : 0
```

Applicable to:

NS-series Sensors

ivx lookup sha256

This command performs lookup on the entered SHA256 hash and returns details such as the verdict, report id, and the query time.

Syntax:

`ivx lookup sha256 <sha256 hash>`

Sample Output:

```
intruShell@ips-ns9200> ivx lookup sha256
1a5e966d3366d7d31654c0db3cde3f8cea1dec6ab7c25f98857ad5119a58e7c6
Connecting to IVX Broker 1:

IVX broker 0 Query Result
    Report id        : 6b99dfef-9bd8-4ebb-b014-8f29c59c4203
    Verdict          : malicious
    Done Time        : 2024-01-03T04:29:27+0000
    Total Query Time : 0.018182 Sec

Connecting to IVX Broker 2:

IVX broker 1 Query Result
    Report id        : 6b99dfef-9bd8-4ebb-b014-8f29c59c4203
    Verdict          : malicious
    Done Time        : 2024-01-03T04:29:27+0000
    Total Query Time : 0.015947 Sec

Connecting to IVX Broker 3:

IVX broker 2 Query Result
    Report id        : 6b99dfef-9bd8-4ebb-b014-8f29c59c4203
    Verdict          : malicious
    Done Time        : 2024-01-03T04:29:27+0000
    Total Query Time : 0.618517 Sec

Connecting to IVX Broker 4:

IVX broker 3 Query Result
    Report id        : 6b99dfef-9bd8-4ebb-b014-8f29c59c4203
    Verdict          : malicious
    Done Time        : 2024-01-03T04:29:27+0000
    Total Query Time : 0.027040 Sec
```

Applicable to:

NS-series and Virtual IPS Sensors

latency-monitor

This command disables the latency monitoring feature or displays the status of latency monitoring feature.

Syntax:

`latency-monitor <disable | status>`

Default Value:

Latency monitoring feature is disabled by default. If disabled, latency monitoring feature does not generate any alert nor does it forward the traffic to layer2 when high latency is observed.

`latency-monitor status`

If latency monitoring is enabled, the following information is displayed:

- latency monitoring status (enable or disable)
- configured action (alert-only or layer2-forward)

Sample Output:

```
intruShell@john> latency-monitor status

latency monitor : Enable

action : alert

restore inline from layer2 : disable

sensitivity Level : low

Unknown-protocol Packets Forwarded Percentage : 0.000000

Unknown-protocol Packets Forwarded Count : 0

Percentage of Packets Forwarded under Latency : 0.000000
```

Applicable to:

NS-series Sensors

latency-monitor enable action

This command enables latency monitoring feature in the Sensor, and also specifies the action to be performed if high latency is observed in the Sensor.

The following are the actions that can be specified in this command:

- **`alert-only`** (generates an alert when a high latency is observed in the Sensor)
- **`put-in-layer2`** (generates an alert and also forwards the traffic to layer2).

These generated alerts can be seen in the **Attack Log**.

Syntax:

`latency-monitor enable action <alert-only | put-in-layer2>`

This command should be executed with a parameter value, else the command is treated as invalid.

NOTE

If **`layer2-forward`** is enabled, it is necessary to set the **`layer2 mode`** to be on. Otherwise the **`layer2-forward`** action does not get executed.

Example:

```
latency-monitor enable action alert-only
```

Applicable to:

NS-series Sensors

latency-monitor restore-inline

When a high latency is observed on the Sensor and the latency monitor is configured, the Sensor remains in layer 2 until a layer 2 deassert is invoked or a Sensor reboots. This command allows the Sensor to come out of layer 2 mode without layer 2 deassert. The Sensor restores to inline from layer 2 if the following conditions are met:

- The latency monitor has put the Sensor in layer 2 mode.
- The Sensor is in good health. If the Sensor is in bad health, a deassert cannot be performed and the Sensor reboots.
- A substantial amount of time has lapsed, as configured using this command, when the Sensor went into layer 2 due to latency. The default time to trigger an automatic layer 2 deassert is 10 minutes.

If the latency continues to exist after the Sensor is restored to inline mode, the Sensor behaves as per the current setting of the latency monitor.

Syntax

```
latency-monitor restore-inline enable <10-60>
```

```
latency-monitor restore-inline disable
```

Parameter	Description
<10-60>	The time to trigger the restore inline from layer 2. It is counted since the time the Sensor moved into layer 2 state due to high latency.

The **`latency-monitor status`** command displays the current status of the latency monitor feature, as well as the current status of the restore-inline feature of the latency monitor.

Applicable to:

NS-series Sensors

latency-monitor sensitivity-level

This command configures the sensitivity level for latency management.

Syntax:

```
latency-monitor sensitivity-level high
```

`latency-monitor sensitivity-level medium`

`latency-monitor sensitivity-level low`

Applicable to:

NS-series Sensors

layer2 mode

This command configures the Layer 2 mode.

Syntax:

`layer2 mode <assert><deassert><off><on>`

assert	Forces the Sensor into Layer 2 Passthru Mode (also known as L2 Mode). This helps in troubleshooting network issues. When this command is used, the Sensor stays in L2 Mode until one of two events occurs: either during Sensor reboot or when the **`layer2 mode deassert`** command is issued.
deas-sert	Forces the Sensor out of Layer 2 Passthru Mode. It is used to re-establish IPS processing after a layer2 mode assert command is issued. This command should not be used to force a Sensor out of L2 Mode if L2 Mode was triggered by a Sensor software failure. Using the command in this manner will trigger a Sensor reboot.
off	Resets the layer 2 mode configuration. If an error occurs in the higher layer processing of the collection subsys-tem, the Sensor reboots immediately instead of entering Layer 2 mode. This command is issued when the Sensor is already forwarding traffic in Layer 2 mode. The Sensor will reboot immediately, attempting to recover full detection functionality.
on	Enables the Layer 2 mode feature. If a failure occurs in the higher layer processing of the collection subsystem, it configures the Sensor to forward all traffic at Layer 2. This command does not force the Sensor to start forwarding traffic in Layer 2 mode immediately.

Default Value:

On

Sample Output:

```
intruShell@john> layer2 mode assert

intruShell@john> show layer2 mode

Mode : enable-immediate

Duration : 10 minutes

Threshold : 1

Occurrences : 0
```

NOTE

The **`status`** command can also be used to check the Layer 2 mode status.

```
intruShell@john> layer2 mode deassert

intruShell@john> status

Layer 2 Status : normal (IDS/IPS)
```

Applicable to:

NS-series Sensors and Virtual IPS Sensors.

loadconfiguration

This command loads the Sensor configuration from the configured TFTP/SCP server. The TFTP/SCP server IP is specified on the Sensor. When the Sensor is added to the ISM, the configuration type should be specified as offline.

Syntax:

```
loadconfiguration WORD

loadconfiguration tftp WORD

loadconfiguration scp WORD
```

where **WORD** stands for the name of the configuration file on the TFTP/SCP server.

Note the following:

- When loading Sensor configuration from the SCP server, you are prompted for the SCP server credentials (username and password). The command succeeds only on providing the correct SCP server credentials.
- When loading Sensor configuration from the SCP server, the pathname of the file should be absolute. When loading from the configured TFTP server, the pathname of the file should be relative to /tftpboot.
- The functionality of **loadconfiguration tftp WORD** is the same as **loadconfiguration WORD**.

Applicable to:

NS-series Sensors

loadimage

This command loads a Sensor image file from the configured TFTP/SCP server.

Syntax:

```
loadimage WORD

loadimage tftp WORD

loadimage scp WORD
```

where **WORD** stands for the name of the image file on the TFTP/SCP server.

Note the following:

- When loading a Sensor image file from the SCP server, you are prompted for the SCP server credentials (username and password). The command succeeds only on providing the correct SCP server credentials.
- When loading a Sensor image file from the SCP server, the pathname of the file should be absolute. When loading from the TFTP server, the pathname of the file should be relative to /tftpboot.
- The functionality of **`loadimage tftp WORD`** is the same as **`loadimage WORD`**.

Applicable to:

NS-series Sensors

loadsavedimage

This command loads a Sensor image of a specific version (WORD) from the archive in SSD to be the next bootable image. If this is an image downgrade, you must issue the **`resetconfig`** command.

Syntax:

```
loadsavedimage WORD
```

Applicable to:

NS-series Sensors

loadsavedimagefrompeer

This command loads a saved Sensor image from the peer Sensor.

Syntax:

```
loadsavedimagefrompeer <Sensor image version>
```

Applicable to:

NS-9300 Sensors

logstat

This command logs certain internal statistics of the Sensor which you can supply to Technical Support using the Manager's **Diagnostics Trace** feature. It is used only for troubleshooting purposes in conjunction with the Technical Support.

Syntax:

```
logstat <all><datapath><mgmt><dos>
```

Parameter	Description
all	Displays all the debug statistics
datapath	Displays the debug statistics for datapath
mgmt	Displays the debug statistics for management processor
dos	Displays the debug statistics for dos

Sample Output:

```
intruShell@john> logstat all

Logstat run:0

Mgmt debug statistics logged
```

Applicable to:

NS-series Sensors

malwarecache

This command enables or disables malware cache for different malware engines.

Syntax:

```
malwarecache (enable|disable) (pdf|flash|gam|gti|ivx|office|tis|all)
```

Sample Output:

```
intruShell@NS9500> malwarecache enable pdf

Malware Cache configuration updated
```

Applicable to:

NS-series Sensors

ntbastat

This command displays the Sensor datapath statistics related to NTBA.

Syntax:

```
set ntbastat [<0-128>] [<0-128>]
```

Sample Output:

```
intruShell@john> ntbastat 15 15

Total netflows created : 0

Templates created : 0

TCP netflows created : 0

UDP netflows created : 0

ICMP netflows created : 0

Total netflows sent : 0

Templates sent : 0

Netflows sent via ring buffer : 0
```

```
Total active netflows : 0

Total free netflow buffers : 1000

Multiple netflows count : 0

Total Dcap L7 fields counts : 0
```

In case of netflow errors, you can see the following details:

```
Total netflows not sent : 0

Erroneous netflows deleted and not sent : 0

Netflows deleted due to other errors and not sent : 0
```

Applicable to:

NS-series Sensors

ping

This command enables you to ping a network host. You can specify either the IPv4 or IPv6 address here. This command pings the Sensor and returns a response with the following values:

Value	Description
icmp_seq	Number of times the Sensor is pinged
ttl	Number of hops between the source and destination
time taken	The average time taken by the Sensor to respond to the ping
packets transmitted	Number of packets transmitted during the ping
packets received	Number of packets received during the ping
packet loss	Number of packets lost during the execution of the command
rtt min/avg/max	Minimum, average and maximum time taken for a round trip in a ping cycle

Syntax:

```
ping <A.B.C.D><A:B:C:D:E:F:G:H> -c <1-100>
```

Parameter	Description
<A.B.C.D>	Denotes the 32-bit IP address written as four eight-bit numbers separated by periods. Each number (A,B,C or D) is an eight-bit number between 0-255.
<A:B:C:D:F:G:H>	Denotes the 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF.
-c <1-100>	Denotes the number of times to ping the Sensor. This is optional and can be used if the Sensor needs to be pinged multiple times.

Sample Output:

- For Sensor, the output is as shown below:

```
intruShell@fc_4050> ping 172.16.100.100
PING 172.16.100.100 with 32[60] bytes of data
40 bytes from host 172.16.100.100: icmp_seq=1 ttl=64 time taken 0.30 msec
--- 172.16.100.100 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0.30ms
rtt min/avg/max = 0.30/0.30/0.30 msec
```

- For Sensor, when it is pinged multiple times, the output is as shown below:

```
intruShell@fc_4050> ping 172.16.100.100 -c 3
PING 172.16.100.100 with 32[60] bytes of data
40 bytes from host 172.16.100.100: icmp_seq=1 ttl=64 time taken 0.41 msec
40 bytes from host 172.16.100.100: icmp_seq=2 ttl=64 time taken 0.20 msec
40 bytes from host 172.16.100.100: icmp_seq=3 ttl=64 time taken 0.19 msec
--- 172.16.100.100 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 0.80ms
rtt min/avg/max = 0.19/0.26/0.41 msec
```

Example:

The following command pings a 128 bit address written as an octet of four hexadecimal numbers.

```
ping 2001:0db8:8a2e:0000:0000:0000:0000:0111
```

Applicable to:

NS-series Sensors

pktcapture-circular attack-id

This command sets the global attack-id to stop circular packet capture.

Syntax:

```
pktcapture-circular attack-id <attack id>
```

Parameter	Description
`<attack id>`	Enter the attack id

To set the global attack id:

Sample Output:

```
intruShell@NS7350> pktcapture-circular attack-id 0x48436b00
global attack id : 0x48436b00
```

To unset the global attack id:

```
intruShell@NS7350> pktcapture-circular attack-id 0

global attack id : 0x0
```

Applicable to:

NS9500 (standalone and stack), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture-circular force-stop

This command is used to stop circular packet capture on the Sensor forcefully.

Syntax:

```
pktcapture-circular force-stop
```

Sample Output:

```
intruShell@NS7350> pktcapture-circular force-stop

Do you want to proceed with stopping packet capture session?

Please enter Y to confirm: Y
```

Applicable to:

NS9500 (standalone and stack), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture-circular intfport

This command continuously captures both incoming and outgoing packets of a monitoring port that match the specified criteria in a circular fashion until stopped. If you have configured the Sensor to receive and send traffic on a single port, you can use this command to capture packets.

The packets are captured by the circular buffer. The circular buffer size varies based on the NS-series or Virtual IPS Sensor. For example, the buffer size for NS9100 is 100MB, the buffer size for VM600 is 58 MB, etc. On reaching the end of the buffer, the oldest or starting packets in buffer are overwritten till the circular packet capture is stopped forcefully. The captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. The saved file is sent to the Manager.

> **NOTE**
>
> If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using this command.

Syntax:

```
pktcapture-circular intfport <monitoring_port> <filter>
```

Parameter	Description
monitoring_port	Port for capturing incoming and outgoing packets. **NOTE** For NS series Sensors (except NS3600), the monitoring ports will be in the format "gx/(x or y)". For the NS3600 Sensor, the monitoring ports will be in the format "x". For Virtual IPS Sensors, the monitoring ports will be in the format "x".
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

Sample Output:

```
intruShell@NS7350-101> pktcapture-circular intfport g1/1 ""

A packet capture file will be sent to the Manager, as per the configuration.

Do you want to proceed with the packet capture session?

Please enter Y to confirm: Y

pktcapture: capture all...
```

Applicable to:

NS9500 (standalone), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture-circular intfport-pair

This command continuously captures both incoming and outgoing packets of monitoring port-pair that match the specified criteria in a circular fashion until stopped. If you have configured the Sensor to receive and send traffic on different ports of monitoring port-pair, you can use this command to capture packets.

The packets are captured by the circular buffer. The circular buffer size varies based on the NS-series or Virtual IPS Sensor. For example, the buffer size for NS9100 is 100MB, the buffer size for VM600 is 58 MB, etc. On reaching the end of the buffer, the

oldest or starting packets in buffer are overwritten till the circular packet capture is stopped forcefully. The captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. The saved file is sent to the Manager.

NOTE

If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using this command.

Syntax:

```
pktcapture-circular intfport-pair <monitoring_port1>-<monitoring_port2> <filter>
```

Parameter	Description
monitoring_port1	Port for capturing incoming packets
monitoring_port2	Port for capturing outgoing packets
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

NOTE

For NS series Sensors (except NS3600), the monitoring ports will be in the format "gx/(x or y)". For the NS3600 Sensor, the monitoring ports will be in the format "x". For Virtual IPS Sensors, the monitoring ports will be in the format "x".

Sample Output:

```
IntruDbg#> pktcapture-circular intfport-pair g1/1-g1/2 ""

A packet capture file will be sent to the Manager, as per the configuration.

Do you want to proceed with the packet capture session?

Please enter Y to confirm: y

pktcapture: capture all...
```

Applicable to:

NS9500 (standalone), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture-circular stack-node

This command continuously captures packets of a NS9500 Sensor configured in stack mode in a circular fashion until stopped. Based on the Sensor configuration, you can capture packets on a single port or in port pair.

The packets are captured by the circular buffer. The buffer size for NS9500 stack is 100MB. On reaching the end of the buffer, the oldest or starting packets in buffer are overwritten till the circular packet capture is stopped forcefully. The captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. The saved file is sent to the Manager.

NOTE

If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using this command.

Syntax

To capture packets on a single port:

```
pktcapture-circular stack-node <stack_node_value> intfport <monitoring_port> <filter>
```

Parameter	Description
stack_node_value	ID of the Sensor in the stack
monitoring_port	Port for capturing incoming and outgoing packets
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

To capture packets in port pair:

```
pktcapture-circular stack-node <stack_node_value> intfport-pair <monitoring_port1>-<monitoring_port2> <filter>
```

Parameter	Description
stack_node_value	ID of the Sensor in the stack

Parameter	Description
monitoring_port1	Port for capturing incoming packets
monitoring_port2	Port for capturing outgoing packets
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

Applicable to:

NS9500 (stack)

pktcapture-force-stop

This command is used to stop packet capture on the Sensor forcefully.

Syntax:

```
pktcapture-force-stop
```

Sample Output:

```
intruShell@NS7350> pktcapture-force-stop

Currently running packet capture session might have been started from Manager.

Do you want to proceed with stopping packet capture session?

Please enter Y to confirm: Y
```

Applicable to:

NS9500 (standalone and stack), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture intfport

This command captures both incoming and outgoing packets of a monitoring port that match the specified criteria. If you have configured the Sensor to receive and send traffic on a single port, you can use this command to capture packets.

The captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. The saved file is sent to the Manager or a SCP server based on the configuration made in the Manager. If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using this command.

NOTE

You can capture packets from the Manager as well. If the Manager is in the process of capturing packets, and at the same time, you run this command, the Sensor will display a message that a packet capture process is already running. Similarly, if you have started packet capture from the CLI, the Manager displays the packet capture **Status** as **Running**. In the Manager, you cannot stop a packet capture session that is started in the CLI and vice-versa. As a best practice, you should start and stop a packet capture session from the same place: either from the CLI or from the Manager.

Syntax:

```
pktcapture intfport <monitoring_port> <filter>
```

Parameter	Description
monitoring_port	Port for capturing incoming and outgoing packets **NOTE** For NS series Sensors (except NS3600), the monitoring ports will be in the format "gx/(x or y)". For the NS3600 Sensor, the monitoring ports will be in the format "x". For Virtual IPS Sensors, the monitoring ports will be in the format "x".
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

Sample Output:

```
intruShell@john> pktcapture intfport g3/1 ""

Packet capture file will be sent to SCP server, as per configuration.

Do you want to proceed with packet capture session?
```

```
Tip: Press "ctrl+k" to terminate a packet capture session.

Please enter Y to confirm: y

pktcapture: capture all...

07:43:16.059394 IP 1.1.1.10.80 > 1.1.1.9.56572: Flags [S.], seq 3430348442, ack 3733665626, win
14480, options [mss 1460,sackOK,TS val 3851607 ecr 4205050,nop,wscale 6], length 0

07:43:16.059400 IP 1.1.1.10.80 > 1.1.1.9.56572: Flags [.], ack 105, win 227, options [nop,nop,TS val
3851609 ecr 4205052], length 0
```

Applicable to:

NS9500 (standalone), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture intfport-pair

This command captures incoming and outgoing packets on different monitoring ports that match the specified criteria. If you have configured the Sensor to receive and send traffic on different ports, you can use this command to capture packets.

The captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. The saved file is sent to the Manager or a SCP server based on the configuration made in the Manager. If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using this command.

> **NOTE**
>
> You can capture packets from the Manager as well. If the Manager is in the process of capturing packets, and at the same time, you run this command, the Sensor will display a message that a packet capture process is already running. Similarly, if you have started packet capture from the CLI, the Manager displays the packet capture **Status** as **Running**. In the Manager, you cannot stop a packet capture session that is started in the CLI and vice-versa. As a best practice, you should start and stop a packet capture session from the same place: either from the CLI or from the Manager.

Syntax:

```
pktcapture intfport-pair <monitoring_port1>-<monitoring_port2> <filter>
```

Parameter	Description
monitoring_port1	Port for capturing incoming packets
monitoring_port2	Port for capturing outgoing packets

Parameter	Description
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

NOTE

For NS series Sensors (except NS3600), the monitoring ports will be in the format "gx/(x or y)". For the NS3600 Sensor, the monitoring ports will be in the format "x". For Virtual IPS Sensors, the monitoring ports will be in the format "x".

Sample Output:

```
intruShell@john> pktcapture intfport-pair g3/1-g3/2 ""

Packet capture file will be sent to SCP server, as per configuration.

Do you want to proceed with packet capture session?

Tip: Press "ctrl+k" to terminate a packet capture session.

Please enter Y to confirm: y

pktcapture: capture all...

08:26:47.784115 IP 1.1.1.9.50573 > 1.1.1.10.80: Flags [S], seq 101908577, win 14600, options [mss 1460,sackOK,TS val 2478593938 ecr 0,nop,wscale 6], length 0

08:26:47.784117 IP 1.1.1.9.50573 > 1.1.1.10.80: Flags [.], ack 4187117816, win 229, options [nop,nop,TS val 2478593939 ecr 2478581502], length 0
```

Applicable to:

NS9500 (standalone), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture mgmt

This command filters and captures packets of the management port. This command is used to debug various integration or connectivity issues on the Management port.

Syntax:

```
pktcapture mgmt <filter>
```

Parameter	Description
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

Sample Output:

```
intruShell@NS7350> pktcapture mgmt "port 22"

A packet capture file will be sent to the Manager, as per the configuration.

Do you want to proceed with the packet capture session?

Tip: Press "ctrl+k" to terminate a packet capture session.

Please enter Y to confirm: Y

09:42:57.698177 IP 10.20.24.24.5137 > 10.1.1.8.22: Flags [S], seq 2072890780, win 64960, options
[mss 1160,nop,wscale 8,nop,nop,sackOK], length 0

09:42:57.698232 IP 10.213.171.81.22 > 10.20.24.24.5137: Flags [S.], seq 2938926341, ack 2072890781,
win 29200, options [mss 1460], length 0

09:42:57.725049 IP 10.20.24.24.5137 > 10.1.1.8.22: Flags [.], ack 1, win 64960, length 0
```

Applicable to:

NS9500 (standalone and stack), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

pktcapture stack-node

This command captures packets of a NS9500 Sensor configured in stack mode. Based on the Sensor configuration, you can capture packets on a single port or in port pair.

The captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. The saved file is sent to the Manager or a SCP server based on the configuration made in the Manager. If you have configured the Manager to send captured packets to a SPAN port, you cannot capture packets by using this command.

NOTE

You can capture packets from the Manager as well. If the Manager is in the process of capturing packets, and at the same time, you run this command, the Sensor will display a message that a packet capture process is already running. Similarly, if you have started packet capture from the CLI, the Manager displays the packet capture **Status** as **Running**. In the Manager, you cannot stop a packet capture session that is started in the CLI and vice-versa. As a best practice, you should start and stop a packet capture session from the same place: either from the CLI or from the Manager.

Syntax

To capture packets on a single port:

```
pktcapture stack-node <stack_node_value> intfport <monitoring_port> <filter>
```

Parameter	Description
stack_node_value	ID of the Sensor in the stack
monitoring_port	Port for capturing incoming and outgoing packets
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

To capture packets in port pair:

```
pktcapture stack-node <stack_node_value> intfport-pair <monitoring_port1>-<monitoring_port2> <filter>
```

Parameter	Description
stack_node_value	ID of the Sensor in the stack
monitoring_port1	Port for capturing incoming packets
monitoring_port2	Port for capturing outgoing packets

Parameter	Description
filter	BPF (Berkeley Packet Filter) for capturing packets. If no filter is provided, all packets are captured. **NOTE** If you do not want to provide a filter, use an empty string ("") as the parameter value. **NOTE** For high throughput devices, when capturing from the Manager, ensure filters are provided such that not more than 2 Gbps of traffic is captured.

Applicable to:

NS9500 (stack)

pktcapturefile

This command uploads the packet capture file to a SCP server or deletes a packet capture file from the Sensor. The action to upload or delete is passed as a parameter to this command.

NOTE

Before running the command, you should configure a valid SCP server. You can configure a SCP server by using **`set scpserver ip`** command. For example:

```
set scpserver ip 192.168.1.1
```

For more information, see set scpserver ip (page 1940).

Syntax:

`pktcapturefile <upload/discard>`

Parameter	Description
upload	Uploads a packet capture file to the SCP server. By default, the captured packets are saved in the `/tftpboot/capture.pcap` file on the Sensor. This command uploads the `capture.pcap` file to the SCP server and deletes the file from the `/tftpboot` directory after the upload.
discard	Deletes the `/tftpboot/capture.pcap` packet capture file in the Sensor.

Sample Output:

```
IntruDbg#> pktcapturefile upload

uploading capture file to scp server 192.168.1.15...

Please enter the SCP User Name : root

Transfer Successful
```

Applicable to:

NS9500 (standalone and stack), NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, NS3x00 series, and Virtual IPS Sensors.

quit

This command enables you to exit the command line interface.

This command has no parameters.

Syntax:

```
quit
```

Applicable to:

NS-series Sensors

raidrepair

This command repairs the RAID1 SSD component exhibiting a fault. Select **`raidrepair current <ssd0|ssd1>`** to repair the faulty SSD within the Sensor.

Select **`raidrepair new <ssd0|ssd1>`** to replace the faulty SSD with a new SSD, and to restore the data on RAID1 it synchronizes the data of the healthy SSD with the new SSD.

> **NOTE**
>
> RAID is not supported on NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3500, and NS3x00 Sensors.

Syntax:

```
raidrepair <new|current> <ssd0|ssd1>
```

Parameter	Description
new	When a complete reimage of a single disk is required
current	When the disk is corrupted
ssd0	Disk is located in the upper bay within the chassis.
ssd1	Disk is located in the lower bay within the chassis.

Applicable to:

NS9500, NS9300, NS9200, and NS9100 Sensors

reboot

This command is used to reboot a device. You must confirm that you want to reboot the device. If hitless reboot is currently available for the device, you are prompted to enter 'h' for hitless and 'y' for a full reboot. Use the **status** command to know if the hitless reboot option is currently available for the device.

> **NOTE**
>
> In case of a full reboot, all the processes of a device are restarted. So, there is a break in the device's function until it comes up again. In case of hitless reboot, only the required processes are restarted. For more information on hitless reboot, see the topic *How to reboot devices* in the *IPS Administration* section.

For NS-series Sensors, you must do a full reboot as hitless reboot is not supported when SSL decryption is enabled.

Syntax:

```
reboot
```

On executing the command for Sensor, the following messages are displayed in the output:

```
intruShell@john> reboot

Please enter Y to confirm: y

rebooting the Sensor...

Broadcast message from root (Fri Mar 29 05:45:14 2014):

The system is going down for reboot NOW!
```

Applicable to:

NS-series Sensors

reconnectalertandpktlogchannels

This command re-establishes the alert and packet log channel connection (broken by issuing a **disconnectalertandpktlog-channels** command) between the Sensor and Manager. The connection can only be re-established when the trust between the Sensor and Manager is not broken (for example, a deinstall breaks trust as well as disconnects the alert and packet log channel and issuing the **reconnectalertandpktlogchannels** command will not re-establish connectivity if the certificates establishing trust between the Sensor and Manager are cleared).

This command has no parameters.

Syntax:

```
reconnectalertandpktlogchannels
```

On executing the command, the following message is displayed:

```
this will take a couple of seconds , please check status on CLI
```

Applicable to:

NS-series Sensors

rescuedisk

The **rescuedisk** command must be executed only during an actual Sensor rescue procedure. This command reformats the SSD and loads a Sensor image of this (WORD) version from the internal flash device onto the SSD. This will be the next bootable image.

> **CAUTION**
>
> Do not execute this command when the Sensor is in good health.

Syntax:

```
rescuedisk <rescue image>
```

> **NOTE**
>
> You can find the rescue images using **show rescueimages** command.

Sample Output:

```
WARNING ... THIS COMMAND WILL REFORMAT YOUR SSD ..?

Please enter Y to confirm:
```

Applicable to:

NS-series Sensors

resetconfig

This command resets all configuration values to their defaults. It deletes or resets values as described in the following table. This command causes an automatic reboot of the Sensor. You must confirm that you want to reboot the Sensor.

Deleted Values	Values Reset to Defaults
• Manager address (and secondary interface's IP address, if configured). This can be IPv4 or IPv6 address. • Certificates establishing trust between Sensor and Manager (shared key value) • Signatures • TFTP server IP address (IPv4 or IPv6 address) • SCP server IP address (IPv4 or IPv6 address) • DoS profile files (learned DoS behavior) • SSL Key • Exception Object • ACL • Advanced Setting	• Monitoring and Response port settings • Management port settings • Manager Install port value • Manager Alert port value • Manager Log port value

This command has no parameters.

Syntax:

`resetconfig`

Applicable to:

NS-Series Sensors

secureerase

The **`secureerase`** command ensures that all data stored on the internal flash is erased and made inaccessible by reformatting the internal flash and rewriting it with random data.

This command has no parameters.

> **NOTE**
> After executing this command, the Sensor reboots automatically.

Syntax:

`secureerase`

The following prompt appears to confirm the erase.

```
WARNING: This command will erase all content and make the sensor inaccessible.
You must install a new image(via netboot or external rescueflash) to
reuse this sensor again.
Do you really want to proceed? Enter 'y' to proceed or 'n' to stop:
```

If you enter **Y**, the data erase continues.

Applicable to:

NS-series Sensors

sensor perf-debug

This command activates the performance debugging on the Sensor for a specified time.

Syntax:

`sensor perf-debug<time in minutes>`

Parameter	Description
time in minutes	Denotes the number of minutes for activating the performance debugging on the Sensor

Applicable to:

NS-series Sensors

sensor perf-debug off

The **`sensor perf-debug off`** command de-activates the performance debugging on the Sensor for a specified time. This command does not clear all the temporary performance debug statistics that are created. It only turns off debugging and the Sensor switches to the normal processing mode.

This command has no parameters.

Syntax:

`sensor perf-debug off`

Applicable to:

NS-series Sensors

sensor perf-debug status

The **`sensor perf-debug status`** command displays the status of the performance debug.

This command has no parameters.

Syntax:

`sensor perf-debug status`

Sample Output:

```
intruShell@john> sensor perf-debug status

perf-debug status : on
```

Applicable to:

NS-series Sensors

sensor-datapath-stat-analysis log

This command logs the analysis of various Sensor datapath statistics into the Sensor log file.

Syntax:

```
sensor-datapath-stat-analysis log
```

Applicable to:

NS-series Sensors

sensor-datapath-stat-analysis show

This command displays the analysis of various Sensor datapath statistics.

Syntax:

```
sensor-datapath-stat-analysis show
```

Sample Output:

```
intruShell@john> sensor-datapath-stat-analysis show

Total pkts received :32130

Total TCP pkts :29682

Total UDP pkts :2430

Total non TCP/UDP pkts :18

Total fragments :0

Total duplicate fragments :0

Total attack detected :7

Total alert generated :8

Total alerts dropped without response :0

Total alerts dropped because of filter setting :0

Total logs sent :9

Total pkts matching L3/L4 UDS :0

Policy Ruleset on Sensor :Default Inline IPS

**Analysis of the statistics**

Attack dropped without response action :0.0000%

Attack dropped because of filter setting :0.0000%
```

```
Traffic detected with attack :0.0218%

Fragmented traffic :0.0000%

TCP Traffic :92.3810%

UDP Traffic :7.5630%

Non TCP/UDP Traffic :0.0560%

Traffic matching L3/L4 UDS :0.0000%

Count of fragments is ZERO

Percentage of logs to alerts sent :112.5000%

Snort signature support enabled
```

Applicable to:

NS-series Sensors

sensor-scan-during-update

This command enables, disables, or shows status of hyperscan during signature files update.

Syntax:

```
sensor-scan-during-update-<enable>|<disable>|<show>
```

Parameter	Description
<enable>	Enables hyperscan during signature files update
<disable>	Disables hyperscan during signature files update
<show>	Shows status of hyperscan during signature files update

Sample Output:

```
intruShell@john> sensor-scan-during-update-show

Hyper scan status is ENABLED
```

Example:

```
sensor-scan-during-update-show
```

Applicable to:

NS-series Sensors

sensordroppktevent

This command enables or disables the monitoring of Sensor load. Whenever the Sensor is overloaded and drops a large number of packets, a system fault is raised in the Manager.

Syntax:

`sensordroppktevent <disable><enable>`

Parameter	Description
<disable>	Disables the monitoring of Sensor load
<enable>	Enables the monitoring of Sensor load. When the Sensor load monitoring is enabled, a critical fault "Sensor Dropping Packets Internally" is displayed on the **Faults** tab in the **Logs** page of the Manager if the Sensor drops packets continuously for 9 seconds or more,. If the packet drop continues, another system fault is generated after every minute. Trellix IPS raises subsequent faults only if the packet loss is continuously present for the entire minute.

Default Value:

Disabled

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

set

The **`set`** command is used to configure the Sensor's name and network information.

Syntax:

`set <command> <value>`

The **`set`** commands and their values are described individually.

set afo port-pair and dst-mac

This command is used to configure the destination MAC address in the heartbeat packets sent by the Active Fail-Open (AFO) kit. These packets will be used by Sensor to determine the status of the AFO kit.

> **NOTE**
>
> Starting with 10.1 Update 10 release, NS-series Sensor models NS9500 and NS7500 support third-party AFO Bypass Kit solutions. To view the list of supported vendors and their AFO kit models, see KB95945. If you are using these third-party AFO kits or Trellix AFO kits, you do not need to configure the MAC address, as the Sensors (NS9500 and NS7500) can automatically detect the heartbeat packets. The **`set afo`** command is useful only for those using other third-party AFO kits that are not included in KB95945.

Syntax:

`set afo <port-pair | all> dst-mac <destination_mac>`

Parameter	Description
<port-pair>	A valid gigabit ethernet monitoring port-pair on the Sensor Valid port-pairs for NS9500, NS7600, NS7500 Sensors are: g0/1-g0/2 |g0/3-g0/4 | g1/1-g1/2 | g1/3-g1/4 | g1/5-g1/6 | g1/7-g1/8 | g2/1-g2/2 | g2/3-g2/4 | g2/5-g2/6 | g2/7-g2/8 | g3/1-g3/2 | g3/3-g3/4 | g3/5-g3/6 | g3/7-g3/8 Valid port-pairs for NS3600 Sensor are: 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 | 13-14
<all>	Includes all the IFO-ACTIVE port-pairs
<destination_mac>	The destination MAC address of the AFO kit which will be used by sensor to determine the status of the AFO kits.

Example 1:

```
intruShell@NS7500> set afo g0/1-g0/2 dst-mac 22:44:66:88:10:12
```

The above command will set the destination MAC address on port-pair g0/1-g0/2.

Example 2:

```
intruShell@NS7500> set afo all dst-mac 22:44:66:88:10:12
```

The above command will set the destination MAC address on all the IFO-ACTIVE port-pairs.

Applicable to:

NS-series Sensors - NS9500, NS7600, NS7500, and NS3600

set attackId list logging

This command is used to enable or disable attack id list logging feature that displays maximum of 5 detected attacks per connection that the Sensor processes. When it is enabled, the Sensor sends a list of attack ids to the Manager via packet logging framework.

Syntax:

```
set attackId list logging <enable|disable>
```

> **NOTE**
>
> To view the status of attack id list logging, you can execute the **`show attackIdList logging status`** command.

Default Value:

disable

Sample Output:

```
intruShell@NS-7200> set attackId list logging enable
```

Applicable to:

NS-Series and Virtual IPS Sensors

set autorecovery

This command disables auto recovery feature even if the Sensor has layer 2 mode is enabled. You can execute this command only if layer2 mode is **On**. When layer 2 mode is **Off**, auto-recovery is always disabled.

You can disable the auto recovery feature for debugging purposes. By disabling the auto recovery feature, the Sensor does not perform auto recovery and remains in layer 2.

> **NOTE**
>
> SSL Decryption are not supported if auto recovery is enabled.

Syntax:

```
set autorecovery <enable|disable>
```

> **NOTE**
>
> If you disable auto recovery, it remains disabled even after disabling and enabling the layer 2 mode. To view the status of auto recovery you can execute the **`show auto recovery status`** command.

Default Value:

enable

Applicable to:

NS-Series Sensors

> **NOTE**
>
> Auto-recovery is not applicable for Virtual IPS Sensors.

set auxport

This command configures the auxiliary port status.

Syntax:

```
set auxport enable
```

```
set auxport disable
```

Applicable to:

NS-series Sensors

set console timeout

The **set console timeout** command specifies the number of minutes of inactivity before the console or SSH session times out.

Syntax:

set console timeout <0 - 1440>

Parameter	Description
<0-1440>	An integer between 0 and 1440. If the value is set to 0, the session will never timeout.

where **<0 - 1440>** is an integer between **0** (never) and **1440** (24 hours).

Example:

set console timeout 60

Default Value:

15 (15 minutes)

Applicable to:

NS-series Sensors

set debugmode passwd

This command configures the CLI Debug mode password.

Syntax:

set debugmode passwd

On executing the command, the following messages are displayed:

Please enter new password:

Please Re-enter new password:

Password successfully changed

Example:

intruShell@john> set debugmode passwd

Please enter new password:

Please Re-enter new password:

Password successfully changed

Applicable to:

NS-series Sensors

set dnsprotect

This command sets the DNS protection mode.

Syntax

```
set dnsprotect <inbound><inbound-outbound><ip-based><off><outbound>
```

Parameter	Description
<inbound>	Sets the DNS protection mode to 'inbound'
<inbound-outbound>	Sets the DNS protection mode to 'inbound-outbound'
<ip-based>	Sets the DNS protection mode to 'ip-based'
<off>	Turns off the DNS protection mode
<outbound>	Sets the DNS protection mode to 'outbound'

Applicable to:

NS-series Sensors

set dospreventionseverity

This command can be used to set the severity for the specified denial-of-service profile. Increasing the DoS prevention severity increases the number of DoS packets dropped.

Syntax:

```
set dospreventionseverity <dos-measure-name> <inbound | outbound> <0-200>
```

Parameter	Description
<dos-measure-name>	Sets the DoS measure name as any one of the following names: 'tcp-syn', 'tcp-syn-ack', 'tcp-fin', 'tcp-rst', 'udp', 'icmp-echo', 'icmp-echo-reply', 'icmp-non-echo-reply', 'ip-fragment',and 'non-tcp-udp-icmp'
<inbound>	Sets the direction to 'inbound'
<outbound>	Sets the direction to 'outbound'
<0-200>	Sets the DoS prevention security

Example:

```
set dospreventionseverity tcp-syn-ack outbound 100
```

Default Value:

30

Applicable to:

NS-Series Sensors

set dpimonitor

This command, when enabled, configures data path attack detection monitoring.

Syntax:

```
set dpimonitor <enable | disable>
```

Default Value:

Disabled

Applicable to:

NS-series Sensors

set dpimonitor-action

The **`set dpimonitor-action`** command configures the action to be performed when the Sensor detects that data path attack detection has stopped. When enabled, the configured default monitor action is taken. If disabled, an alert is raised after the attack detection stops, no further action is taken and the default monitor action settings is ignored.

Syntax:

```
set dpimonitor-action <enable|disable>
```

Applicable to:

NS-series Sensors

set flowvolumelimit enable

This command reports the connections with high volume of data transfer for both inbound and outbound connections. Once a threshold for the flow volume is configured, connections the data transfer of which exceed the configured threshold will be reported using the alert *Flow with high volume has been detected*. Use this command to enable the flow volume limit for both inbound and outbound direction.

Syntax:

```
set flowvolumelimit enable <threshold>
```

Parameter:

Parameter	Description
threshold	The valid range of values for flow volume limit is from 1 to 8192 MB.

Applicable to:

NS-series Sensors

set flowvolumelimit disable

Use this command to disable the flow volume limit for both inbound and outbound direction.

Syntax:

```
set flowvolumelimit disable
```

Applicable to:

NS-series Sensors

set gam-airgap-network

This command allows configuring Gateway Anti-Malware engine initialization in the Sensor within an air gapped network. After executing this command, a Sensor reboot is required for the changes to take effect.

Syntax:

```
set gam-airgap-network <enable | disable>
```

Parameter:

Parameter	Description
`enable`	Enables Gateway Anti-Malware engine initialization in an air gapped network.
`disable`	Disables Gateway Anti-Malware engine initialization in an air gapped network.

Applicable to:

NS-series Sensors

set gigfailopen disable

When this command is executed, the external Fail-open kit will not enter the bypass mode due to link going down, and will continue even when the Sensor is rebooted. The command can be reversed by typing **`set gigfailopendelay <0>`** to enable the bypass mode again.

Syntax:

```
set gigfailopen disable
```

Applicable to:

NS-series Sensors

set gigfailopendelay

This command sets the number of seconds to delay before fail-open kicks in when a gigabit channel loses its link. To display the set value, use the **`show gigfailopendelay`** command.

Syntax:

set gigfailopendelay <0-60>

Parameter	Description
<0-60>	Sets the number of seconds to delay. It is an integer between 0 (no delay) and 60 (60 seconds).

Default Value:

0 (0 second)

Example:

set gigfailopendelay 10

Applicable to:

NS-series Sensors

set hypervisor server ip

This command is used to set the hypervisor server IPv4 or IPv6 address.

Syntax:

set hypervisor server ip

Applicable to:

Virtual IPS Sensors

set inactiveuserslock

This command, when enabled, locks out inactive users. Users not logged in since 35 days are considered as inactive.

By default, the command is disabled.

Syntax:

set inactiveuserslock <enable | disable>

Applicable to:

NS-series Sensors

set intfport id flowcontrol

This command manually enables or disables flow control on the specified gigabit ethernet monitoring port.

Syntax:

set intfport id <port> flowcontrol <on | off>

Parameter	Description
<port>	A valid gigabit ethernet monitoring port on the Sensor Valid port numbers for NS-series are: G0/1 | G0/2 | G1/1 | G1/2 | G1/3 | G1/4 | G1/5 | G1/6 | G1/7 | G1/8 | G1/9 | G1/10 | G1/11 | G1/12 | G2/1 | G2/2 | G2/3 | G2/4 | G2/5 | G2/6 | G2/7 | G2/8 | G2/9 | G2/10 | G2/11 | G2/12 | G3/1 | G3/2 | G3/3 | G3/4 | G3/5 | G3/6 | G3/7 | G3/8
<on>	Enables the flow control on the gigabit ethernet monitoring port
<off>	Disables the flow control on the gigabit ethernet monitoring port

Example:

```
set intfport id G1/2 flowcontrol on
```

Applicable to:

NS-series Sensors

set l2OnDrops

This command configures the settings for Layer 2 mode on drops.

Syntax:

```
set l2OnDrops (enable|disable|sensitivity-level)
```

Parameter	Description
`enable`	Puts the Sensor to Layer 2 mode when high drops are seen
`disable`	Disables Layer 2 mode on drops
`sensitivity-level`	Configures the sensitivity level for Layer 2 mode on drops

Sample Output:

```
intruShell@john> set l2OnDrops enable

intruShell@john> show l2OnDropsConfig

L2OnDrops Stats: Enabled
```

NOTE

To view the status of **`set l2OnDrops`**, provide **`show l2OnDropsConfig`** command.

Applicable to:

NS-series Sensors

NOTE

- The Layer 2 mode must be **'ON'** to configure **`set l2OnDrops (enable|disable|sensitivity-level)`**.
- To automatically restore the Sensor to normal state, configure **`latency-monitor restore-inline`** command. For more information, refer to *latency-monitor restore-inline* (page 1898).
- For more information on **`set l2OnDrops sensitivity-level`** command, refer to *set l2OnDrops sensitivity-level* (page 1932).
- For more information on **`show l2OnDropsConfig`** command, refer to *show l2OnDropsConfig* (page 1993).

set l2OnDrops sensitivity-level

This command configures the sensitivity level for Layer 2 mode on drops.

Syntax:

```
set l2OnDrops sensitivity-level (high|low|medium)
```

Sample Output:

```
intruShell@john> set l2OnDrops sensitivity-level high

intruShell@john> show l2OnDropsConfig

L2OnDrops Sensitivity Level: High
```

NOTE

To view the status of **`set l2OnDrops`**, provide **`show l2OnDropsConfig`** command.

Applicable to:

NS-series Sensors

NOTE

For more information on **`show l2OnDropsConfig`** command, refer to *show l2OnDropsConfig* (page 1993).

set manager alertport

This command specifies the port on which the Manager listens to the Sensor alerts. You can assign any unassigned port for this communication.

If the Sensor and the Manager are separated by a firewall, you must make sure to open the specified port on the firewall. If your Sensor is already installed, deinstall the Sensor before changing this parameter.

Syntax:

```
set manager alertport <0 - 10000>
```

Parameter	Description
<0-10000>	The port number ranging from integer values 0 to 10000.

On executing the command, the following messages are displayed-

- When Sensor is installed:

  `sensor is already installed, please do a deinstall before changing this parameter`

- When Sensor is de-installed:

  `Missing manager alert port, default 8502 used`

Default Value:

Default port number is 8502.

Applicable to:

NS-series Sensors

set manager alertport_RSA-2048-bit

This command specifies the port on which the Manager listens to the Sensor alerts when and Manager and Sensor use 2048-bit encryption. You can assign any unassigned port for this communication.

If the Sensor and the Manager are separated by a firewall, you must make sure to open the specified port on the firewall. If your Sensor is already installed, deinstall the Sensor before changing this parameter.

Syntax:

`set manager alertport_RSA-2048-bit <0 - 10000>`

Parameter	Description
<0-10000>	The port number ranging from integer values 0 to 10,000

Default Value:

Default port number is 8507.

Applicable to:

NS-series Sensors

set manager installsensorport

This command helps specify the port which the Manager uses to exchange configuration information with the Sensor when using 2048 bit encryption. You can assign any unassigned port for this communication.

Syntax:

`set manager installsensorport <0 - 10000>`

Parameter	Description
<0-10000>	The port number ranging from integer values 0 to 10000

On executing the command, the following messages are displayed-

- When Sensor is installed:

  `sensor is already installed, please do a deinstall before changing this parameter`

- When Sensor is de-installed:

  `Missing manager Install Sensor Port, default 8501 used`

Default Value:

Default port number is 8501.

Applicable to:

NS-series Sensors

set manager installsensorport_RSA-2048-bit

This command helps specify the port which the Manager uses to exchange configuration information with the Sensor when using 2048 bit encryption. You can assign any unassigned port for this communication.

If the Sensor and the Manager are separated by a firewall, you must make sure to open the specified port on the firewall. If your Sensor is already installed, deinstall the Sensor before changing this parameter.

Syntax:

`set manager installsensorport_RSA-2048-bit <0 - 10000>`

Parameter	Description
<0-10000>	The port number ranging from integer values 0 to 10,000

Default Value:

Default port number is 8506.

Applicable to:

NS-series Sensors

set manager ip

You can specify the IPv4 or IPv6 address of the Manager server's primary interface using this command.

Syntax:

`set manager ip <A.B.C.D | A:B:C:D:E:F:G:H>`

Parameter	Description
<A.B.C.D>	A 32-bit address written as four eight-bit numbers separated by periods. Each number (A,B,C, or D) represents an eight-bit number between 0-255.
<A:B:C:D:E:F:G:H>	A 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF.

Example:

```
set manager ip 192.34.2.8
```

Or

```
set manager ip 2001:0db8:8a2e:0000:0000:0000:0000:0111
```

NOTE

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::)

Applicable to:

NS-series Sensors

set manager logport

This command helps specify the port on which the Manager listens to the Sensor alerts when and Manager and Sensor use 2048-bit encryption. You can assign any unassigned port for this communication.

If the Sensor and the Manager are separated by a firewall, you must make sure to open the specified port on the firewall. If your Sensor is already installed, deinstall the Sensor before changing this parameter.

Syntax:

```
set manager logport <0 - 10000>
```

Parameter	Description
<0-10000>	The port number ranging from integer values 0 to 10,000

On executing the command, the following messages are displayed-

- When Sensor is installed:

  ```
  sensor is already installed, please do a deinstall before changing this parameter
  ```

- When Sensor is de-installed:

  ```
  Missing manager log port, default 8503 used
  ```

Default Value:

Default port number is 8503.

Applicable to:

NS-series Sensors

set manager logport_RSA-2048-bit

This command helps specify the port on which the Manager listens to the Sensor alerts when and Manager and Sensor use 2048-bit encryption. You can assign any unassigned port for this communication.

If the Sensor and the Manager are separated by a firewall, you must make sure to open the specified port on the firewall. If your Sensor is already installed, deinstall the Sensor before changing this parameter.

Syntax:

```
set manager logport_RSA-2048-bit <0 - 10000>
```

Parameter	Description
<0-10000>	The port number ranging from integer values 0 to 10,000

Default Value:

Default port number is 8508.

Applicable to:

NS-series Sensors

set manager secondary ip

You can specify an IPv4 or IPv6 address for the Manager server's secondary interface using this command.

Syntax:

```
set manager secondary ip <A.B.C.D> | <A:B:C:D:E:F:G:H>
```

Parameter	Description
<A.B.C.D>	A 32-bit address written as four eight-bit numbers separated by periods. Each number (A,B,C, or D) represents an eight-bit number between 0-255.
<A:B:C:D:E:F:G:H>	A 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF.

Example:

```
set manager secondary ip 192.34.2.8
```

Or

```
set manager secondary ip 2001:0db8:8a2e:0000:0000:0000:0000:0111
```

NOTE

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::)

Applicable to:

NS-series Sensors

set mgmtport auto

The **`set mgmtport auto`** command configures the Management port to auto-negotiate the connection between the Sensor and the network device.

This command has no parameters.

Syntax:

```
set mgmtport auto
```

Default Value:

By default, the Management port is set to **auto** (auto-negotiate).

Applicable to:

NS-series Sensors

set mgmtport mtu

You can configure the management port interface Max Transmission Unit (MTU) using this command.

Syntax:

```
set mgmtport mtu <1000-1500>
```

Sample Output:

```
intruShell@john> set mgmtport mtu 1250

MTU set to 1250 for mgmt port
```

Example:

```
intruShell@john> set mgmtport mtu 1000
```

Applicable to:

NS-series Sensors

set mgmtport speed and duplex

This command helps configure the management port to match the speed of the network device connecting to the Sensor and to run in full-duplex or half-duplex mode.

Syntax:

```
set mgmtport speed <10 | 100 | 1000 | 10000> duplex <half | full>
```

Parameter	Description
<10 | 100 | 1000 | 10000>	Sets the speed on the ethernet management port. The speed value can be between 10 and 10000 Mbps depending on the Sensor model used.
<half | full>	Sets the duplex setting on the ethernet management port. Set the value **`half`** for half-duplex and **`full`** for full-duplex.

NOTE

The NS9500, NS7600, and NS7500 Sensor models do not support this command. The speed of the management port in these Sensors is set to **auto** by default.

Default Value:

By default, the management port is set to **auto** (auto-negotiate).

NOTE

Management port speed settings vary depending on the Sensor model used.

NOTE

Availability of half duplex option depends on the management port speed you set. Duplex option is not available in 9100, 9200, and 9300 Sensors.

Applicable to:

NS-series Sensors (except NS9500, NS7600, NS7500, and NS3600)

set mnsconfig

Sensors deployed in mobile networks monitor subscriber traffic and RADIUS accounting traffic that goes out of GGSN to Internet gateway and RADIUS servers. Each mobile device in the network has an IP address. The Sensor parses RADIUS accounting exchanged between GGSN and the RADIUS server and forms an association of IP addresses and subscriber mobile identity details like phone number, IMSI number, and APN. The Sensor also associates the attacks that are detected on the internet traffic with the mobile subscriber identity data and includes them in alerts sent to the Manager.

The following commands are used to enable monitoring RADIUS accounting traffic in mobile networks.

Syntax:

```
set mnsconfig <on | off>
```

Parameter	Description
`on`	Enables capturing and tagging of mobile subscriber data in the alerts sent to the Manager
`off`	Disables capturing and tagging of mobile subscriber data in the alerts sent to the Manager

NOTE

Mobile entries are not persisted across a Sensor reboot.

Default Value:

This feature is disabled by default.

Applicable to:

NS-series Sensors

set mnsconfig radiusLB

This command enables and disables the RADIUS traffic load balancing on the Sensor.

Due to the use of fixed source and destination ports in all RADIUS packets that are exchanged over UDP by the GGSN/RADIUS server, there is a possibility that the Sensor could miss parsing RADIUS accounting traffic at high data rates. Enabling this command prevents such a scenario.

Syntax:

```
set mnsconfig radiusLB <on | off>
```

Parameter	Description
on	Enables RADIUS traffic load balancing
off	Disables RADIUS traffic load balancing

Applicable to:

NS-series Sensors

set nmsuserwriteaccess

This command helps configure read-write access for third part NMS users.

Syntax

```
set nmsuserwriteaccess <enable|disable>
```

Parameter	Description
enable	Enables read-write access to third party NMS users
disable	Disables read-write access to third party NMS users

When enabled, the above command would activate restricted read-write access to the Host Quarantine Group section of the MIB tree. This restricted read-write access would be made available to all the configured NMS third party users.

Applicable to:

NS-series Sensors

set portsettletime

The Sensor enables inline port pairs to act as a true 'wire'. This means that when one port in a pair is DOWN, its peer will also be brought DOWN, and vice versa — when one is UP, its peer will also be brought UP (contingent upon the status of the device to which it is connected). This is achieved via the **`set portsettletime`** command, which enables you to specify the "settle time" for the ports. When a port is enabled and is not UP for a duration equal to the port settling time, the port is considered DOWN.

Since different switches take different amounts of time to negotiate, you must configure this value to a time period appropriate for your network. This value applies to all ports in the Sensor. Wire mode functionality is not enforced during the port settle time.

Syntax:

```
set portsettletime <seconds>
```

Parameter	Description
<seconds>	Indicates the number of seconds between 0 and 300

Default Value:

The default value of is 30 (30 seconds).

Applicable to:

NS-series Sensors

set scpserver ip

You can specify the IPv4 or IPv6 address of your SCP server using this command.

Syntax:

```
set scpserver ip <A.B.C.D> | <A:B:C:D:E:F:G:H>
```

Parameter	Description
<A.B.C.D>	Indicates a 32-bit address written as four eight-bit numbers separated by periods. Each number (A,B,C, or D) represents an eight-bit number between 0-255.
<A:B:C:D:E:F:G:H>	Indicates a 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF.

Applicable to:

NS-series Sensors

set sensor gateway

This command helps specify IPv4 address of the gateway for the Manager server.

Syntax:

```
set sensor gateway <A.B.C.D>
```

Parameter	Description
<A.B.C.D>	A 32-bit address written as four eight-bit numbers separated by periods. Each number (A,B,C, or D) represents an eight-bit number between 0-255.

Sample Output:

For Sensor, the output is as shown below:

```
intruShell@john> set sensor gateway 10.213.174.201

sensor gateway = 10.213.174.201
```

Example:

```
set sensor gateway 192.34.2.8
```

Applicable to:

NS-series Sensors

set sensor gateway-ipv6

This command helps specify the IPv6 address of the gateway for the Manager server.

Syntax:

```
set sensor gateway-ipv6 <A:B:C:D:E:F:G:H>
```

Parameter	Description
<A:B:C:D:E:F:G:H>	A 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF.

Example:

```
set sensor gateway-ipv6 2001:0db8:8a2e:0000:0000:0000:0000:0111
```

NOTE

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::). For example, **`set sensor gateway-ipv6 2001:0db8:8a2e::0111`**

Applicable to:

NS-series Sensors

set sensor ip

You can specify the Sensor's IPv4 address and subnet mask using this command. Changing the Sensor IP requires a Sensor reboot for the changes to take effect. See the **`reboot`** command for instructions on how to reboot the Sensor.

Syntax:

set sensor ip <A.B.C.D E.F.G.H>

Parameter	Description
<A.B.C.D E.F.G.H>	Indicates an IPv4 address followed by a netmask. The netmask strips the host ID from the IP address, leaving only the network ID. Each netmask consists of binary ones (decimal 255) to mask the network ID and binary zeroes (decimal 0) to retain the host ID of the IP address (For example, the default netmask setting for a Class C address is 255.255.255.0).

Sample Output:

For Sensor, the output is as shown below:

```
intruShell@john> set sensor ip 10.213.168.169 255.255.255.0

Sensor IP is already set, new IP will take effect after a reboot

sensor ipv4 = 10.213.168.169, sensor subnet mask = 255.255.255.0
```

Example:

```
set sensor ip 192.34.2.8 255.255.0.0
```

Applicable to:

NS-series Sensors

set sensor ipv6

You can set the Sensor's IPv6 address and subnet mask using this command.

Syntax:

set sensor ipv6 <A:B:C:D:E:F:G:H/I>

Parameter	Description
<A:B:C:D E:F:G.H/I>	Indicates a 64-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF. This is followed by a prefix length I with value between 0 and 128.

Example:

set sensor ipv6 2001:0db8:8a2e:0000:0000:0000:0000:0111/64

NOTE

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::). For example: **set sensor ipv6 2001:0db8:8a2e::0111/64**

Applicable to:

NS-series Sensors

set sensor mode

This command is used to set the operational mode of an NS9500 Sensor. This command takes the following parameters:

Parameter	Description
stack	The Sensor works as part of a stack.
standalone	The Sensor works as standalone.

Syntax:

set sensor mode <stack|standalone>

Applicable to:

NS9500 Sensors only

set sensor name

This command enables you to set the name of the Sensor. This name is used to identify the Sensor to the Manager and to identify the Sensor to the admin in the Manager interface. The name you use here in the CLI to identify the Sensor must match the name you use in the Manager interface, or the Manager and Sensor will be unable to communicate.

Syntax:

set sensor name <WORD> <NODE ID>

Parameter	Description
<WORD>	Indicates a case-sensitive character string up to 25 characters. The string can include hyphens, underscores, and periods, and must begin with a letter.
<NODE ID>	Indicates the node ID of the Sensor if it is part of a stack.

Sample Output:

On executing the command, the following messages are displayed-

- When Sensor is installed:

  sensor is already installed, please do a deinstall before changing this parameter

- When Sensor is de-installed:
  - **intruShell@john> set sensor name admin**

    sensor name = admin

Example:

set sensor name SanJose_Sensor1

Applicable to:

NS-series Sensors

set sensor sharedsecretkey

This command helps specify the shared secret key value that the Manager and Sensor will use to establish a trust relationship.

Type the command as shown in the Syntax below. The Sensor prompts you for a secret key value. The value you enter is not shown. You will be prompted to type the value a second time to verify that the two entries match.

> **NOTE**
>
> The **sharedsecretkey** value you use here in the CLI to identify the Sensor must match the one you use in the Manager interface; or else the Manager and Sensor will be unable to communicate. If you want to change the value, you must change the value in the CLI as well as the manager interface.

Syntax:

```
set sensor sharedsecretkey
```

At the Sensor's prompt for a secret key value, enter a case-sensitive character string between 8 and 25 characters of any ASCII text.

Sample Output:

On executing the command, the following messages are displayed-

- When the Sensor is installed:

  ```
  sensor is already installed, please do a deinstall before changing this parameter
  ```

- When Sensor is de-installed:
  - ```
    intruShell@john> set sensor shared secretkey
    Please enter shared secret key:
    Please Re-enter shared secret key:
    This will take a couple of seconds, please check status on CLI
    ```

Applicable to:

NS-series Sensors

set sessionlimit timeout

Use this command to set a time limit for a user session.

Syntax:

```
set sessionlimit timeout <0-24>
```

The valid range of values for a session are from 0 to 24 hours.

For example, if the session time limit is set to 9 hours, the session is automatically closed once the user has worked on the session for 9 hours.

If the parameter is set as 0, the session timeout does not happen unless the user closes the session.
```

NOTE

The session timeout set is saved and is the same value when the Sensor comes up the next time.

NOTE

The timeout value set is applicable to all users.

Applicable to:

NS-series Sensors

set sshinactivetimeout

This command enables users to configure the CLI SSH login timeout in seconds.

Syntax:

```
set sshinactivetimeout <30-300>
```

The valid range of values for a timeout are from 30 to 300 seconds.

If you are not able to login within the configured time, the login session is automatically closed.

NOTE

The configured value is saved in the Sensor and does not change if the Sensor reboots. The timeout value set is applicable to all users.

Applicable to:

NS-series Sensors

set stack name WORD

This command defines the position of the member sensor in the stack. The stack name should be set along with nodeid. For example: abc-1, abc-2 and so on.

Syntax:

```
set stack name WORD nodeid <1-8>
```

Applicable to:

NS-9500 Sensors

set syncookietcpreset

This command enables users to enable or disable the TCP reset setting.

Syntax:

```
set syncookietcpreset <on | off>
```

Sample output:

- `intruShell@john> set syncookietcpreset on`
  `value on`
- `intruShell@john> set syncookietcpreset off`
  `value off`

Applicable to:

NS-series Sensors

set ta wakeup port

This command enables you to set the wake-up port for Trellix Agent.

Syntax

```
set ta wakeup port [<1-65536>]
```

Applicable to:

NS-series Sensors

set tacacsauthorization

TACACS+ authorization feature provides authorization to access Sensor CLI by matching the service name in the TACACS server with the service name on the Sensor.The Sensor CLI access is given only when there is a matching service name.

The TACACS+ user is allowed to log into the Sensor CLI using his credentials and the session is created using a unique Sensor generated UID, whether authorization is enabled or disabled. Any local database file created for TACACS+ users at the Sensor is not persisted; after reboot, the database entries are created as and when the TACACS+ users login.

The audit log has all the operations performed by the TACACS+ user tagged to the user name.

The **`set tacacsauthorization`** command is used to set the TACACS+ authorization feature.

Syntax:

```
set tacacsauthorization <enable|disable>
```

Parameter	Description
<enable>	Enables the TACACS+ authorization feature
<disable>	Disables the TACACS+ authorization feature

Default Value:

Disable

Applicable to:

NS-series Sensors

set tcpudpchecksumerror drop

The Sensor re-computes TCP and UDP header checksums to determine if their corresponding packets have been corrupted. If the checksum fails, the packet is dropped. This is standard Sensor behavior.

This command has no parameters.

Syntax:

```
set tcpudpchecksumerror drop
```

Applicable to:

NS-series Sensors

set tcpudpchecksumerror forward

When executed, this command prevents the Sensor from dropping the TCP/UDP/ICMP checksum error packets. The Sensor re-computes TCP, UDP and ICMP header checksums to determine if their corresponding packets have been corrupted. If the checksum fails, the packet is dropped. This is standard Sensor behavior.

The **`set tcpudpchecksumerror forward`** command overrides the check, and is useful in situations where the Sensor is located on segments where the IP options Loose Source Record Routing (LSRR) or Strict Source Routing are enabled, which produce valid traffic with invalid checksums that the Sensor would otherwise drop.

This command has no parameters.

Syntax:

```
set tcpudpchecksumerror forward
```

Default Value:

This feature is disabled by default. The Sensor is set to drop packets with invalid headers (that is, the value is set to **`set tcpudpchecksumerror drop`**).

Applicable to:

NS-series Sensors

set tftpserver ip

This command helps specify the IPv4 or IPv6 address of your TFTP server.

Syntax:

```
set tftpserver ip <A.B.C.D> | <A:B:C:D:E:F:G:H>
```

Parameter	Description
<A.B.C.D>	Indicates a 32-bit address written as four eight-bit numbers separated by periods. Each number (A,B,C, or D) represents an eight-bit number between 0-255.
<A:B:C:D:E:F:G:H>	Indicates a 128-bit address written as octet (eight groups) of four hexadecimal numbers, separated by colons. Each group (A,B,C,D, etc.) represents a group of hexadecimal numbers between 0000-FFFF.

Sample Output:

For Sensor, the output is as shown below:

```
intruShell@john> set tftpserver ip 192.34.5.12

TFTP Server IP = 192.34.5.12
```

Example:

```
set tftpserver ip 192.34.2.54
```

Or,

```
set tftpserver ip 2001:0db8:8a2e:0000:0000:0000:0000:0111
```

NOTE

If one or more four-digit group(s) is 0000, the zeros may be omitted and replaced with two colons (::).

Applicable to:

NS-series Sensors

set tiscachepurge interval hours

This command is used to configure the time interval for tiscachepurge feature. The default time interval for purging of Intelligent Sandbox entries is 24 hours. However, the time interval can be configured between 1 hour to 192 hours using the following command.

Syntax:

```
set tiscachepurge interval hours <1-192>
```

Applicable to:

NS-series Sensors

set userconfigvolumedosthreshold

This command enables users to set a DoS threshold for alerting on volume for a particular packet type.

Syntax:

```
set userconfigvolumedosthreshold <dos-measure-name> <direction>
```

Parameter	Description
<dos-measure-name>	Indicates the DoS measure name: one of 'tcp-syn', 'tcp-syn-ack', 'tcp-fin', 'tcp-rst', 'udp', 'icmp-echo', 'icmp-echo-reply', 'icmp-non-echo-reply', 'ip-fragment', 'non-tcp-udp-icmp'
<direction>	Indicates the direction. It can be 'inbound' or 'outbound'.

Example:

```
set userconfigvolumedosthreshold tcp-syn outbound
```

Applicable to:

NS-series Sensors

set vlanbasedrecon

Trellix IPS supports VLAN based reconnaissance attack detection. By default, this option is disabled. When this option is enabled, the reconnaissance attack detection is done on both VLAN and VIDS.

Trellix recommends that you enable this option only if you want the reconnaissance attack detection to be done on a VLAN basis.

Syntax:

```
set vlanbasedrecon <enable|disable>
```

Parameter	Description
enable	Enables VLAN based reconnaissance
disable	Disables VLAN based reconnaissance

Applicable to:

NS9x00 Sensors

setfailopencfg restore-inline

Sensor port pairs deployed in the inline fail-open mode, that is, connected to external passive fail-open kits and, port pairs with built-in fail-open support, are disabled when they go into the bypass mode due to external network link-down events. You can configure to periodically restore all such port pairs from bypass to inline mode using the **`setfailopencfg restore-inline`** command.

> **NOTE**
>
> This feature is not supported for active fail-open kits.

When enabled, the Sensor attempts to restore a port pair from bypass to inline mode periodically according to the configured interval. Thi

Syntax:

```
setfailopencfg restore-inline <enable|disable>
```

Default Value:

Disabled

Applicable to:

NS-series Sensors

setfailopencfg restore-inline-interval

This command enables users to configure the time interval to restore port from bypass to inline mode.

Syntax:

`setfailopencfg restore-inline-interval <5-60 minutes>`

Parameter	Description
5-60 minutes	Time interval (in minutes) at which the Sensor attempts to restore a port-pair from bypass to inline. Default is 5 minutes.

Applicable to:

NS-series Sensors

setfailopencfg internal/external-failopen bypass/inline

This command enables users to configure the behavior of the port pair after Sensor reboot.

`setfailopencfg internal/external-failopen bypass/inline`

Parameter	Description
inline	If the Sensor has a link down and is rebooted (**`setfailopencfg restore-inline`** is disabled/enabled, but is not triggered at the time of reboot), the port-pair restores itself into inline state (by getting enabled and coming up).
bypass	The port pairs stay in the bypass mode (by staying disabled and not coming up).

This configuration is persisted across Sensor reboots.

For the port pairs to be restored from bypass to inline mode, the following conditions should be met:

- The operating mode is inline-fail-open (fail-open support is built in or passive fail-open kits are connected).
- If a passive fail-open kit is used, the kit is connected to the Sensor.
- If the port pair goes into the bypass mode due to monitoring port link down or a missing cable.

When this feature is enabled or you change the time interval, the Sensor checks and attempts to restore the port pairs to the inline mode immediately. Consider the following scenarios.

Scenario1: Change of time interval

The feature is enabled at 11.00 with the default time interval of 5 minutes At 11.03, the port link goes down for a few milliseconds and is then restored. At 11.04, the time interval is changed to 10 minutes. The Sensor checks the port pair and

restores the port pair to the inline mode at 11.14. Subsequently, the Sensor checks the port pairs every 10 minutes (unless the time interval is changed again), that is, the next attempt to restore from bypass to inline mode takes place at 11.24.

Scenario 2: Feature enabled/disabled

The feature is enabled at 11.00 with a default time interval of 5 minutes. At 11.03, the port link goes down for a few milliseconds and is then restored. At 11.04, the feature is disabled. At 11.05, the port pair is admin down. The feature is enabled at 11:07, the Sensor checks the port pair but restores the port pair to the inline mode at 11:12.

NOTE

If you manually disable the port's administrative status, the port continues to remain in the bypass mode even though this feature is enabled.

The Sensor sends a notification to the Manager with a revised timestamp for every failed attempt to restore a port pair from bypass to the inline mode (typically due to link negotiation failure with peer devices). If the restore to inline from bypass operation is successful, the Manager clears prior (bypass) notifications, if any, for that port pair.

setup

This command is used to setup Sensor parameters. You are required to run this command when you newly set up your Sensor or after resetting the Sensor by using the **`factorydefaults`** command.

This command has no parameters.

Syntax:

`setup`

When you enter this command, you are prompted to enter the following:

- Current password
- New password
- System mode

  NOTE

  System mode is available only for the NS9500 Sensors.

- Sensor name
- IP Type (IPv4=1 or IPv6=2 or BOTH=3)
- Sensor IP (IPv4 or IPv6 address or BOTH)
- Sensor subnet mask (IP address)
- Manager primary IP (IPv4 or IPv6 address or BOTH)
- Manager secondary IP (IPv4 or IPv6 address or BOTH)
- Sensor default gateway (IPv4 or IPv6 address or BOTH)

- Management port configuration choice (a/m)
- Shared secret key

> **NOTE**
>
> If you press the **Enter** button, your current settings are taken as default.

Applicable to:

NS-series Sensors

How to change your password

You will be prompted to enter your password when you first logon after entering the **`setup`** command.

1. Type **`setup`** at the prompt.
2. Enter your **current password**.
3. Enter your **new password**.

> **NOTE**
>
> Pressing **Enter** will retain your current password. If you enter a new password you will be asked to confirm the password.

> **NOTE**
>
> If two entries of the password entered does not match or the password is not of minimum length of 8 characters, you will be brought back to the prompt.

How to set the system mode

After entering the password, you will be prompted to select the system mode for the Sensor. The choices for system mode is displayed in the () brackets. The current system mode is displayed in [] brackets.

```
Please select system mode (standalone=1 or stack=2) [standalone =1]:
```

> **NOTE**
>
> Changing the system mode will result in resetting the Sensor configurations and rebooting the Sensor at the end of **`setup`** command.

> **NOTE**
>
> Setting the system mode is applicable only to the NS9500 Sensor.

How to set the Sensor name

After you have entered the password, you are prompted to enter your Sensor name. Your default Sensor name is displayed in the [ ] brackets.

```
Please enter the Sensor name [Sensor_name]:
```

Configuration of the Sensor setup

You can configure the Sensor setup depending on the type of IP address.

- IPv4
- IPv6
- Both IPv4 and IPv6

Configuring the Sensor setup for IPv4 address:

You are prompted if you enter the IP Type as 1. Your default Sensor IPv4 address is displayed in the [ ] brackets. The following prompts are displayed.

```
Please enter the Sensor IP ( A.B.C.D ) [ Sensor_IPv4address ]:

Please enter the Sensor subnet mask ( A.B.C.D ) [Sensor_subnet_mask_IPaddress]:

Please enter the Manager primary IPv4 address ( A.B.C.D ) [ Manager_IPaddress ]:

**You can set the Manager secondary IP in case the Manager has two interfaces**

Press Y to configure Manager secondary IP address [ N ]:
```

If you type **Y**, the following prompt appears:

```
Please enter the Manager secondary IPv4 ( A.B.C.D ) [ Manager_IPaddress ]:

Please enter the Sensor default gateway ( A.B.C.D ) [ Sensor_gateway_IPv4 address ]:

Please enter management port configuration choice(a/m) [port_configuration_selected]:
```

- **a**: Signifies auto configured
- **m**: Signifies manually configured

```
Press Y to set shared secret key now or N to exit [Y]:

Please enter shared secret key:
```

Configuring the Sensor setup for IPv6 address:

You are prompted if you enter the IP Type as 2. Your default Sensor IPv6 address is displayed in the [ ] brackets. The following prompts are displayed.

```
Please enter the Sensor IPV6 address/ subnet prefix length mask ( A:B:.C:D:E:F:G:H/I ) [IPV6 ad-
dress/subnet]:
```

Please enter the Manager primary IPV6 address (A:B:C:D:E:F:G:H) [Manager_IPaddress]:

****You can set the Manager secondary IP in case the Manager has two interfaces****

Please enter the Manager secondary IPv6 address (A:B:C:D:E:F:G:H) [Manager_IPaddress]:

Please enter the Sensor default IPv6 gateway (A:B:C:D:E:F:G:H) [Sensor_gateway_IPv6 address]:

Please enter management port configuration choice(a/m) [port_configuration_selected]:

- **a**: Signifies auto configured
- **m**: Signifies manually configured

Press Y to set shared secret key now or N to exit [Y]:

Please enter shared secret key:

Configuring the Sensor setup for both IPv4 and IPv6 address:

You are prompted if you enter the IP Type as 3. Your default Sensor IPv4 address is displayed in the [ ] brackets. The following prompts are displayed.

Please enter the Sensor IP (A.B.C.D) [Sensor_IPv4address]:

Please enter the Sensor subnet mask (A.B.C.D) [Sensor_subnet_mask_IPaddress]:

Please enter the Sensor IPV6 address/ subnet prefix length mask (A:B:.C:D:E:F:G:H/I) [IPV6 address/subnet]:

Please enter the Manager primary IPv4 address or IPV6 address (A.B.C.D or A:B:C:D:E:F:G:H) [Manager_IPaddress]:

****You can set the Manager secondary IP in case the Manager has two interfaces****

Please enter the Manager secondary IPv4 or IPv6 address (A.B.C.D or A:B:C:D:E:F:G:H) [Manager_IPaddress]:

Please enter the Sensor default gateway (A.B.C.D) [Sensor_gateway_IPv4 address]:

Please enter the Sensor default IPv6 gateway (A:B:C:D:E:F:G:H) [Sensor_gateway_IPv6 address]:

Please enter management port configuration choice(a/m) [port_configuration_selected]:

- **a**: Signifies auto configured
- **m**: Signifies manually configured

Press Y to set shared secret key now or N to exit [Y]:

Please enter shared secret key:

Setting the Sensor subnet mask

You are prompted to enter the Sensor subnet mask. Your default Sensor subnet mask IP address is displayed in the [ ] brackets.

```
Please enter the Sensor subnet mask ( A.B.C.D ) [Sensor_subnet_mask_IPaddress]:
```

How to set the Manager IP address

You are prompted to set the Manager IP address. If your Manager has two NIC cards, then you will be required to set the second NIC card IP address. Your default Manager IP address is displayed in the [ ] brackets. You can set both IPv4 and IPv6 addresses for primary and secondary Managers.

```
Please enter the Manager primary IPv4 address ( A.B.C.D or A:B:C:D:E:F:G:H ) [ Manager_IPaddress ]:

Please enter the Manager primary IPv6 address ( A.B.C.D or A:B:C:D:E:F:G:H ) [ Manager_IPaddress ]:

**You can set the Manager secondary IP in case the Manager has two interfaces**

Press Y to configure Manager secondary IP address [ N ]:

Please enter the Manager secondary IPv4 or IPv6 address ( A.B.C.D or A:B:C:D:E:F:G:H ) [ Manag-
er_IPaddress ]:
```

How to set the Sensor default gateway

You are prompted to set the Sensor's default gateway IP address. Your default Sensor's gateway IP address is displayed in the [ ] brackets. You can set both IPv4 and IPv6 addresses in the Sensor default gateway.

```
Please enter the Sensor default gateway ( A.B.C.D ) [ Sensor_gateway_IPv4 address ]:

Please enter the Sensor default IPv6 gateway ( A:B:C:D:E:F:G:H ) [ Sensor_gateway_IPv6 address ]:
```

How to set the management port configuration

You are prompted to set the status of the management port:

- **a**: auto configured
- **m**: manually configured

```
Please enter management port configuration choice(a/m) [port_configuration_selected]:
```

How to set the shared secret key on the Sensor

Setting the shared secret key on the Sensor is the final step in the setup command.

Enter a shared secret key and reconfirm at the prompt.

```
Press Y to set shared secret key now or N to exit [Y]:

Please enter shared secret key:
```

show

This command displays all the current configuration settings on the Sensor such as model, installed software version, IP address, and Manager details.

This command has no parameters.

Syntax:

show

Information displayed by the **show** command includes the following:

[Sensor Info]

- Date
- System Uptime
- System Type
- System Mode

> **NOTE**
>
> System mode is displayed only for the NS9500 Sensors.

- Software Version
- MGMT Ethernet Port
- System serial number (displays the primary, secondary and master/system serial numbers separately in case of NS9300)

[Sensor Network Config]

- IP Address
- Netmask
- Default Gateway
- Default TFTP server

[Manager Config]

- Manager IP addr
- Install TCP Port
- Alert TCP Port

[Peer Manager Config]

- Manager IP addr
- Install TCP Port
- Alert TCP Port

Sample Output:

- For Sensor, the output is as shown below:

```
intruShell@john> show
[Sensor Info]
```

```
System Name : NS9200
Date : 12/21/2022 - 12:28:59 UTC
System Uptime : 6 days 23 hrs 10 min 13 secs
System Type : NS9200
System Mode : Stack
Serial Number : J021834009
Software Version : 10.1.5.190
Hardware Version : 1.20
MGMT Ethernet port : auto negotiated
MGMT port Link Status : link up
[Sensor Network Config]
IP Address : 10.1.1.1
Netmask : 255.255.255.0
Default Gateway : 10.1.1.2
SSH Remote Logins : enabled
[Manager Config]
Manager IP addr : 10.1.1.3 (primary intf)
Install TCP Port : 8506
Alert TCP Port : 8507
Logging TCP Port : 8508
```

- For NS9300 Sensor, the output is as shown below:

```
intruShell@KAM9300> show
[Sensor Info]
System Name : KAM9300
Date : 12/21/2022 - 11:38:0 UTC
System Uptime : 6 days 22 hrs 03 min 43 secs
System Type : IPS-NS9300
System Serial Number : J073350027
NS9300 P Serial Number : J071328008
NS9300 S Serial Number : J064227B70
Software Version : 10.1.5.190
Hardware Version : 1.00
MGMT Ethernet port : auto negotiated
MGMT port Link Status : link up
[Sensor Network Config]
IP Address : 1.1.1.1
```

```
Netmask : 255.255.255.0
Default Gateway : 1.1.1.5
Default SCPserver : 1.2.3.4
SSH Remote Logins : enabled
[Manager Config]
Manager IP addr : 1.1.1.2 (primary intf)
Install TCP Port : 8506
Alert TCP Port : 8507
Logging TCP Port : 8508
```

Applicable to:

NS-series Sensors

show acl profile

This command displays the ACL alert profile information such as the server IP, UDP port, facility, and priority.

Syntax:

```
show acl profile
```

Sample Output:

```
intruShell@NS_9500> show acl profile
[ACL alert profile information]
ACL server IP is : 10.22.22.2
UDP port : 514
Facility : 4
Priority : 0
```

Applicable to:

NS-series and Virtual IPS Sensors

show acl stats

This command displays statistics about the ACL logs configured on the Sensor.

This command has no parameters.

Syntax:

```
show acl stats
```

Information displayed by the **`show acl stats`** command includes the following:

- Number of ACL log entries received
- Number of suppressed ACL log entries
- Number of ACL log entries sent to the server
- Number of Firewall ACL logs sent through the Manager
- The count of packets matching the Stateless ACL rule which skipped the proxy engine. This counter appears in the output only when SSL Decryption on Inbound/Outbound traffic is enabled.

Sample Output:

```
intruShell@john> show acl stats

[Acl Alerts]

Received : 164

Suppressed : 0

Sent : 164

Sent Direct : 0

Stateless ACL Fwd count : 20

Stateless Pre-ACL lookup hits that skipped proxy : 7
```

Applicable to:

NS-series Sensors

show afo status

This command displays the MAC address detected in the Heartbeat packets sent by the Active Fail-Open (AFO) kit, followed by the current AFO kit state.

Syntax:

```
show afo status <port-pair | all>
```

Parameter	Description
<port-pair>	Set the port-pair for which the status is to be displayed. Valid port-pairs for NS9500, NS7600, NS7500 Sensors are: g0/1-g0/2 |g0/3-g0/4 | g1/1-g1/2 | g1/3-g1/4 | g1/5-g1/6 | g1/7-g1/8 | g2/1-g2/2 | g2/3-g2/4 | g2/5-g2/6 | g2/7-g2/8 | g3/1-g3/2 | g3/3-g3/4 | g3/5-g3/6 | g3/7-g3/8 Valid port-pairs for NS3600 Sensor are: 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 | 13-14
<all>	Display the status of all the IFO-ACTIVE port-pairs.

Sample Output 1:

Figure 813. show fail-open port for a specific port-pair

```
intruShell@NS7500[redacted]> show afo status g1/3-g1/4
-------------------------------------------------------------------------------
 Port Pair     AFO Destination MAC     Fail-Open Switch        Fail-Open Ports
-------------------------------------------------------------------------------
 g1/3-g1/4     22:33:44:55:66:77       PRESENT                 INLINE
-------------------------------------------------------------------------------
```

Sample Output 2:

Figure 814. show fail-open port for all the IFO-ACTIVE port-pairs

```
intruShell@NS7500[redacted]> show afo status all
-------------------------------------------------------------------------------
 Port Pair     AFO Destination MAC     Fail-Open Switch        Fail-Open Ports
-------------------------------------------------------------------------------
 g0/1-g0/2     Auto Detected           PRESENT                 INLINE
 g1/3-g1/4     Auto Detected           PRESENT                 INLINE
 g1/7-g1/8     Auto Detected           PRESENT                 INLINE
-------------------------------------------------------------------------------
```

Depending on the AFO kit physical connection status, the **Fail-Open Switch** and **Fail-Open Ports** columns will display the following status:

Fail-Open Switch	Fail-Open Ports	Description
PRESENT	INLINE	Connection between the Sensor and the AFO kit is up and the Sensor receives heartbeat packets from the AFO kit. These heartbeat packets contain the destination MAC address which matches the MAC address setting in the Sensor. The Manager displays the status as **Present** in this scenario.
ABSENT	UNKNOWN	Connection between the Sensor and the AFO kit is down. The Manager displays the status as **Unknown** in this scenario.
ABSENT	ABSENT	• The Sensor - AFO kit ports/links are up, but the Sensor does not receive the Heartbeat packets. • The Sensor receives the heartbeat packets, but MAC address setting in Sensor does not match the MAC address in the heartbeat packet sent by AFO kits. The Manager displays the status as **Unknown** in this scenario.

Applicable to:

NS-series Sensors - NS9500, NS7600, NS7500, and NS3600

show arp spoof status

The **`show arp spoof status`** command displays whether the ARP spoofing feature is currently enabled or disabled. It is used in conjunction with the ARP spoofing detection feature.

This command has no parameters.

Syntax:

```
show arp spoof status
```

Sample Output:

```
intruShell@Sensor-6050> show arp spoof status

ArpSpoofDetection : Enabled
```

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

show attackIdList logging status

This command shows the status of whether the attackIdList logging is enabled or disabled on the Sensor.

Syntax:

```
show attackIdList logging status
```

Sample Output:

```
intruShell@NS-7200> show attackIdList logging status

attackId List Logging Status enabled
```

Applicable to:

NS-Series and Virtual IPS Sensors

show auditlog

This command displays the system events in audit log based on user input. It displays the following information:

- Date and time of the system event
- User login details (login success/failure, user name, host IP and port number)
- Name of the executed CLI commands (with parameters that are used)

Syntax:

```
show auditlog <[2-50] | all>
```

where [2-50] indicates the number of recent audit log events. This command should be executed with a parameter value, else the command is treated as invalid.

Sample Output:

```
intruShell@john> show auditlog all

Jan 28 09:51:49 2014:EXEC CMD : disable user - admin

Jan 28 09:52:22 2014:EXEC CMD : show auditlog all user - admin

Jan 28 09:52:35 2014:EXEC CMD : show auditlog 3 user - admin
```

Example:

To display the recent 20 events: **`show auditlog 20`**

To display all events: **`show auditlog all`**

Applicable to:

NS-series Sensors

show auditlogtomgr status

This command displays the current configuration status of audit logging feature available in the Sensor for the Manager. By default, this command is disabled.

Syntax:

```
show auditlogtomgr status
```

Sample Output:

```
intruShell@chand-9100-2> show auditlogtomgr status
Audit Logging to Manager : Disabled
```

Applicable to:

NS-series Sensors

show auditlog status

This command displays whether the audit log feature is enabled or disabled.

Syntax:

```
show auditlog status
```

Sample Output:

```
intruShell@john> show auditlog status
Audit Logging : Enabled
```

Default Value:

Enabled

Applicable to:

NS-series Sensors

show autorecovery status

On encountering data path errors, the Sensor goes Layer 2 mode and tries to auto-recover. During a datapath error, the auto-recovery feature reboots the datapath threads without any interruption to traffic.

> **NOTE**
>
> The Sensor should be in good health and in Layer 2 mode for performing the auto-recovery.

If the recovery is successful, the Sensor comes out of Layer 2 mode. If the recovery is not successful, the Sensor remains in Layer 2 mode.

Syntax:

```
show autorecovery status
```

This command has no parameters.

By executing the command, the following status information is displayed:

Status	Description
Auto-recovery enabled	The status of auto-recovery, whether it is **On** or **Off**. When the Layer 2 is enabled, this status will be displayed as **On**.
Auto-recovery attempts	Number of auto-recovery attempts made since last reboot
Last Auto-recovery status	• **Not applicable** - No auto-recovery is attempted • **Success** - Successful auto-recovery • **Failure** - Failure in auto-recovery • **In Progress** - Auto-recovery in progress
Last Auto-recover time	The time when Sensor came out of Layer 2 due to successful auto-recovery

Applicable to:

NS-series Sensors

NOTE

Auto-recovery is supported on Virtual IPS Sensors. However, a Virtual IPS Sensor cannot depend on its software to go to Layer 2 during recovery. So, the traffic is interrupted until all applications are restarted and the Sensor is back to good health.

show auxport status

This command displays the auxiliary port configuration status.

Syntax:

```
show auxport status
```

Sample Output:

```
intruShell@john> show auxport status

Aux Port : Enabled
```

Applicable to:

NS-series Sensors

show botnet-alertstats

The **show botnet-alertstats** command displays the statistics related to advanced botnet detection by a Sensor.

This command has no parameters.

Syntax:

```
show botnet-alertstats
```

Information displayed by the **show botnet-alertstats** command includes the following:

- The count of domains, IP addresses, and URLs detected based on the callback detectors
- The count of DGA bots detected
- The count of suspected DGA command and control servers detected
- The count of communications from your network to DGA command and control servers
- The count of activities monitored for FFSN
- The count of communications from your network to the flux agents of FFSN
- The count of command and control domains detected based on heuristics, such as protocol anomalies and DNS response failures

Sample Output:

```
Callback detector matches : 306

DGA Zombie detected : 5

DGA CnC Server Suspects detected : 25

DGA Zombie to CnC Server callbacks detected : 50

Ip Flux botnet activity detected : 30

IP Flux agent callback detected : 60

Other Zero day botnets detected : 25
```

Applicable to:

NS-series and Virtual IPS Sensors

show capacity mode

This commands displays the capacity requested and the capacity active in the Sensor.

This command has no parameters.

Syntax:

```
show capacity mode
```

Sample Output:

```
intruShell@9500> show capacity mode

[Capacity Mode]

Requested : 30 Gbps

Active : 20 Gbps
```

Applicable to:

NS9500, NS7600, NS7500, NS3600 and NS3500 Sensors

show castoreinfo

This command displays information like CA store issuer, expiry date, serial number, and fingerprint for the global CA store and private CA certificates, if any.

This command has no parameters.

Syntax:

```
show castoreinfo
```

Sample Output:

```
intruShell@NS9100> show castoreinfo

Type: Global CA store

issuer= /C=US/O=SeoTrust Corporation/CN=Seo trust CA

notBefore=Nov 7 19:31:18 2006 GMT

notAfter=Dec 31 19:40:55 2029 GMT

serial=0CG06E5C0816A5AD527FF2EB271711D9

SHA1 Fingerprint=78:28:C1:C4:50:35:3B:CF:D2:96:92:D2:59:3F:7D:44:D9:34:GG:12

Type: private GTI

issuer= /C=US/ST=leyland/L=Country/O=Organization/OU=Private GTI/CN=gtirest.pgti.xyz.com

notBefore=Apr 8 20:13:57 2021 GMT

notAfter=Apr 6 20:13:57 2031 GMT

serial=A1855C1DLEA8MD67

SHA1 Fingerprint=9C:0D:AC:C2:D5:0N:E5:96:6F:D1:4A:C2:3E:57:E3:7N:9C:28:60:71
```

Applicable to:

NS series and Virtual IPS Sensors

show console timeout

This command displays the SSH CLI console timeout in minutes.

Syntax:

```
show console timeout
```

Sample output:

```
intruShell@john> show console timeout

Console timeout : 15 mins
```

Applicable to:

NS-series Sensors

show coppersfpserialnumbers

This command displays the serial numbers of all copper ports having copper SFPs.

This command has no parameters.

Syntax:

```
show coppersfpserialnumbers
```

Applicable to:

NS-series Sensors

show datapath-memory-usage stats

This command displays the signature configuration memory usage details of the device.

This command has no parameters.

Syntax:

```
show datapath-memory-usage stats
```

Sample Output:

```
intruShell@9200> show datapath-memory-usage stats

Attack IDs Usage : 36.1% used

Signature Config Memory Usage : 43.5% used

Sigfile Size : 38.0% used

MSPM Graph size : 39.7% used
```

Applicable to:

NS-series Sensors

show dnsprotect

The **show dnsprotect** command displays the added DNS Spoof protection IP addresses (IPv4, IPv6 or, both) from the Protected Server List (PSL) and the DNS Protection Status.

Syntax:

show dnsprotect <ipv4/ipv6/all>

Parameter	Description
<ipv4>	Indicates the list of DNS Spoof protection IP addresses for IPv4
<ipv6>	Indicates the list of DNS Spoof protection IP addresses for IPv6
<all>	Indicates the list of DNS Spoof protection IP addresses for both IPv4 and IPv6

Sample Output:

```
intruShell@john> show dnsprotect all

[DNS Protection is enabled for inbound connections]

No IPv4 addresses are configured for DNS Protection.

No IPv6 addresses are configured for DNS Protection.
```

Applicable to:

NS-series Sensors

show dnsprotectstat

This command displays the DNS Protection Statistics.

This command has no parameters.

Syntax:

show dnsprotectstat

Applicable to:

NS-series Sensors

show dospreventionprofile

This command displays the specified denial of service profile information for the Sensor, defined in two arguments — a DoS measure name, and a traffic direction. It also displays the DOS prevention profile information for different measures.

Syntax:

show dospreventionprofile <dos-measure-name> <inbound | outbound>

show dospreventionprofile intfport (g0/1 | g0/2 | g1/1 | g1/2 | g1/3 | g1/4 | g1/5 | g1/6 | g1/7 | g1/8 | g1/9 | g1/10 | g1/11 | g1/12 | g2/1 | g2/2 | g2/3 | g2/4 | g2/5 | g2/6 | g2/7 | g2/8

| g2/9 | g2/10 | g2/11 | g2/12 | g3/1 | g3/2 | g3/3 | g3/4 | g3/5 | g3/6 | g3/7 | g3/8 | g4/1 | g4/2 | g5/1 | g5/2 | g5/3 | g5/4 | g5/5 | g5/6 | g5/7 | g5/8 | g5/9 | g5/10 | g5/11 | g5/12 | g6/1 | g6/2 | g6/3 | g6/4 | g6/5 | g6/6 | g6/7 | g6/8 | g6/9 | g6/10 | g6/11 | g6/12 | g7/1 | g7/2 | g7/3 | g7/4 | g7/5 | g7/6 | g7/7 | g7/8) (tcp-syn|tcp-syn-ack|tcp-fin|tcp-rst|udp|icmp-echo|icmp-echo-reply|icmp-non-echo-echoreply|ip-fragment|non-tcp-udp-icmp) (inbound | outbound)

Parameter	Description
<intfport>	Indicates the interface port
<dos-measure-name>	Indicates the DoS measure name: one of 'tcp-syn', 'tcp-syn-ack', 'tcp-fin', 'tcp-rst', 'udp', 'icmp-echo', 'icmp-echo-reply', 'icmp-non-echo-reply', 'ip-fragment', 'non-tcp-udp-icmp'
<direction>	Indicates the direction. It can be 'inbound' or 'outbound'.

Example:

show dospreventionprofile tcp-syn inbound

Information displayed by the **show dospreventionprofile** command includes the following:

- The Sensor's DoS profile
- The traffic direction protected by the profile

Example 1:

intruShell@Sensor-9500> show dosPreventionProfile tcp-syn inbound

where:

- packet type: TCP-SYN IN (0), profile stage: still learning (0)
- long-term average rate=0.000(pkts/s), last_rate=0.000(pkts/s) no attack in progress
- each line: bin_index, IP_prefix/prefix_len, AS, LT, ST, ltR(ate), stR(ate)
- AS(%) -- percentage of the IP address space this bin occupies
- LT(%) -- percentage of long-term traffic that falls into this bin
- ST(%) -- percentage of short-term traffic that falls into this bin
- ltRate -- long-term average traffic rate (in pkts/s) for this bin
- stRate -- short-term traffic rate (in pkts/s) for this bin
- 0: 0.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000
- 1: 128.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000
- 2: 64.0.0.0/2 AS=25.000% LT=25.000% ST=25.00% ltR=0.000 stR=0.000

Example 2:

show dospreventionprofile intfport g2/3 tcp-syn inbound

Applicable to:

NS-series Sensors

NOTE

show dospreventionprofile intfport command is applicable only for NS9300 Sensors.

show dospreventionseverity

This command displays the severity for a specified denial-of-service profile. It also displays the DoS prevention severity information for different measures.

Syntax:

show dosPreventionseverity <dos-measure-name> <inbound | outbound>

Parameter	Description
<dos-measure-name>	Indicates the DoS measure name: one of 'tcp-syn', 'tcp-syn-ack', 'tcp-fin', 'tcp-rst', 'udp', 'icmp-echo', 'icmp-echo-reply', 'icmp-non-echo-reply', 'ip-fragment', 'non-tcp-udp-icmp'
<direction>	Indicates the direction. It can be 'inbound' or 'outbound'.
<intfport>	Indicates the interface port

show dospreventionseverity intfport (g0/1 | g0/2 | g1/1 | g1/2 | g1/3 | g1/4 | g1/5 | g1/6 | g1/7 | g1/8 | g1/9 | g1/10 | g1/11 | g1/12 | g2/1 | g2/2 | g2/3 | g2/4 | g2/5 | g2/6 | g2/7 | g2/8 | g2/9 | g2/10 | g2/11 | g2/12 | g3/1 | g3/2 | g3/3 | g3/4 | g3/5 | g3/6 | g3/7 | g3/8 | g4/1 | g4/2 | g5/1 | g5/2 | g5/3 | g5/4 | g5/5 | g5/6 | g5/7 | g5/8 | g5/9 | g5/10 | g5/11 | g5/12 | g6/1 | g6/2 | g6/3 | g6/4 | g6/5 | g6/6 | g6/7 | g6/8 | g6/9 | g6/10 | g6/11 | g6/12 | g7/1 | g7/2 | g7/3 | g7/4 | g7/5 | g7/6 | g7/7 | g7/8) (tcp-syn|tcp-syn-ack|tcp-fin|tcp-rst|udp|icmp-echo|icmp-echo-reply|icmp-non-echo-echoreply|ip-fragment|non-tcp-udp-icmp) (inbound|outbound)

Sample Output:

intruShell@Sensor-9500> show dospreventionseverity tcp-syn-ack outbound

DOS Prevention Severity for tcp-syn-ack outbound is 30

Example 1:

show dospreventionSeverity tcp-syn-ack outbound

Example 2:

show dospreventionprofile intfport g2/3 tcp-syn inbound

Applicable to:

NS-series Sensors

NOTE

show dospreventionprofile intfport command is applicable only for NS9300 Sensors.

show dpimonitor status

It displays the status of data path attack detection monitoring for that device.

Syntax:

```
show dpimonitor status
```

Sample Output:

```
intruShell@chand-9100-2> show dpimonitor status

Datapath attack detection monitoring disabled
```

Applicable to:

NS-series Sensors

show dpimonitor-action status

This command displays whether the monitor action for datapath attack detection is applied or not.

Syntax:

```
show dpimonitor-action status
```

Sample Output:

```
intruShell@chand-9100-2> show dpimonitor-action status

Monitor action ignored for dpi attack detection
```

Applicable to:

NS-series Sensors

show dxl status

This command displays the status of Trellix DXL for that device.

Sample output

```
intruShell@NS7250> show dxl status

Trellix Data Exchange Layer

Configuration Status : Enabled

Status : Running

Version : 6.0.3.847

Connection Status : Connected

Certificate Status : Present
```

```
Trellix Agent

Mode : Managed

Status : Running

Version : 5.7.7.406

Wakeup Port : 44

Trellix ePO - On-prem

IP|Name : 10.200.100.200|WIN-00GOU69FF17|WIN-00GOU69FF17

Trellix ePO - On-prem activity time : 2022-12-02 06:17:33
```

Applicable to:

NS-series and Virtual IPS Sensors

show eventlog

, When executed, this command displays the logged Sensor events.

Syntax:

```
show eventlog <2-50 | all>
```

Sample Output:

```
intruShell@john> show eventlog 2

Jan 6 10:16:05 2023: %LINK-STATUS: Interface port G3/2 changed state to UP

Jan 6 10:16:05 2023: %LINK-STATUS: Interface port G3/4 changed state to DOWN
```

Applicable to:

NS-series Sensors

showfailopencfg

This command displays the current fail-open configuration.

Syntax:

```
showfailopencfg
```

Sample Output:

```
intruShell@john> showfailopencfg

External Passive Failopen Configuration : INLINE

Periodically Restore Inline-Failopen : DISABLED

Restore Inline-Failopen interval : 5 minutes
```

Applicable to:

NS-series Sensors

show failover-status

This command shows whether failover is enabled on the Sensor, the status of the peer Sensor, and the fail-open action of the Sensor.

Syntax:

```
show failover-status
```

Information displayed by the **`show failover-status`** command includes the following:

- **Failover Enabled:** The command will return -
  - **YES:** If failover is enabled
  - **NO:** If failover is disabled
  - **UNKNOWN:** If it is not explicitly set
- **Peer Status:** Shows if failover is enabled, and whether the peer Sensor is UP or DOWN
- **Fail-open Action:** Shows whether the monitoring port for fail-open is enabled or disabled

> **NOTE**
>
> When you enable fail-open on a HA pair, the same monitoring ports are enabled for fail-open on both the primary and secondary Sensors.

Applicable to:

NS-series Sensors

show festats

This command shows the statistics of the internal modules of the Sensor and is solely used for debugging purposes.

Syntax:

```
show festats
```

Sample Output

```
IntruDbg#> show festats

Frontend Stats:

----------------------------------------

FrontEnd [0]

Total Packets recieved : 8
```

```
Total Packets transmitted : 8

FrontEnd [1]

Total Packets recieved : 6

Total Packets transmitted : 6

FrontEnd [2]

Total Packets recieved : 4

Total Packets transmitted : 4

FrontEnd [3]

Total Packets recieved : 0

Total Packets transmitted : 0

FrontEnd [4]

Total Packets recieved : 0

Total Packets transmitted : 0

FrontEnd [5]

Total Packets recieved : 0

Total Packets transmitted : 0

----------------------------------------
```

Applicable to:

NS-Series Sensors

show flows

This command displays how many flows exist in the current traffic.

This command has no parameters.

Syntax:

```
show flows
```

Information displayed by the **show flows** command are as follows:

- Total TCBs
- Total free TCBs
- Total active TCP flows
- Total TCP flows in timewait

- Total active UDP flows
- Total flows in SYN state
- Total TCP flows created
- Total abandoned TCP handshakes
- syncookie inbound status
- syncookie outbound status
- Total syn cookie proxy connections
- Total dequote flows count

In addition to the above mentioned information, this command displays the following information when executed in debug mode of NS-series Sensors:

- Total in-use CB Hash Buckets found
- Total invalid CB Hash Buckets found
- CB Syn List status
- CB Free List status

Sample Output:

```
intruShell@john> show flows

Total TCBs = 88612

Total free TCBs = 88609

Total active TCP flows = 3

Total TCP flows in timewait = 0

Total active UDP flows = 20

Total flows in SYN state = 1

Total TCP flows created = 15944

Total abandoned TCP handshakes = 302

syncookie inbound status = Inactive

syncookie outbound status = Inactive

Total syn cookie proxy connections = 0

Total dequote flows count = 20
```

Applicable to:

NS-series Sensors

show flowvolumelimit config

This command displays the flow volume limit configuration.

Syntax:

```
show flowvolumelimit config
```

Sample Output:

```
intruShell@john> show flowvolumelimit config

flow volume threshold is 40MB.
```

Applicable to:

NS-series Sensors

show gam-airgap-network status

This command displays availability of Gateway Anti-Malware engine initialization for the Sensor in an air gapped network.

Syntax:

```
show gam-airgap-network status
```

Sample Output:

```
MyCompany@NS-series> show gam-airgap-network status

GAM Airgap Network(Current) : Disabled

GAM Airgap Network(Active) : Disabled
```

Applicable to:

NS-series Sensors

show gam-behavioral-scan status

This command displays the status of behavioral scan on the Gateway Anti-Malware engine as enabled or disabled.

Syntax:

```
show gam-behavioral-scan status
```

Sample output:

```
intruShell@NS7250_149> show gam-behavioral-scan status

GAM Behavioral Scan for Airgap Network : Enabled

GAM Airgap Network : Enabled
```

Applicable to:

NS-series Sensors

show gam engine stats

This command displays statistics related to the Gateway Anti-Malware engine, such as engine status, GAM engine version, GAM DAT version, anti-virus DAT version, and so on.

Syntax:

```
show gam engine stats
```

Sample Output:

```
intruShell@NS7250> show gam engine stats

Local GAM Engine Statistics:

---------------------------

Engine Status: Initialized

Gateway Anti-Malware Engine Version: 7001.2023.4166

Gateway Anti-Malware DAT Version: 8321

Anti-Malware Engine Version: 6600.9927

Anti-virus DAT Version: 11003

Last Update time: 1/5/2024 - 7:47:49 UTC

Last Successful Update time: 1/5/2024 - 7:47:49 UTC

Total number of Scan Threads: 5

Total Full update success count: 0

Total Full update failure count: 0

Total Incr update success count: 0

Total Incr update failure count: 0

Total Manager Full update success count: 3

Total Manager Full update failure count: 0

Total config issue update failure count: 2

(config issue - Trust/DNS/Proxy config issues)
```

Applicable to:

NS-series Sensors

show gigfailopendelay

This command displays the current delay before fail-open operation takes effect on a Sensor with a Gigabit Fail-open kit installed.

This command has no parameters.

Syntax:

```
show gigfailopendelay
```

Sample Output:

```
intruShell@john> show gigfailopendelay

Failopen delay : 600 seconds
```

Applicable to:

NS-series Sensors

show gti config

The **show gti config** command displays the GTI server configuration information.

This command has no parameters.

Syntax:

```
show gti config
```

Sample output:

If you have enabled integration with the Private GTI Server/IP address:

```
intruShell@Sensor> show gti config

Primary Nameserver IP : 10.1.1.1

Secondary Nameserver IP : Not Configured

[File reputation configuration]

GTI REST Server : Private

GTI REST Server URL : https://private.cloud.com

[IP/URL reputation configuration]

GTI Server : Private

GTI server IP : 10.1.1.5
```

If you have not enabled integration with the Private GTI Server, the command displays the configuration details for Public GTI Server:

```
intruShell@Sensor> show gti config
```

```
Primary Nameserver IP : 10.1.1.1

Secondary Nameserver IP : Not Configured

[File reputation configuration]

GTI REST Server : Public

GTI REST Server URL : https://nsp.rest.gti.trellix.com/1

[IP/URL reputation configuration]

GTI Server : Public

GTI server IP : 0.0.0.0

[Proxy configuration]

Proxy host : 10.1.2.2

Proxy port : 0001

Proxy username : ""
```

Applicable to:

NS-series and Virtual IPS Sensors

show gti stats

This command displays the statistics of the IP and URL sent and received from the GTI server.

Syntax:

```
show gti stats <ip|url>
```

Sample output:

```
GTI server connection status is ok

[GTI Query Statistics]

Query sent count :0

Query received count :0
```

Applicable to:

GTI stats for IP addresses: NS-series Sensors

GTI stats for URL: NS9500, NS9200, NS9100, NS7600, NS7500, NS7300, NS7200, and NS3600 Sensors

show h2 config

This CLI command displays details related to HTTP2 configurations such as: status, flow allocation, and others.

Syntax:

show h2 config

Sample Output:

```
intruShell@NS7500> show h2 config

 HTTP2 Config:

  Device HTTP2 Processing                          : Enabled
  HTTP2 Flow Alloc %                               : 5
  HTTP2 Total Flows Allocated                      : 549477
  Include Decoded Pkt in Attack Pkt Log            : Yes
```

Applicable to:

NS9500, NS7600, NS7500, and NS3600 Sensors

show h2 connections

This CLI command displays statistics related to HTTP2 connections.

Syntax:

show h2 connections

Sample Output:

```
intruShell@NS7500> show h2 connections

HTTP2 Context Stats:

  Context Alloc Succ                               : 1152
  Context Alloc Fail                               : 0
  Context DeAlloc Succ                             : 1152
```

Applicable to:

NS9500, NS7600, NS7500, and NS3600 Sensors

show h2 frames

This CLI command displays the count of various frames processed and settings-frames related statistics.

Syntax:

show h2 frames

Sample Output:

```
intruShell@NS7500_105> show h2 frames

HTTP2 Frame Parse Stats:
```

```
  Frame Handle Count
    fh_DATA                                   : 1452
    fh_HEADERS                                : 2296
    fh_PRIORITY                               : 40
    fh_RST_STREAM                             : 255
    fh_SETTINGS                               : 4678
    fh_PUSH_PROMISE                           : 82
    fh_PING                                   : 49
    fh_GOAWAY                                 : 149
    fh_WINDOW_UPDATE                          : 1096
    fh_CONTINUATION                           : 64
  Unknown Frames                              : 8


HTTP2 Settings-Frames Stats:

  Num HdrTableSize seen                       : 79
  Num EnablePush seen                         : 796
  Num MaxConcurrentStrms seen                 : 1146
  Num InitialWindowSize seen                  : 1963
  Num MaxFrameSize seen                       : 76
  Num MaxHdrListSize seen                     : 38
```

Applicable to:

NS9500, NS7600, NS7500, and NS3600 Sensors

show h2 header-decoder

This CLI command displays the HTTP2 header block decode statistics.

Syntax:

`show h2 header-decoder`

Sample Output:

```
intruShell@NS7500_105> show h2 header-decoder

HTTP2 Header Decoder Stats:

   Header Block Decode Success                : 2284
   Header Block Decode Error                  : 27
```

Applicable to:

NS9500, NS7600, NS7500, and NS3600 Sensors

show h2 resource

This CLI command displays various HTTP2 resources such as: H2 context, H2 stream, and others.

Syntax:

`show h2 resource`

Sample Output:

```
intruShell@NS7500_105> show h2 resource

 HTTP2 Resource Pool Stats:
                                                    Available       Total

  H2 Context Pool:                                  549477          549477
  H2 Stream Pool:                                   5494878         5494878
  H2 Stream Table Block Pool:                       8791824         8791824
  H2 Dynamic Table Pool:                            1098978         1098978
  H2 DT Header Buffer Pool:                         4395912         4395912
  H2 DT Entry Pool:                                 32969340        32969340
  H2 DT Entry Block Pool:                           3296934         3296934
  H2 Pseudo Header Buffer Pool:                     1098966         1098966
  H2 Attack Timer Pool:                             137357          137357
  H2 Settings Fields Pool:                          1648455         1648455
```

Applicable to:

NS9500, NS7600, NS7500, and NS3600 Sensors

show h2 streams

This CLI command displays statistics related to HTTP2 streams.

Syntax:

`show h2 streams`

Sample Output:

```
intruShell@NS7500_105> show h2 streams

HTTP2 Streams Stats:

  Stream Creation (HEADERS) Succ                  : 1286
  Stream Creation (PUSH_PROMISE) Succ             : 73
  Stream Creation (HEADERS) Fail                  : 0
  Stream Creation (PUSH_PROMISE) Fail             : 0
  Stream Termination (EndStream)                  : 884
  Stream Termination (RstStream)                  : 85
  Stream Termination (Goaway)                     : 27
  Stream Alloc Succ                               : 1359
  Stream Alloc Fail                               : 0
  Stream DeAlloc Succ                             : 1359
  Stream DeAlloc (Timer)                          : 1185
```

```
  Stream DeAlloc (Inactive)                          : 0
  Stream DeAlloc (Connection Cleanup)                : 363
```

Applicable to:

NS9500, NS7600, NS7500, and NS3600 Sensors

show inactiveuserslock status

This command shows the configuration status for locking inactive CLI users other than the Admin user.

Syntax:

```
show inactiveuserslock status
```

Sample Output:

```
intruShell@john> show inactiveuserslock status

Inactive Users Locking : Disabled
```

Applicable to:

NS-series Sensors

show inlinepktdropstats

This command displays how many monitored packets have been dropped by a port in inline mode.

Syntax:

```
show inlinepktdropstats <port>
```

Parameter	Description
<port>	sets the port for which the statistics is to be displayed. Valid port numbers for NS-series are: g0/1 | g0/2 | g0/3 | g0/4 | g1/1 | g1/2 | g1/3 | g1/4 | g1/5 | g1/6 | g1/7 | g1/8 | g1/9 | g1/10 | g1/11 | g1/12 | g2/1 | g2/2 | g2/3 | g2/4 | g2/5 | g2/6 | g2/7 | g2/8 | g2/9 | g2/10 | g2/11 | g2/12 | g3/1 | g3/2 | g3/3 | g3/4 | g3/5 | g3/6 | g3/7 | g3/8 | all

Takes a single argument which is the port for which to show statistics.

Information displayed by the **`show inlinepktdropstats`** command includes the count for each of the following categories:

- IP checksum errors
- TCP checksum errors
- UDP checksum errors
- ICMP checksum errors
- ACL-related packets dropped
- Out-Of-Context/Bad packets dropped

- Sensor cold-start-related packets dropped
- Off/HdrLen error packets dropped
- dropped attack packets (or, blocked packets)
- IP reassembly timeout packets dropped
- TCP Out-Of-Order timeout packets dropped
- Dropped packets containing TCP protocol errors
- Dropped packets containing UDP protocol errors
- Dropped packets containing ICMP protocol errors
- Dropped packets containing IP protocol errors
- Packets dropped due to the Sensor being out of resources
- Dropped packets containing CRC errors
- Dropped IP-spoofed packets
- ICMPv6 checksum error drop count
- IPv6 reassembly timeout drop count
- ICMPv6 Protocol error drop count
- IPv6 Protocol error drop count
- Host Quarantine IPv4 packet drop count
- Host Quarantine IPv6 packet drop count
- Other Layer-2 error packets dropped
- IP sanity check packets dropped
- IPv6 sanity check packets dropped
- Total IP No Credit Packets dropped
- Count of other Layer-2 packets dropped

The count for the following categories is displayed only when you run the **`show inlinepktdropstats all`** command.

- Total Inline Forward dropped
- Count of miscellaneous packets dropped at front-end
- Count of miscellaneous packets dropped at back-end
- Count of miscellaneous packets dropped at NIC
- Count of miscellaneous packets dropped at BMC switch
- (Applicable to NS7600 Sensor only) Count of packets dropped due to oversubscription. This count is triggered when the throughput exceeds the subscription limit. This is a subset of **`Total Other Layer-2 Packets Dropped`**.
- (Applicable to NS7600 Sensor only) Count of packets not dropped though oversubscribed. This count is triggered when when the subscribed license capacity is reached but packets are not dropped.

Sample Output:

```
intruShell@john> show inlinepktdropstats all

IP Checksum Error Drop Count : 0
```

```
TCP Checksum Error Drop Count : 0

UDP Checksum Error Drop Count : 0

ICMP Checksum Error Drop Count : 0

ICMPv6 Checksum Error Drop Count : 0

ACL Drop Count : 0

Out-Of-Context/Bad Packet Drop Count : 0

Cold Start Drop Count : 0

Off/HdrLen Error Drop Count : 0

Attack Packet Drop Count : 0

IP Reassembly Timeout Drop Count : 0

IPv6 Reassembly Timeout Drop Count : 0

TCP Out-Of-Order Timeout Drop Count : 0

TCP Protocol Error Drop Count : 0

UDP Protocol Error Drop Count : 0

ICMP Protocol Error Drop Count : 0

ICMPv6 Protocol Error Drop Count : 0

IP Protocol Error Drop Count : 0

IPv6 Protocol Error Drop Count : 0

System Out-of-Resource Drop Count : 0

Host Quarantine IPv4 Packet Drop Count : 0

Host Quarantine IPv6 Packet Drop Count : 0

Conn Limiting Packet Drop Count : 0

Frontend Misc Packet Drop Count : 44243

Misc Backend Pkt Drop Count : 0

DoS Attack Packets Dropped : 0

Stateless ACL Drop Count : 0

Total CRC Error Packets Dropped : 0

Total Other Layer-2 Error Packets Dropped : 0

Total Other Layer-2 Packets Dropped : 27903423745
```

```
Total IP Spoofed Packets dropped : 0

Total IP Sanity Check Packets dropped : 0

Total IPv6 Sanity Check Packets dropped : 0

Total IP No Credit Packets dropped : 0

Total Inline Forward dropped : 0

Switch Misc Packets Drop Count : 27625

Misc NIC Pkt Drop Count : 183086

Packets dropped due to oversubscription  : 41145921942 (Subset of "Total Other Layer-2 Packets Dropped")

Packets NOT dropped though oversubscribed: 23547617804
```

Example:

```
show inlinepktdropstats g0/2
```

Applicable to:

NS-series Sensors

show ingress-egress stat

This command applies to Virtual Security System instances. In other words, it applies only to the security appliances installed on hypervisors through the integration with Intel® Security Controller.

For Virtual Security System instances, the **show intfport** command is not available; you instead can use the **show ingress-egress stat** command to view the number of packets received, forwarded, and dropped by the Virtual Security System instance.

It is also applicable to AWS environment where it displays traffic statistics.

This command has no parameters.

Syntax:

```
show ingress-egress stat
```

Sample Output:

```
intruShell@John> show ingress-egress stat

Total Packets Received : 1213299664

Total Packets Sent : 1213295243

Total Packets Dropped : 0
```

Applicable to:

Virtual Security System instances and AWS Environment

show intfport

This command shows the status of the specified Sensor port. Note that specifying a non-existent port results in an error.

Syntax:

```
show intfport <port>
```

Parameter	Description
<port>	Sets the port for which the status is to be displayed. Valid port numbers for NS-series Sensors (except NS3600) are: g0/1 | g0/2 | g1/1 | g1/2 | g1/3 | g1/4 | g1/5 | g1/6 | g1/7 | g1/8 | g1/9 | g1/10 | g1/11 | g1/12 | g2/1 | g2/2 | g2/3 | g2/4 | g2/5 | g2/6 | g2/7 | g2/8 | g2/9 | g2/10 | g2/11 | g2/12 | g3/1 | g3/2 | g3/3 | g3/4 | g3/5 | g3/6 | g3/7 | g3/8 | WORD | all Valid port-pairs for NS3600 Sensor are: 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 | 13-14

Information displayed by the **`show intfport`** command includes the following:

- Whether the port's administrative status is enabled or disabled
- The Sensor's operational status
- The Sensor's operating mode
- Whether full-duplex mode is enabled
- The port's configured traffic direction (inside or outside)
- The speed of the 10/100 ports, if applicable
- The speed of the Gigabit ports, if applicable
- The peer port's supported link mode
- The peer ports negotiated duplex and speed
- The auto-negotiating configuration
- Total packets received
- Total packets sent
- Total CRC errors received
- Total CRC errors sent
- Whether the flow control is on (this applies only to Sensor gigabit ports)

Sample Output:

For Sensors, the output is as shown below:

```
intruShell@john> show intfport g1/2

Displaying port g1/2

Administrative Status : ENABLED (since Thu Jan 5 03:36:51 2023)
```

Operational Status : UP (since Thu Jan 5 03:38:02 2023)

Operating Mode : INLINE_FAIL_OPEN_ACTIVE

Duplex : FULL

Port Connected to : OUTSIDE

Port Speed : 10 GBPS

Actual Port Property : Fiber, Trellix Certified

Configured Port Property: Fiber, Allow any vendor certified connector

Additional Porttype Info:

Total Packets Received : 882391

Total Packets Sent : 882191

Total CRC Errors Rcvd : 0

Total Other Errors Rcvd : 0

Total CRC Errors Sent : 0

Total Other Errors Sent : 0

Flow Control Status : OFF

Fail-Open Switch : PRESENT

Fail-Open Port : INLINE

Layer 2 Status : DISABLED

Applicable to:

NS-series and Virtual IPS Sensors. The command does not apply to Virtual Security System instances; use the **show ingress-egress stat** command instead.

show ivx config

This command displays the IVX appliance configuration details.

Syntax:

show ivx config

Sample Output:

```
intruShell@john> show ivx config
IVX Primary Cluster Configuration:
IVX Broker 1:
        IP Address type                 : IPv4
```

```
        Server IPv4                     : 10.213.2.54
        Connection config               : ENABLED
        IVX UserName                    : admin
        Certificate validation          : DISABLED
        Authentication Status           : Successful
        Proxy for IVX Communication     : DISABLED
IVX Broker 2:
        IP Address type                 : IPv4
        Server IPv4                     : 10.213.2.210
        Connection config               : ENABLED
        IVX UserName                    : admin
        Certificate validation          : DISABLED
        Authentication Status           : Successful
        Proxy for IVX Communication     : DISABLED
```

Applicable to:

NS-series and Virtual IPS Sensors

show ivx stats brokerid

This command displays statistics specific to IVX appliance broker ID(s).

Syntax:

`show ivx stats brokerid <1 | 2 | 3 | 4 | 5 | all>`

Information displayed by the **`show ivx stats brokerid`** command includes the following:

- Counters related to authentication
- Counters related to SHA2 cache when configured with IVX
- Counters related to file submission to the IVX engine
- Counters related to report status

Sample Output:

```
intruShell@john> show ivx stats brokerid all

[ Auth ]
Auth requests sent : 96
Auth responses received : 68
Auth responses as OK : 68
Auth errors : 28
Last Auth time : Thu Dec 14 04:57:35 2023
Last auth error time : Thu Dec 14 00:15:54 2023
Max Auth time (sec.): 0

[ Cache ]
sha2 cache requests : 0
sha2 cache responses : 0
```

```
sha2 cache misses : 0
sha2 cache timeouts : 0
sha2 cache errors : 0
Last sha2 query time : NA
Last sha2 query error time : NA
Last sha2 query file md5 : NA
Last sha2 query file name : NA
Last sha2 response file md5 : NA
Last sha2 query time (sec.) : 0
Last md5 drop time : NA

[ File Submission ]
Submission requests sent : 0
Submission responses received : 0
Submission errors : 0
Submission response parse errors : 0
Submission Timeouts : 0
Last submit time : NA
Last submitted file md5 : NA
Last submitted file name : NA
Last submission error time : NA
Max scan time (sec.) : 0
Max upload time (sec.) : 0

[ Reports status ]
Report requests sent : 0
Report responses received : 0
Report responses successful : 0
Report responses with errors : 0
Report response parse errors : 0
Timeouts in receiving responses : 0
Reports/Results Pending : 0
Pending list free nodes : 400
Pending ignored (timedout): 0
Pending list errors : 0
Last report time : NA
Last report error time : NA
Last report file md5 : NA
Max report poll time (sec.) : 0

Scan requests received : 0
Number of files ignored(load) : 0
Number of files ignored(auth error) : 0
Number of files ignored(IVX disabled) : 0
```

NOTE

In some cases, the IVX appliance might be reporting multiple HTTP 4xx and 5xx errors. If you encounter such errors, please contact Trellix support.

Applicable to:

NS-series and Virtual IPS Sensors

show ivx status brokerid

This command displays the connection status of the IVX appliance broker ID(s).

Syntax:

`show ivx status brokerid <1 | 2 | 3 | 4 | 5 | all>`

Sample Output:

```
intruShell@john> show ivx status brokerid all

IVX broker 1 connection status    : Connected

IVX broker 2 connection status    : Connected

IVX broker 3 connection status    : Disconnected

IVX broker 4 connection status    : Disconnected

IVX broker 5 connection status    : Disconnected

IVX engine curl-verbose         : Disabled
```

Applicable to:

NS-series and Virtual IPS Sensors

show ivxcloud config

This command displays the IVX Cloud configuration details.

Syntax:

`show ivxcloud config`

Sample Output:

```
intruShell@john> show ivxcloud config
IIVX Cloud Configuration:
        Connection config               : ENABLED
        IVX Cloud host name             : feapi.marketplace.apps.fireeye.com
```

```
IVX Cloud port                  : 443
IVX Cloud Service Status        : Running
Proxy for IVX Communication     : ENABLED
```

Applicable to:

NS-series and Virtual IPS Sensors

show ivxcloud stats

This command displays statistics specific to IVX Cloud.

Syntax:

`show ivxcloud stats`

Information displayed by the **`show ivxcloud stats`** command includes the following:

- Counters related to authentication
- Counters related to md5 cache when configured with IVX Cloud
- Counters related to file submission to IVX Cloud
- Counters related to report status

Sample Output:

```
intruShell@john> show ivxcloud stats
[ Auth ]
Auth requests sent : 102
Auth responses received : 72
Auth responses as OK : 74
Auth errors : 28
Last Auth time : Thu Dec 14 05:50:42 2023
Last auth error time : Thu Dec 14 00:15:54 2023
Max Auth time (sec.): 2

[ Cache ]
md5 cache requests : 0
md5 cache responses : 0
md5 cache misses : 0
md5 missed due to Throttling  : 0
md5 cache timeouts : 0
md5 cache errors : 0
Last md5 query time : NA
Last md5 query error time : NA
Last md5 query file md5 : NA
Last md5 query file name : NA
Last md5 response file md5 : NA
Last md5 query time (sec.) : 0
Last md5 drop time : NA
```

```
[ File Submission ]
Submission requests sent : 0
Submission responses received : 0
Submission errors : 0
Submission response parse errors : 0
Submission Timeouts : 0
Last submit time : NA
Last submitted file md5 : NA
Last submitted file name : NA
Last submission error time : NA
Max scan time (sec.) : 0
Max upload time (sec.) : 0

[ Reports status ]
Report requests sent : 0
Report responses received : 0
Report responses successful : 0
Report responses with errors : 0
Report response parse errors : 0
Timeouts in receiving responses : 0
Reports/Results Pending : 0
Pending list free nodes : 200
Pending ignored (timedout): 0
Pending list errors : 0
Last report time : NA
Last report error time : NA
Last report file md5 : NA
Max report poll time (sec.) : 0

Scan requests received : 0
Number of files ignored(load) : 0
Number of files ignored(auth error) : 0
Number of files ignored(IVX disabled) : 0
Last error reported : "Failed to connect to feapi.marketplace.apps.fireeye.com
port 443: Connection refused"
```

NOTE

In some cases, IVX Cloud might be reporting multiple HTTP 4xx errors. If you encounter such errors, please contact Trellix support.

Applicable to:

NS-series and Virtual IPS Sensors

show ivxcloud status

This command displays the connection status of the IVX Cloud.

Syntax:

`show ivxcloud status`

Sample Output:

```
intruShell@john> show ivx status
IVX engine connection status    : Connected
IVX engine curl-verbose         : Disabled
```

Applicable to:

NS-series and Virtual IPS Sensors

show l2OnDropsConfig

The command displays the status configurations of Layer 2 mode on drops.

Syntax:

`show l2OnDropsConfig`

Sample Output:

`intruShell@john> show l2OnDropsConfig`

`L2OnDrops Stats: Enabled`

`L2OnDrops Sensitivity Level: High`

Applicable to:

NS-series Sensors

show l7ae status

The command displays the layer7 application analysis configuration.

Syntax:

`show l7ae status`

Sample Output:

`intruShell@john> show l7ae status`

`IS Attack Detection status: Good`

Applicable to:

NS-series Sensors

show l7ddosstat

This command displays the various layer 7 DDoS related statistics.

Syntax

```
show l7ddosstat
```

Sample output

```
intruShell@john> show l7ddosstat

[L7 DDOS Stats]

L7ddos active http connections : 10000

L7ddos Drop Count : 1426

L7ddos Slow Connections closed : 0

L7ddos Challenge Sent Count : 2

L7ddos Challenge Valid Count : 1

L7ddos Challenge Failed Count : 0
```

Applicable to:

NS-series Sensors

show layer2 forward intfport

The command displays the layer2 forward statistics for the configured scanning exception rules.

Syntax:

```
show layer2 forward intfport <port>
```

Parameter	Description
<port>	Sets the port for which the status is to be displayed. Valid port numbers for NS-series are: G0/1 | G0/2 | G1/1 | G1/2 | G1/3 | G1/4 | G1/5 | G1/6 | G1/7 | G1/8 | G1/9 | G1/10 | G1/11 | G1/12 | G2/1 | G2/2 | G2/3 | G2/4 | G2/5 | G2/6 | G2/7 | G2/8 | G2/9 | G2/10 | G2/11 | G2/12 | G3/1 | G3/2 | G3/3 | G3/4 | G3/5 | G3/6 | G3/7 | G3/8 | all

Sample Output:

```
intruShell@john> show layer2 forward intfport G1/8

Layer2 forward packets : 0
```

Applicable to:

NS-series Sensors

show layer2 mode

This command displays all the Layer 2 Passthru feature settings. These settings are configured in the Manager user interface; some of the settings are configured through the CLI. Layer 2 Passthru is configured within the Manager user interface.

This command has no parameters.

Syntax:

`show layer2 mode`

Information displayed by the show layer2 mode command includes the following:

- Status of the Layer 2 Passthru feature (whether it is on or off)
- The set duration
- The set threshold
- The number of occurrences that have occurred within the previous duration

Sample Output:

```
intruShell@john> show layer2 mode

Mode : on

Duration : 10 minutes

Threshold : 1

Occurrences : 0
```

Applicable to:

NS-series Sensors

show malwareenginestats

This command displays the malware engine statistics.

This command has no parameters.

Syntax:

`show malwareenginestats`

Sample Output:

```
intruShell@NS9500> show malwareenginestats
MALWARE STATISTICS FOR IPS Analysis(pdf) Engine:
-----------------------------------------------
Files Submitted: 0
Files Processed: 0

Clean Files: 0
Very High Malware Confidence Matches: 0
High Malware Confidence Matches: 0
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
```

```
Unknown Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0

MALWARE STATISTICS FOR IPS Analysis(flash) Engine:
-------------------------------------------------
Files Submitted: 0
Files Processed: 0

Clean Files: 0
Very High Malware Confidence Matches: 0
High Malware Confidence Matches: 0
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
Unknown Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0

MALWARE STATISTICS FOR IPS Analysis(office) Engine:
--------------------------------------------------
Files Submitted: 0
Files Processed: 0

Clean Files: 0
Very High Malware Confidence Matches: 0
High Malware Confidence Matches: 0
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
Unknown Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0

MALWARE STATISTICS FOR Gateway Anti-Malware ENGINE:
---------------------------------------------------
Files Submitted: 0
Files Processed: 0

Clean Files: 0
Very High Malware Confidence Matches: 0
High Malware Confidence Matches: 0
```

```
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
Unknown Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0

MALWARE STATISTICS FOR GTI FILE Reputation ENGINE:
-------------------------------------------------
Files Submitted: 0
Files Processed: 0

Clean Files: 0
Very High Malware Confidence Matches: 0
High Malware Confidence Matches: 0
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
Unknown Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0

MALWARE STATISTICS FOR FILE SAVE ENGINE:
-------------------------------------------------
Files Submitted: 0
Files Processed: 20

MALWARE STATISTICS FOR BLOCKLIST ENGINE:
-------------------------------------------------
Files Submitted: 0
Files Processed: 0

Very High Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0



MALWARE STATISTICS FOR Trellix Intelligent Sandbox ENGINE:
-------------------------------------------------
Files Submitted: 0
Files Processed: 0
```

```
Number of files dropped by TIS under load/error: 0
Clean Files: 0
Very High Malware Confidence Matches: 0
High Malware Confidence Matches: 0
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
Unknown Malware Confidence Matches: 0

Alert Generated: 0
Files Blocked: 0
Connection Reset: 0

MALWARE STATISTICS FOR IVX ENGINE:
-------------------------------------------------
Files Submitted: 20
Files Processed: 20

Number of files ignored(load): 0
Number of files ignored(auth error): 0
Number of files ignored(IVX disabled): 0
Clean Files: 0
Very High Malware Confidence Matches: 20
High Malware Confidence Matches: 0
Medium Malware Confidence Matches: 0
Low Malware Confidence Matches: 0
Very Low Malware Confidence Matches: 0
Unknown Malware Confidence Matches: 0

Alert Generated: 20
Files Blocked: 20
Connection Reset: 20
```

Applicable to:

NS-series Sensors.

show malwarefilestats

The **show malwarefilestats** command displays the malware file statistics.

This command has no parameters.

Syntax:

show malwarefilestats

Sample Output:

intruShell@john> show malwarefilestats

```
MALWARE STATISTICS FOR PE (EXE,DLL,SYS,COM,etc.) Files:

Number of files sent: 2

Number of response Received: 2

Number of files ignored: 0

MALWARE STATISTICS FOR MS Office Files:

------------------------------------------------------------

Number of files sent: 11355

Number of response Received: 9403

Number of files ignored: 1952

MALWARE STATISTICS FOR PDF Files:

------------------------------------------------------------

Number of files sent: 0

Number of response Received: 0

Number of files ignored: 0

MALWARE STATISTICS FOR Compressed (Zip,RAR) Files:

------------------------------------------------------------

Number of files sent: 15987

Number of response Received: 14601

Number of files ignored: 1386

MALWARE STATISTICS FOR APK Files:

------------------------------------------------------------

Number of files sent: 118

Number of response Received: 94

Number of files ignored: 24

MALWARE STATISTICS FOR JAR Files:

------------------------------------------------------------

Number of files sent: 466

Number of response Received: 399

Number of files ignored: 67
```

```
MALWARE STATISTICS FOR Flash Files:

-----------------------------------------------------------

Number of files sent: 31

Number of response Received: 27

Number of files ignored: 4
```

Applicable to:

NS-series Sensors

show managercacertinfo

This command displays detailed information of the CA-signed leaf certificate of the Manager when the Sensor has established trust using CA-signed certificate.

Syntax:

```
show managercacertinfo
```

Sample output:

```
intruShell@CC_NS-9200> show sensorcacertinfo

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

98:a5:29:46:e2:45:91:c1

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=CA, L=locality, O=TrellixOrgName, OU=NSBU_OrgUnit, CN=CN_ICA4/emailAddress=pra-
nay@ica4.com

Validity

Not Before: Jul 16 09:59:00 2018 GMT

Not After : Jul 18 09:59:00 2018 GMT

Subject: C=US, ST=sensor_state, L=sensor_city, O=sensor_org, OU=sensor_depart, CN=sensor_16th_July

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)
```

```
Modulus:
00:e2:3a:0e:8b:e2:54:a7:e5:91:70:0c:95:c9:2e:
02:9a:9c:a8:e5:f7:ee:7d:78:ed:ac:a1:50:21:6b:
d5:e7:e7:61:30:be:1c:fa:3b:59:ed:d5:0d:67:46:
eb:03:0f:17:99:93:16:ca:a5:4a:ea:63:44:3c:f7:
48:6a:7b:eb:e3:f3:df:f1:c1:8d:57:ef:ff:6f:7f:
b2:93:d4:e6:90:63:56:91:fa:25:30:c7:99:38:45:
d8:36:21:81:bd:a7:09:87:6b:8f:f1:5e:02:d4:24:
aa:90:df:bb:f9:7f:9f:f8:13:2d:60:9a:71:94:1c:
72:bb:b0:e9:8c:3a:b9:23:bf:fd:f8:ff:d8:d0:d1:
b9:77:4a:6e:49:74:ab:d8:72:7c:eb:c5:39:7b:d5:
4c:59:e7:f8:34:3d:11:e4:32:a9:8f:f8:45:f5:d4:
40:54:c4:cf:ac:03:0f:e3:0f:4f:c6:d8:af:ea:48:
ce:26:8d:3f:bb:6d:5b:00:42:08:c0:3c:c8:6b:0b:
5f:a1:b3:47:41:0e:7c:e2:51:f3:a7:54:cf:6d:7a:
a6:83:70:7e:2e:43:5c:d9:9d:eb:53:09:01:ac:48:
6c:2c:e6:80:22:a5:bd:19:79:05:88:4f:2d:72:57:
c8:f4:29:b7:12:78:41:4e:ee:aa:e2:b8:7e:61:fc:
dd:61
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign, Encipher Only,
Decipher Only
X509v3 Extended Key Usage: critical
TLS Web Server Authentication, TLS Web Client Authentication , E-mail Protection, Time Stamping,
Microsoft Commercial Code Signing, Microsoft Server Gated Crypto, Microsoft Encrypted File System
Signature Algorithm: sha256WithRSAEncryption
```

```
69:32:ad:ad:5b:5a:2a:e5:d5:00:be:4b:cd:ed:f5:d9:06:77:

21:27:be:78:ba:e2:52:3d:51:57:1f:cc:79:14:77:23:55:b3:

c8:ab:7d:bf:9a:b8:58:89:f9:fd:34:ac:b7:fb:30:f1:0a:37:

3a:9e:dc:73:c0:50:1d:32:be:4b:73:18:41:3c:46:ea:a8:fa:

00:be:b5:fa:4c:2d:82:8d:4f:86:f4:11:df:cc:13:9d:12:b0:

12:e8:50:1e:50:ff:12:52:d0:bf:ef:5f:55:34:f6:61:c7:21:

7c:58:f4:cf:6d:cf:79:a0:ed:7b:12:2a:b5:19:21:de:99:1b:

13:46:c4:a1:28:db:18:35:ff:b0:1e:ea:67:13:50:c7:0d:a4:

ab:dc:e2:ee:eb:25:b2:96:cb:23:8d:d0:c7:a2:4b:c5:67:ba:

99:98:aa:e6:04:d7:d1:1d:f6:e7:77:2a:fa:0c:ea:ee:c0:68:

b2:b8:8f:7f:19:3e:a4:a0:57:be:f7:c8:cd:00:8c:c0:0b:25:

65:d9:43:11:d9:4c:36:c1:b0:c6:8f:a8:ef:19:13:bd:03:3e:

0c:1b:4b:60:89:fd:d8:6c:51:04:ba:3b:c2:ee:0d:e0:f3:76:

56:d6:8b:c5:e2:c6:94:48:a6:c6:94:73:83:84:99:e0:83:73:

7c:d3:c4:1d
```

Applicable to:

NS-series Sensors

show mem-usage

This command displays the system memory usage details of the device.

This command has no parameters.

Syntax:

```
show mem-usage
```

The **show mem-usage** command also gives the average percentage usage (Avg.) and the maximum percentage usage (Max.) of these entities on all the processing elements.

The L7Dcap counter descriptions are as follows:

- **Avg. Used L7 Dcap flows across all PEs** — Average percentage of L7Dcap flows used from the value configured in the Manager across all the Processing Engines in the Sensor
- **Max. Used L7 Dcap flows on a single PE** — Percentage of L7Dcap flows used from the maximum value that a single Processing Engine manages

Sample Output:

- For Sensors, the output is as shown below:

```
Avg. Used TCP and UDP Flows across all PEs : 0%
Max. Used TCP and UDP Flows on a single PE : 0%
Avg. Used Fragmented IP Flows across all PEs : 0%
Max. Used Fragmented IP Flows on a single PE : 0%
Avg. Used ICMP Flows across all PEs : 0%
Max. Used ICMP Flows on a single PE : 0%
Avg. Used SSL Flows across all PEs : 0%
Max. Used SSL Flows on a single PE : 0%
Avg. Used Fragment Reassembly Buffers across all PEs : 0%
Max. Used Fragment Reassembly Buffers on a single PE : 0%
Avg. Used Packet Buffers across all PEs : 0%
Max. Used Packet Buffers on a single PE : 0%
Avg. Used Attack Marker Nodes across all PEs : 0%
Max. Used Attack Marker Nodes on a single PE : 0%
Avg. Used Shell Marker Nodes across all PEs : 0%
Max. Used Shell Marker Nodes on a single PE : 0%
Avg. Used L7 Dcap flows across all PEs : 0%
Max. Used L7 Dcap flows on a single PE : 0%
```

Applicable to:

NS-series Sensors

show mgmtport

The **show mgmtport** command displays all the current configuration settings for the Sensor Management port.

This command has no parameters.

Syntax:

```
show mgmtport
```

Information displayed by the **show mgmtport** command includes the following:

- The Sensor's Management port value (10000Mbps, 1000Mbps, 100Mbps, or auto-negotiate)
- The Sensor's Management port link status (what speed the two devices settled upon—typically the highest common setting)
- What mode has been settled upon
- The link status
- The capabilities of the Management port (possible values are: 10000baseTx-FD, 1000baseTx-FD, 100baseTx-FD, 100baseTx-HD)

- What the Management port is advertising its capabilities as (possible values are: 10000baseTx-FD, 1000baseTx-FD, 100baseTx-FD, 100baseTx-HD)
- The characteristics of its link partner (possible values are: 10000baseTx-FD, 1000baseTx-FD, 100baseTx-FD, 100baseTx-HD)

Sample Output:

For Sensor, the output is as shown below:

```
intruShell@john> show mgmtport

MGMT Ethernet port : auto negotiated

Settings for MGMT port :

Supported link modes: 100baseT/Full

1000baseT/Full

10000baseT/Full

Advertised link modes: 100baseT/Full

1000baseT/Full

10000baseT/Full

Advertised pause frame use: No

Advertised auto-negotiation: Yes

Speed: 1000Mb/s

Duplex: Full

Auto-negotiation: on

Link detected: yes

eth0 Link encap:Ethernet HWaddr 00:1E:67:BB:B3:B1

inet addr:10.208.15.91 Bcast:0.0.0.0 Mask:255.255.255.0

inet6 addr: fe80::21e:67ff:febb:b3b1/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:13164765 errors:0 dropped:1216912 overruns:0 frame:0

TX packets:1886946 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:7487476603 (7140.6 Mb) TX bytes:175263884 (167.1 Mb)
```

Applicable to:

NS-series Sensors

show mnsconfig

This command displays the status of mobile network security (enabled or disabled).

Syntax

```
show mnsconfig
```

Sample output

```
intruShell@Sensor-6050> show mnsconfig

Mobile network security status : Disabled

Radius Load balancing config : Disabled
```

Applicable to:

NS-series Sensors

show msoffice-fdi stats

This command displays number of MS Office sub-files (files compressed within a file) and total compressed bytes sent for decompression as part of MS Office file deep inspection. It also displays average size of decompressed files in bytes.

This command has no parameters.

Syntax:

```
show msoffice-fdi stats
```

Sample Output:

```
intruShell@NS-9100> show msoffice-fdi stats

Note: Below all stats are for MS-Office sub files (files compressed within MS-Office file)

Number of files submitted for decompression : 6

Total compressed bytes sent for decompression : 6595

Total decompressed bytes : 36138

Avg size of decompressed file(bytes) : 6023
```

Applicable to:

NS-series and Virtual IPS Sensors

show netstat

This command displays the management port netstat output.

This command has no parameters.

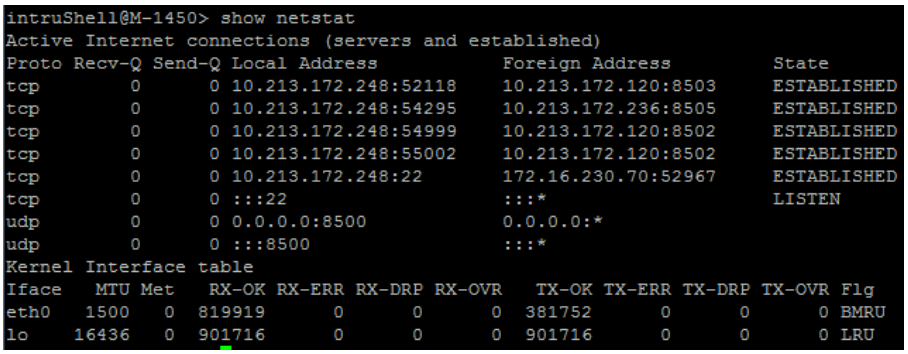
Syntax:

show netstat

Sample Output:

- For Sensor, the output is as shown

Figure 815. show netstat command output for Sensors



Applicable to:

NS-series Sensors

show nmsuserwriteaccess status

This command displays the current SNMP restricted read-write access status (enabled or disabled).

Syntax:

show nmsuserwriteaccess status

Sample Output:

intruShell@john> show nmsuserwriteaccess status

NMS User Write Access Status : Enabled

Applicable to:

NS-series Sensors

show outofcontext acllookup

This command displays whether ACL lookup is enabled or disabled on out-of-order packets.

Syntax:

show outofcontext acllookup

Sample Output:

intruDB > show outofcontext acllookup

OOC Acl Lookup Status : Disabled

Applicable to:

NS-series Sensors

show parsetunneledtraffic status

Use the **`show parsetunneledtraffic status`** CLI command to know the current status of tunneling configuration.

This command has no parameters.

To enable or disable the tunneling configuration of a Sensor, use the **`set parsetunneledtraffic`** command. For more information on tunneling configuration, see the *Trellix Intrusion Prevention System Product Guide*.

Syntax:

```
show parsetunneledtraffic status
```

Sample Output:

```
intruShell@john> show parsetunneledtraffic status

Tunneling Status : Enabled
```

Applicable to:

NS-series and Virtual IPS Sensors. For Virtual Security System instances, this command is available in debug mode.

show pktcapture status

This CLI command displays the packet capture status and configuration.

> **NOTE**
>
> If you observe any errors or memory leaks in the **`show pktcapture status`** command output, you must tune the packet capture filters. If the **`Frontend Packet Capture Mbuf Clone Error Cnt`** is non-zero and increasing, you must reboot the Sensor.

Syntax:

```
show pktcapture status
```

Sample Output:

Normal mode:

```
IntruShell@Test-Sensor#> show pktcapture status

Packet Capture Status :Not Running

Send Captured Packets To :Manager

Packet Capture Rule Set File Status :Present

Packet Capture File Status :PCAP File Not Present
```

```
Total Packet Capture Count :0

File Max Size :100 MB
```

Debug mode:

```
IntruDbg#> show pktcapture status

Packet Capture Status :Running

Send Captured Packets To :Manager

Packet Capture Rule Set File Status :Not Present

Packet Capture File Status :PCAP File Not Present

Datapath 0 :

l7ae Egress matched pkt sent cnt :13693

l7ae Egress pkt clone err cnt :0

l7ae Egress pkt chain err cnt :0

l7ae Egress pkt capture enable cnt :0

l7ae Egress pkt capture disable cnt :0

l7ae Egress Jumbo pkt skip cnt :0

.....

Datapath 15 :

l7ae Egress matched pkt sent cnt :171626

l7ae Egress pkt clone err cnt :0

l7ae Egress pkt chain err cnt :0

l7ae Egress pkt capture enable cnt :0

l7ae Egress pkt capture disable cnt :0

l7ae Egress Jumbo pkt skip cnt :0

Across All datapaths

l7ae Egress matched pkt sent cnt :1788707

l7ae Egress pkt clone err cnt :0

l7ae Egress pkt chain err cnt :0

l7ae Egress Jumbo pkt skip cnt :0

Frontend Egress Matched Pkt Sent Cnt :174147703
```

```
Frontend Ingress Matched Pkt Sent Cnt :175939455

Frontend Ingress Pkt Capture Jumbo Frames Skip Cnt :0

Frontend Egress Pkt Capture Jumbo Frames Skip Cnt :0

Frontend Packet Capture Mbuf Clone Error Cnt :0

Frontend Packet Capture Mbuf Chain Error Cnt :0

Frontend Packet Capture Enable Count :0

Frontend Packet Capture Disable Count :0

Total Packet Capture Count :327136912

File Max Size :100 MB
```

This command displays the following additional counters in debug mode:

- **l7ae Egress matched pkt sent cnt** - Number of matched incoming packets that are sent from each backend processor to the packet capture process
- **l7ae Egress pkt clone err cnt** - Number of clone errors for outgoing packets on each backend processor
- **l7ae Egress pkt chain err cnt** - Number of mbuf chain errors encountered for outgoing packets
- **l7ae Egress pkt capture enable cnt** - Number of times the packet capture filter is applied for each backend processor
- **l7ae Egress pkt capture disable cnt** - Number of times the packet capture filter is removed from each backend processor
- **Frontend Ingress Matched Pkt Sent Cnt** - Number of matched incoming packets that are sent to packet capture process from frontend processor
- **Frontend Egress Matched Pkt Sent Cnt** - Number of matched outgoing packets sent to packet capture process from frontend processor
- **Frontend Packet Capture Mbuf Clone Error Cnt** - Number of mbuf clone errors
- **Frontend Packet Capture Mbuf Chain Error Cnt** - Number of mbuf chain error
- **Frontend Packet Capture Enable Count** - Number of times the packet capture filter is applied for frontend processor
- **Frontend Packet Capture Disable Count** - Number of times the packet capture filter is removed from frontend processor

Applicable to:

NS-series Sensors

show pluggable-module

This command displays the status of the pluggable module(s) inserted into the specified slot(s) located within the chassis front panel.

Syntax:

```
show pluggable-module (g1|g2|g5|g6|all)
```

Sample output:

```
intruShell@NS9300-Bohol2> show pluggable-module g2

[Port Module G2 ]

Module System Type : 8-port SFP+

Supported Speeds : 10Gbps/1Gbps

Module Status : Active

Total Ports : 8
```

Applicable to:

NS7x00 and NS9x00 Sensors

show portsettletime

This command displays the configured portsettletime.

This command has no parameters.

Syntax:

```
show portsettletime
```

Sample Output:

```
intruShell@john> show portsettletime

Port settle delay : 30 seconds
```

Applicable to:

NS-series Sensors

show powersupply

When executed, this CLI command displays the Sensor power supply information.

Syntax:

```
show powersupply
```

Sample Output:

```
intruShell@john> show powersupply

Power Supply (A) : Present : health = OK

Power Supply (B) : Present : health = NOPOWER
```

Applicable to:

NS-series Sensors

show previous256byteslogging status

This command displays the status of the previous 256 bytes logging feature — whether enabled or disabled.

Syntax

```
show previous256byteslogging status
```

Sample output

```
intruShell@Sensor-6050> show previous256byteslogging status

Logging of previous 256bytes is disabled.
```

Applicable to:

NS-series Sensors

show raid status

This command displays the operation status of both SSDs in Trellix Intrusion Prevention System operating in RAID1 mode.

> **NOTE**
>
> RAID is not supported on NS7500, NS7x50, NS7x00, NS5x00, and NS3x00 Sensors.

Syntax:

```
show raid status
```

Sample output:

```
intruShell@NS9300-Bohol2> show raid status

SSD 0 STATUS : good

SSD 1 STATUS : good

NS9300 Secondary SSD 0 STATUS : good

NS9300 Secondary SSD 1 STATUS : good
```

Applicable to:

NS9500, NS9300, NS9200, and NS9100 Sensors

show rescueimages

The **`show rescueimages`** CLI command displays version numbers of a list of up to five Sensor images currently archived in the internal flash device.

Syntax:

show rescueimages

Sample output:

intruShell@NS9300-Bohol2> show rescueimages

NS9300P

NS9300S

Applicable to:

NS-series Sensors

show respport r1

This command displays all the current configuration settings for the Sensor Response port.

This command has no parameters.

Syntax:

show respport r1

On executing the command, the information displayed in the output includes the following:

- The Sensor's Response port value (1000Mbps, 100Mbps, 10Mbps, or auto-negotiate)
- The Sensor's Response port link status (what speed the two devices settled upon—typically the highest common setting)
- What mode has been settled upon
- The link status
- Statistics for the Response port

Sample Output:

intruShell@john> show respport r1

Response Ethernet port : auto negotiated

Settings for MGMT port :

Supported link modes: 100baseT/Full

1000baseT/Full

10000baseT/Full

Advertised link modes: 100baseT/Full

1000baseT/Full

10000baseT/Full

Advertised pause frame use: No

Advertised auto-negotiation: Yes

```
Speed: Unknown!

Duplex: Unknown! (255)

Auto-negotiation: on

Link detected: no

eth1 Link encap:Ethernet HWaddr 00:1E:67:58:9E:3F

UP BROADCAST MULTICAST MTU:1500 Metric:1

RX packets:0 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

Response Port Statistics

Total Packets Sent : 0
```

Applicable to:

NS-series Sensors

show savedalertinfo

In the event that connectivity between the Sensor and the Manager is interrupted, the Sensor saves alert data internally. This data is sent to the Manager when connectivity is re-established and the internal information is deleted. This command shows the number of alerts and packet logs that have been saved within the Sensor.

Information displayed by the **`show savedalertinfo`** command includes the following:

- Whether a file of saved alerts exists (if the connectivity between Sensor and Manager is currently established, no file will exist)
- Number of saved alerts and their size
- Whether a file of saved packet logs exists
- Number of saved packet logs and their size

This command has no parameters.

Syntax:

```
show savedalertinfo
```

Sample Output:

```
intruShell@john> show savedalertinfo

Saved Alert Status : Alerts = 456, Size = 81168

Saved Packet Status : No Saved File
```

Applicable to:

NS-series Sensors

show savedimages

This command displays version numbers of a list of up to ten Sensor images currently archived in the SSD.

Syntax:

```
show savedimages
```

Sample Output:

```
intruShell@NS9500> show savedimages

10.1.5.92

10.1.5.107

10.1.5.116

10.1.5.153

10.1.5.170
```

Applicable to:

NS-series Sensors only

show sensorcacertinfo

This command displays detailed information of the CA-signed leaf certificate of the Sensor.

Syntax:

```
show sensorcacertinfo
```

Sample output:

```
intruShell@CC_NS-9200> show sensorcacertinfo

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

98:a5:29:46:e2:45:91:c1

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=CA, L=locality, O=TrellixOrgName, OU=NSBU_OrgUnit, CN=CN_ICA4/emailAddress=pra-
nay@ica4.com
```

```
Validity

Not Before: Jul 16 09:59:00 2018 GMT

Not After : Jul 18 09:59:00 2018 GMT

Subject: C=US, ST=sensor_state, L=sensor_city, O=sensor_org, OU=sensor_depart, CN=sensor_16th_July

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:e2:3a:0e:8b:e2:54:a7:e5:91:70:0c:95:c9:2e:

02:9a:9c:a8:e5:f7:ee:7d:78:ed:ac:a1:50:21:6b:

d5:e7:e7:61:30:be:1c:fa:3b:59:ed:d5:0d:67:46:

eb:03:0f:17:99:93:16:ca:a5:4a:ea:63:44:3c:f7:

48:6a:7b:eb:e3:f3:df:f1:c1:8d:57:ef:ff:6f:7f:

b2:93:d4:e6:90:63:56:91:fa:25:30:c7:99:38:45:

d8:36:21:81:bd:a7:09:87:6b:8f:f1:5e:02:d4:24:

aa:90:df:bb:f9:7f:9f:f8:13:2d:60:9a:71:94:1c:

72:bb:b0:e9:8c:3a:b9:23:bf:fd:f8:ff:d8:d0:d1:

b9:77:4a:6e:49:74:ab:d8:72:7c:eb:c5:39:7b:d5:

4c:59:e7:f8:34:3d:11:e4:32:a9:8f:f8:45:f5:d4:

40:54:c4:cf:ac:03:0f:e3:0f:4f:c6:d8:af:ea:48:

ce:26:8d:3f:bb:6d:5b:00:42:08:c0:3c:c8:6b:0b:

5f:a1:b3:47:41:0e:7c:e2:51:f3:a7:54:cf:6d:7a:

a6:83:70:7e:2e:43:5c:d9:9d:eb:53:09:01:ac:48:

6c:2c:e6:80:22:a5:bd:19:79:05:88:4f:2d:72:57:

c8:f4:29:b7:12:78:41:4e:ee:aa:e2:b8:7e:61:fc:

dd:61

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical
```

```
CA:FALSE

X509v3 Key Usage:

Digital Signature, Key Encipherment, Data Encipherment, Certificate Sign, CRL Sign, Encipher Only,
Decipher Only

X509v3 Extended Key Usage: critical

TLS Web Server Authentication, TLS Web Client Authentication , E-mail Protection, Time Stamping,
Microsoft Commercial Code Signing, Microsoft Server Gated Crypto, Microsoft Encrypted File System

Signature Algorithm: sha256WithRSAEncryption

69:32:ad:ad:5b:5a:2a:e5:d5:00:be:4b:cd:ed:f5:d9:06:77:

21:27:be:78:ba:e2:52:3d:51:57:1f:cc:79:14:77:23:55:b3:

c8:ab:7d:bf:9a:b8:58:89:f9:fd:34:ac:b7:fb:30:f1:0a:37:

3a:9e:dc:73:c0:50:1d:32:be:4b:73:18:41:3c:46:ea:a8:fa:

00:be:b5:fa:4c:2d:82:8d:4f:86:f4:11:df:cc:13:9d:12:b0:

12:e8:50:1e:50:ff:12:52:d0:bf:ef:5f:55:34:f6:61:c7:21:

7c:58:f4:cf:6d:cf:79:a0:ed:7b:12:2a:b5:19:21:de:99:1b:

13:46:c4:a1:28:db:18:35:ff:b0:1e:ea:67:13:50:c7:0d:a4:

ab:dc:e2:ee:eb:25:b2:96:cb:23:8d:d0:c7:a2:4b:c5:67:ba:

99:98:aa:e6:04:d7:d1:1d:f6:e7:77:2a:fa:0c:ea:ee:c0:68:

b2:b8:8f:7f:19:3e:a4:a0:57:be:f7:c8:cd:00:8c:c0:0b:25:

65:d9:43:11:d9:4c:36:c1:b0:c6:8f:a8:ef:19:13:bd:03:3e:

0c:1b:4b:60:89:fd:d8:6c:51:04:ba:3b:c2:ee:0d:e0:f3:76:

56:d6:8b:c5:e2:c6:94:48:a6:c6:94:73:83:84:99:e0:83:73:

7c:d3:c4:1d
```

Applicable to:

NS-series Sensors

show sensordroppktevent status

This CLI command displays whether the option to generate a system fault in the Manager (whenever the Sensor is overloaded and drops a large number of packets) is enabled or disabled.

This command has no parameters.

Syntax:

show sensordroppktevent status

Applicable to:

NS-series Sensors

In case of Virtual Security System instances, this command is available in debug mode.

show sensor-load

This **show sensor-load** command shows you the following information:

- Average of load (traffic) seen on all processing elements
- Maximum of load (traffic) seen on a single processing element

Syntax:

show sensor-load

Sample Output:

On executing the command, the following messages are displayed:

- When the Sensor-load in ON

  intruShell@john> show sensor-load

  Average load across all PEs : 0% (approx.)

  Maximum load on a single PE : 0% (approx.)

- When the Sensor-load is OFF

  CPU usage tracking is currently disabled. It can be enabled on the Advanced Device Settings page of the Manager GUI.

Applicable to:

NS-series Sensors

show sessionlimit timeout

This command is used to display the session limit timeout set previously using the **set sessionlimit timeout** command.

Syntax:

show sessionlimit timeout

Sample Output:

intruShell@john> show sessionlimit timeout

sessionlimit timeout : 2hours

Applicable to:

NS-series Sensors

show snort config

The **show snort config** command displays the Snort engine configuration as selected through the Trellix IPS Manager.

Syntax:

```
show snort config
```

Sample Output:

```
[Snort Rule Engine Support]

Requested : Suricata Snort

Active : Suricata Snort
```

> **NOTE**
>
> You should reboot the Sensor if the **Requested** and **Active** values are different.

Applicable to:

NS-series Sensors (except for NS7600 and NS3600 Sensors)

show ssh config

This command displays the current ssh package version, ciphers, and protocols used in client and server profile.

Syntax:

```
show ssh config
```

Sample Output

```
intruShell@RTB_9500_14_43> show ssh config

SSH Version: OpenSSH_7.8p1, OpenSSL 1.0.2zf-fips 21 Jun 2022

SSH Client Configuration :

Ciphers : aes256-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com

MACs : hmac-sha2-256,hmac-sha2-512

KexAlgorithms : ecdh-sha2-nistp256

SSH Server Configuration :

Ciphers : aes256-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com

MACs : hmac-sha2-256,hmac-sha2-512

KexAlgorithms : ecdh-sha2-nistp256

Public key Authentication : Enabled
```

```
Password Authentication : Enabled
```

Applicable to:

NS-series and Virtual IPS Sensors

show sshaccesscontrol status

This command displays the SSH access control configuration status and settings.

Syntax:

```
show sshaccesscontrol status
```

Sample Output:

```
intruShell@john> show sshaccesscontrol status

[SSH AccessControl is Disabled]

[SSH Accesscontrol Network list]

Network : any/any
```

Applicable to:

NS-series Sensors

show sshauth status

The **show sshauth status** command, when executed on CLI, displays the SSH authentication status.

Syntax:

```
show sshauth status
```

Sample output:

```
SSH PasswordAuthentication : Enabled

SSH PublicKeyAuthentication : Enabled
```

Applicable to:

NS-series Sensors

show sshinactivetimeout

This command displays the CLI SSH session inactivity timeout.

Syntax:

```
show sshinactivetimeout
```

Sample Output:

```
intruShell@john> show sshinactivetimeout

SSH inactive timeout : 300 sec
```

Applicable to:

NS-series Sensors

show sshlog status

Use this command to display the current SSH logging status.

Syntax:

```
show sshlog status
```

Sample Output:

```
intruShell@john> show sshlog status

SSH Logging : Enabled
```

Applicable to:

NS-series Sensors

show sslcert-usage

It displays the following certificate details for all the certificates used for the known-key method:

- Name of the certificate
- Certificate ID
- Certificate issuer details
- Last time the certificate was used

Syntax:

```
show sslcert-usage
```

Sample Output:

```
intruShell@Sensor-1> show sslcert-usage

SSL cert serialNum 18B13FDBADA074FC3C28F

SSL cert id 1001

SSL issuer /C=IN/ST=KA/L=BGL/O=Trellix/OU=Eng/CN=default_server_cert_1k_1/emailAddress=xyz@trel-
lix.com

SSL certMatch Time 1/1/1970 - 0:00:00 UTC

============================
```

Applicable to:

NS-series and Virtual IPS Sensors

show ssl config

The **show ssl config** command displays the configuration details for SSL on the Sensor.

This command has no parameters.

Information displayed by the **show ssl config** command includes the following:

- Whether SSL will be enabled the next time the Sensor reboots, and how many SSL flows will be supported
- Whether SSL decryption is currently active and how many SSL flows are supported
- How long the session is kept alive after the connection associated with that session ends (default is 5 minutes)
- Whether the packet logging is enabled for attacks detected in an SSL tunnel
- Whether SSL decryption keys are present on the Sensor
- The number of SSL decryption keys present

Syntax:

```
show ssl config
```

Sample Output:

```
intruShell@john> show ssl config

[SSL Decryption Support]

Requested : no

Supported : Inbound (200000 flows)

[Inbound]

SSL Session Lifetime : 5 min

SSL Pkt Logging : disabled

SSL Shared Key Decrypt : enabled

[SSL Decryption Keys]

Present : no
```

Applicable to:

NS-series Sensors

show ssl stats

This CLI command displays SSL decryption statistics for the Sensor.

SSL decryption is enabled in one direction at a given point of time. The command displays SSL statistics for the direction in which the decryption is enabled.

Syntax:

```
show ssl stats <inbound|outbound>
```

Applicable to:

NS-series Sensors

Inbound SSL Decryption

When SSL decryption is enabled only for RSA ciphers, the following information is displayed:

- The names of any certificates loaded into the Manager, and how many times they have been used in sessions since the Sensor was last rebooted.
- The number of certificates passed for which the Sensor had no matching certificates

When SSL decryption is enabled for DHE/ECDHE ciphers that includes RSA ciphers as well, the following information is displayed:

- Number of SSL records processed by the Sensor
- Number of matched shared SSL keys
- Number of Active SSL Agent connections for IPv4 and IPv6 IP addresses

Syntax:

```
show ssl stats inbound known-key
```

Sample output:

```
No Certs are present

[Certs Matched]

Number of certs Mismatched : 822

Number of SSL records processed by SSL module : 4998793

Matched SSL Shared Keys : 12

Total SSL Shared Keys : 79

Active SSL Agent connections(v4) : 81

Active SSL Agent connections(v6) : 0

Total SSL Agent connections(v4) : 87

Total SSL Agent connections(v6) : 0
```

Applicable to:

When using only RSA ciphers: NS-series Sensors

When using DHE/ECDHE ciphers: NS9500, NS9x00, NS7600, NS7500, NS7x00 and NS5x00 series Sensors

When SSL decryption is enabled using proxy, the following information is displayed:

- Name of the Certificate
- Number of times the certificate was used
- Number of times decryption was bypassed

Syntax:

```
show ssl stats inbound proxy <cpu|exceptions|port|sessions|sslinfo|status>
```

Parameter	Description
`cpu`	Displays the CPU utilization for the last 1, 4, and 64 seconds
`port`	Displays the statistics for the configured VLAN ports
`sessions`	Displays the number of sessions per port
`sslinfo`	Displays the statistics for the SSL connection, such as handshake, session information, and so on
`status`	Displays if SSL decryption is configured and enabled

Sample output:

```
intruShell@john-9500> show ssl stats inbound proxy status

Decryption configured: yes

Decryption enabled: yes

Decryption engine ready: yes

Engine provisioning status: (requested=yes ; done=yes)
```

Applicable to:

NS9500 and NS7500 Sensors only

Outbound SSL Decryption

The command displays the following information when outbound SSL decryption is enabled:

Parameter	Description
`cpu`	Displays the CPU utilization for the last 1, 4, and 64 seconds
`exceptions`	Displays the status for the exceptions added to the URL allow list
`port`	Displays the statistics for the configured VLAN ports
`sessions`	Displays the number of sessions per port
`sslinfo`	Displays the statistics for the SSL connection, such as handshake, session information, and so on
`status`	Displays if SSL decryption is configured and enabled

Syntax:

```
show ssl stats outbound proxy <cpu|exceptions|port|sessions|sslinfo|status>
```

Sample output:

```
intruShell@Perf_7200> show ssl stats outbound proxy status

Decryption configured: yes

Decryption enabled: yes

Decryption engine ready: yes

Engine provisioning status: (requested=yes ; done=yes)
```

Applicable to:

NS9500, NS9100, NS9200, NS7500, NS7300, and NS7200 Sensors

show ssl stats inbound known-key agents

This command displays the number of Agents connected to the Sensor.

It is applicable only when inbound SSL decryption is enabled for DHE/ECDHE ciphers.

Syntax:

```
show ssl stats inbound known-key agents
```

Sample output:

```
[Connected Agents]

10.1.2.3:35412(v4)

10.1.2.3:35352(v4)

10.1.2.3:35354(v4)

10.1.2.3:35358(v4)

10.1.2.3:35410(v4)

10.1.2.3:35408(v4)

10.1.2.3:35356(v4)

10.1.2.3:35361(v4)

10.1.2.3:35363(v4)

10.1.2.3:35367(v4)
```

Applicable to:

NS9500, NS9x00, NS7600, NS7500, NS7x00, NS5x00, and NS3600 series Sensors

show sslagentaccesscontrol status

This command displays the Trellix SSL Agent status and the number of connections from the Agents to the Sensor.

Syntax:

```
show sslagentaccesscontrol status
```

Sample output:

```
SSL Agent Accesscontrol MaxConnections: 256

[SSL Agent Accesscontrol Network list]

Network 1: 10.213.2.0/24

Network 2: 10.213.174.0/24

Network 3: 10.213.174.0/16

Network 4: 10.213.172.0/16

[IPv6 SSL Agent Accesscontrol Network list]

Network : none/none
```

Applicable to:

NS9500, NS9x00, NS7600, NS7500, NS7x00, NS5x00, and NS3600 series Sensors

show stack info

It displays the following details of a stack:

- Name of the stack
- Number of active nodes in the stack
- Node ID of the Sensor
- Node ID of the Sensor on the left in the stack
- Node ID of the Sensor on the right in the stack
- Node ID of the Sensor that is reachable from the port 0/1
- Node ID of the Sensor that is reachable from the port 1/1

Syntax:

```
show stack info
```

Sample Output:

```
intruShell@john> show syslog statistics

[Stack Info]

Stack Name : Stack

Current active nodes in Stack : 3

[Node Info]
```

```
Node Id : 3

Left Neighbor : None

Right Neighbor : 2

[Stacking Layout]

Reachable via stack port 1 : None

Reachable via stack port 2 : 2 (30Gbps)->1 (30Gbps)
```

Applicable to:

NS9500 stack Sensor

show suricata sbstats

This CLI command displays the rule, packet, and alert statistics of the Suricata Snort engine.

Syntax:

```
show suricata sbstats
```

Sample output:

```
Snort Rule Stats:

Total Rules Processed:: 6

Total Rules Loaded:: 6

Total Rules Failed:: 0

Snort Packet Stats:

Total pkts sent to Suricata:: 18289

Total tcp ctrl pkts sent to Suricata:: 127

Total tcp v6 ctrl pkts sent to Suricata:: 0

Total tcp data pkts sent to Suricata:: 0

Total tcp v6 data pkts sent to Suricata:: 0

Total udp pkts sent to Suricata:: 18098

Total udp v6 pkts sent to Suricata:: 0

Total icmp pkts sent to Suricata:: 64

Total icmp v6 pkts sent to Suricata:: 0

Snort Alert Stats:

Total Alerts:: 0
```

```
Alerts with Drop Action:: 0

Alerts for TCP Ctrl Pkts:: 0

Alerts for TCP Ctrl Pkts, with Drop Action:: 0

Alerts for TCP(IPv6) Ctrl Pkts:: 0

Alerts for TCP(IPv6) Ctrl Pkts, with Drop Action:: 0

Alerts for TCP Data Pkts:: 0

Alerts for TCP Data Pkts with Drop Action:: 0

Alerts for TCP(IPv6) Data Pkts:: 0

Alerts for TCP(IPv6) Data Pkts with Drop Action:: 0

Alerts for UDP Pkts:: 0

Alerts for UDP Pkts with Drop Action:: 0

Alerts for UDP(IPv6) Pkts:: 0

Alerts for UDP(IPv6) Pkts with Drop Action:: 0

Alerts for ICMP Pkts:: 0

Alerts for ICMP Pkts with Drop Alerts:: 0

Alerts for ICMP(IPv6) Pkts:: 0

Alerts for ICMP(IPv6) with Drop Action:: 0

Ignored Alerts:: 0
```

Applicable to:

NS-series Sensors (except for NS7600 and NS3600 Sensors)

show suricata enginestats

This command displays the statistics of the Suricata Snort engine.

Syntax:

```
show suricata enginestats
```

Sample output:

```
Snort Engine Stats:

DataPath:: 0

Ethernet packets:: 0

IPV4 packets:: 0
```

```
IPV6 packets:: 0

TCP packets:: 0

UDP packets:: 0

ICMPV4 packets:: 0

ICMPV6 packets:: 0

PPP packets:: 0

PPPOE packets:: 0

SCTP packets:: 0

SLL packets:: 0

GRE packets:: 0

Teredo packets:: 0

MPLS packets:: 0

Erspan packets:: 0

IPV4 in IPV6 packets:: 0

IPV6 in IPV6 packets:: 0

TCP sessions:: 0

TCP session not inspected (memcap reached):: 0

Invalid checksum (packets rejected):: 0

Packets associated with no flow:: 0

Syn Packets:: 0

Syn Ack packets:: 0

Rst packets:: 0

Segments not reassembled (Memcap reached):: 0

segments not reassembled (Depth reached):: 0

segments not reassembled (Stream gap):: 0

Flow memcap Reached:: 0

Flow manager closed pruned:: 0

Flow manager new pruned:: 0

Flow manager est pruned:: 0
```

```
Flow manager bypassed pruned:: 0

Flow Spare:: 0

Emergency mode entered:: 0

Emergency mode returned:: 0

Flow tcp reuse:: 0

Flow manager flows checked:: 0

Flow manager flows no timeout:: 0

Flow manager flows timeout:: 0

Flow manager flows timeout in use:: 0

Flow manager flows removed:: 0

Flow manager rows checked:: 65536

Flow manager rows skipped:: 65536

Flow manager rows empty:: 0

Flow manager rows busy:: 0

Flow manager rows max length:: 0

TCP memuse:: 409600

TCP reassembly memuse:: 12332832

HTTP memuse:: 0

DNS memuse:: 0

DataPath:: 1

Ethernet packets:: 11573

IPV4 packets:: 11573
```

Applicable to:

NS-series Sensors (except for NS7600 and NS3600 Sensors)

show syncookietcpreset

It displays the configuration of TCP Reset sent for timed out TCP 3WH when syncookie is active.

Syntax:

```
show syncookietcpreset
```

Sample Output:

```
intruShell@john> show syncookietcpreset

SynCookie TCP RESET setting : Enabled
```

Applicable to:

NS-series Sensors

show syslog connection status

This command displays the syslog connection status — whether the syslog message has been sent successfully or not.

Syntax:

```
show syslog connection status
```

Sample Output:

```
intruShell@john> show syslog connection status

Connection status: Syslog message has been sent successfully
```

Applicable to:

NS-series and Virtual IPS Sensors

show syslog profile

It displays the syslog alert profile information, such as the server IP, UDP port, facility, priority, policy based notify, quarantine based notify, and severity based notify.

Syntax:

```
show syslog profile
```

Sample Output:

```
intruShell@NS_9500> show syslog profile

[Syslog alert profile information]

Syslog server IP : 10.1.1.1

UDP port : 514

Facility : 4

Priority : 0

Policy Based Notify : Disable

Quarantine Based Notify : Disable

Severity Based Notify : Notify All Severity Alerts
```

Applicable to:

NS-series and Virtual IPS Sensors

show syslog statistics

It displays the number of alerts detected by the Sensor or received from Sensor analysis, the number of alerts sent by the Sensor to the syslog server, and the number of alerts not sent by the Sensor to the syslog server, which, in other words, is suppressed.

Syntax:

```
show syslog statistics
```

Sample Output:

```
intruShell@john> show syslog statistics

[syslog Alert]

Received : 34062

Sent : 15451

Suppressed : 18611
```

Applicable to:

NS-series Sensors

show tacacs

This CLI command displays the current TACACS+ configuration for the Sensor.

Information displayed by the **show tacacs** command includes the following:

- Whether TACACS+ remote authentication for Sensor CLI users is enabled (on)
- Whether encryption of the TACACS+ traffic is enabled
- Whether the TACACS+ authorization feature is enabled
- The IP address of the configured TACACS+ server(s), if any

This command has no parameters.

Syntax:

```
show tacacs
```

Sample Output:

```
intruShell@john> show tacacs

[TACACS+ Config]

Authentication : Enable

Traffic Encryption : Enable

Authorization : Enabled
```

```
Server 1 IP : 10.213.172.87
```

Applicable to:

NS-series Sensors

show tcpipstats

The **show tcpipstats** command reports TCP/IP statistics for traffic flowing through the entire Sensor.

The **show tcpipstats** command displays the count for each of the following categories:

- TCP packets
- UDP packets
- IP fragments
- TCP resets
- ICMP packets received
- ICMP unreachables sent

This command has no parameters.

Syntax:

```
show tcpipstats
```

Sample Output:

```
intruShell@john> show tcpipstats

TCP Packets : 4202310216

UDP Packets : 163289410

IP Fragments : 163554316

TCP Resets : 0

ICMP Packets Received : 78340266

ICMP Unreachables Sent : 0
```

Applicable to:

NS-series Sensors

show tcpudpchecksumerror

The Sensor recomputes TCP/UDP/ICMP header checksums to determine and show if the corresponding packets have been corrupted.

This command has no parameters.

Syntax:

show tcpudpchecksumerror

Sample Output:

```
intruShell@john> show tcpudpchecksumerror

tcpudpicmpchecksumerror : Forward
```

Applicable to:

NS-series Sensors

show tiestats

It displays the total requests and responses to file reputation requests and number of file reputation responses per source, the sources being Enterprise score, Intelligent Sandbox, Global Threat Intelligence, and external provider.

Sample Output:

```
[TIE Statistics]

***Total file reputation requests and responses***

Total file reputation requests : 5

Successful file reputation requests : 5

Trellix File Reputation handled requests : 0

Total file reputation responses : 5

Successful file reputation responses : 5

***Number of file reputation responses per source***

Total responses from gti : 5

Total responses from enterprise : 5

Total responses from external provider : 4

Total responses from tis : 3
```

Applicable to:

NS-series Sensors

show transceiver serial-number

This command displays the status of the pluggable module(s) inserted into the specified slot(s) of transceiver.

Syntax:

```
show transceiver serial-number (g0/1|g0/2|g1/1|g1/2|g1/3|g1/4|g1/5|g1/6|g1/7|g1/8|g1/9|g1/10|
g1/11|g1/12|g2/1|g2/2|g2/3|g2/4|g2/5|g2/6|g2/7|g2/8|g2/9|g2/10|g2/11|g2/12|g3/1|g3/2|g3/3|g3/4|g3/5|
g3/6|g3/7|g3/8|WORD|all)
```

Sample Output:

```
intruShell@john> show transceiver serial-number all

-------------------------

Slot-0 [FIXED MODULE : 2-port QSFP]

G0/1 : Transceiver is Absent.

G0/2 : Transceiver is Absent.

-------------------------

Slot-1 [empty]

-------------------------

Slot-2 [empty]

-------------------------

Slot-3 [FIXED MODULE : 8-port RJ45]

Not Applicable
```

NOTE

For RJ-45 module, serial number is not applicable.

Applicable to:

NS5x00, NS7x00 and NS9x00 Sensors

show urlrepstats

It displays the statistics gathered when checking for the URL reputation, such as the number of requests sent to the control plane, number of times an attack was triggered, number of times various header fields were processed, distribution of reputation scores, and any errors.

Syntax:

```
show urlrepstats
```

Sample Output:

```
Requests sent to control plane : 4

Responses received from control plane : 4

Number of queries triggered at DPlane : 5

Number of times attack got triggered : 4

Number of times alert gen failed : 0
```

```
Number of DP cache lookups : 5

Number of DP cache lookup matches : 2

DP cache hit ratio : 40%

Number of times attack triggered from cache lookup : 1

Number of valid DP cache entries : 2

Number of DP cache entries added : 2

Number of DP cache entries timedout : 0

Number of responses received after flow timeout : 0

Number of times tsproc returned ERROR : 1

responses from ctl plane without matching request at data plane : 0

Number of Reputations with clean(Minimum) score : 0

Number of reputations with Low(Unverified) score : 0

Number of reputations with Medium score : 4

Number of reputations with High score : 0

Number of reputations with Invalid score : 0

Number of reputations with Malicious score : 4

Number of times URI header L7Dcap was invoked : 5

Number of times Host header L7Dcap was invoked : 2

Number of times Referer header L7Dcap was invoked : 3

Number of times SNI Host header L7Dcap was invoked : 0

Number of times SSL Cert CN header L7Dcap was invoked : 0

No of connects from backend to control plane passed : 20

No of connects from backend to control plane failed : 0

No of times connection with control plane closed : 0

No of Reputation requests to control plane failed : 0

No of Reputation requests to control plane failed due to disconnect: 0
```

Applicable to:

NS-series Sensors

show userconfigvolumedosthreshold

This command displays the specified user-defined DoS threshold for alerting on volume for a particular packet type.

Syntax:

```
show userconfigvolumedosthreshold <dos-measure-name> <direction>
```

Parameter	Description
<dos-measure-name>	Indicates the DoS measure name: one of 'tcp-syn', 'tcp-syn-ack', 'tcp-fin', 'tcp-rst', 'udp', 'icmp-echo', 'icmp-echo-reply', 'icmp-non-echo-reply', 'ip-fragment', 'non-tcp-udp-icmp'
<direction>	Indicates the direction. It can be 'inbound' or 'outbound'.

Sample Output:

```
intruShell@Sensor-6050> show userconfigvolumedosthreshold icmp-echo-reply inbound

User did not configure threshold for icmp-echo-reply inbound
```

Example:

`show userconfigvolumedosthreshold icmp-echo-reply inbound` returns one of the following responses:

- The threshold value configured using **`set userconfigvolumedosthreshold icmp-echo-reply inbound`**
- If the threshold was not configured, the message *User did not configure threshold for icmp-echo-reply inbound*

Applicable to:

NS-series Sensors

show userInfo stats

This command displays the user, group, and Trellix Logon Collector (TLC) related statistics.

Syntax:

```
show userInfo stats
```

Sample Output:

```
intruShell@john> show userInfo stats

[User Info Stats]

Bulk File download count : 2

Incr File download count : 0

User Info count : 1

Group Info count : 0

IP Info count : 0
```

Applicable to:

NS-series Sensors

show vlanbasedrecon status

This command displays the status of VLAN-based reconnaissance.

The Attack Details panel in the Manager Attack Log displays VLAN ID in reconnaissance alert messages. The VLAN ID is included in fault notifications and reports.

> **NOTE**
>
> In case of a fail-over pair, the feature has to be enabled on both the Sensors.

For more information, see the *Trellix Intrusion Prevention System Product Guide*.

Syntax:

```
show vlanbasedrecon status
```

Sample Output:

```
intruShell@john> show vlanbasedrecon status

Vlan Based Reconnaissance attack detection disabled
```

Applicable to:

NS-series Sensors

shutdown

This command halts the Sensor so you can turn it off. You can turn off the Sensor manually after a minute. The Sensor does not turn off automatically. You must confirm that you want to shut down the Sensor.

This command has no parameters.

Syntax:

```
shutdown
```

Applicable to:

NS-series Sensors

snmpv2Support

You can obtain access to the read-only components of the Trellix IPS MIBs using SNMP v2.

Configure the NMS IP address on the Manager. See the *Trellix Intrusion Prevention System Product Guide* for more details.

Syntax:

`snmpv2Support enable <CommunityString>`

This command enables SNMP v2 support.

Parameter	Description
CommunityString	The SNMP community string to authenticate access to MIB objects and functions

`snmpv2Support disable`

This command disables SNMP v2 support.

`snmpv2Support status`

This command displays the status of SNMP v2 support (enabled or disabled).

Applicable to:

NS-series Sensors

sshaccesscontrol resetlist

This command deletes the entire list of hosts or networks that are configured for SSH access.

Syntax:

`sshaccesscontrol resetlist`

Applicable to:

NS-series Sensors

sshd disable

This command stops the SSH daemon (sshd), preventing remote administration of the Sensor. With sshd stopped, you can interact with the Sensor only via the Console.

This command has no parameters.

Syntax:

`sshd disable`

Default Value:

The SSH daemon is enabled by default.

Applicable to:

NS-series Sensors

sshd enable

This CLI command starts the SSH daemon (sshd), which enables remote administration of the Sensor from any command line.

This command has no parameters.

Syntax:

`sshd enable`

Default Value:

After the SSH daemon is started, you can log on to the Sensor remotely using the following syntax:

`ssh admin<Sensor IP address>`

or

`ssh -l admin <Sensor IP address>`

You will be prompted for the admin password. When you have successfully logged in, you will be able to use the CLI as if you were using it from the Console.

- You cannot use remote administration to configure the Sensor initially; you must configure the Sensor (including its IP address) for the first time from the Console.
- You may have up to five concurrent SSH sessions.

Applicable to:

NS-series Sensors

sshlogupload WORD

Use this command to upload the SSH log file to the TFTP Server.

Ensure the following before using this command:

- The TFTP Server IP address must be set using the command **`set tftpserver ip <server_ip>`**
- Ensure the file with the corresponding file name exists on the TFTP Server with write permissions for all.

The file uploaded on the TFTP Server is the TAR file containing one or more zipped files. Perform the following steps to access the files:

- Untar the file using the command **`tar –xvf <filename>`** to get the individual zipped files.
- Each file must be unzipped using the command **`gunzip <zipped_file>`** to view the file.

Syntax:

`sshlogupload <filename>`

A sample SSH log message is displayed below:

```
Sep 16 09:09:52 localhost kernel: SSHD_DROP:IN=eth0 OUT=
MAC=00:06:92:25:9d:80:00:0b:bf:a1:b7:fc:08:00 SRC=172.16.232.47 DST=172.16.199.89 LEN=48 TOS=0x00
PREC=0x00 TTL=127 ID=4286 DF PROTO=TCP SPT=2821 DPT=22 WINDOW=65535 RES=0x00 SYN URGP=0
```

Log Message Fields	Description
SSHD_DROP	Denotes the number of minutes for activating the performance debugging on the Sensor
IN=etho	Interface the packet was received from; empty value for locally generated packets
OUT=	Interface the packet was sent to; empty value for locally received packets
MAC=00:06:92:25:9d:80:00:0b:bf:a1:b7:fc:08:00	The MAC field consisting of 14 entities, separated by colons, and this can read as the following: Dest MAC= 00:06:92:25:9d:80 — The destination MAC address Src MAC=00:0b:bf:a1:b7:fc — The source MAC address Type=08:00 — Ethernet frame carrying an IPv4 datagram
SRC=172.16.232.47	The source IP address
DST=172.16.199.89	The destination IP address
LEN=48	The total length of IP packet in bytes
TOS=0x00	The Type Of Service, “Type” field
PREC=0x00	The Type Of Service, “Precedence” field
TTL=127	The remaining Time To Live is 127 hops
ID=4286	The unique ID for this IP datagram shared by all fragments, if fragmented
DF	Do not Fragment flag
PROTO=TCP	The protocol name
SPT=2821	The source port
DPT=22	The destination port
WINDOW=65535	The number of bits specified on the “Window Scale” TCP option
RES=0x00	The reserved bits
SYN	The synchronize flag and is only exchanged at TCP connection establishment
URGP=0	The urgent flag

Applicable to:

NS-series Sensors

sshpasswdauth

You can configure the password based authentication to login to the Sensor using this command.

Syntax:

`sshpasswdauth <enable|disable>`

where **`<enable>`** allows SSH password based authentication and **`<disable>`** stops SSH password based authentication.

Default Value:

enable

Example:

```
sshpasswdauth enable
```

Applicable to:

NS-series Sensors

sslagentaccesscontrol resetlist

This command deletes the entire access list of SSL agents that are configured for accessing the Sensor.

Syntax:

```
sslagentaccesscontrol resetlist
```

Applicable to:

NS-series Sensors

status

This command displays Sensor system status, such as System Health, Manager communication, signature set details, total number of alerts detected, and total number of alerts sent to the Manager.

This command has no parameters.

Syntax:

```
status
```

Sample Output:

For Sensor, the output is as shown below:

```
intruShell@john> status

[Sensor]

System Initialized : yes

System Health Status : good

System Capacity : 750 Mbps
```

> **NOTE**
>
> System Capacity is displayed only for NS9500, NS7600, NS7500, NS3600, and NS3500 Sensors.

```
Layer 2 Status : normal (IDS/IPS)
```

```
Installation Status : complete

IPv6 Status : Parse and Detect Attacks

Reboot Status : Not Required

Guest Portal Status : up

Hitless Reboot : Not-Available

Last Reboot reason : reboot issued from CLI

Mode Change Status : Not-Applicable

[Signature Status]

Present : yes

Version : 11.9.0.5

Power up signature : good

Geo Location database : Present

DAT file : Present

Version : 3376.0

[Manager Communications]

Trust Established : yes (Self Signed cert support)

Alert Channel : up

Log Channel : up

Authentication Channel : up

Last Error : None

Alerts Sent : 961

Logs Sent : 974

[Alerts Detected]

Signature : 4246 Alerts Suppressed : 3483

Scan : 0 Denial of Service : 2

Malware : 4

[NTBA Communication]

Status : up

IP : 10.213.174.132
```

```
Port : 8505

[TIS Communication]

Status : up

IP : 10.200.100.60

Port(Secure) : 8505
```

The same status message appears in an NTBA Appliance also.

> **NOTE**
>
> In NS9300 Sensor, if the Sensor reboots due to mismatch in software version, the **status** command specifies the reason **recovered from sw version mismatch** in **Last Reboot reason**.

> **NOTE**
>
> For NS9500 and NS3500 Sensors, the **status** command also displays the current throughput based on the license purchased. If signature set is not detected in the Sensor, **No license** is displayed.

> **NOTE**
>
> If there is a failure in establishing trust between the Sensor and Manager due to mismatch in shared secret key, the **Last Error** displays the message **Alert Channel - Install Keys Mismatch**. In such an instance, check the shared secret key on the Manager and set it on the Sensor using **set sensor sharedsecretkey** command.

Applicable to:

NS-series Sensors

suricata

This command enables or disables packet forwarding to the Suricata engine.

Syntax:

```
suricata <on> | <off>
```

Option	Definition
on	Enables packet forwarding to the Suricata engine
off	Disables packet forwarding to the Suricata engine

Note the following:

- This command is not a substitute for enabling or disabling the Suricata engine which is available in the Manager.
- Disabling packet forwarding using this command does not release the resources held by the Suricata engine; it only suspends packet forwarding to the Suricata engine.

- This command is only for debugging purposes.

Applicable to:

NS-series Sensors (except for NS7600 and NS3600 Sensors)

tiscache autopurge

This command purges the cache entries made in the Sensor for the files sent to Trellix Intelligent Sandbox for analysis. By default, the command is enabled.

Syntax:

```
tiscache autopurge <enable|disable>
```

Applicable to:

NS-series Sensors

tiscache autopurge status

This command displays whether the tiscache autopurge feature is enabled or disabled. By default, the command is enabled.

Syntax:

```
tiscache autopurge status
```

Sample Output:

```
intruShell@NS7250> tiscache autopurge status

TIS Cache Auto Purge On

Cache Purge Interval is 24 hours
```

Applicable to:

NS-series Sensors

traceupload

This command uploads an encoded diagnostic trace file to the configured TFTP server, from which you can send it to the Trellix Technical Support for diagnosing a problem with the Sensor. A trace upload facility is also available in the Manager interface.

Syntax:

```
traceupload WORD
```

where **WORD** stands for the file name to which the trace must be written.

Note the following:

- Before executing this command, configure TFTP server on NTBA Appliance by running the **set tftpserver ip** command.

- When loading a trace file from the configured TFTP server, the pathname of the file should be relative to /tftpboot.
- Before executing this command (uploading on the TFTP server), ensure that the file is created on the TFTP server with write permissions for all.

NOTE

As part of **traceupload** command, additional information is collected using logstat. Due to this, additional time is required to collect logs from the Sensor, and can take around 10-30 minutes based on the Sensor model.

On executing the command, the following messages are displayed:

```
Please enter Y to confirm: y

Uploading trace file to TFTP server

Trace file uploaded successfully to TFTP server.
```

Applicable to:

NS-series Sensors

vlanbridgestp

This command configures the vlan bridging on the STP packet.

Syntax:

```
vlanbridgestp <enable|disable|drop>
```

Parameter	Description
enable	Enables the vlan bridging on the STP packet
disable	Disables the vlan bridging on the STP packet
drop	Drops the vlan bridging on the STP packet

Applicable to:

NS-series Sensors

watchdog

The watchdog process reboots the device whenever an unrecoverable failure is detected in the device.

Syntax:

```
watchdog <on | off | status>
```

Parameter	Description
<on>	Enables the watchdog

Parameter	Description
<off>	Disables the watchdog. Use it when a Sensor reboots continuously due to repeated system failure.
<status>	Displays the status of the watchdog process ('on' or 'off')

Sample Output:

- For Sensor, the output is as shown below:

```
intruShell@john> watchdog status
watchdog = off
```

Applicable to:

NS-series Sensors

IPS CLI Commands - Debug Mode

This section details the commands that can be run in Debug mode.

Log on to the Sensor with a valid user name (username is **admin**) and password (default is **admin123**). At the command prompt, type **debug** to log on to debug mode.

At the command prompt, type **disable** to get out of debug mode. To log off, type **exit**.

> **NOTE**
>
> In debug mode, you can run the normal and debug mode commands.

40to10conversion

Use this command to convert G0 ports (G0/1 and G0/2) on NS9x00 Sensors to run in 10 Gigabit Ethernet mode instead of the 40 Gigabit Ethernet mode.

> **NOTE**
>
> This configuration persists across Sensor reboots.

> **NOTE**
>
> A separate adaptor is needed to convert QSFP interface into a SFP+ interface. Contact Support for more information.

Syntax:

```
40to10conversion <enable|disable>
```

Applicable to:

NS9100 and NS9200 Sensors.

aclstat

This command shows ACL statistics for each datapath.

Syntax:

```
aclstat
```

Sample Output:

```
IntruDbg#> aclstat

datapath 19 :

Total number of packets: 0

TCP ACL Drop count: 0

TCP ACL Deny count: 0

TCP ACL Ignore count: 0

IPRF ACL Deny count: 0

IPRF ACL Reject count: 0

IPRF ACL Ignore count: 0

UDP ACL Deny count: 0

UDP ACL Ignore count: 0

ICMP Deny count: 0

ICMP Ignore count: 0

Other IP Deny count: 0

Other IP Ignore count: 0
```

Applicable to:

NS-series Sensors

allow intfport id connector

This command configures the supported SFP vendor for the monitoring ports.

Syntax:

```
allow intfport id <port> connector (all-vendors|trellix-only)
```

Parameter	Description
<port>	Valid port numbers for NS-series are: G0/1 | G0/2 | G1/1 | G1/2 | G1/3 | G1/4 | G1/5 | G1/6 | G1/7 | G1/8 | G1/9 | G1/10 | G1/11 | G1/12 | G2/1 | G2/2 | G2/3 | G2/4 | G2/5 | G2/6 | G2/7 | G2/8 | G2/9 | G2/10 | G2/11 | G2/12

Example:

```
allow intfport id g0/1 connector trellix-only
```

```
allow intfport id g0/2 connector all-vendors
```

Applicable to:

NS-series Sensors

appidstat

The command fetches and displays Application ID statistics from single or all datapath processors.

Syntax

```
appidstat <1-16|all>
```

Parameters	Description
1-16	displays appid statistics for the datapath processor specified
all	displays appid statistics for all datapath processors

Sample Output

```
IntruDbg#> appidstat 1
```

```
datapath 1 :
```

```
Total AppIds Detected: 0
```

```
Total AppIds Reported: 0
```

```
Node Exhausted: 0
```

```
Pcre match errors: 0
```

```
Detection Beyond Scan Depth: 0
```

```
Max Parent Depth Exceeded: 0
```

Applicable to:

NS-series Sensors

arp static

This command configures the static ARP entries.

Syntax:

```
arp static-add <A.B.C.D> <A:B:C:D:E:F> <port>
```

```
arp static-delete <A.B.C.D> <port>
```

Parameter	Description
<port>	Valid port numbers for NS-series are: g0/1 | g0/2 | g1/1 | g1/2 | g1/3 | g1/4 | g1/5 | g1/6 | g1/7 | g1/8 | g1/9 | g1/10 | g1/11 | g1/12 | g2/1 | g2/2 | g2/3 | g2/4 | g2/5 | g2/6 | g2/7 | g2/8 | g2/9 | g2/10 | g2/11 | g2/12 | g3/1 | g3/2 | g3/3 | g3/4 | g3/5 | g3/6 | g3/7 | g3/8

Example:

```
arp static-add 1.1.1.9 00:0C:29:A0:C6:5F g2/2
```

```
arp static-delete 209.165.202.255 g2/2
```

Applicable to:

NS-series, Virtual IPS Sensors, and Virtual Security System instances

clearnistats

This command clears all the NI config and metadata statistics counters in the Sensor, when integration with Trellix Network Investigator is enabled.

Syntax:

```
clearnistats
```

Applicable to:

NS-series and Virtual IPS Sensors

clrdnseliststats

This command clears statistics related to DNS exception list. This command has no parameters.

Syntax

```
clrdnseliststats
```

Applicable to:

NS-series and Virtual IPS Sensors

clrdpdstats

This command clears device profile related statistics. This command has no parameters.

Syntax:

```
clrdpdstats
```

Applicable to:

NS-series and Virtual IPS Sensors

clrtscache

This command clears Sensor's internal cache memory for IP reputation. This command has no parameters.

Syntax

```
clrtscache
```

Sample Output

```
IntruDbg#> clrtscache

This command will take a while to complete, please check sensor.dbg for status

Also please note that TS lookups will be disabled during this time
```

Applicable to:

NS-series and Virtual IPS Sensors

clr stack protocol

This command clears stack protocol statistics counters in the Sensor.

This command takes the following parameters:

Parameter	Description
all	Clears all the stack protocol statistics.
rxPkts	Clears the statistics of the packets received from other nodes in the stack.
txPkts	Clears the statistics of the packets transmitted to other nodes in the stack.
timeout	Clears the timeout received at the ports of the Sensor.

Syntax:

```
clr stack protocol <all|rxPkts|txPkts|timeout>
```

Applicable to:

NS9500 Sensors stack only

clr stack stats otherNodePktsProcessed

This command clears the statistics for the packets received and processed from the other nodes of the stack.

This command has no parameters.

Syntax:

```
clr stack stats otherNodePktsProcessed
```

Applicable to:

NS9500 Sensors stack only

clrconnlimithost

This command clears Connection Limiting host table.

Syntax:

`clrconnlimithost`

Applicable to:

NS-series Sensors

datapathstat

This command shows datapath statistics and details for all parameters. You can enter a single parameter to fetch the details.

Syntax:

`datapath core <core_number|all> parameter <param|all>`

Parameter	Description
core_number	can be a value between 0 - 31
param: The possible values for the parameter option are listed below.	
datapath-cache-errors	datapath cache errors
dp-rx-fcs-error-cnt	dp recv fcs error count
dp-tx-fcs-error-cnt	dp sent fcs error count
fifo-dumm	fifo dumm
fifo-inuse-or-double-rx-free-errors	fifo in use or double recd free errors
fifo-inuse-or-double-tx-free-errors	fifo in use or double sent free errors
free-fifo	free fifo
free-tx-buf	free sent buffer
get-rx-buf-failed	get recd buffer failed
get-tx-buf	get sent buffer
get-tx-buf-failed	get sent buffer failed
ip-checksum-err-pkt-count	ip checksum err pkt count
rx-bad	bad recd
rx-buf-added	recd buffer added
rx-bytes	bytes recd

Parameter	Description
rx-cnt	recd count
rx-descriptors-avail	recd descriptors avail
rx-empty	empty recd
rx-frames	frames recd
rx-high-watermark-cnt	recd high watermark count
rx-low-watermark-cnt	recd low watermark count
rx-retry	retry recd
rx-too-big	too big recd
sensor-load	display Sensor load
tcp-checksum-err-pkt-count	tcp checksum err pkt count
tx-bytes	bytes sent
tx-cnt	sent count
tx-done	sent done
tx-frames	frames sent
tx-full-cnt	sent full count
tx-pending-cnt	sent pending count
udp-checksum-err-pkt-count	udp checksum err pkt count

Sample Output:

```
IntruDbg#> datapath core all parameter all

core 1

Tx frames: 0

Tx bytes: 0

Rx frames: 0

Rx bytes: 0

Rx bad: 0

Rx empty: 0

Rx retry: 0

Rx too big: 0

free fifo: 0

IP checksum err pkt count: 0

TCP checksum err pkt count: 0
```

```
UDP checksum err pkt count: 0

rx descriptors avail: 0

rx low watermark cnt: 0

rx high watermark cnt: 0

free tx buf: 0

tx done: 0

get tx buf: 0

get tx buf failed: 0

get rx buf failed: 0

tx dcnt: 0

rx dcnt: 0

rx buf added: 0

datapath cache errors: 0

fifo dumm: 0

Tx full cnt: 0

Tx pending cnt: 0

Fifo inuse/double Tx free errors: 0

Fifo inuse/double Rx free errors: 0

dp-rx-fcs-error-cnt: 0

dp-tx-fcs-error-cnt: 0

sensor-load: 0
```

Applicable to:

NS-series Sensors

datapathstat intfport

This command displays the datapath statistics and the details of all the parameters for an interface port. You can also enter a single parameter to fetch the details.

Syntax:

```
datapathstat intfport <id> core <core_number|all> parameter <param|all>
```

Parameter	Description
id	Valid interface port ID
core_number	Valid core number that is a numeric value in a range specific to the Sensor model
param: The possible values for the parameter option are listed below.	
• tx-frames	Frames sent
• tx-bytes	Bytes sent
	Frames received
• rx-frames • rx-bytes	Bytes received
• ip-checksum-err-pkt-count	Total number of checksum error packets in IP traffic
• tcp-checksum-err-pkt-count	Total number of checksum error packets in TCP traffic
• udp-checksum-err-pkt-count	Total number of checksum error packets in UDP traffic
• rx-count	Data path packet count received

Sample Output:

```
IntruDbg#> datapathstat intfport g3/8 core 1 parameter all
```

	Datapath:	DP 0	DP 1	DP 2	DP 3	DP 4	DP 5
core 1	Tx frames:	0	0	0	0	0	0
	Tx bytes	0	0	0	0	0	0
	Rx frames:	0	0	0	0	0	0
	Rx bytes:	0	0	0	0	0	0
	IP checksum err pkt count:	0	0	0	0	0	0
	TCP check-sum err pkt count:	0	0	0	0	0	0
	UDP check-sum err pkt count:	0	0	0	0	0	0
	rx count:	0	0	0	0	0	0

Applicable to:

NS-series and Virtual IPS Sensors

disable

This CLI command, when executed, disables debug mode and switches back to normal CLI mode.

Syntax:

disable

Applicable to:

NS-series Sensors

dossampling

By default, sub-sampling is enabled due to which the packet count in DoS alerts shows lower than that of the actual attack, on UDP traffic. You can disable or enable sub-sampling using this command.

Syntax:

dossampling <enable|disable> <inbound|outbound>

Example:

dossampling enable inbound

dossampling enable outbound

dossampling disable inbound

dossampling disable outbound

Applicable to:

NS-series Sensors

dossampling status

Displays the status of **dossampling** (enabled or disabled).

Syntax:

dossampling status

Sample Output:

```
IntruDbg#> dossampling status
sub-sampling enabled in inbound direction
sub-sampling enabled in outbound direction
```

Applicable to:

NS-series Sensors

downloadgamupdate

This command downloads GAM updates by sending request to the GAM update server.

Syntax

downloadgamupdate

Sample Output

Full Gam Update Request sent

Applicable to:

NS-series Sensors

dumpdebuglog

The **dumpdebuglog** command filters the sensor.log file for log messages that are coming from a particular specified module. It displays logs based on number of lines or all logs.

Syntax:

dumpdebuglog <SupportedModuleName> <(1-1000)lines(s)(Or)running>

where:

- **<SupportedModuleName>** can be cli, controlChannel, correlationEng, intfw, logging, logNode, packetLog, snmpAgent, systemCtrl, ivSensor, monitor, ssl, sig, authgw, sgap, sm, tsproc, nacfo, nacpolicy, deviceProfile, sofa, qvm, rad or artemis.
- **<(1-1000)lines(s)(Or)running >** specifies the number of lines of latest logs coming from the specified module. If **running**, prints all the logs coming from the specified module.

Applicable to:

NS-series Sensors

dumpDevProfTableEntry

This command displays the specific Device Profile Table entry.

Syntax:

dumpDevProfTableEntry (ip | mac) WORD

dumpDevProfTableToLog

This command logs the Device Profile Table data into the Sensor log file.

Syntax:

dumpDevProfTableToLog (ip| mac | all | stats)

dumpdgastats

This CLI command, when executed, dumps data related to bots and C&C servers suspicious for DGA to a debug file. This command is used for debugging purposes. Use this command to provide diagnostic data to Trellix Technical Support.

This command has no parameters.

Syntax:

dumpdgastats

Applicable to:

NS-series and Virtual IPS Sensors

dumpdnseliststats

This command dumps the statistics related to DNS exception list on the CLI. The output contains statistics specific to each datapath processor and also provides a cumulative statistics of all datapath processors. This command has no parameters.

Syntax

dumpdnseliststats

Sample Output

```
IntruDbg#> dumpdnseliststats

datapath 0 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 1 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 2 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 3 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0
```

```
Number of matches in Reserved Domain Exception list : 0
Number of matches in User Configured Domain Exception list : 0
datapath 4 :
Number of Reserved Domain list Searches Done: 0
Number of User Configured Exception list searches done: 0
Number of matches in Reserved Domain Exception list : 0
Number of matches in User Configured Domain Exception list : 0
datapath 5 :
Number of Reserved Domain list Searches Done: 0
Number of User Configured Exception list searches done: 0
Number of matches in Reserved Domain Exception list : 0
Number of matches in User Configured Domain Exception list : 0
datapath 6 :
Number of Reserved Domain list Searches Done: 0
Number of User Configured Exception list searches done: 0
Number of matches in Reserved Domain Exception list : 0
Number of matches in User Configured Domain Exception list : 0
datapath 7 :
Number of Reserved Domain list Searches Done: 0
Number of User Configured Exception list searches done: 0
Number of matches in Reserved Domain Exception list : 0
Number of matches in User Configured Domain Exception list : 0
datapath 8 :
Number of Reserved Domain list Searches Done: 0
Number of User Configured Exception list searches done: 0
Number of matches in Reserved Domain Exception list : 0
Number of matches in User Configured Domain Exception list : 0
datapath 9 :
Number of Reserved Domain list Searches Done: 0
```

```
Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 10 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 11 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 12 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 13 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 14 :

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

datapath 15 :
```

```
Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0

------ DGA Bot Exception list Stats Info cumulative across all Sibyte -----

Number of Reserved Domain list Searches Done: 0

Number of User Configured Exception list searches done: 0

Number of matches in Reserved Domain Exception list : 0

Number of matches in User Configured Domain Exception list : 0
```

Applicable to:

NS-series and Virtual IPS Sensors

dumpdnsexcplistentries

This command, when executed, dumps the reserved and user-configured DNS exception entries to sensor.dbg file. The DNS exception list contains details of user-configured domains which are not subject to DNS botnet analysis. This command has no parameters.

Syntax:

```
dumpdnsexcplistentries
```

Applicable to:

NS-series and Virtual IPS Sensors

dumpmalwarecache

This command, when executed, dumps the malware cache entries present in the Sensor from different malware engines in `/usr/local/etc/malwareCache.log` file.

Syntax:

```
dumpmalwarecache <dbg|opt>
```

Parameter	Description
dbg	Dumps the cache entries from all the malware engines
opt	Dumps the cache entries from IVX and TIS engine only

Sample Output

```
IntruDbg#> dumpmalwarecache dbg

Msg sent to dump Malware Cache in malwareCache.log
```

Applicable to:

NS-series and Virtual IPS Sensors

filerep gti md5

This command displays the file reputation query response for the md5 hash from the GTI server configured in the Manager.

Syntax:

```
filerep gti md5 <md5_hash>
```

Parameter	Description
`md5_hash`	Enter the md5 hash of the file for which you want the GTI response.

NOTE

You can use this command to test connection to the GTI server configured in the Sensor and for debug purpose.

Sample Output:

```
IntruDebug#> filerep gti md5 83f6ac96f6e8188daaff089ed936cbde

DONE: https://nsp.rest.gti.trellix.com/1 => (total time 1.255940)

response: 0x7f810808

dirtiness: 0x8

malware score: very high
```

Applicable to:

NS-series and Virtual IPS Sensors

force_ssmode_trust

This command is used to enable or disable the use of self-signed certificate for trust establishment or to check if the trust is established using self-signed or CA-signed certificate.

Syntax:

```
force_ssmode_trust <on|off|status>
```

The following parameters are available for this command:

Option	Definition
`on`	Establish trust with the Manager using self-signed certificate.
`off`	Establish trust with the Manager using CA-signed certificate.

Option	Definition
status	Displays the following: **on** - The Sensor is using self-signed certificate to establish trust with the Manager. **off** - The Sensor is using CA-signed certificate to establish trust with the Manager.

Applicable to:

NS-series Sensors

getauthstats

This command displays authentication details such as logged user stats and web server status. This command has no parameters.

Syntax:

```
getauthstats
```

Sample Output:

```
IntruDbg#> getauthstats

sgap Status = up.

Web Server Status = up.

Web Server Certificate Status = default

auth channel = up

peer auth channel = down

rxUnknownMsgTypeCount = 0.

rxUnknownISMMsgTypeCount = 0.

rxUnknownPeerMsgTypeCount = 0.

policyGetCount = 0.

policyUpdateCount = 0.

usrAuthCount = 0.

usrAuthSuccessCount = 0.

usrAuthFailCount = 0.

usrSelfRegCount = 0.

usrSelfRegSuccessCount = 0.

usrSelfRegFailCount = 0.
```

```
usrDisableCount = 0.

hostHealthCount = 0.

peerUsrDisableCount = 0.

reqISMPendingCount = 0.

reqISMTimeoutCount = 0.

reqPeerPendingCount = 0.

reqPeerTimeoutCount = 0.

authReqPendingCount = 0.
```

Applicable to:

NS-series Sensors

getccstats

The **getccstats** command displays the statistics of the Sensor control channel module.

Syntax:

```
getccstats
```

Sample Output:

```
IntruDbg#> getccstats

sigfile tables = accessible.

manager-sensor trust = established.

sensor installation = complete

alert channel = up

peer alert channel = down

throttleThreshold = 1.

throttleInterval = 0.

throttleAction = 1.

failoverAction = 2.

failoverStatus = 3.

peerStatus = 5.

fail-open Action = 2.

rxSysEvCount = 14.
```

```
putSysEvUnCount = 0.

rxSysEvDecodeUnCount = 8.

txSysEvCount = 14.

rxSigAlertCount = 0.

rxScanAlertCount = 0.

rxDosAlertCount = 0.

rxTSMaliciousAlertCount = 0.

txAlertCount-Primary = 0.

txAlertCount-Secondary = 0.

txPerfAlertCount-Primary = 13.

txPerfAlertCount-Secondary = 0.

txAppIdStatsAlertCount-Primary = 0.

txAppIdStatsAlertCount-Secondary = 0.

throttleCount = 0.

copyPortDropCount = 0.

unknownPortInStandbyDropCount = 0.

rxAlertDecodeUnCount = 0.

rxCorrFlagReAlertCountt = 0.

rxScanFilterReAlertCount = 0.

rxShellCodeAlertCount = 0.

sslConflictAlertCount = 0.

sslConflictTimeCount = 0.

rxAlertFromCECount = 0.

txAlertToCECount = 0.

AlertsInRngBufPriCount = 0.

AlertsInRngBufSecCount = 0.

PutAlertInRngBufUnCount = 0.

ScanCorrAlertLogSubNodeThrottleOnCount = 0.

ScanCorrAlertLogNodeFlowOffCount = 0.
```

```
ScanCorrAlertLogSubNodeAddCount = 0.

ScanCorrAlertLogSubNodeAddFailedCount = 0.

ScanCorrAlertLogNodeAddCount = 0.

ScanCorrAlertLogNodeAddFailedCount = 0.

ScanCorrLogIdZeroCount = 0.

ScanCorrLogIdNonZeroCount = 0.

DummyAddLogNodeAddCount = 0.

DummyAddAlertLogNodeAddFailedCount = 0.

DummyAddLogSubNodeAddCount = 0.

DummyAddAlertLogSubNodeAddFailedCount = 0.

DummyAddLogSubNodeThrottleOnCount = 0.

DummyAddLogSubNodeThrottleOffCount = 0.

DummyAddLogNodeFlowOffCount = 0.

DummyFoundLogSubNodeThrottleOnCount = 0.

DummyFoundLogSubNodeThrottleOffCount = 0.

DummyFoundLogNodeFlowOffCount = 0.

DummyFoundLogNodeAlreadyThrottledCount = 0.

DummyFoundLogNodeCopyPortOffCount = 0.

AddLogNodeAddCount = 0.

AddLogNodeAddFailedCount = 0.

AddLogSubNodeAddCount = 0.

AddLogSubNodeAddFailedCount = 0.

AddLogSubNodeThrottleOnCount = 0.

AddLogSubNodeThrottleOffCount = 0.

AddLogNodeFlowOffCount = 0.

FoundLogSubNodeThrottleOnCount = 0.

FoundLogSubNodeThrottleOffCount = 0.

FoundLogNodeAlreadyThrottledCount = 0.

FoundLogNodeFlowOffCount = 0.
```

```
FoundLogNodeWasOrigDummyNodeCount = 0.

FoundLogSubNodeWasOrigDummyNodeCountNowThrottled = 0.

FoundLogSubNodeWasOrigDummyNodeCountNowNotThrottled = 0.

aclAlertThrottleMaxIpPair = 10.

aclAlertThrottleInterval = 120.

aclAlertThrottleAction = 1.

aclAlertThrottleThreshold = 5.

aclAlertDirectToSyslog = 2.

rxAclAlertCount = 0.

aclThrottleCount = 0.

txAclAlertCount = 0.

ezAlertThrottleMaxIpPair = 10.

ezAlertThrottleInterval = 120.

ezAlertThrottleAction = 1.

ezAlertThrottleThreshold = 5.

ezAlertDirectToSyslog = 0.

rxEzAlertCount = 0.

ezThrottleCount = 0.

txEzAlertCount = 0.

LogIdNodeListCount = 0.

GrpIdNodeListCount = 0.

LogIdListPtr = 0.

LogIdBlockPtr = 0.

LogIdSubListPtr = 0.

LogIdSubBlockPtr = 0.

LogIdHTPtr = 0.

GrpIdListPtr = 0.

GrpIdBlockPtr = 0.

GrpIdHTPtr = 0.
```

```
RxCorrSigAlertFromCECount = 0.

DatapathAlertSBFloodOnCount = 0.

RxSigAlertWithPLCount = 0.

RxPSAlertWithPLCount = 0.

RxHSAlertWithPLCount = 0.

TxPLlistDropMsgCount = 0.

TxPLlistSendMsgCount = 0.

fwdChangePLModeReqCount = 0.

fwdDelPLMsgCount = 0.

RxUnknown MsgId Count = 0.

Reboot/Wrap Count = 2015.

PL Reboot/Wrap Count = 2015.

purgeCnt0 = 0.

purgeCnt1 = 0.

AlertsInRngBufPriCount = 0.

AlertsInRngBufSecCount = 0.

PutAlertInRngBufUnCount = 0.

osfpUpdateMsgRxCnt = 0.

osfpInactivateMsgRxCnt = 0.

osfpMacOnlyDelMsgRxCnt = 0.

osfpUpdateMsgTxCnt = 0.

osfpInactivateMsgTxCnt = 0.

osfpMacOnlyDelMsgTxCnt = 0.

osfpBulkUpdateMsgRxCnt = 0.

osfpBulkInactivateMsgRxCnt = 0.

osfpBulkUpdateMsgTxCnt[EMS_PRIMARY] = 0.

osfpBulkUpdateMsgTxCnt[EMS_SECONDARY] = 0.

osfpBulkInactivateMsgTxCnt[EMS_PRIMARY] = 0.

osfpBulkInactivateMsgTxCnt[EMS_SECONDARY] = 0
```

Applicable to:

NS-series Sensors

getcestats

The **getcestats** command displays the statistics of the Sensor co-relation engine module.

Syntax:

```
getcestats
```

Sample Output:

```
IntruDbg#> getcestats

rxCount = 1, txCount = 0, unCount = 0,

reCount = 0.

sigAlertRxCount = 0, sigAlertTxCount = 0.

sigAlertReCount = 0, sigAlertPlMarkDelCount = 0.

RxUnknown MsgId Count = 0.

RxPLModeChangeReqCount: 0, rstCorrPktLogging Flag = 0.

packetLogSentCCCount = 0,

packetLogDropPLMsgCount = 0.

corrSigAlertTxCount = 0.

scanAlertTxCount = 0.

sweepAlertTxCount = 0.

scanRxCount = 0, scanAlertCount = 0.

sweepRxCount = 0, sweepAlertCount = 0.

osfpRxCount = 0, osfpAlertCount = 0.

bfRxCount = 0, bfAlertCount = 0.

svcRxCount = 0, svcAlertCount = 0.

genCorrRxCount = 0, genCorrAlertCount = 0.
```

Applicable to:

NS-series Sensors

getnistats

This command fetches and displays counter specifics related to NI config and metadata export, when integration with Trellix Network Investigator is enabled. This command has no parameters.

Information displayed by the **getnistats** command includes the following:

- Counters related to NI config that include configuration polling (requests and responses) made to NI by the Sensor, authentication token error, NI DB fetch error, etc.
- Counters related to NI metadata that include netflow and metadata export to NI

Syntax:

```
getnistats
```

Sample Output:

```
IntruDbg#> getnistats

NI Config Counters

-------------------------------------

NI Total Config Requests Made Count = 226

Total NI Config Response Success Count = 221

Total NI Config Response Failure Count = 5

NI Config Invalid Appliance Identifier Error Count = 0

NI Config Invalid Auth Token Error Count = 4

NI Config Internal DB Fetch Error Count = 0

NI Config Request Timeout Error Count = 1

NI Config Internal Failure Count = 0

NI Metadata Counters

-------------------------------------

NI Netflow Export Success Count = 492011

NI Netflow Metadata Export Success Count = 45099

NI Netflow Ring Buffer Count = 2

NI Metadata Authentication Failure Error Count = 21

NI Metadata Other Error Count = 0

NI Metadata Request Timeout Error Count = 0

NI Neflow Export Failure Count = 0
```

```
NI Metadata Export Failure Count = 0

NI Netflow Node Alloc Failure Count = 0

NI Messages Discarded Due To Config Update = 17
```

Applicable to:

NS-series and Virtual IPS Sensors

getmdrinfo

This command shows Manager Disaster Recovery (MDR) information, such as number of managers and IP address details. This command has no parameters.

Syntax:

```
getmdrinfo
```

Sample Output:

```
IntruDbg#> getmdrinfo

No Of Managers = 1.

Active Ems Ip Address = 172.16.229.189.

Ems Priority = standalone

Ems HA Status = active

Ems HA Mode = standalone
```

Applicable to:

NS-series Sensors

getplstats

The **getplstats** command displays the statistics of the Sensor packet channel module.

Syntax:

```
getplstats
```

Sample Output:

```
IntruDbg#> getplstats

sigfile tables : accessible.

log channel = up

peer log channel = down

rxLogCount = 0.
```

```
txLogCount-Primary = 0.

txLogCount-Secondary = 0.

rxLogDecodeUnCount = 0.

rxZeroLenLogCount = 0.

sslConflictLogCount = 0.

sslConflictTimeCount = 0.

DeleteLogIdMsgCount = 0.

ToBeDeletedLogIdNodeCount = 0.

LogNodeDeletedCount = 0.

DeleteGrpIdMsgCount = 0.

ToBeDeletedGrpIdNodeCount = 0.

LogNodeThrottleOnCount = 0.

LogNodeNotFlowCount = 0.

PktReCount = 0.

CopyPortNodeCount = 0.

DecodeSubLogMissed = 0.

DecodeLogMissed = 0.

DeleteLogMissed = 0.

DecAlreadyDelLogIdNodeCount = 0.

DecAlreadyExpLogIdNodeCount = 0.

DecScanCorrLogIdNodeCount = 0.

DecodeGrpMissed = 0.

DeleteGrpMissed = 0.

DecAlreadyDelGrpIdNodeCount = 0.

DecAlreadyExpGrpIdNodeCount = 0.

NumSavePacketLogs = 0.

NumSavePacketLogsSent = 0.

NumSavePacketLogsReCount = 0.

NumSavePacketLogsRlCount = 0.
```

```
RxDelPLMsgCount = 0.

RxSendPLMsgCount = 0.

ModeChangeReqSentCount = 0.

Current Mode = 0.

RxUnknown MsgId Count = 0.

numXLLogCreateCount = 0.

numXLLogDeleteCount = 0.

purgeCnt0 = 0.

purgeCnt1 = 0.

LogsInRngBufPriCount = 0.

LogsInRngBufSecCount = 0.

PutLogInRgBufUnCount = 0.
```

Applicable to:

NS-series Sensors

getsastats

The **getsastats** command displays the statistics of the SNMP subagent.

Syntax:

```
getsastats
```

Sample Output:

```
IntruDbg#> getsastats

swImageVersion = 10.1.5.190

hwVersion = 1.20

serial number = S025250127.

signature set version = 10.9.35.3.

system type = IPS-NS9200.

Recvd datapaths and dos Init Done message from system controller.

Sent SNMP ready message to control channel.

Sigfile flag = 0

Number of datapaths = 8.
```

```
Connection to datapath 0 is ok.

Connection to datapath 1 is ok.

Connection to datapath 2 is ok.

Connection to datapath 3 is ok.

Connection to datapath 4 is ok.

Connection to datapath 5 is ok.

Connection to datapath 6 is ok.

Connection to datapath 7 is ok.

DOS connection status is ok.

IPv6 Status DISABLED

GTI Proxy Host 0.0.0.0

GTI Proxy Port 0

GTI Proxy Username ""

UsrIdAclfileDwnldCnt = 0

UsrIdAclIncrUpdtCnt = 0

osfpPersistMsgTxCount = 108
```

Applicable to:

NS-series Sensors

getscstats

The **getscstats** command displays the statistics of the Sensor system controller.

Syntax:

```
getscstats
```

Sample Output:

```
IntruDbg#> getscstats

sysctrl ready to send INIT_ACKs to datapaths and dos

Acld Sigfile flag reset.

initial sigfile applied msg : received from datapaths and dos.

dos has sent INIT_DONE.

datapath 0 has sent INIT_DONE.
```

```
datapath 1 has sent INIT_DONE.

datapath 2 has sent INIT_DONE.

datapath 3 has sent INIT_DONE.

datapath 4 has sent INIT_DONE.

datapath 5 has sent INIT_DONE.

datapath 6 has sent INIT_DONE.

datapath 7 has sent INIT_DONE.

dos has sent READY.

datapath 0 has sent READY.

datapath 1 has sent READY.

datapath 2 has sent READY.

datapath 3 has sent READY.

datapath 4 has sent READY.

datapath 5 has sent READY.

datapath 6 has sent READY.

datapath 7 has sent READY.

Prefix 8.0.4E22.0.0
```

Applicable to:

NS-series Sensors

ninetflowstat

This command displays internal statistics specifics related to netflow and L7 metadata from datapath side, when the integration with Trellix Network Investigator is enabled.

`ninetflowstat` command takes two arguments:

- Core id number for the starting datapath/sibyte
- Core id number for the ending datapath/sibyte

> **NOTE**
>
> The core id numbers for starting and ending datapath/sibyte vary based on different Sensor models.

if no argument is specified, it displays netflow counters for all datapaths/sibytes.

Syntax:

ninetflowstat

Sample Output:

```
IntruDbg#> ninetflowstat

Core id range is not selected, Displaying ALL

Total Netflows Sent to NI : 570732

Total Metadata Sent to NI : 46468

Total Netflow MAX Nodes Allocated : 4000

Total Netflow Available Nodes : 4000

Total Nodes allocated : 628893

Total Nodes freed : 628893

Total Nodes allocation failed : 822366

Total TCP Flows Created : 513220

Total ICMP Flows Created : 3117

Total UDP Flows Created : 112556

Total TCP Flows Sent : 463849

Total UDP Flows Sent : 103767

Total ICMP Flows sent : 3116

Total Invalid TCP netflows : 0

Total High Load Netflow Creation Failed : 127072

Total Erroneous Netflows : 0

Total Multiple Netflows : 0

Total Netflows Creation error unknown : 0

Total XFF Netflows : 0

Total Netflows Creation error failover traffic : 0

Total Netflows creation error IPV6 traffic : 0

Total Netflows Send error : 4

Total Metadata Send error : 0

Total Netflow Socket error : 0
```

Applicable to:

NS-series and Virtual IPS Sensors

importcacertfile

This command imports CA cert file from the configured SCP server to the Sensor. The CA file should be in Base64 encoded format (such as .pem, .cer, and .crt).

The uploaded file will override any pre-existing cert store and it will be persisted across reboots. Different cert stores are maintained for public and private GTI. CA cert store for the public GTI gets pushed from the Manager to the Sensor when you establish trust between the Manager-Sensor. For private GTI, however, the CA cert store should use **`importcacertfile`** command to import it to the Sensor.

> **NOTE**
>
> The CLI command **`resetconfig`** removes both public and private cert stores from the Sensor.

Syntax:

```
importcacertfile scp <public|pvt> <filepath>
```

Parameter	Description
`public`	CA certificate file for public server
`pvt`	CA certificate file for private server
`<filepath>`	Filepath of the CA certificate file in the SCP server

Sample output:

```
importcacertfile scp pvt/home/test/my-ca-bundle.cer
```

Applicable to:

NS-series and Virtual IPS Sensors

ipfragstats

This command displays IP fragment statistics and details for the IP fragments, such as number of IP fragments received or dropped. This command has no parameters.

Syntax:

```
ipfragstats
```

Sample Output:

```
IntruDbg#> ipfragstats

datapath 56 :

Total number of IP Fragments received: 4172481

Total number of IP Flows: 3606080
```

```
Number of Duplicate fragments: 564254

Fwd Overlap old data packets: 5358

Number of Fragments dropped: 0

Fragments dropped for invalid options: 0

Number of Flows TimedOut: 3605366

Backward Overlap old data packets: 0

Fwd Overlap new data packets: 0

Backward Overlap new data packets: 0

Num Flows dropped for invalid checksum: 0

Error getting fifo buffers: 0

Number of Invalid Fragments: 0

Error getting Reassembled lists: 0

Number of fragments recvd after timeOut: 0

Number of jumbo frags forwaded: 0

Number of jumbo frags constructed: 0

Fragment requests submitted to DM: 3608227

Fragment DM operations completed: 3608227

Last fragment requests submitted to DM: 0

Last fragment DM operations completed: 0

DM invoked fragCB with NULL args: 0

DM invoked lastFragCB with NULL args: 0

Num fragment flows force freed: 0
```

Applicable to:

NS-series Sensors

ipreassembly timeout millisecond

This command enables you to configure the IP Fragmentation reassembly timeout period in milliseconds.

Syntax:

```
ipreassembly timeout millisecond (0 | <250-30000>)
```

Example:

`ipreassembly timeout millisecond 0`

`ipreassembly timeout millisecond 300`

Applicable to:

NS-series Sensors

layer2 mode

This command enables you to configure the Layer 2 mode.

Syntax:

`layer2 mode <assert | deassert> <port>`

Parameter	Description
assert	Forces the Sensor port into Layer 2 Pass-Through Mode (also known as L2 Mode). This helps in troubleshooting network issues. When this command is used, the Sensor stays in L2 Mode until one of two events occurs: either during the Sensor reboot or when the **`layer2 mode deassert`** command is issued.
deassert	Forces the Sensor port out of Layer 2 Pass-Through Mode. It is used to re-establish IPS processing after the **`layer2 mode assert`** command is issued. This command must not be used to force a Sensor out of L2 Mode if L2 Mode was triggered by a Sensor software failure. Using the command in this manner triggers a Sensor reboot.
port	Sets the port for which assert or deassert action needs to be performed. Valid port numbers for NS7x00, NS7x50, NS7500, NS7600, NS9x00, and NS9500 Sensors are: G0/1 | G0/2 |G0/3 | G0/4 | G1/1 | G1/2 | G1/3 | G1/4 | G1/5 | G1/6 | G1/7 | G1/8 | G1/9 | G1/10 | G1/11 | G1/12 | G2/1 | G2/2 | G2/3 | G2/4 | G2/5 | G2/6 | G2/7 | G2/8 | G2/9 | G2/10 | G2/11 | G2/12 | G3/1 | G3/2 | G3/3 | G3/4 | G3/5 | G3/6 | G3/7 | G3/8 Valid port numbers for NS3600 are: 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 | 13-14

Default Value:

On

Sample Output:

`IntruDbg#> layer2 mode assert g0/1-g0/2`

> **NOTE**
>
> To check the Layer 2 configuration on individual interface, run **`show layer2 portlevel`** command.

Applicable to:

NS3600, NS7x00, NS7x50, NS7500, NS7600, NS9x00, and NS9500 Sensors

layer2 mode deassert-all

This CLI command forces all the ports of the Sensor, previously set to assert, out of Layer 2 Passthru Mode.

This command has no parameter.

Syntax:

```
layer2 mode deassert-all
```

Example:

The following command resets the layer 2 mode configuration.

```
IntruDbg#>layer2 mode deassert-all

Currently no port pair have layer2 config enabled
```

Applicable to:

NS-series Sensors

l7dpstat

This command displays the statistics of packets for which the scanning was skipped due to load.

Syntax:

```
l7dpstat
```

Sample Output:

```
IntruDbg#> l7dpstat

datapath 0:

l7DatapathInstCnt: 7173

l7PriDatapathInstCnt: 0

l7DatapathPktCnt: 2115

l7PriDatapathPktCnt: 0

l3LoopCnt: 76426667

datapath 1:

l7DatapathInstCnt: 143

l7PriDatapathInstCnt: 0

l7DatapathPktCnt: 9

l7PriDatapathPktCnt: 0
```

```
l3LoopCnt: 2248470949
```

Applicable to:

NS-series Sensors

l7show

This command shows layer 7 processing statistics for all datapaths.

Syntax:

```
l7show
```

Sample Output:

```
IntruDbg#> l7show

datapath 37 :

Total packets received: 37501712

pkt total: 0

Byte total: 0

Max extra binary scan pkts per monitored pkt: 0

Protocol for max extra binary scan pkts count: 0

datapath 38 :

Total packets received: 26998825

pkt total: 0

Byte total: 0

Max extra binary scan pkts per monitored pkt: 0

Protocol for max extra binary scan pkts count: 0
```

Applicable to:

NS-series Sensors

loadbalance

This command is related to forwarding of packets.

Syntax:

```
loadbalance < pre-fe| post-fe| normal>
```

Parameter	Description
pre-fe	All packets are forwarded before front end processing.
post-fe	All packets are subjected to front end processing but are forwarded before backend processing.
normal	All packets are subjected to both front end and backend processing before being forwarded.

Applicable to:

NS-series Sensors

logShowCfg

This command displays the management module message log level.

Syntax:

```
logShowCfg
```

Sample Output:

```
IntruDbg#> logShowCfg

Logging is ON, mode: send to syslog

controlChannel (id = 0) : level = 0 (emergency)

correlationEng (id = 1) : level = 0 (emergency)

packetLog (id = 2) : level = 0 (emergency)

snmpAgent (id = 3) : level = 0 (emergency)

systemCtrl (id = 4) : level = 0 (emergency)

ivSensor (id = 5) : level = 0 (emergency)

cli (id = 6) : level = 0 (emergency)

monitor (id = 7) : level = 0 (emergency)

ssl (id = 8) : level = 0 (emergency)

sig (id = 9) : level = 0 (emergency)

logging (id = 10) : level = 0 (emergency)

logNode (id = 11) : level = 0 (emergency)

authgw (id = 13) : level = 0 (emergency)

sgap (id = 14) : level = 0 (emergency)

radm (id = 15) : level = 0 (emergency)

qvm (id = 16) : level = 0 (emergency)
```

```
radi (id = 17) : level = 0 (emergency)

artemis (id = 18) : level = 0 (emergency)

intfw (id = 19) : level = 0 (emergency)

tsproc (id = 20) : level = 0 (emergency)

rm (id = 22) : level = 0 (emergency)

deviceProfile (id = 24) : level = 0 (emergency)

sofa (id = 25) : level = 0 (emergency)
```

Applicable to:

NS-series Sensors

maidstat

This command displays multi-attack ID (botnet) statistics.

Syntax:

```
maidstat
```

Sample Output:

```
IntruDbg#> maidstat

Core id range is not selected, Displaying ALL Regular MAID Component Attack IDs Processed = 0

Known Bot Component Attack IDs Processed = 0

Zero Day Component Attack IDs Processed = 0

Nested Component Attack IDs Processed = 0

Nested Alert Processed= 0

Regular MAID Alerts Raised = 0

Known Bot Alerts Raised = 0

Zero Day Alerts Raised = 0

Regular MAID Alerts Not Sent = 0

Known Bot Alerts Not Sent = 0

Zero Day Alerts Not Sent = 0

Number of Component Attack IDs Over Threshold Met = 0

Number of Component Attack IDs Over Threshold Not Met = 0

Regular MAID Correlation Un-Success = 0
```

```
Known Bot Correlation Un-Success = 0

Zero Day Correlation Un-Success = 0

Zero Day TS Bad Reputation Heuristic = 0

Zero Day TS Good Reputation Ignored = 0

MAID Component Alert sent = 0

Next AND Stage Transition = 0

Out Of Order AND Stage = 0

MAID Correlation Tracked For Destination = 0

Hosts State Info Free Buffers = 2000 (2000)

Correlation AID State Free Buffers = 10000 (10000)

Component AID State Free Buffers = 50000 (50000)

Peer Hosts Info Free Buffers = 80000 (80000)

Zero Day AID State Free Buffers = 6000 (6000)

Zero Day Component AID State Free Buffers = 30000 (30000)

Hosts State Info Buffer Allocation Failed = 0

Correlation AID State Buffer Allocation Failed = 0

Component AID State Buffer Allocation Failed = 0

Peer Hosts Info Buffer Allocation Failed = 0

Zero Day AID State Buffer Allocation Failed = 0

Zero Day Component AID State Buffer Allocation Failed = 0

MAID Table Lookup Failed = 0

MAID Total Memory Used = 8980000
```

Applicable to:

NS-series Sensors

managerChanState

Use this command to view, enable or disable the state SSL channel between the Sensor and the Manager. This command is applicable to the SSL channels of the primary as well as secondary Manager.

Syntax:

```
managerChanState <on|off|status>
```

Example:

```
IntruDbg#> managerChanState status

managerChanState is On
```

Applicable to:

NS-series Sensors

niantic_stats

This command is used to show or clear the statistics related to packets and bytes for the NIC ports in the NS-series Sensors. In Virtual IPS Sensors, it shows or clears the statistics related to packets and bytes for the monitoring ports. This command is primarily used for debugging purposes.

The port numbers used here are internal NIC port numbers. So, the user should have a fair understanding of the internal NIC port mapping to be able to work with this command.

NOTE

- If you observe any errors or memory allocation failures (**`RX-nombuf errs`**) in the **`niantic_stats show`** command output, you must tune the packet capture filters.
- The queue level statistics are not shown in the **`niantic_stats show`** command output for NS9500 and NS7500.

Syntax:

```
niantic_stats <show|clr><<0-n>|all>
```

Parameter	Description
show	Shows the packets and bytes statistics for the NIC ports
clr	Clears the packets and bytes statistics for the NIC ports
n	• For 3100, 3200, 5100, 5200, 7100, 7150, 7250, and 7350 Sensors, the port numbers range from integer values 0 to 1. • For 3500, 7200, 7300, and 7500 Sensors, the port numbers range from integer values 0 to 3. • For 3600 Sensors, the port numbers range from integer values 0 to 13. • For 7600 Sensors, the port numbers range from integer values 0 to 7. • For 9100, 9200, 9300 Sensors, the port numbers range from integer values 0 to 15. • For 9500 Sensor, the port numbers range from integer values 0 to 11. • For IPS-VM600 and IPS-VM5000 Sensors, the port numbers range from integer values 0 to 5 and they directly map to the monitoring ports.
all	Either shows or clears the statistics for all the NIC ports

Sample Output:

```
IntruDbg#> niantic_stats show 4
```

```
Writing in PID 49929

EAL: ######################## NIC statistics for port 4 ########################

EAL: TX-packets: 780622 TX-errors : 0 TX-bytes : 87428520

EAL: RX-packets: 26 RX-errors : 0 RX-bytes : 2652

EAL: RX-crcerrs: 0 RX-nombuf errs: 0 RX-missed: 0

EAL: RX-lenerrs: 0 RX-rucerrs : 0 RX-roc : 0

EAL: Q0 RX-pkts: 26 RX-bytes : 2652 RX-drop : 0

EAL: Q0 TX-pkts: 546448 TX-bytes : 59015240

EAL: Q1 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q1 TX-pkts: 78059 TX-bytes : 8430372

EAL: Q2 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q2 TX-pkts: 78058 TX-bytes : 8430264

EAL: Q3 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q3 TX-pkts: 78057 TX-bytes : 8430156

EAL: Q4 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q4 TX-pkts: 0 TX-bytes : 0

EAL: ################################################################################
```

Applicable to:

NS-series and Virtual IPS Sensors

niantic_stats-sec

This command is used to show or clear the statistics of packets and bytes for the NIC ports of the secondary Sensor in the primary Sensor.

Syntax:

```
niantic_stats-sec <show|clr><<0-15>|all>
```

Parameter	Description
show	Shows the statistics of packets and bytes for the NIC ports
clr	Clears the statistics of packets and bytes for the NIC ports
0-15	The port numbers ranging from integer values 0 to 15
all	Either shows or clears the statistics for all the NIC ports

Sample Output:

```
IntruDbg#> niantic_stats-sec show 4

argv[1] :4

PortNum :5

Writing in PID 120432

EAL: ######################## NIC statistics for port 4 ########################

EAL: TX-packets: 323373 TX-errors : 0 TX-bytes : 36217776

EAL: RX-packets: 0 RX-errors : 0 RX-bytes : 0

EAL: RX-crcerrs: 0 RX-nombuf errs: 0 RX-missed: 0

EAL: RX-lenerrs: 0 RX-rucerrs : 0 RX-roc : 0

EAL: Q0 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q0 TX-pkts: 80845 TX-bytes : 8731260

EAL: Q1 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q1 TX-pkts: 80843 TX-bytes : 8731044

EAL: Q2 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q2 TX-pkts: 80843 TX-bytes : 8731044

EAL: Q3 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q3 TX-pkts: 80842 TX-bytes : 8730936

EAL: Q4 RX-pkts: 0 RX-bytes : 0 RX-drop : 0

EAL: Q4 TX-pkts: 0 TX-bytes : 0

EAL: ############################################################################
```

Applicable to:

NS9300P Sensors only

ntbaChnstate

Configure the channel between the Sensor and the NTBA using this command.

Syntax:

```
ntbaChnstate <on> <off>
```

Parameter	Description
<on>	Establishes the channel between the Sensor and the NTBA

Parameter	Description
<off>	Stops the channel between the Sensor and the NTBA

Example:

```
ntbaChnstate on
```

Applicable to:

Virtual IPS Sensors

packetcapture

This command is used to start or stop packet capture in VMware NSX, AWS, and Azure Platforms, or upload captured packet files.

Syntax:

```
packetcapture <start><stop><upload>
```

Parameter	Description
start	Starts packet capture
stop	Stops packet capture
upload	Uploads captured packet files

Applicable to:

Virtual IPS Sensors

pptsetprioritytrafficratio

Upon execution, this command lets the ratio in which high priority traffic is given preference compared to normal priority traffic during packet processing.

Syntax

```
pptsetprioritytrafficratio
```

The default value is 3; in this case for every 3 packets processed from the high priority packet queue, only one packet is processed from the normal priority packet queue.

You can set the ratio with the values 1-5, 1 being the least priority ratio and 5 being the best priority ratio.

Applicable to:

NS-series Sensors

reset debugmode passwd

This command enables you to reset the password for entering into the debug mode.

NOTE

This command can be executed only from the debug mode.

Syntax:

```
reset debugmode passwd
```

Applicable to:

NS-series Sensors

resetalertstats

It enables users to reset the statistics of the alert channel.

Syntax:

```
resetalertstats
```

Sample Output:

```
IntruDbg#> resetalertstats

Alert and Log statistics reset to zero
```

Applicable to:

NS-series Sensors

reset-gam-update

This command deletes the Gateway Anti-Malware engine related data in the Sensors.

NOTE

After executing this command, the Sensor will reboot automatically if it is running on software version prior to 11.1 Update 5.

Upon executing this command in a Sensor running on 11.1 Update 5 or later version of software, the user's CLI control will be halted for up to 30 seconds to complete certain background activities. Users are recommended to wait until this operation completes without aborting it.

Syntax:

```
reset-gam-update
```

Applicable to:

NS-series Sensors

rspstat

This CLI command displays the datapath attack response related statistics. This command has no parameters.

Syntax:

```
rspstat
```

Sample Output:

```
IntruDbg#> rspstat

datapath 19 :

Number of TCP RST's sent: 0

Number of ICMP Msg's sent: 0

Number of VIDS's : 0

Number of Common AttackIds: 912865040

Number of Attacks dropped: 0

Number of packets received with Invalid VIDS Id: 0

Number of packets received with Invalid AttackId: 0

Count of out of list errors: 0

Number of Failover Packets freed: 0

Number of Attack Packets freed: 0

Number of Attacks received: 0

Number of packets received from PRPT: 0

Packets freed due to 'block' policy: 0

Number of packets forwarded inline: 0

Number of alerts with NO_RESP action: 0

Number of System events received: 0

Number of alerts suppressed by filters: 0

Number of attacks throttled: 0

Number of attacks Superseded by Alert-Correlation: 14

Number of ARP packets received: 0

Number of 'dropAlerts Only' throttled: 0

TCP attacks dropped due to blocking: 0

UDP attacks dropped due to blocking: 0

ARP attacks dropped due to blocking: 0
```

```
IP attacks dropped due to blocking: 0
```

Applicable to:

NS-Series and Virtual IPS Sensors

sensor perf-debug show

This command displays the top 5 protocol statistics as observed by the Sensor. The traffic details on the Sensor are based on the **sensor perf-debug** time settings.

Syntax:

```
sensor perf-debug show
```

Sample Output:

```
IntruDbg#> sensor perf-debug show
```

```
No traffic detected on sensor
```

Applicable to:

NS-series Sensors

sensor perf-debug upload-protoStats

This command enables you to upload the datapath protocol statistics to the management module.

Syntax:

```
sensor perf-debug upload-protoStats
```

Applicable to:

NS-series Sensors

set aidlog

This command logs the details for a specific attack ID. A maximum of 3 logs are added for an attack ID. These logs are generated at /tftpboot/aidlog/.

Syntax:

```
set aidlog <off> <enable <WORD> | disable <WORD>>
```

Where <WORD> is the attack ID.

Parameter	Description
<off>	Turns off the further logging of all enabled attacks but retains the existing logs
<enable>	Turn on the attack ID log.
<disable>	Turn off the attack ID log.

NOTE

The aidlog can be enabled only for 4 attacks at a time.

Applicable to:

NS-series Sensors

set auditlog-failure-respcfg

This command specifies the response action for audit logging failure.

Syntax:

```
set auditlog-failure-respcfg <continue-inspection| shutdown-appliance>
```

Parameters	Description
`continue-inspection`	The Sensor continues inspection without any response action on audit logging failure.
`shutdown-appliance`	The Sensor shuts down on audit logging failure.

Example:

```
NS9200> set auditlog-failure-respcfg continue-inspection
```

Applicable to:

NS-series Sensors

set fe-switch-hardware-hashing-method

This command is used to select the hashing method to distribute traffic through the Sensor.

Note the following:

- In a HA pair, when you execute the command on the primary Sensor, the command is set on the secondary Sensor also.
- Sensor reboot does not change settings for the hashing method.

Syntax:

```
set fe-switch-hardware-hashing-method <include_MPLS><exclude_MPLS>
```

Parameter	Description
include_MPLS	When the incoming traffic to the Sensor is MPLS (Multiprotocol Label Switching) traffic, select this method. **NOTE** This method will evenly distribute the MPLS traffic to the Sensor.
exclude_MPLS	This is enabled by default when the incoming traffic to the Sensor is non-MPLS traffic.

Sample output:

```
IntruDbg#> set fe-switch-hardware-hashing-method include_MPLS

include_MPLS : Rtag9 hashing algorithm to load balance traffic to trunk group(Id=10) is set
```

Applicable to:

NS9300 Sensors only

set gam-behavioral-scan config

This command allows you to enable or disable behavioral scan on the Gateway Anti-Malware engine.

> **NOTE**
>
> Gateway Anti-Malware engine behavioral scan is enabled by default.
>
> This command can be executed only when GAM is enabled in air gap network. Refer to the command [set gam-airgap-network] to enable or disable GAM in air gap networks.

Syntax:

```
set gam-behavioral-scan config <enable | disable>
```

Parameter:

Parameter	Description
`enable`	Enables behavioral scan on the Gateway Anti-Malware engine.
`disable`	Disables behavioral scan on the Gateway Anti-Malware engine.

Applicable to:

NS-series

set gti filerep cert-check

This command enables or disables server certificate validation for private GTI.

> **NOTE**
>
> Certificate validation for public GTI is always enabled.

Syntax:

```
set gti filerep cert-check <enable|disable>
```

Parameter	Description
enable	Enables server certificate check option for private GTI

Parameter	Description
disable	Disables server certificate check option for private GTI

Applicable to:

NS-series and Virtual IPS Sensors

set gti filerep curl-verbose

This command enables or disables curl-verbose log.

Syntax:

```
set gti filerep curl-verbose <enable|disable>
```

Parameter	Description
enable	Enables the curl-verbose log **NOTE** The output is present in `/usr/local/etc/artemisDebug.out`
disable	Disables the curl-verbose log

Applicable to:

NS-series and Virtual IPS Sensors

set gti filerep ro-flag

This command is used to enable or disable ro-flag in file reputation query.

NOTE

When enabled, GTI server does not consider this query for data mining purpose.

Syntax:

```
set gti filerep ro-flag <enable|disable>
```

Parameter	Description
enable	Enables ro-flag in GTI file reputation queries
disable	Disables ro-flag in GTI file reputation queries

Applicable to:

NS-series and Virtual IPS Sensors

set gzip decode limit

This command is used to set maximum size for http response to be decompressed upon gzip encoding.

Syntax:

```
set gzip decode limit
```

Applicable to:

NS-series Sensors

set inline drop packet log

This command enables users to configure the maximum value of dropped packet information to be logged in the Sensor log file.

Syntax:

```
set inline drop packet log <0-255>
```

Sample Output:

```
IntruDbg#> set inline drop packet log 200

set inline drop packet log 200
```

Applicable to:

NS-series Sensors

set inline traffic prioritization

Inline traffic prioritization gives preference to inline traffic over SPAN traffic during period of heavy load in the network. It is disabled by default, but can be configured through the CLI. You can view its status using this command.

Syntax:

```
set inline traffic prioritization <enable | disable>
```

Applicable to:

NS-series and Virtual IPS Sensors

set intfport id

This command sets the admin status, operating mode, flowcontrol, and speed on the specified gigabit ethernet monitoring port. You can also use this command to set the specified Ethernet monitoring port to full-duplex or half-duplex.

It is not mandatory to use all the following parameters for this command.

Syntax:

`set intfport id <port> <mediatype copper | optical> <adminstatus up | down> <duplex full|half> <flowcontrol gig | auto> <operating mode ifo | ifc | tap| span> <speed 100GBPS | 100MBPS | 100MBPS-auto | 10GBPS | 10GBPS-auto | 10MBPS | 1GBPS | 1GBPS-auto | 40GBPS> <fec disable | enable>`

Parameter	Description
<port>	A valid ethernet monitoring port on the Sensor Valid port numbers for NS-series Sensors (except NS3600) are: g0/1 | g0/2 | g1/1 | g1/2 | g1/3 | g1/4 | g1/5 | g1/6 | g1/7 | g1/8 | g1/9 | g1/10 | g1/11 | g1/12 | g2/1 | g2/2 | g2/3 | g2/4 | g2/5 | g2/6 | g2/7 | g2/8 | g2/9 | g2/10 | g2/11 | g2/12 | g3/1 | g3/2 | g3/3 | g3/4 | g3/5 | g3/6 | g3/7 | g3/8 Valid port-pairs for NS3600 Sensor are: 1-2 | 3-4 | 5-6 | 7-8 | 9-10 | 11-12 | 13-14
<mediatype>	Sets interface media type to Copper or Optical Fibre
<adminstatus>	Enables or disables the interface port
<duplex>	Sets this interface port to full or half duplex
<operating mode>	Changes the operating mode in-line fail-open line fail-close, tap or span
<speed>	Sets interface port speed to 100GBPS, 40GBPS, 10GBPS, 1GBPS, 100MBPS, 10MBPS, 10GBPS auto negotiate, 1GBPS auto negotiate, and 100MBPS auto negotiate **NOTE** This does not apply to the NS3600 Sensor.
<fec>	Enables or disables forward error connection **NOTE** This option is applicable only when you have attached a 2-port QSFP28 module.

Example:

`set intfport id g2/2 speed 1GBPS-auto`

Applicable to:

NS-series Sensors

set ipfrag

This command enables or disables IP fragment reassembly processing on datapaths.

Syntax:

`set ipfrag <on | off>`

Applicable to:

NS-series Sensors

set ipsforunknownudp

This command configures the status of IPS processing for unknown UDP packets.

Syntax:

```
set ipsforunknownudp <enable | disable>
```

Applicable to:

NS-series Sensors

set l3

This command enables or disables the layer 3 packet processing on datapaths.

> **NOTE**
> This setting should be reconfigured if the Sensor is rebooted.

Syntax:

```
set l3 <on | off>
```

Applicable to:

NS-series Sensors

set l7

This command enables or disables layer 7 packet processing and attack detection on datapaths.

> **NOTE**
> This setting should be reconfigured if the Sensor is rebooted.

Syntax:

```
set l7 <on | off>
```

Applicable to:

NS-series Sensors

set l7ddosresponse

Configure the layer7 DDoS response status using this command.

Syntax:

set l7ddosresponse <enable | disable>

Applicable to:

NS-series Sensors

set loglevel

This command assigns the log level for modules at each Sensor processing unit.

Syntax:

set loglevel <all | dos | dp | mgmt>

Applicable to:

NS-series Sensors

set loglevel dos

This command sets the DoS module message log level.

Syntax:

show loglevel dos (all | <0-21>) <0-16>

On executing the command, the following message is displayed:

IntruDbg#> set loglevel dos all 1

WARNING!!!: Changing the log level can adversely affect sensor performance. This should be used selectively under guidance from Support or Development.

Excessive logging can result in sensor reboot.

Please enter Y to set loglevel now: Y

Applicable to:

NS-series Sensors

set loglevel dp WORD

This command sets the log level of the backend processor module messages.

Syntax:

set loglevel dp WORD (all | <0-67>) <0-16>

On executing the command, the following message is displayed:

IntruDbg#> set loglevel dp WORD all 10

WARNING!!!: Changing the log level can adversely affect sensor performance. This should be used selectively under guidance from Support or Development.

```
Excessive logging can result in sensor reboot.

Please enter Y to set loglevel now: Y
```

Applicable to:

NS-series Sensors

set loglevel mgmt

This command sets the management module message log level.

Syntax:

```
set loglevel mgmt (all | <0-12>) <0-15>
```

On executing the command, the following message is displayed:

```
IntruDbg#> set loglevel mgmt 5 15

WARNING!!!: Changing the log level can adversely affect sensor performance. This should be used
selectively under guidance from Support or Development.

Excessive logging can result in sensor reboot.

Please enter Y to set loglevel now: Y
```

Applicable to:

NS-series Sensors

set malware split session parsing

This command enables or disables malware inspection of files that are downloaded as multiple segments.

Syntax:

```
set malware split session parsing <on/off>
```

Applicable to:

NS-series Sensors

set malwareEngine

Use this command to enable/disable the following malware engines for Advanced Malware inspection.

Syntax:

```
set malwareEngine <pdf|flash|gti|gam|ivx|tis|mapk|office> <enable|disable>
```

Parameter:

Parameter	Description
pdf|flash|gti|gam|ivx|tis|mapk|office	Enter the malware engine you wish to enable: • Trellix IPS Analysis • GTI File Reputation • Gateway Anti-Malware (GAM) • Intelligent Virtual Execution (IVX) engine • Trellix Intelligent Sandbox
enable	Enable malware engine
disable	Disable malware engine

Sample Output:

```
IntruDBg#> set malwareEngine pdf enable

Successfully set pdf engine state to enable
```

Applicable to:

NS-series Sensors

set malwareEngine gam clean-forward

This command helps enable or disable the clean forwarding by the Gateway Anti-Malware engine.

When enabled, if the Gateway Anti-Malware engine flags a file as clean, the scanned file is forwarded to the next malware engine.

When disabled, if the Gateway Anti-Malware engine flags a file as clean, the scanned file is not forwarded to the next malware engine.

Syntax:

```
set malwareEngine gam clean-forward <enable|disable>
```

Applicable to:

NS-series Sensors

set mgmtprocessrestart

The Sensor often reboots due to crashes in the management module processes, causing a downtime. Using this command, you can enable the restart of the management module processes, which restores the Sensor to normal functionality without going through the complete reboot cycle.

If any of the following four processes have been crashed/killed, the system tries to restart all of them automatically.

- Zebra (Individual process - takes 3-5 seconds approx.)
- Process Group : If any one of the processes (either control channel, correlation engine, or pktlog) goes down, all the three are stopped and restarted in the following sequence:

- Correlation Engine (Process group - takes 15 -20 seconds approx.)
- Packet Log Channel (Process group)
- Control Channel (Process group)

Syntax:

`set mgmtprocessrestart enable`

Use this command to enable the restart of the management module processes.

`set mgmtprocessrestart disable`

Use this command to disable the restart of the management module processes.

In case the Control Channel group restarts, the Alert and PktLog channels flap at the Manager. The reason for this flap is unknown at the Manager, as the process which maintains the means of communication (that is, the alert channel) to the Manager is being restarted. These are not logged at the Sensor in the `events.log` file.

- The process restart is visible only from the Sensor's default logs and not on the CLI.
- If the process is crashed/killed more than 3 times in an hour, the Sensor goes for an auto-recovery or warm reboot depending on the configuration.
- This feature is enabled by default.
- For debugging management issues, you can keep the watchdog off. Sensor remains in bad health and does not try to recover.

Applicable to:

NS-series Sensors

set ms-office

This command configures the MS Office response decode.

Syntax:

`set ms-office <enable|disable|max|pktCnt>`

Parameter	Description
enable	Enables MS Office response decode
disable	Disable MS Office response decode
max	MS Office maximum bin to decode per flow
pktCnt	MS Office response packet count

Example:

`set ms-office enable`

Applicable to:

NS-series Sensors

set nianticrecovery

This command enables or disables autorecovery once we recognize that Niantic transmission has stopped.

This command has no parameters.

Syntax:

```
set nianticrecovery
```

Applicable to:

NS9x00 series Sensors

set outofcontext acllookup

Use this command to enable/disable ACL lookup on out-of-order packets.

Syntax:

```
set outofcontext acllookup <enable|disable>
```

Applicable to:

NS-series Sensors

set recon

Use this command to enable or disable reconnaissance attacks detection.

> **NOTE**
> This setting should be reconfigured if the Sensor is rebooted.

Syntax:

```
set recon <on | off>
```

Applicable to:

NS-series Sensors

set sslDebug disable certid

This command is used to disable SSL debug logs for a particular certificate ID.

Syntax:

```
set sslDebug disable certid <certid>
```

Parameter:

Parameter	Description
certid	The value for certificate ID is between 1000–9999.

Applicable to:

NS-series Sensors

set sslDebug enable certid

This command is used to enable SSL debug logs for a particular certificate ID. It includes the following information:

- Checks if the traffic received matches with the certificate ID
- Checks if the traffic is decrypted

Syntax:

```
set sslDebug enable certid <certid>
```

Parameter:

Parameter	Description
certid	The value for certificate ID is between 1000–9999.

Applicable to:

NS-series Sensors

show 40to10conversion status

This CLI command displays the status of the G0 ports (G0/1 and G0/2) on NS9x00 Sensors.

Syntax:

```
show 40to10conversion status
```

Sample Output:

```
IntruDbg#> show 40to10conversion status

40to10 conversion is DISABLED ret(0)
```

Applicable to:

NS9100 and NS9200 Sensors.

show ab stats

The **`show ab stats`** command displays the status of the updated and total entries in the allow list and the block list while using custom fingerprints. It also displays the details of the last file fingerprint download to the Sensor from the Manager.

Syntax:

```
show ab stats
```

Sample output:

```
IntruDbg#> show ab stats

[Allow Block File Hash Stats]

--------------------

Last FFP download type : BULK

Last FFP download status : SUCCESS

Last FFP download time(UTC) : 10:3:17, 2/24/2023

AB bulk file download count : 5

AB bulk download success count : 2

AB bulk download failure count : 0

AB incr file download count : 9

AB incr download success count : 7

AB incr download failure count : 0

IPS Manager AB md5 hash count : 200000

IPS Manager md5 allow hash count : 0

IPS Manager md5 block hash count : 200000

cache AB md5 hash count : 0

IPS Manager AB sha256 hash count : 4001

IPS Manager sha256 allow hash count : 4001

IPS Manager sha256 block hash count : 0
```

Applicable to:

NS-series and Virtual IPS Sensors.

show aidlog status

This command displays the status of the attack ID logging.

Syntax:

```
show aidlog status
```

Sample Output:

```
IntruDbg#> show aidlog status
```

```
Attack id log : On
```

Applicable to:

NS-series Sensors

show all syslog statistics

This command displays all the syslog statistics, such as the alerts received, transmitted, dropped, and the total count of the alerts received, transmitted, and dropped.

Syntax:

```
show all syslog statistics
```

Sample Output:

```
IntruDbg#> show all syslog statistics

[Syslog alert Received]

-----------------------------------

Signature Alert with PL count : 0

Botnet Alert count : 0

Signature Alert Count : 0

Signature L7 Dcap Alert Count : 0

Signature L7 DcapDataAlert count : 0

Heuristic Alert count : 0

Malware Alert count : 0

Port Scan Alert count : 0

Host Sweep Alert count : 0

ACL Alert count : 0

Statistics Anamoly Alert count : 0

Threshold Anamoly Alert count : 0

TS Malicious Alert count : 0

SSP Alert count : 0

SS Alert count : 0

Port Scan With PL Alert count : 0

Host Sweep With PL Alert count : 0
```

```
MAID Alert count : 0

[Syslog alert Transmitted]

-----------------------------------

Signature Alert with PL count : 0

Botnet Alert count : 0

Signature Alert count : 0

Signature L7 Dcap Alert count : 0

Signature L7 DcapDataAlert count : 0

Heuristic Alert count : 0

Malware Alert count : 0

Port Scan Alert count : 0

Host Sweep Alert count : 0

ACL Alert count : 0

Statistics Anamoly Alert count : 0

Threshold Anamoly Alert count : 0

TS Malicious Alert count : 0

SSP Alert count : 0

SS Alert count : 0

Port Scan With PL Alert count : 0

Host Sweep With PL Alert count : 0

MAID Alert count : 0

[Syslog alert Dropped/Blocked]

-----------------------------------

Signature Alert with PL count : 0

Botnet Alert count : 0

Signature Alert Count : 0

Signature L7 Dcap Alert Count : 0

Signature L7 DcapDataAlert count : 0

Heuristic Alert count : 0
```

```
Malware Alert count : 0

Port Scan Alert count : 0

Host Sweep Alert count : 0

ACL Alert count : 0

Statistics Anamoly Alert count : 0

Threshold Anamoly Alert count : 0

TS Malicious Alert count : 0

SSP Alert count : 0

SS Alert count : 0

Port Scan With PL Alert count : 0

Host Sweep With PL Alert count : 0

MAID Alert count : 0

[Total syslog alert count]

-----------------------------------

Total recieved syslog alert : 0

Total transmitted syslog alert : 0

Total dropped syslog alert : 0

[PRINT END]
```

Applicable to:

NS-series and Virtual IPS Sensors.

show all datapath error-counters

This command displays the various error counters in the datapath packet processing.

Syntax:

```
show all datapath error-counters
```

Sample Output:

```
IntruDbg#> show all datapath error-counters

Error Counter From Datapath id: 0

=====================================================

Error Counter of L3 Task
```

```
=======================================================

l3CheckAndTriggerPktDelayCnt :0

ipOffsetLenIndxErrCnt :0

udpOffsetLenIndxErrCnt :0

icmpCksumErrCnt :0

tcpOffsetLenIndxErrCnt :0

tcpRstErrCount :0

tcpIllegalPktErrCount :0

tcpInvalidStateErrCount :0

tcpWindowErrCount :0

tcpNoFlowErrCount :0

l7PsErrCount :0

numFOPktsSentError :0

numErrSendingPktToPME :0

l3FFPipeAddErrors :0

sslErrorDecRxPkt :0

binDectErrorDecRxPkt :0

ipOffsetLenIndxErrMMCnt :0

ipv6OffsetLenIndxErrCnt :0

ipv6OffsetLenIndxErrMMCnt :0

iprfErrCount :0

iprfOffsetLenIndxErrCnt :0

tcpErrCount :0

tcpPawsErrCount :0

tcpNoFlowErrFFMatchedFlag :0

udpErrCount :0

udpNoFlowErrCount :0

udpProbeErrCnt :0

tcpSensorDestinedErrCnt :0
```

```
tcpIprfSensorDestinedErrCnt :0

fbdToFpgaErrorCount :0

icmpErrCount :0

otherIPErrCount :0

otherIPv6ErrCount :0

cSegDataLenErrCnt :0

icmpv6CksumErrCnt :0

icmpv6ErrCount :0

arpErrPktCount :0

fbdSendErrors :0

fbdPktInitErrorCount :0

icmpNoFlowErrCount :0

icmpv6NoFlowErrCount :0

vlanBrConfigErrorCount :0

vlanBrMappingErrorCount :0

=========================================================

Error Counter of Response Task

=========================================================

numStatSendError :0

acrbCorrelateErrorCnt :0

numStatLogIdError :0

numStatLogFlowIdError :0

numStatLogSendError :0

numErrCreateLogId :0

numStatErrorDeleteLogId :0

alert_buf_alloc_err :0

alert_buf_getSemErr :0

alert_buf_retSemErr :0

alert_msgSemErr :0
```

```
l7Dcap_buf_alloc_error :0

numStatRngBufFull :0

l7_dcap_rngBuf_errors :0

cb_inactive_errors :0

numStatListsError :0

numErrSetTcpTask :0

=========================================================

Error Counter of SSLtask

=========================================================

sslPktNoContextErrors :0

ssl_decrypt_v2MasterErrs :0

ssl_decrypt_v3PreMasterErrs :0

dssl_cryptoErr :0

dssl_otherErrs :0

ssl_error :0

pkbufSaeCrtError :0

pkbufSaeDestErrors :0

pkbufSaeFragErrors :0

pkbufSendCryptErrors :0

pkbufSendRsaErrors :0

sessionFreeErr :0

ssl_type_error :0

=========================================================

Error Counter of Scan Task

=========================================================

ScanGetFifoErrors :0

=========================================================

Error Counter of L7 Task

=========================================================
```

```
l7UnhandledErrorCount :0

eofPktErr :0

l7CntrHardwarePMEPacketErrorCt :0

l7CntrBScanErrors :0

l7CntrPMEDequoteErrorCt :0

l7RcvRbInPipeErrors :0

AtdtCntrResponseModuleErrorsOnAttackRaise:0

ddAllocErr :0

dequoteErrNoFree :0

=========================================================

Error Counter of TcpUdpTask

=========================================================

tu4NacDirectIndexErrorCount :0

hqCtrlPktErrorCount :0

AclClientConnectionErr :0

AclClientMsgErrCount :0

nacHttpRedirectErrorCount :0

tcpConnAckPAWSErrCounter :0

tcpConnAckWinErrCounter :0

tcpConnAckWin0ErrCounter :0

tcpCBArrayIdxErr :0

tuErrorSendEOFCount :0

tuErrorSendEOFSemCount :0

tuEofFlowBufFlowIdErrCnt :0

=========================================================

Error Counter of TlvTask

=========================================================

BadEccErrort :0

CorEccErrort :0
```

```
xff_buf_alloc_err :0

ipChkSumErrorDropCount :0

tcpChkSumErrorDropCount :0

udpChkSumErrorDropCount :0

icmpChkSumErrorDropCount :0

icmpv6ChkSumErrorDropCount :0

offHdrLenErrorDropCount :0

tcpProtocolErrorCount :0

udpProtocolErrorCount :0

icmpProtocolErrorCount :0

icmpv6ProtocolErrorCount :0

ipProtocolErrorCount :0

ipv6ProtocolErrorCount :0

L3L4ErrorDropCount :0

=======================================================

Error Counter of hscan

=======================================================

ivHsConsumeTokenErrors :0

ivHsMakeStatePoolErrors :0

ivHsNonStreamNoDbErrors :0

resFromMgmtHashErr :0

resFromMgmtTimerErr :0

resFromMgmtErrorMgmt :0

resFromMgmtErrorArtemis :0

rstErr :0

TkdtCntrHwarePMResultErrors :0

=======================================================

Error Counter of sw-pm

=======================================================
```

```
g_numErrsSendingPktsToMSPM :0

g_numErrsSendingPktsToPCRE :0

g_pendingAllocErrs :0

g_ErrorExtPendingList1 :0

g_ErrorExtPendingList2 :0

g_ErrorExtPendingList3 :0

g_ErrorExtPendingList4 :0

=========================================================

Error Counter of IvCrpto

=========================================================

ivCrypto_rsaCommandErrs :0

ivCrypto_rsaPkcsErrs :0

ivCrypto_desLengthErrs :0

ivCrypto_desCommandErrs :0

ivCrypto_arc4CommandErrs :0

ivCrypto_aesLengthErrs :0

ivCrypto_aesCommandErrs :0

ivRemoteCryptoBadContextErrors :0

ivRemoteCryptoCtxInitFailedErrors :0

ivRemoteCryptoErrorsWhileCreating :0

ivRemoteCryptoErrorsWhileSending :0

ivRemoteCryptoCertMatchErrors :0

ivRemoteCryptoOpenCallCntWrapErrors :0

=========================================================

Error Counter of IPFragTask

=========================================================

ip6CopyErrCount :0

ip6defragErrCount :0

dmIP6FragCallbackError :0
```

```
dmIP6LastFragCallbackError :0

ipCopyErrCount :0

ipdefragErrCount :0

numStatFifoError :0

numStatFragBuffersError :0

dmFragCallbackError :0

dmLastFragCallbackError :0

icmpFragErrCnt :0

sgapRspPktErrCnt :0

sgapReqPktErrCnt :0

sgapRSTPktErrCnt :0

=========================================================

Error Counter of BDecode

=========================================================

smbGenericErrorMultipleHdrs :0

=========================================================

Error Counter of IFSF

=========================================================

IFSFErr :0

=========================================================

Error Counter of connLimiting

=========================================================

connRspRstErrCnt :0

connRspHostQErrCnt :0

putConnRefErrCnt[0] :0

putConnRefErrCnt[1] :0
```

Applicable to:

NS-series Sensors

show amchannelencryption status

This command displays the anti-malware channel encryption status.

Syntax:

```
show amchannelencryption status
```

Sample Output:

```
IntruDbg#> show amchannelencryption status

AntiMalware Channel Encryption status enabled
```

> **NOTE**
>
> The status will always be enabled.

Applicable to:

NS-series Sensors

show attack count

This command displays the total number of attacks detected in a datapath.

Syntax:

```
show attack count
```

Sample Output:

```
IntruDbg#> show attack count

Datapath 0 :

Total attacks detected = 6963

Datapath 1 :

Total attacks detected = 1674303
```

Applicable to:

NS-series Sensors

show auditlog-failure-respcfg status

It displays the response action configured for audit logging failure.

> **NOTE**
>
> This command can be used on a DoDIN APL-compliant Sensor only.

Syntax:

```
show auditlog-failure-respcfg status
```

Sample Output:

```
intruShell@NS9200_119> show auditlog-failure-respcfg status

Configured action for audit logging failure : continue-inspection
```

show botnet-usage

This CLI command displays botnet usage and statistics.

Syntax:

```
show botnet-usage
```

Sample output:

```
IntruDbg#> show botnet-usage

DAT File Status :Present

DAT File version : 778.0

Total IPv4 URL Entries : 0

Total IPv4 URL Entries Successful LookUps : 0

Total IPv6 URL Entries : 0

Total IPv6 URL Entries Successful LookUps : 0

Total URL Entries : 1414

Total URL Entries Successful LookUps : 0

Total Domain Entries : 1783

Total Domain Entries Successful LookUps : 0

Total Failed LookUps(False+/-) : 0

Total Bot IPv4 Seen : 0

Total Bot IPv6 Seen : 0

Total Entries Allocated : 720000

Total Entries Used : 115092

Total Entries Skipped(Same Domain Multiple URI) : 221

Total Entries Upgraded(Whole Domain Upgraded) : 0

Total DNS Domain Block Entries Successful Lookups : 5
```

```
Total DNS Failed Lookups : 3

Total DNS Resp Parse Succ : 0

Total DNS Resp Parse Failure : 0

Total DNS Resp Domains extracted successfully : 0

Total DNS Resp parsing forced complete : 0

Total DNS Resp A records extracted successfully : 0

Total DNS Resp AAAA records extracted successfully : 0

Total DNS Resp A records extraction failures : 0

Total DNS Resp AAAA records extraction failures : 0

Total exception matches found : 5

Total DAT block domain entries : 1316

DNS Sinkhole IP : 0x7f000001

DNS Sinkhole TTL (min) : 1
```

Applicable to:

NS-series Sensors

show boundarydcapmatchstats

This command displays counters related to HTTP POST multipart. These counters are further categorized as Boundary DCAP counters, Boundary Match counters and HeldBytes counters.

Syntax:

```
show boundarydcapmatchstats
```

Sample output:

```
IntruDbg#> show boundarydcapmatchstats

Core id range is not selected, Displaying ALL
```

Boundary DCAP counters:

```
Total Boundary Nodes Alloc'd Count: 45640

Total Boundary Nodes Alloc Fail Count: 0

Total Boundary Nodes Free Success Count: 45594

Total Boundary Nodes Free Failure Count: 0

Total Boundary Node DCAPALLOC Fail Count 1: 0
```

```
Total Boundary Node DCAPALLOC Fail Count 2: 7071

Total Boundary Node DCAPAPPEND Fail Count 1: 0

Total Boundary Node DCAPAPPEND Fail Count 2: 0

Total Boundary Node DCAPAPPEND Fail Count 3: 7023

Total Boundary Node Invalid Pointer Address: 0

Total Boundary Node Double Free Pointer Address: 1
```

Boundary Match counters:

```
Total Boundary Match Success Count: 129529

Total Boundary Match (Last boundary) Success Count: 27787

Total Boundary Match Failure Count: 21256

Total Boundary Match Partial Count: 42420

Total Boundary Match Invalid Boundary Count: 287

Total Boundary Match Invalid Boundary Length Count: 0
```

HeldBytes counters:

```
No. of times BytesToHold set by BoundaryMatch: 44329

No. of times bytes held while sending File Data: 15741

No. of times BoundaryMatch cleared BytesToHold: 28462

No. of times Trigger-Token bytes were held: 9325

No. of times sendHeldBytes set by BoundaryMatch: 887

No. of times sendHeldBytes set by CheckTrigger: 8303

No. of times Held bytes Prepended: 9111

No. of times Held bytes Prepend failed: 0

No. of times Held bytes cleared: 157072
```

Applicable to:

NS-series and Virtual IPS Sensors

show connlimithost

This command shows Connection Limiting host table stats.

Syntax:

```
show connlimithost
```

Sample Output:

```
IntruDbg#> show connlimithost

[connLimiting HostTbl Stats]

Max Host Cnt : 131072

Current Host Cnt : 0
```

Applicable to:

NS-series Sensors

show connlimitstat

This command, when executed, displays Connection Limiting statistics.

Syntax:

```
show connlimitstat
```

Sample Output:

```
IntruDbg#> show connlimitstat

[connLimiting Stats]

Blocked Connection Cnt : 0

TCP RST Connection Cnt : 0

Quarantine Cnt : 0

Alert Cnt : 0
```

Applicable to:

NS-series Sensors

show datapath processunits

This command displays the number of process units in a datapath.

Syntax:

```
show datapath processunits
```

Sample Output:

```
IntruDbg#> show datapath processunits

Datapath 0:

Process unit count 1
```

```
Process priority unit count 0

Datapath 1:

Process unit count 0

Process priority unit count 0
```

Applicable to:

NS-series Sensors

show doscfg

This command displays front end configuration.

Syntax:

```
show doscfg
```

Sample Output:

```
IntruDbg#> show doscfg

Layer2 assert

INTF PORT 0

AdminStatus UP

OperatingMode INLINE_FAIL_CLOSED

Duplex : FULL

InOutType INSIDE

Mdix setting : DISABLED

10/100 Port Speed : NOT APPLICABLE

GigSpeedConfig AUTONEG
```

Applicable to:

NS-series Sensors

show feature status

This CLI command displays the enable/disable status of the following features:

- HTTP Response Scanning
- Heuristic Web Application
- NTBA
- L7 Data Collection

- X-Forwarded-For
- Advanced Botnet Detection
- Advanced Traffic Detection
- HTTP Response Decompression
- HTTP2 Processing
- HTTP2 Server Push Config
- Microsoft Office File Deep Inspection
- Web Server Protection
- Malware Detection
- IP Reputation
- Device Profiling
- IPS Simulation
- SSL Decryption
- GTI Server

NOTE

HTTP2 Server Push Config is displayed only when it is enabled in the Manager.

Syntax:

```
show feature status
```

Sample Output:

```
IntruDbg#> show feature status

HTTP Response Scanning : Enabled

NTBA : Disabled

Heuristic Web Application : Disabled

L7 Data Collection : Enabled

X-Forwarded-For : Enabled

Advanced Botnet Detection : Disabled

Advanced Traffic Detection : Enabled

Web Server Protection : Disabled

HTTP Response Decompression : Enabled

MS Office File Deep Inspection : Enabled

URL Reputation : Disabled
```

```
HTTP2 Processing : Enabled

HTTP2 Server Push Config : Enabled

IP Reputation : Disabled

Device Profiling : Disabled

IPS Simulation : Disabled

Malware Detection : Disabled

SSL Decryption : Disabled
```

Applicable to:

NS-series and Virtual IPS Sensors

> **NOTE**
>
> HTTP2 details are available only for NS9500, NS7600, NS7500, and NS3600 Sensors.

show fe-switch-hardware-hashing-method

This command displays the hashing method used to distribute traffic through the Sensor.

This command has no parameters.

Syntax:

```
show fe-switch-hardware-hashing-method
```

Sample output:

```
IntruDbg#> show fe-switch-hardware-hashing-method

fe-switch-hardware-hashing-method : include_MPLS
```

Applicable to:

NS9300 Sensors only

show gam scan stats

This command displays statistics of the scans performed by the GAM engine on the files submitted for scanning.

Syntax:

```
show gam scan stats
```

Sample Output:

```
Local GAM Scan Statistics:

-------------------------
```

```
Total scan requested: 2

Total scan submitted to GAM: 2

Total Successful Scans: 2

Total Scan Failures: 0

Total scan misc error count: 0

Total scan req skipped due to filesize mismatch: 0

Total scan req skipped due to timeout in Queue : 0
```

Applicable to:

NS-series Sensors

show geoloc v4

This command allows users to lookup the geographical location for a specified IPv4 address.

Syntax:

```
show geoloc v4 <IP address>
```

Example:

```
IntruDbg#> show geoloc v4 8.8.8.8

Entered IP address is valid IPv4 Address

Country code : 840

Country name : united states
```

Applicable to:

NS-series and Virtual IPS Sensors

show gti filerep status

This command displays run-time information on the server certificate validation status based on the type configured.

This command has no parameters.

Syntax:

```
show gti filerep status
```

Sample Output:

For public,

```
IntruDbg#> show gti filerep status

[Server Certificate Validation]
```

```
Type : public

URL : https://nsp.rest.gti.trellix.com/1

Validation : enabled

CA cert store : present

Validation status : success
```

For private,

```
IntruDbg#> show gti filerep status

[Server Certificate Validation]

Type : private

URL : https://10.12.20.18/1

Validation : disabled
```

Applicable to:

NS series and Virtual IPS Sensors

show http-ms decode stats

This command shows decoding related settings for MS office Malware engine.

Syntax:

```
show http-ms decode stats
```

Sample Output:

```
IntruDbg#> show http-ms decode stats

HTTP response decoding status : DISABLED(For all physical interfaces)

MS-Office response decoding status : DISABLED(For all physical interface)

Maximum size of decode content per flow : 52428800

Ms-Office supported max bin no. : 25

Ms-Office Max Pkt per stream : 5
```

Example:

```
show http-ms decode stats
```

Applicable to:

NS-series Sensors

show ni status

This command displays NI feature status (enabled or disabled) and the communication status between Trellix NI and Trellix IPS solution. It also shows other configuration details related to NI integration, such as NI appliance IP address, port, Client Group name, and NI config polling duration as set in the Client Group. Additionally, it displays NI L7 metadata configuration status (enabled or disabled), and the protocols for which it is enabled.

> **NOTE**
>
> Currently, IPS Sensors support the export of L7 metadata related to HTTP, HTTPS, HTTP2, SMTP, and FTP protocols only to NI.

Syntax:

```
show ni status
```

Sample Output:

```
IntruDbg#> show ni status

NI Feature Status : ENABLED

NI IP Address : 10.1.1.1

NI IP Port : 443

NI Group Name : IPSSantaClara

NI Communication Status : UP

NI Config Poll timer : 30:00 minutes

NI Metadata Config : ENABLED

NI Protocols Enabled : HTTP
```

Applicable to:

NS-series and Virtual IPS Sensors

show ingress-egress stat

This command applies to Virtual Security System instances. In other words, it applies only to the security appliances installed on hypervisors through the integration with Intel® Security Controller.

For Virtual Security System instances, the **`show intfport`** command is not available; you instead use **`show ingress-egress stat`** to view the number of inbound and outbound packets received, forwarded, and dropped by the Virtual Security System instance.

It is also applicable to AWS environment and displays traffic statistics.

This command has no parameters.

Syntax:

```
show ingress-egress stat
```

Sample Output:

```
IntruDbg#> show ingress-egress stat

Total Packets Received : 310004

Total Packets Sent : 0

Total Packets Dropped : 0

Total Packets Received Byte : 61278498

Total Packets Sent Byte : 0

Total Rx IDS Packets : 310004

Total Rx IPS Packets : 0

Total Rx INBOUND Packets : 163204

Total Rx OUTBOUND Packets : 146800

Total Tx IPS Response Packets : 0

Total Tx Jumbo skipped Packets : 0

Total Rx Hello Packets : 70965

Total Tx Hello Packets : 70965

Total Tx EAGAIN error : 0

Total Tx EMSGSIZE error : 0

Total Tx send error : 0

Total Rx alloc error : 0

Total Rx EAGAIN/block error : 249575729961

Total Rx refill : 310516

Total Rx non-hello and zero length : 0
```

Applicable to:

Virtual Security System instances and AWS Environment

show inline traffic prioritization status

Inline traffic prioritization gives preference to inline traffic over SPAN traffic during period of heavy load in the network. It is disabled by default, but can be configured through the CLI. You can view its status using this command.

```
show inline traffic prioritization status
```

Sample Output

```
Inline Traffic Prioritization Status enabled
```

Applicable to:

NS-series and Virtual IPS Sensors

show ipsforunknownudp status

This command displays the configuration status of IPS processing for unknown UDP packets.

Syntax:

```
show ipsforunknownudp status
```

Sample Output:

```
IntruDbg#> show ipsforunknownudp status
```

```
IPS for Unknown UDP is enabled
```

Applicable to:

NS-series Sensors

show ipfrag status

This command displays the IP fragment reassembly processing status.

Syntax:

```
show ipfrag status
```

Sample Output:

```
IntruDbg#> show ipfrag status
```

```
IP Fragment processing enabled
```

Applicable to:

NS-series Sensors

show l3 status

This CLI command displays the layer 3 packet processing status on datapaths.

Syntax:

```
show l3 status
```

Sample Output:

```
IntruDbg#> show l3 status
```

Layer3 processing enabled

Applicable to:

NS-series Sensors

show l7 status

The **show l7 status** displays the layer 7 protocol parsing and attack detection status on datapaths.

Syntax:

show l7 status

Sample Output:

IntruDbg#> show l7 status

Layer7 processing enabled

Applicable to:

NS-series Sensors

show l7dcap-usage

Information displayed by the **show l7dcap-usage** command includes the following:

- Layer-7 Dcap Buffers Allocated at Initialization
- Layer-7 Dcap Buffers Available now
- Layer-7 Dcap Buffers Allocated Errors
- Layer-7 Dcap Alert Buffers Allocated
- Layer-7 Dcap Alert Buffers Available
- Layer-7 Dcap Alert Buffers Allocate Error
- Layer-7 Dcap Regular Alerts Sent
- Layer-7 Dcap Special Alerts sent
- Layer-7 Dcap Context End Alerts Sent
- Layer-7 Dcap CB InActive when DCAP Called

Syntax:

show l7dcap-usage

Sample Output:

IntruDbg#> show l7dcap-usage

Layer-7 Dcap Buffers Allocated at Init 5600

Layer-7 Dcap Buffers Available now 5565

```
Layer-7 Dcap Buffers Alloc Errors 0

Layer-7 Dcap Alert Buffers Allocated 16384

Layer-7 Dcap Alert Buffers Available 16384

Layer-7 Dcap Alert Buffers Allocate Error 0

Layer-7 Dcap Regular Alert's Sent 0

Layer-7 Dcap Special Alert's sent 0

Layer-7 Dcap Context End Alert's Sent 0

Layer-7 Dcap CB InActive when DCAP Called 0

Layer-7 Dcap Ring Buffer Errors 0

Alert Ring Buffer Full Cnt 0

Num Alerts Dropped at Sensors 0

Layer-7 Dcap Fifo Check Seen 0
```

Applicable to:

NS-series Sensors

show l7ddosresponse status

This command displays whether layer 7 DDoS response is enabled or disabled. Layer 7 DDoS response is enabled by default. When enabled, the Sensor drops packets for server-based DDoS functionality (Maximum simultaneous connections to the web server exceeds the threshold) or, quarantines for client-based DDoS functionality (Maximum URL request rate exceeds the threshold).

Syntax:

```
show l7ddosresponse status
```

Sample Output:

```
IntruDbg#> show l7ddosresponse status

L7ddos Response Status enabled
```

Applicable to:

NS-series Sensors

show layer2 forward

This command shows all the TCP, UDP ports, and the VLAN IDs that are enabled for layer 2 forwarding.

Syntax:

```
show layer2 forward <all|tcp|udp|vlan>
```

Parameter	Description
<all>	Shows all the port numbers(TCP,UDP) and VLAN IDs that are enabled for layer 2 forwarding
<tcp>	Shows all the TCP port numbers that are enabled for layer 2 forwarding
<udp>	Shows all the UDP port numbers that are enabled for layer 2 forwarding
<vlan>	Shows all the VLAN IDs that are enabled for layer 2 forwarding

Sample Output:

```
intruShell@john> show layer2 forward all

TCP ports: 50

UDP ports:

VLAN Ids:

All :

g0/1-g0/2 :

g3/1-g3/2 :

g3/3-g3/4 :

g3/5-g3/6 :

g3/7-g3/8 :
```

Example:

The sample output above shows the **`show layer2 forward`** command used for showing all the port numbers (TCP,UDP) and vlan IDs that are enabled for layer 2 forwarding.

Applicable to:

NS-series Sensors

show layer2 portlevel

This command displays the configuration of layer2 settings for the Sensor port pair.

Syntax:

```
show layer2 portlevel
```

Sample Output:

```
IntruDbg#> show layer2 portlevel

Currently no port pair have layer2 config enabled
```

Applicable to:

NS-series Sensors

show layer2 reason

This command displays why the Sensor moved to layer 2 mode.

Syntax:

`show layer2 reason`

Sample Output:

`IntruDbg#> show layer 2 reason`

`Layer2 reason: assert`

The Sensor goes into layer2 during clear active flows.

Applicable to:

NS-series Sensors

show malwareclientstats

The command displays the malware client statistics in all scan engines for all supported file types.

Syntax:

`show malwareclientstats`

Sample output

```
IntruDbg#> show malwareclientstats
Core id range is not selected, Displaying ALL
---------------------------------
SOFA CLIENT FILE-ENGINE STATISTICS:
---------------------------------
SOFA CLIENT FILE TYPE PE (EXE,DLL,SYS,COM,etc.) Files (1) STATISTICS:
---------------------------------

Dcap Start Cnt: 20
Dcap End Cnt: 20
Dcap End-At-Offset Cnt: 0
New-File-Dwnld Pkt Cnt: 20
File-Data Pkt Cnt: 0
Scan-Req Pkt Cnt: 20
Error-Out Pkt Cnt: 20
New-File-Dwnld-Rsp Pkt Cnt: 0
Scan-Rsp Pkt Cnt: 20
Error-In Pkt Cnt: 0
Session Timer Allocated: 20
Session Timer Freed: 20
Session Timer Triggered: 0
Scan Timer Allocated: 0
```

```
Scan Timer Freed: 0
Scan Timer Triggered: 0
Pkt-Hold Timer Allocated: 20
Pkt-Hold Timer Freed: 20
Pkt-Hold Timer Triggered: 0

SOFA CLIENT STATISTICS IPS Analysis(pdf) Engine FOR FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr : 0
Scan Rsp Discarded: 0
Error Result Cnt : 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset : 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS IPS Analysis(flash) Engine FOR FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr : 0
Scan Rsp Discarded: 0
Error Result Cnt : 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
```

```
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset : 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS IPS Analysis(office) Engine FOR FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr : 0
Scan Rsp Discarded: 0
Error Result Cnt : 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset : 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS Gateway Anti-Malware ENGINE AND FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr : 0
Scan Rsp Discarded: 0
Error Result Cnt : 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
```

```
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset : 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS GTI File Reputation ENGINE AND FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr: 0
Scan Rsp Discarded: 0
Error Result Cnt: 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset: 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS FILE SAVE ENGINE AND FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 20
Scan Rsp Cnt: 20
Scan Rsp Rcvd Within Pkt-Hold Tmr: 20
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr: 0
```

```
Scan Rsp Discarded: 0
Error Result Cnt: 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset: 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS BLOCKLIST ENGINE AND FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr: 0
Scan Rsp Discarded: 0
Error Result Cnt: 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset: 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS Trellix Intelligent Sandbox ENGINE AND FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 0
```

```
Scan Rsp Cnt: 0
Scan Rsp Rcvd Within Pkt-Hold Tmr: 0
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr: 0
Scan Rsp Discarded: 0
Error Result Cnt: 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 0
Resp-Action No-Block: 0
Resp-Action Alert: 0
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 0
Resp-Action No-TCP-Reset: 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 0
Malware Score Unknown: 0

SOFA CLIENT STATISTICS IVX ENGINE AND FILE TYPE PE (EXE,DLL,SYS,
COM,etc.) Files (1):

Scan Req Cnt: 20
Scan Rsp Cnt: 20
Scan Rsp Rcvd Within Pkt-Hold Tmr: 20
Scan Rsp Rcvd Within Scan Tmr: 0
Scan Rsp Rcvd Within Sess Tmr: 0
Scan Rsp Discarded: 0
Error Result Cnt: 0
L7-DCAP Copy Cnt: 0
L7-DCAP Copy Error Cnt: 0
Resp-Action Block: 20
Resp-Action No-Block: 0
Resp-Action Alert: 20
Resp-Action No-Alert: 0
Resp-Action TCP-Reset: 20
Resp-Action No-TCP-Reset: 0
Clean Files: 0
Malware Score Very-Low: 0
Malware Score Low: 0
Malware Score Medium: 0
Malware Score High: 0
Malware Score Very-High: 20
Malware Score Unknown: 0
```

Applicable to:

NS-series Sensors

show malwaredcapstats

This command displays the data capture statistics of all the files downloaded through the Sensor.

Syntax:

```
show malwaredcapstats
```

Sample output

```
IntruDbg#> show malwaredcapstats

Core id range is not selected, Displaying ALL

Total Session Nodes Alloced Count: 9

Total Session Nodes Alloced Error Count: 0

Total Session Nodes Alloced Freed Count: 9

Total Sofa Dcap Alloc Count: 9

Total Sofa Dcap Start Count: 9

Total Sofa Dcap End Count: 9

Total Sofa Dcap End At Offset Count: 0

Total New File Downloads Pkt Count: 9

Total Scan Req Pkt Count: 9

Total Session Timer Alloced Count: 9

Total Session Timer Alloced Error Count: 0

Total Session Timer Triggered Count: 3

Total Pkt Hold Timer Alloc Count: 9

Total Pkt Hold Time Alloc Err Count: 0

Total Retrans Pkt Drop Count: 0

Pkt Buffer Alloc Err Count: 0

HTTP files Ignored (Size): 0

SMTP files Ignored (Size): 0

Files Ignored (Filetype): 0

Total Sofa Dcap Start Without Closing Prev Session: 0
```

Total Sofa flows closed due to RST before Dcapend: 3

Applicable to:

NS-series and Virtual IPS Sensors

show malwareEngine status

This CLI command displays the status of the following malware engines:

- GTI File Reputation
- Trellix IPS Analysis
- Gateway Anti-Malware (GAM)
- Intelligent Virtual Execution (IVX) engine
- Trellix Intelligent Sandbox

Syntax:

show malwareEngine status

Sample Output:

```
IntruDBg#> show malwareEngine status
IPS Analysis(pdf) Engine        : Enable
GTI Engine              : Enable
GAM Engine              : Enable
TIS Engine              : Enable
IPS Analysis(flash) Engine      : Enable
IPS Analysis(office) Engine     : Enable
IVX Engine      : Enable
```

Applicable to:

NS-series Sensors

show malwareEngine gam clean-forward

This command displays the clean forwarding status of the Gateway Anti-Malware engine.

Syntax:

show malwareEngine gam clean-forward

Applicable to:

NS-series Sensors

show malwareserverstats

This command displays the malware server statistics in all scan engines for all supported file types.

Syntax:

```
show malwareserverstats
```

Sample Output:

```
IntruDbg#> show malwareserverstats
Packet Holder Statistics:
------------------------
Pkt Hldr Alloc Cnt: 3979.
Pkt Hldr Free Cnt: 3969.
Pkt Hldr Alloc Error Cnt: 0.
Packet Holder Error Statistics:
------------------------------
Pkt hlder buf in Use and allocated again: 0.
Pkt hlder buf double frees: 0.
Write Holder Statistics:
-----------------------
Write Hldr Alloc Cnt: 4.
Write Hldr Free Cnt: 4.
Write Hldr Alloc Error Cnt: 0.
Session Node Statistics:
-----------------------
Session Node Alloc Cnt: 1.
Session Node Free Cnt: 1.
Session Close Cnt: 1.
Session Node Alloc Error Cnt: 0.
FileManager Node Statistics:
---------------------------
FM Node Alloc Cnt: 1.
FM Node Free Cnt: 1.
FM Alloc Err Cnt: 0.
```

```
FM Free Error Cnt: 0.

Session Timer Statistics:

------------------------

Session Timer Add Cnt: 1.

Session Timer Delete Cnt: 1.

Session Timer Trigger Cnt: 0.

Session Timer Reupdate Trigger Cnt: 0.

Ctrl Msg Session Timer Cnt: 0.

Session Timer Add Error Cnt : 0.

Scan Timer Statistics:

----------------------

Scan Timer Add Cnt: 1.

Scan Timer Delete Cnt: 1.

Scan Timer Trigger Cnt: 0.

Ctrl Msg Scan Timer Cnt: 0.

Scan Timer Add Error Cnt: 0.

SOFA Thread Load Statistics:

----------------------------

Server Thread Load: 0.

External Write Load: 0.

Internal Write Load: 0.

PDF-JS Scan Load: 0.

Manager Write Load: 0.

IVX Write Load: 0.

File Upload to Manager Load: 0.

Flash Scan Thread Load: 0.

SOFA Control Message Statistics:

--------------------------------

Ctrl Msg via Socket Pkt Cnt: 96.
```

```
Ctrl Msg Pkt Processed by SOFA-Server: 107.

Ctrl Msg Read Error Cnt: 0.

Ctrl Msg Sigfile Parse Msg Cnt: 0.

SOFA Protocol Statistics:

------------------------

Sibyte to SBC Pkt Read Cnt: 220.

Sibyte to SBC Pkt Processed by SOFA-Server: 220.

Sibyte to SBC Pkt Read Discard Cnt: 0.

Sofa-Protocol New File Dwnld Req Pkt Cnt: 1.

Sofa-Protocol File Data Pkt Cnt: 217.

Sofa-Protocol Scan Req Pkt Cnt: 1.

Sofa-Protocol Error Msg In Pkt Cnt: 1.

Sofa-Protocol Pkt seq num mismatch cnt: 0.

SOFA Session Close Message Statistics:

------------------------

Sofa Server Session time out Cnt: 0.

Sofa Server scan time out Cnt: 0.

Sofa Server Abort transfer Cnt: 0.

Sofa Client Session time out Cnt: 1.

Sofa Client scan time out Cnt: 0.

Sofa Client Abort transfer Cnt: 0.

Sofa-Protocol New File Dwnld Rsp Pkt Cnt: 0.

Sofa-Protocol Error Msg Out Pkt Cnt: 0.

Sofa-Protocol Scan Rsp Pkt Cnt: 2.

Scan Rsp File Info Pkt Cnt: 1.

Multi-Flow New File Dwnld Req Pkt Cnt: 0.

Multi-Flow File Data Pkt Cnt: 0.

Multi-Flow Scan Req Pkt Cnt: 0.

Multi-Flow Error Msg In Pkt Cnt: 0.
```

```
Multi-Flow Md5 Calculated cnt: 0.

Multi-Flow Error Msg Out Pkt Cnt: 0.

Multi-Flow Scan Rsp Pkt Cnt: 0.

Multi-Flow Scan Rsp File Info Pkt Cnt: 0.

UDF Statistics:

---------------

UDF Scan-Q Add Cnt: 1.

Scan Rsp UDF Pkt Cnt: 1.

Artemis Statistics:

-------------------

Artemis Scan-Q Add Cnt: 1.

Artemis Cache hit Cnt: 0.

Ctrl Msg Artemis Rslt Cnt: 1.

Scan Rsp Artemis Pkt Cnt: 1.

Artemis DNS Channel Request/Response Statistics:

Total No. Sofa Artemis request received: 0.

Total No. Artemis request sent out: 0.

Total No. Artemis successful response: 0.

Nameserver connectivity errors: 0.

GTI nameserver malformed replies: 0.

Files unknown to GTI: 0.

GTI no data: 0.

Queries dropped due to configuration/memory: 0.

GTI bad queries: 0.

Unknown errors: 0.

Artemis File-Rep REST Statistics:

Total Request Artemis received from SOFA: 1.

Total Request Artemis sent to curl(GTI): 1.

Total Artemis REST successful response: 1.
```

```
Total Artemis REST Unresolved Queries: 0.

Total Valid Rep Received from GTI: 1.

REST Internal GTI Server Error: 0.

REST Invalid JSON Format Error: 0.

REST Unsupported Operation Error: 0.

REST Missing mandatory parameter Error: 0.

REST Incorrect GTI protocol format Error: 0.

REST Max number of operations exceeded Error: 0.

REST Invalid protocol version Error: 0.

REST Duplicate parameter Error: 0.

REST Missing mandatory client info param Error: 0.

REST Empty mandatory parameter Error: 0.

REST Invalid mandatory parameter format Error: 0.

REST Failed to Connect Error: 0.

REST Empty Input Error: 0.

REST Empty client information parameter Error: 0.

REST Invalid client info param format Error: 0.

REST Duplicate client information parameter Error: 0.

REST Generic GTI Server error Error: 0.

REST Other GTI Server Error: 0.

REST pre CURL Error: 0.

REST Client ID Not Available: 0.

REST Manager-GUID Not Available: 0.

REST CURL perform failed Error: 0.

REST HTTP BAD REQUEST Error: 0.

REST HTTP UNAUTHORIZED Error: 0.

REST HTTP UNSUPPORTED MEDIATYPE Error: 0.

REST Other HTTP Error: 0.

REST Error in parsing JSON response object: 0.
```

```
REST Hash not found in GTI server Error: 0.

REST CA Cert validation Error: 0.

REST GTI server safemode response: 0.

REST GTI server safemode response lastseen: Thu, 01 Jan 1970 00:00:00 GMT.

IPS Analysis(pdf) Engine Statistics:

--------------------------

IPS Analysis(pdf) Scan-Q Add Cnt: 0.

IPS Analysis(pdf) Scan-DQ Cnt: 0.

IPS Analysis(pdf) Scan Discard Cnt: 0.

IPS Analysis(pdf) Scan Skip Cnt: 0.

IPS Analysis(pdf) Cache hit Cnt: 0.

IPS Analysis(pdf) Scan Skip Cnt: 0.

Ctrl Msg IPS Analysis(pdf) Rslt Cnt: 0.

Scan Rsp IPS Analysis(pdf) Pkt Cnt: 0.

IPS Analysis(flash) Engine Statistics:

--------------------------

IPS Analysis(flash) Scan-Q Add Cnt: 0.

IPS Analysis(flash) Scan-Q Skip Cnt(due to heavy load): 0.

IPS Analysis(flash) Scan Discard Cnt: 0.

IPS Analysis(flash) Cache hit Cnt: 0.

Ctrl Msg IPS Analysis(flash) Rslt Cnt: 0.

Scan Rsp IPS Analysis(flash) Pkt Cnt: 0.

Err Rsp IPS Analysis(flash) Pkt Cnt: 0.

IPS Analysis(office) Engine Statistics:

--------------------------

IPS Analysis(office) Scan-Q Add Cnt: 0.

IPS Analysis(office) Scan-Q Skip Cnt(due to heavy load): 0.

IPS Analysis(office) Scan Discard Cnt: 0.

IPS Analysis(office) Cache hit Cnt: 0.
```

```
Ctrl Msg IPS Analysis(office) Rslt Cnt: 0.

Scan Rsp IPS Analysis(office) Pkt Cnt: 0.

Err Rsp IPS Analysis(office) Pkt Cnt: 0.

File Save Statistics:

---------------------

File Save Q Add Cnt: 0.

File Save DQ Cnt: 0.

File Save Discard Cnt: 0.

Ctrl Msg File Save Rslt Cnt: 0.

Scan Rsp File Save Pkt Cnt: 0.

Gateway Anti Malware Statistics:

-------------------------------

Scan-Q Add Cnt: 0.

GAM Cache hit Cnt: 0.

Scan Rsp Pkt Cnt: 0.

Trellix Intelligent Sandbox Dynamic Analysis Statistics:

--------------------------------

Scan-Q Add Cnt: 0.

Scan Rsp Pkt Cnt: 0.

TIS Protocol Statistics:

------------------------

Status Query Pkt Cnt: 0

New Dwnld Req Pkt Cnt: 0

File Data Pkt Cnt: 0

New Dwnld Req uncomplete Pkt Cnt: 0

Scan Req Pkt Cnt: 0

Error Msg Out Pkt Cnt: 0

Error Msg Out Pkt Err Cnt: 0

New Dwnld Rsp Pkt Cnt: 0
```

```
Scan Rsp Pkt Cnt: 0 0

Scan Rsp not received from TIS within Session time: 0

Error Msg In Pkt Cnt: 0

AV Result Cache hit Cnt: 0

Dynamic Result Cache hit Cnt: 0

TIS Cache Auto Purge Cnt: 1

TIS Delayed Response Cnt: 0

New Dwnld Req Pkt Error Cnt: 0

New Dwnld Req Session time out Cnt: 0

File Data Pkt Error Cnt: 0

Scan Req Pkt Error Cnt: 0

TIS Channel Statistics:

----------------------

Rcv Buf Null Cnt: 0.

Wrong Channel Cfg: 0.

SSL Pkt Rcv Err: 0

Keep Alive Send Err Cnt: 0

Keep Alive Miss Cnt: 0

Keep Alive Sent Cnt: 0

Keep Alive Response Cnt: 0

Channel Initialization Attempt Cnt: 0

IVX Protocol Statistics:

----------------------

Scan-Q Add Cnt: 71

Cache hit Cnt: 0

IVX Cache hit Cnt: 34

Submission Req Cnt: 36

Report Req Cnt: 69

Scan + Cache Rsp Cnt: 71
```

```
Report Rsp success Cnt: 36

Reports/Results pending Cnt: 0

Pending list free nodes Cnt: 200

Pending ignored (timedout): 0

Auth Error Cnt: 0

Report Error Cnt: 0

File submission Error Cnt: 0

SHA-256 Req Error Cnt: 0

Manager Protocol Statistics:

---------------------------------

MD5 Hash Query Pkt Cnt: 0

MD5 Hash Query Error Pkt Cnt: 0

New Dwnld Req Pkt Cnt: 0

New Dwnld Req Error Pkt Cnt: 0

File Data Pkt Cnt: 0

File Data Error Pkt Cnt: 0

End of File Pkt Cnt: 0

End of File Error Pkt Cnt: 0

New Dwnld Response Pkt Cnt: 0

New Dwnld Error Response Pkt Cnt: 0

MD5 Hash Query Response Pkt Cnt: 0

Malware Cache Statistics:

---------------------------------

Cache Utilization %%: 0.00 %

Cache Nodes utilized: 0

Cache Nodes Total available: 80000

# of times cache purged: 0

GAM Protocol Statistics:

---------------------------------
```

```
GAM New File Download Request from Manager: 0

GAM File Download Data from Manager: 0

GAM File End Request from Manager: 0

GAM File Download Err msg Sent to Manager: 0

GAM File Download Request to GAM Engine: 0

GAM File Download Request Err to GAM Engine: 0

MD5 of last file extracted: f70664bb0d45665e79dnd9113c5e4d0f4

SHA1 of last file extracted: 67cf01ee7ff0e65uhf7ec78chgf274077153add4e

SHA256 of last file extracted: 8cb40e8dce05482907ff83b39911831daf20e4a69ee63a6aac523c880eed1acf

[Trellix Intelligent Sandbox Communication]

Status: up

[Trellix SOFA Primary Manager Communication]

Status: Up

[Trellix SOFA MDR Manager Communication]

Status: Down

Down Reason: Error obtaining channel status
```

Applicable to:

NS-series Sensors

show max cseg list count

This command shows maximum CSEG list count for each CPU.

Syntax:

```
show max cseg list count
```

Sample Output:

```
IntruDbg#> show max cseg list count

CPU(1) Max Cseg List count: 1025

CPU(2) Max Cseg List count: 1026

CPU(3) Max Cseg List count: 1029

CPU(4) Max Cseg List count: 1038

CPU(5) Max Cseg List count: 1025
```

```
CPU(6) Max Cseg List count: 1025

CPU(7) Max Cseg List count: 1026

CPU(8) Max Cseg List count: 1027

CPU(9) Max Cseg List count: 1025

CPU(10) Max Cseg List count: 1027

CPU(11) Max Cseg List count: 1024
```

Applicable to:

NS-series Sensors

show mgmtcfg

This command displays various management (control path) configurations. Details include information about ports, packet logging, alert throttle, layer configuration, TACAS, ACL, NTP, latency monitor, and GTI proxy. This command has no parameters.

Syntax:

```
show mgmtcfg
```

Sample Output:

```
IntruDbg#> show mgmtcfg
 FAILOVERGRP CFG
    FailoverAction DISABLED
        PeerIPaddr 0
     HeartbeatTime 5
 HeartbeatRetryCnt 3
    FailoverMode STANDALONE
    FailopenAction DISABLED

 INTF PORT 0
        EnableInternalTap TRUE
 INTF PORT 1
        EnableInternalTap TRUE
 INTF PORT 2
        EnableInternalTap TRUE
 INTF PORT 3
        EnableInternalTap TRUE
 INTF PORT 4
        EnableInternalTap TRUE
 INTF PORT 5
        EnableInternalTap TRUE
 INTF PORT 6
        EnableInternalTap TRUE
 INTF PORT 7
        EnableInternalTap TRUE
```

```
INTF PORT 8
        EnableInternalTap TRUE
INTF PORT 9
        EnableInternalTap TRUE
INTF PORT 10
        EnableInternalTap TRUE
INTF PORT 11
        EnableInternalTap TRUE
INTF PORT 12
        EnableInternalTap TRUE
INTF PORT 13
        EnableInternalTap TRUE
INTF PORT 14
        EnableInternalTap TRUE
INTF PORT 15
        EnableInternalTap TRUE
INTF PORT 16
        EnableInternalTap TRUE
INTF PORT 17
        EnableInternalTap TRUE
INTF PORT 18
        EnableInternalTap TRUE
INTF PORT 19
        EnableInternalTap TRUE
INTF PORT 20
        EnableInternalTap TRUE
INTF PORT 21
        EnableInternalTap TRUE
INTF PORT 22
        EnableInternalTap TRUE
INTF PORT 23
        EnableInternalTap TRUE
INTF PORT 24
        EnableInternalTap TRUE
INTF PORT 25
        EnableInternalTap TRUE
INTF PORT 26
        EnableInternalTap TRUE
INTF PORT 27
        EnableInternalTap TRUE
INTF PORT 28
        EnableInternalTap TRUE
INTF PORT 29
        EnableInternalTap TRUE
INTF PORT 30
        EnableInternalTap TRUE
INTF PORT 31
        EnableInternalTap TRUE
```

```
INTF PORT 32
        EnableInternalTap TRUE
INTF PORT 33
        EnableInternalTap TRUE

Packet Logging CFG
    ServerIP 127.0.0.1
  ServerPort 8503
   Encryption ENABLED
   ServerV6IP

Alert Throttle CFG
  Threshold 1
  Interval 120
   Action  DISABLED
  Global Threshold 10

LAYER2 CFG
            Mode ENABLED
          Duration 10
         Threshold 1
      OccurrenceCnt 0
      FirstTimeIdx 0
       LastTimeIdx 0
  OccurrenceTime[0] 0
  OccurrenceTime[1] 0
  OccurrenceTime[2] 0
  OccurrenceTime[3] 0
  OccurrenceTime[4] 0
  OccurrenceTime[5] 0
  OccurrenceTime[6] 0
  OccurrenceTime[7] 0
  OccurrenceTime[8] 0
  OccurrenceTime[9] 0
       RebootCount 0

TACACS CFG
   Authentication  Disabled
   Traffic Encryption  Enabled
   Authorization  Disabled

ACL CFG
   Alert Throttle MaxIp Pair 10
   Alert Throttle Interval 120
   Alert Throttle Action  Enabled
   Alert Throttle Threshold 5
   Alert Direct to Syslog 1
```

```
  NMS CFG
    NMS User Write Access Status       : Enabled
    No NMS IPv4 Addresses are configured.
    No NMS IPv6 Addresses are configured.

    No NMS User's are configured.

  MPE CFG
    [Configured MPE details]

    MPE Server IP address = 0.0.0.0
    MPE Anonymous Port = 8443
    MPE Listen Port = 0
    MPE Trusted Port = 8444
    MPE Anonymous URI = /nac/certrequest
    MPE Trusted URI = /nac/engine
    MPE Connection Failure Timeout = 32
    MNAC Agent GUID Port = 8444
    MNAC OS Capability = 0
    MNAC TTL Config = 131074

EZ-LOG-ALERT-THROTTLE CFG
          Max IP Pair 10
          Throttle Interval 120
          Throttle Action  Enabled
          Throttle Threshold 5
          Alert Direct to Syslog 1
SGAP CFG
          Auth channel timeout 50

          SGAP status config 1

PERFORMANCE ALERT CFG
          Perf Alert Status 1
          Perf Alert Parameters 63800000
          Perf Alert Duration 3

THRESHOLD BASED ALARM CFG
          Alarm Status 1
          Alarm Duration 1
          Number of Alarm Entries 3

      Alarm Index     : 1
      Alarm Sample Type   : 0
      Alarm Raising Threshold : 90
      Alarm Falling Threshold : 70
      Alarm Startup Type  : 1
      Alarm Description   : High Usage
```

```
      Alarm Sample Type Index : 0 0 0 0 0 0 0 0

      Alarm Index     : 3
      Alarm Sample Type   : 2
      Alarm Raising Threshold : 90
      Alarm Falling Threshold : 70
      Alarm Startup Type  : 1
      Alarm Description   : High Usage
      Alarm Sample Type Index : 0 0 0 0 0 0 0 0

      Alarm Index     : 12
      Alarm Sample Type   : 1
      Alarm Raising Threshold : 90
      Alarm Falling Threshold : 70
      Alarm Startup Type  : 1
      Alarm Description   : High Usage
      Alarm Sample Type Index : 0 0 0 0 0 0 0 0

MISCELLANEOUS CFG
          Console Timeout = 0
          SSH Inactive Timeout = 300
          Aux Port Status = Enabled
          Auditlog Status = Enabled
  Auditlogtomgr Status = Enabled
          Mgmt Autorecovery Status = Enabled
          Host Persistence Config 1
          Artemis Threshold Config 1
          Datapath attack detection monitor action  = Ignored
          Pdf Cache = Enabled
          Flash Cache = Enabled
          Msas Cache = Enabled
          GAM Cache = Enabled
          SSH Password Authentication = Enabled
          Miscellaneous Flags 3145742
       GAM auto update enable 0x1
       GAM auto update time interval 90
       TIS channel sleep interval 375
       Sensor cert migrate action 2
       Audit logging failure response : continue-inspection


SCP CFG
       SCP IPv4 = 10.213.222.66

NTP CFG
      NTP Server1 IPv4 0.0.0.0
      NTP Server1 IPv6 = ::
      POLL 6
```

```
       AUTH DISABLE

       NTP Server2 IPv4 0.0.0.0
       NTP Server2 IPv6 = ::
       POLL 6
       AUTH DISABLE



 GTI Proxy CFG
        GTI Proxy Host = webgateway.itm.mcafee.com
        GTI Proxy Port = 9090
        GTI Proxy Username = ""
        GTI Proxy Host Type = 2
        GTI Private Cloud IP Address Type = IPv4
        GTI Private Cloud IP Address = 0.0.0.0
        GTI Private Cloud Connection Config = DISABLED
        GTI Private Cloud Certificate Status = Not present

 NTBA CFG
        IP Address type = 4
       Server IPv4 = 0.0.0.0
        Server Port = 8505
        Connection config = 2
        Channel Encryption  = 1

 TIS CFG
        IP Address type = 4
       Server IPv4 = 0.0.0.0
        Server Port = 8505
        Connection config = 2
        Channel Encryption  = 1
        TIS Profile/User Name = nsp
        TIS Profile/User Id  = 2

 IVX CFG
IVX Primary Cluster Configuration:
IVX Broker 1:
        IP Address type                : IPv4
        Server IPv4                    : 10.213.2.35
        Connection config              : ENABLED
        IVX UserName                   : admin
        Certificate validation         : DISABLED
        Authentication Status          : Successful
        Proxy for IVX Communication    : DISABLED
IVX Broker 2:
        IP Address type                : IPv4
        Server IPv4                    : 10.213.2.54
```

```
        Connection config               : ENABLED
        IVX UserName                    : admin
        Certificate validation          : DISABLED
        Authentication Status           : Successful
        Proxy for IVX Communication     : DISABLED
IVX Broker 3:
        IP Address type                 : IPv4
        Server IPv4                     : 10.213.2.209
        Connection config               : ENABLED
        IVX UserName                    : admin
        Certificate validation          : DISABLED
        Authentication Status           : Successful
        Proxy for IVX Communication     : DISABLED
IVX Broker 4:
        IP Address type                 : IPv4
        Server IPv4                     : 10.213.2.210
        Connection config               : ENABLED
        IVX UserName                    : admin
        Certificate validation          : DISABLED
        Authentication Status           : Successful
        Proxy for IVX Communication     : DISABLED
IVX Broker 5:
        IP Address type                 : IPv4
        Server IPv4                     : 10.213.2.214
        Connection config               : ENABLED
        IVX UserName                    : admin
        Certificate validation          : DISABLED
        Authentication Status           : Successful
        Proxy for IVX Communication     : DISABLED


 RADIUS CFG
    Authentication  Disabled
    Primary RADIUS Server IPv4 Address: 0.0.0.0
    Primary RADIUS Server Authentication Port: 1812
    Primary RADIUS Server Accounting Port: 1813
    Primary RADIUS Server Connection Timeout: 6
    Backup  RADIUS Server IPv4 Address: 0.0.0.0
    Backup  RADIUS Server Authentication Port: 1812
    Backup  RADIUS Server Accounting Port: 1813
    Backup  RADIUS Server Connection Timeout: 6

 INSIGHTS TELEMETRY CFG
    Status : Disabled
    TenantId :
    Primary Manager GUID : x-x-x-x
    Secondary Manager GUID :
```

Applicable to:

NS-series Sensors

show mem-usage

The **show mem-usage** command displays the system memory usage details of the device. It also gives the average percentage usage (Avg.) and the maximum percentage usage (Max.) of these entities on all the processing elements.

This command has no parameters.

Syntax:

```
show mem-usage
```

Sample Output:

```
IntruDbg#> show mem-usage

Avg. Used TCP and UDP Flows across all PEs : 0%

Max. Used TCP and UDP Flows on a single PE : 1%

Avg. Used Fragmented IP Flows across all PEs : 0%

Max. Used Fragmented IP Flows on a single PE : 0%

Avg. Used ICMP Flows across all PEs : 0%

Max. Used ICMP Flows on a single PE : 0%

Avg. Used SSL Flows across all PEs : 0%

Max. Used SSL Flows on a single PE : 0%

Avg. Used Fragment Reassembly Buffers across all PEs : 0%

Max. Used Fragment Reassembly Buffers on a single PE : 0%

Avg. Used Packet Buffers across all PEs : 3%

Max. Used Packet Buffers on a single PE : 3%

Avg. Used Attack Marker Nodes across all PEs : 1%

Max. Used Attack Marker Nodes on a single PE : 1%

Avg. Used Shell Marker Nodes across all PEs : 0%

Max. Used Shell Marker Nodes on a single PE : 0%

Avg. Used L7 Dcap flows across all PEs : 3%

Max. Used L7 Dcap flows on a single PE : 4%

Datapath Attack IDs Usage : 31.1%
```

```
Datapath Signature Config Memory Block [0] Usage: 39.4% (current)

Datapath Signature Config Memory Block [1] Usage: 39.4% (old)

Datapath Sigfile Size : 33.5%

Datapath MSPM Graph Size : 36.0%
```

Applicable to:

NS-series Sensors

show mgmtnetstats

This command displays the network statistics on IP, ICMP, TCP, UDP, IPv6, and SNMP.

Syntax:

```
show mgmtnetstats
```

Sample Output:

```
IntruDbg#> show mgmtnetstats
```

IP:

```
398030 total packets received

8246 with invalid addresses

0 forwarded

0 incoming packets discarded

353329 incoming packets delivered

376126 requests sent out
```

ICMP:

```
5230 ICMP messages received

0 input ICMP message failed.
```

ICMP input histogram:

```
destination unreachable: 5228

echo requests: 2

5232 ICMP messages sent

0 ICMP messages failed
```

ICMP output histogram:

```
destination unreachable: 5230
```

echo replies: 2

TCP:

1442 active connections openings

953 passive connection openings

0 failed connection attempts

21 connection resets received

110 connections established

103212 segments received

108050 segments send out

63 segments retransmited

0 bad segments received.

52 resets sent

UDP:

239034 packets received

5230 packets to unknown port received.

622 packet receive errors

262844 packets sent

TcpExt:

2 packets pruned from receive queue because of socket buffer overrun

ArpFilter: 0

941 TCP sockets finished time wait in fast timer

3470 delayed acks sent

Quick ack mode was activated 41 times

10 times the listen queue of a socket overflowed

10 SYNs to LISTEN sockets ignored

125 packets directly queued to recvmsg prequeue.

911341 packets directly received from backlog

63345 packets directly received from prequeue

29939 packets header predicted

```
719 packets header predicted and directly queued to user

TCPPureAcks: 3686

TCPHPAcks: 37362

TCPRenoRecovery: 0

TCPSackRecovery: 0

TCPSACKReneging: 0

TCPFACKReorder: 0

TCPSACKReorder: 0

TCPRenoReorder: 0

TCPTSReorder: 0

TCPFullUndo: 0

TCPPartialUndo: 0

TCPDSACKUndo: 0

TCPLossUndo: 1

TCPLoss: 0

TCPLostRetransmit: 0

TCPRenoFailures: 0

TCPSackFailures: 0

TCPLossFailures: 0

TCPFastRetrans: 0

TCPForwardRetrans: 0

TCPSlowStartRetrans: 0

TCPTimeouts: 32

TCPRenoRecoveryFail: 0

TCPSackRecoveryFail: 0

TCPSchedulerFailed: 0

TCPRcvCollapsed: 129

TCPDSACKOldSent: 0

TCPDSACKOfoSent: 0
```

TCPDSACKRecv: 0

TCPDSACKOfoRecv: 0

TCPAbortOnSyn: 0

TCPAbortOnData: 0

TCPAbortOnClose: 9

TCPAbortOnMemory: 0

TCPAbortOnTimeout: 5

TCPAbortOnLinger: 0

TCPAbortFailed: 0

TCPMemoryPressures: 0

IPv6:

Ip6InReceives:0

Ip6InHdrErrors:0

Ip6InTooBigErrors:0

Ip6InNoRoutes:0

Ip6InAddrErrors:0

Ip6InUnknownProtos:0

Ip6InTruncatedPkts:0

Ip6InDiscards:0

Ip6InDelivers:0

Ip6OutForwDatagrams:0

Ip6OutRequests:24

Ip6OutDiscards:0

Ip6OutNoRoutes:0

Ip6ReasmTimeout:0

Ip6ReasmReqds:0

Ip6ReasmOKs:0

Ip6ReasmFails:0

Ip6FragOKs:0

```
Ip6FragFails:0

Ip6FragCreates:0

Ip6InMcastPkts:0

Ip6OutMcastPkts:24

Icmp6InMsgs:0

Icmp6InErrors:0

Icmp6InDestUnreachs:0

Icmp6InPktTooBigs:0

Icmp6InTimeExcds:0

Icmp6InParmProblems:0

Icmp6InEchos:0

Icmp6InEchoReplies:0

Icmp6InGroupMembQueries:0

Icmp6InGroupMembResponses:0

Icmp6InGroupMembReductions:0

Icmp6InRouterSolicits:0

Icmp6InRouterAdvertisements:0

Icmp6InNeighborSolicits:0

Icmp6InNeighborAdvertisements:0

Icmp6InRedirects:0

Icmp6OutMsgs:24

Icmp6OutDestUnreachs:0

Icmp6OutPktTooBigs:0

Icmp6OutTimeExcds:0

Icmp6OutParmProblems:0

Icmp6OutEchoReplies:0

Icmp6OutRouterSolicits:9

Icmp6OutNeighborSolicits:9

Icmp6OutNeighborAdvertisements:0
```

Icmp6OutRedirects:0

Icmp6OutGroupMembResponses:0

Icmp6OutGroupMembReductions:0

Udp6InDatagrams:0

Udp6NoPorts:0

Udp6InErrors:0

Udp6OutDatagrams:0

SNMP:

snmpInPkts: 3753

snmpOutPkts: 1854

snmpInBadVersions: 0

snmpInBadCommunityNames: 0

snmpInBadCommunityUses: 0

snmpInASNParseErrs: 0

snmpInTooBigs: 0

snmpInNoSuchNames: 0

snmpInBadValues: 0

snmpInReadOnlys: 0

snmpInGenErrs: 0

snmpInTotalReqVars: 7109

snmpInTotalSetVars: 336

snmpInGetRequests: 1195

snmpInGetNexts: 65

snmpInSetRequests: 62

snmpInGetResponses: 0

snmpInTraps: 0

snmpOutTooBigs: 0

snmpOutNoSuchNames: 5

snmpOutBadValues: 0

```
snmpOutGenErrs: 0

snmpOutGetRequests: 0

snmpOutGetNexts: 0

snmpOutSetRequests: 0

snmpOutGetResponses: 1854

snmpOutTraps: 0

snmpEnableAuthenTraps: 2

snmpSilentDrops: 0

snmpProxyDrops: 0
```

Applicable to:

NS-series Sensors

show mgmtprocessrestart status

This command displays the status of **`set mgmtprocessrestart`** (enabled or disabled).

Syntax:

```
show mgmtprocessrestart status
```

Sample Output:

```
IntruDbg#> show mgmtprocessrestart status

[Management Process-Restart settings]

Mgmt Process-restart configuration : Enabled
```

Applicable to:

NS-series Sensors

show nianticrecovery status

This command displays whether autorecovery is enabled on detection of stoppage of Niantic transmission.

Syntax:

```
show nianticrecovery status
```

Applicable to:

NS9x00 series Sensors

show pktcapture status

This CLI command displays the packet capture status and configuration.

> **NOTE**
>
> If you observe any errors or memory leaks in the **show pktcapture status** command output, you must tune the packet capture filters. If the **Frontend Packet Capture Mbuf Clone Error Cnt** is non-zero and increasing, you must reboot the Sensor.

Syntax:

```
show pktcapture status
```

Sample Output:

Normal mode:

```
IntruShell@Test-Sensor#> show pktcapture status

Packet Capture Status :Not Running

Send Captured Packets To :Manager

Packet Capture Rule Set File Status :Present

Packet Capture File Status :PCAP File Not Present

Total Packet Capture Count :0

File Max Size :100 MB
```

Debug mode:

```
IntruDbg#> show pktcapture status

Packet Capture Status :Running

Send Captured Packets To :Manager

Packet Capture Rule Set File Status :Not Present

Packet Capture File Status :PCAP File Not Present

Datapath 0 :

l7ae Egress matched pkt sent cnt :13693

l7ae Egress pkt clone err cnt :0

l7ae Egress pkt chain err cnt :0

l7ae Egress pkt capture enable cnt :0

l7ae Egress pkt capture disable cnt :0
```

```
l7ae Egress Jumbo pkt skip cnt :0

.....

Datapath 15 :

l7ae Egress matched pkt sent cnt :171626

l7ae Egress pkt clone err cnt :0

l7ae Egress pkt chain err cnt :0

l7ae Egress pkt capture enable cnt :0

l7ae Egress pkt capture disable cnt :0

l7ae Egress Jumbo pkt skip cnt :0

Across All datapaths

l7ae Egress matched pkt sent cnt :1788707

l7ae Egress pkt clone err cnt :0

l7ae Egress pkt chain err cnt :0

l7ae Egress Jumbo pkt skip cnt :0

Frontend Egress Matched Pkt Sent Cnt :174147703

Frontend Ingress Matched Pkt Sent Cnt :175939455

Frontend Ingress Pkt Capture Jumbo Frames Skip Cnt :0

Frontend Egress Pkt Capture Jumbo Frames Skip Cnt :0

Frontend Packet Capture Mbuf Clone Error Cnt :0

Frontend Packet Capture Mbuf Chain Error Cnt :0

Frontend Packet Capture Enable Count :0

Frontend Packet Capture Disable Count :0

Total Packet Capture Count :327136912

File Max Size :100 MB
```

This command displays the following additional counters in debug mode:

- **l7ae Egress matched pkt sent cnt** - Number of matched incoming packets that are sent from each backend processor to the packet capture process
- **l7ae Egress pkt clone err cnt** - Number of clone errors for outgoing packets on each backend processor
- **l7ae Egress pkt chain err cnt** - Number of mbuf chain errors encountered for outgoing packets
- **l7ae Egress pkt capture enable cnt** - Number of times the packet capture filter is applied for each backend processor

- **l7ae Egress pkt capture disable cnt** - Number of times the packet capture filter is removed from each backend processor
- **Frontend Ingress Matched Pkt Sent Cnt** - Number of matched incoming packets that are sent to packet capture process from frontend processor
- **Frontend Egress Matched Pkt Sent Cnt** - Number of matched outgoing packets sent to packet capture process from frontend processor
- **Frontend Packet Capture Mbuf Clone Error Cnt** - Number of mbuf clone errors
- **Frontend Packet Capture Mbuf Chain Error Cnt** - Number of mbuf chain error
- **Frontend Packet Capture Enable Count** - Number of times the packet capture filter is applied for frontend processor
- **Frontend Packet Capture Disable Count** - Number of times the packet capture filter is removed from frontend processor

Applicable to:

NS-series Sensors

show prioritytraffic ratio

This command displays the ratio in which high priority traffic is given preference compared to normal priority traffic during packet processing.

Syntax:

```
show prioritytraffic ratio
```

Sample Output:

```
IntruDbg#> show prioritytraffic ratio
```

```
Priority Traffic Ratio: 3
```

The sample above indicates that for every 3 packets processed from the high priority packet queue, only one packet is processed from the normal priority packet queue. The default value while setting the priority traffic ratio is 3.

Applicable to:

NS-series Sensors

show recon status

The **`show recon status`** command displays reconnaissance attack detection status.

> **NOTE**
>
> This setting should be reconfigured if the Sensor is rebooted.

Syntax:

```
show recon status
```

Sample Output:

```
IntruDbg#> show recon status

Reconnaissance attack detection enabled
```

Applicable to:

NS-series Sensors

show saved alerts

This command displays the total number and size of alerts that are saved.

Syntax:

```
show saved alerts
```

Sample Output:

```
IntruDbg#> show saved alerts

Saved Alert Status :Alerts = 455, Size = 80990
```

Applicable to:

NS-series Sensors

show saved packets

This command displays the total number of packets that are saved.

Syntax:

```
show saved packets
```

Sample Output:

```
IntruDbg#> show saved packets

Saved Packet Status : No Saved File
```

Applicable to:

NS-series Sensors

show sbcfg

The **show sbcfg** command displays various datapath configuration. This command has no parameters.

Syntax:

```
show sbcfg
```

Sample Output:

```
IntruDebug#> show sbcfg
```

```
IP CFG

IPFragmentTimer 30

OverlapOption OLD_DATA

TTLConfigMode NO_TTL_CHECKING

TTLThreshold 32

TTLResetValue 32

SmallestFragmentSize 256

SmallestFragmentThreshold 10000

IP Fragment Reassembly ENABLE

IPV6OverlapOption OLD_DATA

IPV6SmallestFragmentSize 48

IPV6SmallestFragmentThreshold 10000

TCP CFG

SupportedUDPFlows 100000

TCBInactivityTimer 10

TCPSegmentTimer 60

TCP2MSLTimer 10

InactiveFlowRstEnabled 2

DropReTxTCPEnabled 2

ColdStartTime 60

ColdStartDropAction FORWARD_FLOWS

NormalizationOnOffOption OFF

TcpOverlapOption NEW_DATA

SynAckPermittedOption 1

TCPOptionThreshold 100

DropOnPAWSFail ENABLE

TimeStampEchoMatchFail ENABLE

DropMD5Option ENABLE

UnsolicitedUDPPktsTimeout 60
```

```
SynProxyEnable DISABLE

AckScanDiscardTime 15

HalfOpenConnResetEnable RST_3WH_DISABLE

OutOfContextTcpPktEnable PERMIT_OUT_OF_ORDER

synCookieConfig Inbound-DISABLE Outbound-DISABLE

synCookieInboundThreshold 102400

synCookieOutboundThreshold 102400

synCookieMss 536

Tcpudpicmpchecksumerror Drop

flow volume threshold is 0MB.

DNSRedirectConfig disabled

Syn Cookie TCP Reset Send Enable status : Enabled (1)

DNS sinkhole TTL 720

DNS sinkhole IP 127.0.0.1

Oversubscription value: 0

BackendLimit Value: 0x1c2002d

INTF PORT 0

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 1

OperatingMode INLINE_FAIL_CLOSED
```

```
FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 2

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 3

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0
```

```
Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 4

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 5

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 6

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid
```

```
Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 7

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 8

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 9
```

```
OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 10

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 11

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0
```

```
Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 12

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 13

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 14

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE
```

```
FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 15

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 16

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1
```

```
INTF PORT 17
OperatingMode INLINE_FAIL_CLOSED
FullDuplex ENABLED
InOutType OUTSIDE
FEC Invalid
Monitoring Port IP - 0.0.0.0
Monitoring Port Netmask - 0.0.0.0
Monitoring Port Gateway - 0.0.0.0
Monitoring Port Vlan ID - 0
Monitoring Port NBAD Config Status - 0
Monitoring Port AppId Stats Alert Config Status - 1
INTF PORT 18
OperatingMode INLINE_FAIL_CLOSED
FullDuplex ENABLED
InOutType INSIDE
FEC Invalid
Monitoring Port IP - 0.0.0.0
Monitoring Port Netmask - 0.0.0.0
Monitoring Port Gateway - 0.0.0.0
Monitoring Port Vlan ID - 0
Monitoring Port NBAD Config Status - 0
Monitoring Port AppId Stats Alert Config Status - 1
INTF PORT 19
OperatingMode INLINE_FAIL_CLOSED
FullDuplex ENABLED
InOutType OUTSIDE
FEC Invalid
Monitoring Port IP - 0.0.0.0
Monitoring Port Netmask - 0.0.0.0
```

```
Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 20

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 21

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 22

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED
```

```
InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 23

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 24

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0
```

```
Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 25

OperatingMode INLINE_FAIL_CLOSED

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 1

INTF PORT 26

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 27

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0
```

```
Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 28

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 29

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 30

OperatingMode INLINE_FAIL_OPEN
```

```
FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 31

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 32

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType INSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0
```

```
Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

INTF PORT 33

OperatingMode INLINE_FAIL_OPEN

FullDuplex ENABLED

InOutType OUTSIDE

FEC Invalid

Monitoring Port IP - 0.0.0.0

Monitoring Port Netmask - 0.0.0.0

Monitoring Port Gateway - 0.0.0.0

Monitoring Port Vlan ID - 0

Monitoring Port NBAD Config Status - 0

Monitoring Port AppId Stats Alert Config Status - 0

RESP PORT 1

AdminStatus ENABLED

Operational Status : Down

FullDuplex ENABLED

Speed 3

PktDestination SWITCH

ALERT THROTTLE CFG

CorrelationTime 5

PKTLOG CFG

MaxPktsPerFlow 1000

DOS CFG

DosPktLogging DISABLED

FAILOVER CFG

FailoverAction DISABLED

FailoverMode FAILOVER_MODE_STANDALONE

SSL CFG
```

```
SessionCacheLifetime 5

SupportAction 0

PktLogging DISABLED

ShKey Decrypt DISABLED

ResponseProcEnable DISABLED

Configured SSL inbound mode 0

Current SSL inbound mode 0

Configured SSL outbound mode 0

Current SSL outbound mode 0

Outbound PktLogging DISABLED

Outbound SessionCacheLifetime : 5

Outbound Unknown Server Certificate : 1

Outbound Untrusted Server Certificate : 3

Outbound Unsupported cipher suite : 1

Outbound Unsupported Server Certificate : 1

Outbound Unknown URL Category : 0

ACL Log Alert CFG

Alert Logging Disabled

DNSPROTECTION IPV4 CFG

No IPv4 DNS Protection IP's are configured

DNSPROTECTION IPV6 CFG

No IPv6 DNS Protection IP's are configured

SENSOR LOAD CFG

Sensor Load Computation is set to off

TUNNELING CFG

Tunneling is disabled

OVERSUBSCRIPTION CFG

Oversubscription level 0

IPS SIMULATION CFG
```

```
Ips Simulation is disabled

PKTDROP SYSEVENT CFG

PktDrop sysevent is disabled

IP REASSEMBLY TIMEOUT FORWARD CFG

IP Reassembly timeout forward is disabled

IP Reassembly timeout in milli second is 0

BDD threshold value : 20

BDD threshold value : 20

BDD threshold value for base64-smtp: 0

Max Unknown Port SSL Connections: 0

LDPENDING CFG

LDPENDING CFG is set to actual-load

Miscellaneous CFG

Misc Flags 41216

Mon Port Ping Status : Disabled

Datapath attack detection monitoring : Disabled

IBAC Host Auth Status : Enabled

Sibyte Smpt Load Balancing Status : Disabled

IPS for Unknown UDP is enabled

EZ-LOG-ALERT CFG

EzAlertLogging 5

NBAD CFG

NBAD Sensor IP Address 0.0.0.0

NBAD Sensor Port 0

NBAD IPS Primary Mon Port Id 1

NBAD IPS Secondary Mon Port Id 2

NBAD OS Finger Printing Status 0

NBAD App Finger Printing Status 0

NBAD SSL Flow Data Capture Status 0
```

NBAD TCP Capture Config : Enabled

NBAD UDP Capture Config : Enabled

NBAD ICMP Capture Config : Disabled

Miscellaneous CFG

TAPA Protocol Config : 0

Latency Monitor Status : 0

Artemis Detection Mode : 1

Malware UD Detection Mode : 1

GTIfilelookup timeout : 6

Overwrite GZIP : 0

Unknown Proto Scan Depth : 256

NAC DHCP Pxe Config : 39321602

L7 DCap Percent Flows : 20

L7 DCap Buffer Size : 1500

Misc Flags 41216

Mon Port Ping Status : Disabled

Datapath attack detection monitoring : Disabled

IBAC Host Auth Status : Enabled

Unknown Proto Scandepth Status : Enabled

Sibyte Smpt Load Balancing Status : Disabled

AppId Stats Alert Status : Enabled

Requested Snort Rule Engine Config : Trellix Snort

Active Snort Rule Engine Config : Trellix Snort

MPE Additional CFG

Number of Additional MPE IP Addresses 0

NAC host tracking configuration

NAC host tracking disabled

Dxl Config

EPO IP4 10.213.169.103

```
EPO IP6 ::

EPO IP TYPE 4

EPO PORT 8443

EPO Action 3

EPO Username admin

DXL Enable/Disable 1

TIS CFG

IP Address type = 0

TIS Profile/User Name = nsp

TIS Profile/User Id = 2
```

Applicable to:

NS-series Sensors

show sensor health

It displays the Sensor health information.

Syntax:

```
show sensor health
```

Sample Output:

```
IntruDbg#> show sensor health

bootflag = off

sensor health = good

health of control channel = good

health of correlation engine = good

health of snmp master agent = good

health of snmp sub agent = good

health of packet log = good

health of system controller = good

health of CLI = good

health of Log Main = good

health of Log Task = good
```

```
health of SGAP = good

health of AuthGw = good

health of ACLDaemon = good

health of TrustedSource = good

health of BCM = good
```

Applicable to:

NS-series Sensors

show ssl stats sensor

This command is used to display the Inbound SSL Task connection, packet, and session statistics.

Syntax:

```
show ssl stats sensor
```

Sample output:

```
IntruDbg#> show ssl stats sensor

SSL connection exhausted : 0

SSL connection recycled : 0

SSL packets with no connection : 0

SSL session allocation error : 0

SSL unsupported Diffie Hellman cipher suite : 0

SSL unsupported export cipher : 0

SSL unsupported or unknown cipher : 0

SSL session recycled : 0

SSL session ref exhausted : 0

SSL session exhausted : 0

SSL Connection Key Matched : 39
```

Applicable to:

NS9500, NS9x00, NS7600, NS7500, NS7x00, NS5x00 and NS3600 series Sensors

show stack protocol

This command displays the statistics for the stack protocols.

Syntax:

```
show stack protocol <all|rxPkts|txPkts|timeout>
```

Parameter	Description
all	Displays all the stack protocol statistics
rxPkts	Displays the statistics of the packets received from other nodes in the stack
txPkts	Displays the statistics of the packets transmitted to other nodes in the stack
timeout	Displays the timeout received at the ports of the Sensor

Sample Output:

```
intruShell@john> show stack protocol all

RX STATS

Protocol Pkts received on stacking port-1:

From Node-id: 1

Destined to ALL Nodes

DISCOVERY_MSG Pkts : 14

From Node-id: 2

Destined to ALL Nodes

DISCOVERY_MSG Pkts : 17

Protocol Pkts received on stacking port-2:

From Node-id: 1

Destined to ALL Nodes

DISCOVERY_MSG Pkts : 6982

DISCOVERY_TERMINATED_MSG Pkts : 3

From Node-id: 2

Destined to ALL Nodes

DISCOVERY_MSG Pkts : 6984

TX STATS

Protocol Pkts transmitted on stacking port-1:

Destined to ALL Nodes

DISCOVERY_MSG Pkts : 29 Errors : 0

DISCOVERY_TERMINATED_MSG Pkts : 3 Errors : 0
```

Protocol Pkts transmitted on stacking port-2:

DISCOVERY_MSG Pkts : 6997 Errors : 0

DISCOVERY_TERMINATED_MSG Pkts : 6969 Errors : 0

TOPOLOGY_CHANGE_MSG Pkts : 1 Errors : 0

TIME-OUT STATS

Stacking Protocol Time-out on stacking port-1: 0

Stacking Protocol Time-out on stacking port-2: 0

Applicable to:

NS9500 stack Sensors only

show stack stats otherNodePktsProcessed

This command displays the statistics for the packets received and processed from the other nodes of the stack.

This command has no parameters.

Syntax:

show stack stats otherNodePktsProcessed

Sample Output:

Pkts from Node ID: 2 processed by this node: 20

Applicable to:

NS9500 stack Sensors only

show startup stats

This command displays the startup initialization information.

Syntax:

show startup stats

Sample Output:

IntruDbg#> show startup stats

Controller ready to send INIT_ACKs to datapaths and dos.

initial READY msg : received from datapaths and dos.

dos has sent INIT_DONE.

datapath0 has sent INIT_DONE.

```
datapath1 has sent INIT_DONE.

dos has sent READY.

datapath0 has sent READY.

datapath1 has sent READY.
```

Applicable to:

NS-series Sensors

show static-arp

It displays the static ARP entries.

Syntax:

```
show static-arp
```

Sample Output:

```
IntruDbg#> show static-arp

No of Arp Entry in The Cache is: 0

Dump of ARP Cache Entries completed!
```

Applicable to:

NS-series Sensors

show statistics alerts

This command displays the alert statistics (signature alerts, reconnaissance alerts, and ACL logs) that are sent to the Manager.

Syntax:

```
show statistics alerts
```

Sample Output:

```
IntruDbg#> show statistics alerts

Datapath 12 :

Signature alerts sent to mgmt = 249895

Reconnaissance alerts sent to mgmt = 5456257

ACL Logs sent to mgmt = 0

Datapath 13 :

Signature alerts sent to mgmt = 252880
```

```
Reconnaissance alerts sent to mgmt = 5660890

ACL Logs sent to mgmt = 0
```

Applicable to:

NS-series Sensors

show statistics icmp

This command displays the ICMP statistics. It includes the following information:

- ICMP echo request packets
- ICMP echo reply packets
- ICMP unsol(icited) reply packets
- ICMP other packets
- ICMP total packets
- ICMP dropped under load
- ICMP dropped checksum error

Syntax:

```
show statistics icmp
```

Sample Output:

```
IntruDbg#> show statistics icmp

Datapath36

ICMP Echo Request packets: 154207

ICMP Echo Reply packets: 0

ICMP Unsol. Reply packets: 0

ICMP Other packets: 536697

ICMP Total Packets processed: 690904, 0

ICMP Dropped under load: 0

ICMP Dropped w/cksum error: 59053

Datapath37

ICMP Echo Request packets: 391658

ICMP Echo Reply packets: 98

ICMP Unsol. Reply packets: 0

ICMP Other packets: 1186879
```

```
ICMP Total Packets processed: 1578635, 0

ICMP Dropped under load: 0

ICMP Dropped w/cksum error: 50956
```

Applicable to:

NS-series Sensors

show statistics ipfrag

This command displays the IP fragment statistics in a data path. It includes the following information:

- Total number of IP
- Fragments received
- Total number of IP flows
- Number of duplicate fragments
- Number of fragments dropped
- Fragments dropped for invalid options
- Number of flows timeout
- Number of flows dropped for invalid checksum
- Number of invalid fragments
- Error getting reassembled lists
- Number of fragments received after timeout

Syntax:

```
show statistics ipfrag
```

Sample Output:

```
IntruDbg#> show statistics ipfrag

datapath 44 :

Total number of IP Fragments received: 2738083

Total number of IP Flows: 2363420

Number of Duplicate fragments: 372877

Number of Fragments dropped: 0

Fragments dropped for invalid options: 0

Number of Flows TimedOut: 2363174

Num Flows dropped for invalid checksum: 0

Error getting data buffers: 0
```

```
Number of Invalid Fragments: 0

Error getting Reassembled lists: 0

Number of fragments recvd after timeOut: 0

datapath 45 :

Total number of IP Fragments received: 2702704

Total number of IP Flows: 2331529

Number of Duplicate fragments: 369732

Number of Fragments dropped: 0

Fragments dropped for invalid options: 0

Number of Flows TimedOut: 2331267

Num Flows dropped for invalid checksum: 0

Error getting data buffers: 0

Number of Invalid Fragments: 0

Error getting Reassembled lists: 0

Number of fragments recvd after timeOut: 0
```

Applicable to:

NS-series Sensors

show statistics l4

It displays the layer 4 statistics. It includes the following information:

- Total layer 4 flow blocks
- Total SYN flow blocks
- Total active TCP flows
- Total Inactive TCP flows
- Total TCP in timewait
- Total active UDP flows
- Total flows in SYN state
- Total free TCBs
- Total created flows
- Total timeout flows

Syntax:

show statistics l4

Sample Output:

```
IntruDbg#> show statistics l4

Datapath 46 :

Total Layer4 flow blocks: = 24097

Total SYN flow blocks: = 11670

Total active TCP flows: = 22515

Total inactive TCP flows: = 0

Total TCP in timewait: = 143

Total active udp flows: = 1434

Total flows in SYN state: = 687

Total free TCBs: = 0

Total created flows: = 5798921

Total timedout flows: = 2460478

Datapath 47 :

Total Layer4 flow blocks: = 24097

Total SYN flow blocks: = 11670

Total active TCP flows: = 22539

Total inactive TCP flows: = 0

Total TCP in timewait: = 121

Total active udp flows: = 1437

Total flows in SYN state: = 666

Total free TCBs: = 0

Total created flows: = 5824819

Total timedout flows: = 2430180
```

Applicable to:

NS-series Sensors

show statistics tcp

This command displays the TCP statistics of a datapath for an ID range. It includes the following information:

- TCP total packets
- TCP total packets
- TCP drop count
- TCP error count

Syntax:

```
show statistics tcp
```

Sample Output:

```
IntruDbg#> show statistics tcp

Id range is not selected, Displaying ALL

Datapath 12 :

TCP total packets = 5103671, 57258772

TCP drop count = 32494

TCP error count = 0

Datapath 13 :

TCP total packets = 6370552, 52346671

TCP drop count = 50846

TCP error count = 0
```

Applicable to:

NS-series Sensors

show statistics udp

The command displays the UDP statistics. It includes the following information:

- UDP Total packets
- UDP Dropped packets
- UDP TimedOut UDP Resp(onse) packets
- UDP ACL Deny count

Syntax:

```
show statistics udp
```

Sample Output:

```
IntruDbg#> show statistics udp

Id range is not selected, Displaying ALL
```

```
Datapath21

UDP Total packets: 10341384, 99820895

UDP Dropped packets: 0

UDP TimedOut UDP Resp. packets: 0

UDP ACL Deny count: 0

Datapath22

UDP Total packets: 11333650, 126239382

UDP Dropped packets: 0

UDP TimedOut UDP Resp. packets: 0

UDP ACL Deny count: 0
```

Applicable to:

NS-series Sensors

show syslog profile

This command displays the syslog alert profile information such as the server IP, UDP port, facility, priority, policy based notify, quarantine based notify, severity based notify and the syslog alert templates.

Syntax:

```
show syslog profile
```

Sample Output:

```
IntruDbg#> show syslog profile

[Syslog alert profile information]

Syslog server IP : 10.11.11.1

UDP port : 514

Facility : 4

Priority : 0

Policy Based Notify : Disable

Quarantine Based Notify : Disable

Severity Based Notify : Notify All Severity Alerts

Syslog Alert Template : $IV_SENSOR_NAME$ detected $IV_DIRECTION$ attack $IV_ATTACK_NAME$ (severity =
$IV_ATTACK_SEVERITY$). $IV_SOURCE_IP$:$IV_SOURCE_PORT$ -> $IV_DESTINATION_IP$:$IV_DESTINATION_PORT$
(result = $IV_RESULT_STATUS$) $IV_MALWARE_FILE_SHA256_HASH$ $IV_MALWARE_FILE_SHA1_HASH$ $IV_MAL-
```

WARE_FILE_NAME$ $IV_MALWARE_FILE_MD5_HASH$ IV_SOURCE_IP IV_SOURCE_PORT $IV_DESTINATION_PORT$ $IV_DESTINATION_IP$

Applicable to:

NS-series and Virtual IPS Sensors

show tis channel

This command displays the channel used by Sensor to communicate with Intelligent Sandbox.

By default, SSL channel is used. You can switch between TCP and SSL channel to send files for scanning.

> **NOTE**
>
> For TCP channel, make sure that the listening port 8506 is set on Intelligent Sandbox. From an Intelligent Sandbox appliance, execute the **set nsp-tcp-channel** CLI command to enable or disable TCP channel.

Syntax:

```
show tis channel
```

Sample output:

```
IntruDbg#> show tis channel

TIS IPS channel type:SSL

IntruDbg#> show tis channel

TIS IPS channel type:TCP
```

Applicable to:

NS-series Sensors

show xff-usage

This command displays the XFF usage details.

Syntax:

```
show xff-usage
```

Sample Output:

```
IntruDbg#> show xff-usage

XFF Buffers Allocated at Init 379264

XFF Buffers Available Now 379264

XFF Buffers Alloc Error 0
```

```
XFF Header Seen 0

XFF BAD IP's Received 0

XFF BAD IPv4 Received 0

XFF BAD IPv6 Received 0

XFF Good IPv4 Received 0

XFF Good IPv6 Received 0

XFF IPv4 Seen in Attack Packets 0

XFF IPv6 Seen in Attack Packets 0
```

Applicable to:

NS-series Sensors

switch tis channel

It uses the SSL or TCP channel to send files for scanning to Intelligent Sandbox. By default, the Sensor uses SSL channel for communication with Intelligent Sandbox.

> **NOTE**
>
> For TCP channel communication, make sure that the listening port 8506 is set on Intelligent Sandbox. From Intelligent Sandbox, execute the **`set nsp-tcp-channel`** CLI command to enable or disable TCP channel.

Syntax:

```
switch tis channel <tcp | ssl>
```

Example:

```
IntruDbg#> switch tis channel tcp

IntruDbg#> switch tis channel ssl
```

Applicable to:

NS-series Sensors

tisChnstate WORD

This command configures the Sensor-Intelligent Sandbox server channel status.

Syntax:

```
tisChnstate WORD
```

Applicable to:

NS-series Sensors

tustat

This command shows TCP and UDP statistics for all datapaths.

Syntax:

```
tustat
```

Sample Output:

```
IntruDbg#> tustat

datapath 1:

total TCBs: = 138617

total SYN TCBS: = 69308

total active TCP flows: = 15145

total inactive TCP flows: = 14450

total tcp in timewait: = 1328

total active udp flows: = 5189

total flows in SYN state: = 3174

total free TCBs: = 101939

total created flows: = 14806372

total timedout flows: = 7018811

syncookie inbound status: = Active

syncookie outbound status: = Active

total syncookie proxy connections: = 2

total invalid cb hash buckets: = 0

CB syn list status: = Valid

CB free list status: = Valid
```

NOTE

The **`syncookie inbound status`**, **`syncookie outbound status`**, **`total syncookie proxy connections`**, **`total invalid cb hash buckets`**, **`CB syn list status`**, and **`CB free list status`** counters are available only in NS-series Sensors.

Applicable to:

NS-series Sensors

unknownapktocloud

Use this command to view, enable or disable the upload of unknown mobile .apk files to the Manager. If disabled, the Sensor will not generate unknown mobile .apk alerts.

Syntax:

`unknownapktocloud <on|off|status>`

Sample Output:

```
intruDBg#> unknownapktocloud status

unknownapktocloud = on
```

Applicable to:

NS-series Sensors

Manager Shell Commands

This section details the commands that can run in Manager shell of the Trellix IPS Manager running on MLOS.

aide

This command allows the user to perform advanced intrusion detection environment operations

Syntax:`aide <parameter>`

> **NOTE**
>
> To get a list of parameters for the **`aide`** command, execute **`aide -h`** command.

audit

This command displays the list of commands in Manager shell to perform actions on the audit service.

This command has no parameters.

Syntax:`audit`

Sample Output:

```
IPSManager> audit

Expected one of

restart Restart Audit service

start Start Audit service
```

status Show Audit Status

stop Stop Audit service

audit status

This command displays whether the audit service in the Linux based Manager is running.

This command has no parameters.

Syntax:audit status

Sample Output:

```
IPSManager> audit status
Redirecting to /bin/systemctl status auditd.service
 auditd.service - Security Auditing Service
Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; vendor preset: disabled)
Active: active (running) since Tue 2019-08-20 13:23:53 UTC; 3h 25min ago
Docs: man:auditd(8)
https://github.com/linux-audit/audit-documentation
Process: 1568 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
Process: 1561 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
Main PID: 1562 (auditd)
CGroup: /system.slice/auditd.service
1562 /sbin/auditd
1564 /sbin/audispd
```

auditctl

This command assists in controlling the kernel audit system.

Syntax:auditctl <parmeters>

> **NOTE**
>
> For the list of **auditctl** command parameters, execute **auditctl** command in the Manager shell.

aureport

This command displays summary report of the audit system logs.

This command has no parameters.

Syntax:aureport

Sample output:

```
IPSManager> aureport

Summary Report

======================

Range of time in logs: 01/01/70 00:00:00.000 - 08/21/19 13:53:36.990

Selected time for report: 01/01/70 00:00:00 - 08/21/19 13:53:36.990

Number of changes in configuration: 987

Number of changes to accounts, groups, or roles: 27

Number of logins: 12

Number of failed logins: 2

Number of authentications: 48

Number of failed authentications: 9

Number of users: 3

Number of terminals: 13

Number of host names: 8

Number of executables: 25

Number of commands: 25

Number of files: 85

Number of AVC's: 50

Number of MAC events: 15

Number of failed syscalls: 4

Number of anomaly events: 1

Number of responses to anomaly events: 0

Number of crypto events: 224

Number of integrity events: 0

Number of virt events: 0

Number of keys: 22
```

```
Number of process IDs: 1556

Number of events: 10679
```

ausearch

This command allows search operations in the audit logs.

Syntax:`ausearch <parameters>`

> **NOTE**
>
> For the list of **ausearch** command parameters, execute **ausearch** command in the Manager shell.

Sample output:

```
IPSManager> ausearch -i -p 1586

----

type=PROCTITLE msg=audit(08/21/19 13:48:03.930:747) : proctitle=/sbin/autrace /usr/bin/df

type=SYSCALL msg=audit(08/21/19 13:48:03.930:747) : arch=x86_64 syscall=close success=yes exit=0
a0=0x4 a1=0x7f2d8cf11760 a2=0x0 a3=0x7f2d8d55ca50 items=0 ppid=1584 pid=1586 auid=admin uid=root
gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=23 comm=autrace
exe=/usr/sbin/autrace subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)

----

type=PROCTITLE msg=audit(08/21/19 13:48:03.930:748) : proctitle=/sbin/autrace /usr/bin/df

type=SYSCALL msg=audit(08/21/19 13:48:03.930:748) : arch=x86_64 syscall=fstat success=yes exit=0
a0=0x1 a1=0x7ffe4c170da0 a2=0x7ffe4c170da0 a3=0x7ffe4c171020 items=0 ppid=1584 pid=1586 auid=ad-
min uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0
ses=23 comm=autrace exe=/usr/sbin/autrace subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key=(null)
```

autrace

This command allows tracing system calls and processes.

Syntax:`autrace <program>`

Sample output:

```
IPSManager> autrace /usr/bin/df

Waiting to execute: /usr/bin/df

Filesystem 1K-blocks Used Available Use% Mounted on

tmpfs 8209424 9244 8200180 1% /run
```

```
/dev/mapper/fs-root 34867872 1429900 31643720 5% /

/dev 8209424 0 8209424 0% /dev

tmpfs 8209424 0 8209424 0% /dev/shm

Cleaning up...

Trace complete. You can locate the records with 'ausearch -i -p 1586'
```

avvdat

This command helps in installing or updating the antivirus dat signatures for uvscan.

Syntax:avvdat -i <parameter>

> **NOTE**
>
> To get a list of parameters for the **avvdat** command execute **avvdat -h** command.

Sample Output:

```
IPSManager> avvdat -i /opt/scpfiles/avvdat-xxxx.zip

Install provided DAT file.

avvdat:Must be root. Attempting to sudo ...

Install provided DAT file.

avvdat:Installing /opt/scpfiles/avvdat-xxxx.zip ...

Archive: /opt/scpfiles/avvdat-xxxx.zip

inflating: avvclean.dat

inflating: avvnames.dat

inflating: avvscan.dat

inflating: legal.txt

Success:Installed:/opt/scpfiles/avvdat-xxxx.zip
```

cat

It displays the content of the file specified in the command.

Syntax:cat <filepath>

Sample Output:

```
IPSManager> cat /opt/scpfiles/infoLogs_2019_04_02_02_07_07.tar
```

```
2019-03-29 04:05:53,410 INFO [Timer-12] [logCorId1553832353408] iv.core.MalwareDownSelectorReport-Scheduler - Malware File Downselector Report Check end

2019-03-29 04:07:52,910 INFO [Timer-12] [logCorId1553832472909] iv.malware.MalwareFileDAO - getMalwareFilesByEngineWithIncompleteReportWithoutScoreAndRcentlyModified - no entry found for engine: 64

2019-03-29 04:07:52,911 INFO [Timer-12] [logCorId1553832472909] iv.malware.MalwareFileDAO - getMalwareFilesByEngineWithIncompleteReportWithoutScoreAndRcentlyModified - no entry found for engine: 4

2019-03-29 04:07:52,912 INFO [Timer-12] [logCorId1553832472909] iv.malware.MalwareFileDAO - getMalwareFilesByEngineWithIncompleteReportWithoutScoreAndRcentlyModified - no entry found for engine: 256

2019-03-29 04:07:52,912 INFO [Timer-12] [logCorId1553832472909] iv.malware.MalwareFileDAO - getMalwareFilesWithIncompleteReportAndRcentlyModified - no entry found

2019-03-29 04:07:53,409 INFO [Timer-12] [logCorId1553832473409] iv.core.MalwareDownSelectorReport-Scheduler - Malware File Downselector Report Check start
```

certtool

This command allows certificate generation in the Linux based Manager.

Syntax:`certtool <parameter>`

> **NOTE**
>
> For the list of parameters for the **`certtool`** command, execute **`certtool --help`** command in the Manager shell.

clear

This command clears the Manager shell screen.

Syntax:

```
clear
```

collect

This command displays the list of commands in Manager shell for collecting informational logs.

This command has no parameters.

Syntax:

```
collect
```

Sample Output:

```
IPSManager> collect

Expected one of
```

logs Collect all the required logs and create a tar in /opt/scpfiles

collect logs

The **collect logs** command is used to collect and create tar for all files in the **IPSManager/App/bin** folder.

This command has no parameters.

Syntax:collect logs

Sample Output:

IPSManager> collect logs

Logs collected successfully. View the infoLogs tar using command 'show files'

copyCertsToSyslogDir

It copies the certificates and keys from **/opt/scpfiles** directory to **/etc/syslogcerts** directory.

This command has no parameters.

Syntax:

copyCertsToSyslogDir

Sample Output:

IPSManager> copyCertsToSyslogDir

[sudo] password for admin:

cron

It displays the list of commands in Manager shell to perform actions on the cron service in the Linux based Manager.

This command has no parameters.

Syntax:

cron

Sample Output:

IPSManager> cron

Expected one of

restart Restart Cron service

start Start Cron service

status Show Cron Status

stop Stop Cron service

cron restart

The **cron restart** command is used to restart the cron service in the Linux based Manager.

This command has no parameters.

Syntax:cron restart

Sample Output:

```
IPSManager> cron restart

Redirecting to /bin/systemctl restart crond.service
```

cron start

The **cron start** command is used to turn on the cron service in the Linux based Manager.

This command has no parameters.

Syntax:

```
cron start
```

Sample Output:

```
IPSManager> cron start

Redirecting to /bin/systemctl start crond.service
```

cron status

This command displays whether the cron service in the Linux based Manager database is running.

This command has no parameters.

Syntax:

```
cron status
```

Sample Output:

```
IPSManager> cron status

Redirecting to /bin/systemctl status crond.service

 crond.service - Command Scheduler

Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor preset: enabled)

Active: active (running) since Tue 2019-08-20 13:45:32 UTC; 2h 51min ago

Main PID: 1835 (crond)

CGroup: /system.slice/crond.service
```

```
1835 /usr/sbin/crond -n

Aug 20 13:45:32 IPSManager systemd[1]: Started Command Scheduler.

Aug 20 13:45:32 IPSManager systemd[1]: Starting Command Scheduler...

Aug 20 13:45:32 IPSManager crond[1835]: (CRON) INFO (RANDOM_DELAY will be scaled with factor
23% ...ed.)

Aug 20 13:45:32 IPSManager crond[1835]: (CRON) INFO (running with inotify support)

Aug 20 13:45:32 IPSManager crond[1835]: (CRON) INFO (@reboot jobs will be run at computer's start-
up.)

Hint: Some lines were ellipsized, use -l to show in full.
```

cron stop

The **cron stop** command is used to turn-off the cron service in the Linux based Manager.

This command has no parameters.

Syntax:cron stop

Sample Output:

```
IPSManager> cron stop

Redirecting to /bin/systemctl stop crond.service
```

crontab

It allows creating cron jobs.

Syntax:crontab <parameters>

> **NOTE**
>
> For the list of **crontab** command parameters, execute **crontab --help** command in the Manager shell.

database

This command displays the list of commands in Manager shell to perform actions on the Manager database.

This command has no parameters.

Syntax:

database

Sample Output:

```
IPSManager> database
```

```
Expected one of

start Start MariaDB service

status Show MariaDB Status

stop Stop MariaDB service
```

database start

The **database start** command is used to start the Manager database.

This command has no parameters.

Syntax:database start

Sample Output:

```
IPSManager> database start

Starting mariadb (via systemctl): [ OK ]
```

database status

This command displays whether the Manager database is running.

This command has no parameters.

Syntax:database status

Sample Output:

```
IPSManager> database status

SUCCESS! MariaDB running (1140)
```

database stop

The **database stop** command is used to turn-off the Manager database.

This command has no parameters.

Syntax:database stop

Sample Output:

```
IPSManager> database stop

[sudo] password for admin:

Stopping mariadb (via systemctl): [ OK ]
```

database shell

This command allows users to enter the database shell.

Syntax:dbShell

NOTE

- Use the following credentials for logging in to the database shell:

  Username: **admin**

  Password: **admin123**

- Use the following credentials for logging in to the Public Cloud database shell:

  Username: **admin** or **root**

  Password: **<Last 6 digits of the instance ID**

  To know the Manager server instance ID, run the **status** command in the Manager shell.

NOTE

For security reasons, Trellix recommends that you change the database password.

IMPORTANT

The database password can be a combination of alphabets [both uppercase (A-Z) and lowercase (a-z)], numbers [0-9] and/or, special characters like "~ ` ! @ # $ % - * _ + [ ] : ; , ( ) ? { }".

NOTE

You should enter the specific database to perform operations in it. To access a particular database execute **use <database_name>**. The database options available in the MariaDB are **information_schema**, **lf**, **mysql**, **performance_schema**, and **test**.

Sample Output:

```
IPSManager> dbShell

Please enter DB User: admin

[sudo] password for admin:

Enter password:

Welcome to the MariaDB monitor. Commands end with ; or \g.

Your MariaDB connection id is 13179

Server version: 10.3.13-MariaDB-log MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
MariaDB [(none)]> use lf

Database changed

MariaDB [lf]>
```

NOTE

You can perform operations in the database shell using MariaDB commands. For more information, see MariaDB documentation.

date

This command displays the date in the Linux based Manager.

This command has no parameters.

Syntax:`date`

Sample Output:

```
IPSManager> date

Tue Aug 20 16:22:16 UTC 2019
```

deleteCerts

This command deletes the certificate specified in the command from the **`/etc/syslogcerts`** directory.

This command has no parameters.

Syntax:`deleteCerts <file_name>`

Sample Output:

```
IPSManager> deleteCerts newcert.crt
```

delete file

It deletes files from **`/opt/scpfiles`** folder in the Linux based Manager.

Syntax:`deleteFile <File_name>`

NOTE

The file name in the command must include the file extension type. For example, if you are deleting a file named **`infolog`** and the file type for info log is **`.tar`**, then the file name to be given in the command is **`infolog.tar`**.

Sample Output:

```
IPSManager> deleteFile infoLogs_2018_11_26_11_04_23.tar
```

delete temp file

This command deletes the file from the **/temp/** directory.

This command has no parameters.

> **NOTE**
>
> The **deleteTmpFile** can only delete files located in the **/temp/** directory.

Syntax:deleteTmpFile <file_name>

Sample Output:

```
IPSManager> deleteTmpFile depmod.txt

[sudo] password for admin:
```

df

This command displays the disk space summary of the Linux based Manager.

This command has no parameters.

Syntax:df

Sample Output:

```
IPSManager> df

Filesystem 1K-blocks Used Available Use% Mounted on

/dev 15485156 0 15485156 0% /dev

tmpfs 15485156 0 15485156 0% /dev/shm

tmpfs 15485156 9432 15475724 1% /run

/dev/mapper/fs-root 20426576 2337896 17028024 13% /

tmpfs 15485156 0 15485156 0% /sys/fs/cgroup

tmpfs 15485156 0 15485156 0% /dev/fs

/dev/mapper/fs-opt 78054092 10923912 63142112 15% /opt

/dev/sda1 376807 39216 318135 11% /boot
```

du

This command displays the disk space usage of files and directories in the Linux based Manager.

This command has no parameters.

Syntax:du

Sample output:

```
IPSManager> du

8220 ./config

4 ./.gnupg/private-keys-v1.d

36 ./.gnupg

8 ./.ssh

56 ./mysqlErrAndLogs

12 ./watchDogfiles

9024 .
```

edit

This command allows the user to edit the file specified in the command.

Syntax: `edit <filename>`

> **NOTE**
>
> This command will edit the file using vi-editor. Trellix recommends you use vi_editor commands to perform operations on the files.

> **NOTE**
>
> You can only edit the files listed under the output of **`show editables`** command.

env

This command displays information about the Linux based Manager environment.

This command has no parameters.

Syntax:env

Sample Output:

```
IPSManager> env

USER=admin

LOGNAME=admin

HOME=/home/admin
```

```
PATH=/usr/local/bin:/usr/bin

MAIL=/var/mail/admin

SHELL=/bin/restrictShell.py

SSH_CLIENT=10.1.1.1 60940 22

SSH_CONNECTION=10.1.1.1 60940 10.2.2.2

SSH_TTY=/dev/pts/0

TERM=xterm

SELINUX_ROLE_REQUESTED=

SELINUX_LEVEL_REQUESTED=

SELINUX_USE_CURRENT_RANGE=

XDG_SESSION_ID=16

XDG_RUNTIME_DIR=/run/user/500

LINES=53

COLUMNS=211
```

exit

The **exit** command is used to close the Manager shell session.

This command has no parameters.

Syntax:exit

fdisk

This command helps users perform disk partitioning operations in the Linux based Manager.

Syntax:fdisk <parameters>

firewall_cmd

This command allows users perform system firewall configuration activities.

Syntax:firewall_cmd <parameters>

> **NOTE**
>
> For the list of **firewall_cmd** command parameters, execute **firewall_cmd --help** command in the Manager shell.

firewalld

It displays the list of commands in Manager shell to perform actions on firewall service in the Linux based Manager.

This command has no parameters.

Syntax:`firewalld`

Sample output:

```
IPSManager> firewalld

Expected one of

restart Restart Firewall service

start Start Firewall service

status Show Firewall Status

stop Stop Firewall service
```

firewalld restart

This command, when executed, restarts the firewall service in the Linux based Manager.

This command has no parameters.

Syntax:`firewalld restart`

Sample output:

```
IPSManager> firewalld restart

Redirecting to /bin/systemctl restart firewalld.service
```

firewalld start

The **`firewalld start`** command is used to start the firewall service in the Linux based Manager.

This command has no parameters.

Syntax:`firewalld start`

Sample output:

```
IPSManager> firewalld start

Redirecting to /bin/systemctl start firewalld.service
```

firewalld status

This command displays whether the firewall service in the Linux based Manager is running.

This command has no parameters.

Syntax:firewalld status

Sample Output:

```
IPSManager> firewalld status

Redirecting to /bin/systemctl status firewalld.service

 firewalld.service - firewalld - dynamic firewall daemon

Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: disabled)

Active: active (running) since Tue 2019-08-20 15:18:07 UTC; 2s ago

Docs: man:firewalld(1)

Main PID: 377 (firewalld)

CGroup: /system.slice/firewalld.service

377 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Aug 20 15:18:07 IPSManager systemd[1]: Starting firewalld - dynamic firewall daemon...

Aug 20 15:18:07 IPSManager systemd[1]: Started firewalld - dynamic firewall daemon.

Aug 20 15:18:07 IPSManager firewalld[377]: WARNING: ebtables-restore and ebtables are missing,
di...all.

Aug 20 15:18:07 IPSManager firewalld[377]: WARNING: iptables not usable, disabling IPv4 firewall.

Hint: Some lines were ellipsized, use -l to show in full.
```

firewalld stop

The **firewalld stop** command is used to turn-off the firewall service in the Linux based Manager.

This command has no parameters.

Syntax:firewalld stop

Sample Output:

```
IPSManager> firewalld stop

[sudo] password for admin:

Redirecting to /bin/systemctl stop firewalld.service
```

free

This command displays the Linux based Manager memory and swap memory information.

This command has no parameters.

Syntax:free

Sample Output:

```
IPSManager> free

total used free shared buff/cache available

Mem: 30970316 709764 29138820 9440 1121732 29801220

Swap: 4095996 0 4095996
```

head

It displays first ten entries of the file specified in the command.

Syntax:head <filepath>

Sample Output:

```
IPSManager> head /opt/scpfiles/infoLogs_2019_04_02_02_07_07.tar

/home/admin/infologs/0000755000076400007640000000000001345054171301375 2ustar adminadmin/home/admin/infologs/c3p0.log0000644000076400007640000000014714134505417130152310ustar adminadmin2019-03-28 10:04:59,597 INFO [MLog-Init-Reporter] [] com.mchange.v2.log.MLog - MLog clients using slf4j logging.

2019-03-28 10:04:59,967 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po configuration values:

2019-03-28 10:04:59,967 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.maxStatements = 0

2019-03-28 10:04:59,967 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.initialPoolSize = 10

2019-03-28 10:04:59,967 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.minPoolSize = 10

2019-03-28 10:04:59,968 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.maxPoolSize = 40

2019-03-28 10:04:59,968 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.idleConnectionTestPeriod = 300

2019-03-28 10:04:59,968 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.maxIdleTime = 300

2019-03-28 10:04:59,968 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.maxRetryAttempts = 60

2019-03-28 10:04:59,968 INFO [main] [] com.intruvert.utility.dao.C3POConnectionFactory - c3po.connection.debugUnreturnedConnectionStackTraces = false
```

history

It lists the commands executed in current Manager shell session.

This command has no parameters.

Syntax:history

Sample Output:

```
IPSManager> history

clear

list

show system info

show memory usage

show system memory

history
```

iptables

This command allows you to perform actions on the iptables.

Syntax:iptables <parameters>

> **NOTE**
>
> To get a list of parameters for the **iptables** command, execute **iptables --h** command.

journalctl

This command displays systemd logs.

This command has no parameters.

Syntax:journalctl

```
IPSManager> journalctl

-- Logs begin at Fri 2019-04-26 05:09:54 UTC, end at Mon 2019-04-29 04:57:39 UTC. --

Apr 26 05:09:54 IPSManager systemd-journal[1642]: Runtime journal is using 8.0M (max allowed 1.4G,
trying to leave 2.2G free of 14.7G available  current limit 1.4G).

Apr 26 05:09:54 IPSManager kernel: Linux version 4.19.23-1.mlos3.x86_64 (admin@mlosbld.ctdev.net)
(gcc version 7.3.1 20180303 (MLOS 7.3.1-2.mlos3) (GCC)) #1 SMP Sun Feb 17 11:44:28 MST 2019
```

```
.....................
Apr 26 05:09:54 IPSManager kernel: 3 base 0600000000 mask FF00000000 write-back
Apr 26 05:09:54 IPSManager kernel: 4 base 0700000000 mask FF80000000 write-back
```

kill

This command allows the user to forcefully kill a process running in the Linux based Manager.

Syntax:`kill <parameter>`

> **NOTE**
>
> To get a list of parameters for the **`kill`** command, use **`kill -h`** command.

last

This command displays the list of recent logins and related information.

This command has no parameters.

Syntax:`last`

Sample Output:

```
IPSManager> last
admin pts/0 10.1.2.1 Tue Apr 30 01:50 still logged in
admin pts/0 10.1.1.1 Thu Apr 4 08:24 - 11:30 (03:05)
reboot system boot 4.19.23-1.mlos3. Thu Apr 4 06:51 - 09:33 (25+02:42)
admin tty1 Thu Apr 4 06:44 - 06:50 (00:06)
root tty1 Thu Apr 4 06:01 - 06:17 (00:15)
reboot system boot 4.9.124-1.mlos3. Thu Apr 4 06:01 - 06:51 (00:49)
```

list

This command displays all Manager shell commands supported for the current user role.

This command has no parameters.

Syntax:`list`

logger

The **`logger`** command in the Manager shell allows manual logging of any event to the system logs.

Syntax:logger <parameter>

lvextend

This command helps users in extending logical volume in the Linux based Manager.

Syntax:lvextend <parameters>

mail

The **mail** command is used to send or receive mails from the Linux based Manager

> **NOTE**
>
> For the list of parameters for **mail** command, execute **mail -h** command in the Manager shell.

manager

This CLI command displays the list of commands for performing Manager service actions in the Linux based Manager.

This command has no parameters.

Syntax:manager

Sample Output:

```
IPSManager> manager

Expected one of

restart Restart NSM Service

start Start NSM Service

status Show NSM Status

stop Stop NSM Service
```

manager start

The **manager start** command is used to start the Manager service.

This command has no parameters.

Syntax:manager start

Sample Output:

```
IPSManager> manager start

Redirecting to /bin/systemctl start manager.service
```

manager status

The **manager status** command displays if the Manager is active or inactive.

This command has no parameters.

Syntax:manager status

Sample Output:

```
IPSManager> manager status

 manager.service - IPS Manager Daemon

Loaded: loaded (/etc/systemd/system/manager.service; enabled; vendor preset: disabled)

Active: active (running) since Mon 2022-09-26 14:55:36 UTC; 8h ago

Process: 1542 ExecStart=/opt/IPSManager/App/bin/manager start (code=exited, status=0/SUCCESS)

Main PID: 1551 (sh)

CGroup: /system.slice/manager.service

1551 sh /opt/IPSManager/App/bin/tms.sh

1594 /opt/IPSManager/App/jre/bin/java -server -Xms1024m -Xmx11225m -Xss8m -XX:NewRatio=4 -XX:+Use-
ParallelOldGC...

Sep 26 14:55:36 IPSManager systemd[1]: Starting IPS Manager Daemon...

Sep 26 14:55:36 IPSManager manager[1542]: Starting IPS..

Sep 26 14:55:36 IPSManager systemd[1]: Started IPS Manager Daemon.
```

manager stop

The **manager stop** command is used to stop the Manager service.

This command has no parameters.

Syntax:manager stop

Sample Output:

```
IPSManager> manager stop

Redirecting to /bin/systemctl stop manager.service.
```

move automated backups

The **moveAutomatedBackups** command is used to move the automatically scheduled Manager/Central Manager backups from **/opt/IPSManager/App/ScheduledBackups/** folder to **/opt/scpfiles** directory.

This command has no parameters.

Syntax:moveAutomatedBackups

Sample Output:

```
IPSManager> moveAutomatedBackups

IPSManager>

IPSManager> show files

scheduledBackup_Weekly_2018_11_25__00_05_02.dmp scheduledBackup_Weekly_2018_11_25__00_05_02.jar
```

move manual backups

The **moveManualBackups** command is used to move the manually generated Manager/Central Manager backups from **/opt/IPSManager/App/Backups/** folder to **/opt/scpfiles** directory.

This command has no parameters.

Syntax:moveManualBackups

Sample Output:

```
IPSManager> moveManualBackups

[sudo] password for admin:

IPSManager> show files

Manual_backup.dmp Manual_backup.jar
```

netstat

The **netstat** command displays active TCP ports, ethernet statistics, IP routing table, IPv4 statistics, and ports used by the host machine.

Syntax:netstat <IP_Address>

Sample Output:

```
IPSManager> netstat 10.1.1.1

Active Internet connections (w/o servers)

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 0 548 IPSManager.qadoma:ssh 10.4.7.1:52531 ESTABLISHED

Active UNIX domain sockets (w/o servers)

Proto RefCnt Flags Type State I-Node Path

unix 3 [ ] DGRAM 7364 /run/systemd/notify
```

networkmanager

This CLI displays commands in the Manager shell for controlling System Network Manager.

This command has no parameters.

Syntax: `networkmanager`

Sample Output:

```
IPSManager> networkmanager

Expected one of
```

disable	Disable system network Manager service
enable	Enable system network Manager service
restart	Restart system network Manager service
start	Start system network Manager service
status	Show system network Manager status
stop	Stop system network Manager service

nmcli

This command is used to gather network related information as well as perform network operations.

Syntax: `nmcli`

Sample Output:

```
IPSManager> nmcli

1: lo: <LOOPBACK, UP, LOWER_UP>; Mtu 11111 qdisc noqueue state UNKNOWN group default q1 en 1000

1ink/loopback 00:00:00:00:00:00 abc 00:00:00:00:00:00

inet 10.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

2: eth0: <BROADCAST, MULTICAST, UP, LOWER_UP>; Mtu 1500 qdisc pfifo_fast state UP gr oup default
qlen 1000

link/ether 00:00:00:11:00:11 abc 00:00:00:ff:00:00

inet 10.1.1.1/24 abc 10.1.1.255 scope global eth0

valid 1ft forever preferred 1ft forever
```

ntp

This command displays the list of commands in Manager shell to perform actions on Network Time Protocol (NTP) daemon in MLOS.

This command has no parameters.

Syntax:ntp

Sample Output:

```
IPSManager> ntp

Expected one of

restart Restart ntp daemon service

start Start ntp daemon service

status Show ntp daemon service

stop Stop ntp daemon service
```

ntp restart

It restarts Network Time Protocol (NTP) daemon in MLOS.

This command has no parameters.

Syntax:ntp restart

Sample Output:

```
IPSManager> ntp restart

Redirecting to /bin/systemctl restart ntpd.service
```

ntp start

The **ntp start** command enables Network Time Protocol (NTP) daemon in MLOS.

This command has no parameters.

Syntax:ntp start

Sample Output:

```
IPSManager> ntp start

error reading information on service ntpd: No such file or directory

Unable to enable the service ntpd

Redirecting to /bin/systemctl start ntpd.service
```

ntp status

This command displays whether the Network Time Protocol (NTP) daemon is enabled or disabled in MLOS.

This command has no parameters.

Syntax:ntp status

Sample Output:

```
IPSManager> ntp status

Redirecting to /bin/systemctl status ntpd.service

? ntpd.service - Network Time Service

Loaded: loaded (/usr/lib/systemd/system/ntpd.service; disabled; vendor preset: disabled)

Active: inactive (dead)
```

ntpstat

This command reports the synchronisation state of the NTP daemon running on the local machine.

This command has no parameters.

Syntax:`ntpstat`

Sample Output:

```
IPSManager> ntpstat

synchronised to NTP server (10.x.x.x) at stratum 3

time correct to within 180 ms

polling server every 256 s
```

ntp stop

The **`ntp stop`** command disables Network Time Protocol (NTP) daemon in MLOS.

This command has no parameters.

Syntax:`ntp stop`

Sample Output:

```
IPSManager> ntp stop

[sudo] password for admin:

Redirecting to /bin/systemctl stop ntpd.service
```

ping

This command is used to ping a network host.

You can specify either a domain name or IPv4 address.

Syntax:`ping <ipv4 address/domain name>`

Sample Output:

```
IPSManager> ping 10.2.2.2

PING 10.208.15.62 (10.2.2.2) 56(84) bytes of data.

64 bytes from 10.2.2.2: icmp_seq=1 ttl=127 time=2.60 ms

64 bytes from 10.2.2.2: icmp_seq=2 ttl=127 time=6.28 ms

64 bytes from 10.2.2.2: icmp_seq=3 ttl=127 time=6.01 ms

64 bytes from 10.2.2.2: icmp_seq=4 ttl=127 time=5.99 ms

64 bytes from 10.2.2.2: icmp_seq=5 ttl=127 time=6.18 ms

--- 10.2.2.2 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4005ms

rtt min/avg/max/mdev = 2.601/5.416/6.287/1.412 ms
```

postconf

This command allows the user to configure and display parameters regarding the postfix mail system.

Syntax:postconf <parameter>

> **NOTE**
>
> To get a list of parameters for the **postconf** command, use **postconf -h** command.

postfix

It displays the list of commands in Manager shell to perform actions on the postfix service in the Linux based Manager.

This command has no parameters.

Syntax:postfix

Sample Output:

```
IPSManager> postfix

Expected one of

restart Restart Postfix service

start Start Postfix service

status Show Postfix Status

stop Stop Postfix service
```

postfix restart

This command restarts postfix service in the Linux based Manager.

This command has no parameters.

Syntax:postfix restart

Sample output:

```
IPSManager> postfix restart

Redirecting to /bin/systemctl restart postfix.service
```

postfix start

The **postfix start** command is used to start the postfix service in the Linux based Manager.

This command has no parameters.

Syntax:postfix start

Sample Output:

```
IPSManager> postfix start

Starting mariadb (via systemctl): [ OK ]
```

postfix status

This command displays whether the postfix service is running in the Linux based Manager.

This command has no parameters.

Syntax:postfix status

Sample Output:

```
IPSManager> postfix status

Redirecting to /bin/systemctl status postfix.service

 postfix.service - Postfix Mail Transport Agent

Loaded: loaded (/usr/lib/systemd/system/postfix.service; enabled; vendor preset: disabled)

Active: active (running) since Tue 2019-08-20 14:27:31 UTC; 4s ago

Process: 3587 ExecStop=/usr/sbin/postfix stop (code=exited, status=0/SUCCESS)

Process: 3621 ExecStart=/usr/sbin/postfix start (code=exited, status=0/SUCCESS)

Process: 3617 ExecStartPre=/usr/libexec/postfix/chroot-update (code=exited, status=0/SUCCESS)

Process: 3614 ExecStartPre=/usr/libexec/postfix/aliasesdb (code=exited, status=0/SUCCESS)

Main PID: 3702 (master)

CGroup: /system.slice/postfix.service
```

```
3702 /usr/libexec/postfix/master -w

3703 pickup -l -t unix -u

3704 qmgr -l -t unix -u

Aug 20 14:27:31 IPSManager systemd[1]: Starting Postfix Mail Transport Agent...

Aug 20 14:27:31 IPSManager postfix/master[3702]: daemon started -- version 2.10.1, configura-
tion /...fix

Aug 20 14:27:31 IPSManager systemd[1]: Started Postfix Mail Transport Agent.

Hint: Some lines were ellipsized, use -l to show in full.
```

postfix stop

The **postfix stop** command is used to turn-off the postfix service in the Linux based Manager.

This command has no parameters.

Syntax:postfix stop

Sample Output:

```
IPSManager> postfix stop

Redirecting to /bin/systemctl stop postfix.service
```

ps

This command displays process status of the Linux based Manager.

This command has no parameters.

Syntax:ps

Sample Output:

```
IPSManager> ps

PID TTY TIME CMD

693 pts/1 00:00:00 restrictShell.p

724 pts/1 00:00:00 ps
```

publicKeyAuth

This command allows the user to perform Public Key Authentication for remote Machine.

Syntax:publicKeyAuth

Sample Output:

```
IPSManager> publicKeyAuth
```

```
[sudo] password for admin:
Please provide with the following inputs.
[Tue Dec 10 13:12:54 IST 2019] : Enter The SCP Server IP : 10.1.1.1
[Tue Dec 10 13:12:54 IST 2019] : Enter SCP Server UserName : admin
[Tue Dec 10 13:12:54 IST 2019] : Checking if .ssh/ already exists.
[Tue Dec 10 13:12:54 IST 2019] : The /home/admin/.ssh already exists!
[Tue Dec 10 13:12:54 IST 2019] : Checking if public key already exists.
[Tue Dec 10 13:12:54 IST 2019] : The /home/admin/.ssh/id_rsa.pub does not exists!
[Tue Dec 10 13:12:54 IST 2019] : Creating a key pair.
Generating public/private rsa key pair.
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:CshRToUOUNy3n0PJdLoKlEDojS+PEY3xexUWTSlS5xo admin@LinuxManager
The key's randomart image is:
+---[RSA 2048]----+
|.*o.oooo+o. |
|..++o..++o. |
|. O+.ooEo= |
| * *+ ..B |
| =.o .+So |
| o o.o .= |
| = .... . |
| . . . |
| |
+----[SHA256]-----+
[Tue Dec 10 13:12:54 IST 2019] : Successfully created the key pair.
[Tue Dec 10 13:12:54 IST 2019] : Changing permissions of local .ssh/ dir
[Tue Dec 10 13:12:54 IST 2019] : Successfully changed the permissions of the dir/file to 700
```

```
[Tue Dec 10 13:12:54 IST 2019] : Transfering public key to remote machine. The operation might ask for password.

/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"

/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys

FIPS mode initialized

admin@10.1.1.1's password:

[Tue Dec 10 13:12:54 IST 2019] : Successfully copied the key to 10.1.1.1

[Tue Dec 10 13:12:54 IST 2019] : Modifying .ssh/ related dir/file permissions on the remote machine. The operation might ask for password.

FIPS mode initialized

admin@10.1.1.1's password:

[Tue Dec 10 13:12:54 IST 2019] : Successfully modified the permissions of .ssh/authorized_keys on remote machine.
```

reboot

This command reboots the Linux based Manager.

This command has no parameters.

Syntax:reboot

reset

This command is used to reset the Manager shell session.

The reset command is used to exit from a command execution. The abrupt abortion of a command execution results in abnormal behavior of the Manager shell. In such scenarios, the **reset** command is used to regain control of Manager shell.

Syntax:reset

resize2fs

This command helps users in resizing the file system of the Linux based Manager.

Syntax:resize2fs <parameters>

run

It runs an executable mentioned in the command from **IPSManager/App/bin** folder.

The executables available in the **IPSManager/App/bin** folder are as follows:

Executable file	Description
changeDbRootPass.sh	Change root password of the database.
dbBackup.sh	Back up the Manager database to folder.
dbrestore.sh	Restores database to the Manager
dbtuning.sh	Tunes the Manager database
initdb.sh	Installs or upgrades the Maria database in the Manager
passwordchange.sh	Resets Maria database password of the Manager
pruning.sh	Prunes events in the Manager
SolrQuery.sh	Runs a query on Solr database
AlertTLVReader.sh	Parses the alerts from the Sensor
CACertsFileGen.sh	Helps in replacing Trellix signed SSL certificate on the Manager with a CA authority signed SSL certificate
InfoCollector.sh	Collects information logs like Manager logs, Configuration Backups etc.
changeOwnerToAdmin.sh	Change the owner of the Manager directory and subdirectories in **/opt** folder from root to admin.
MalwareDecrypter.sh	Decrypts malware reports received from external malware detection engines
keytool.sh	Imports keys or certificates from external servers
auditPartEnc.sh	Encryption and configuration changes to audit partition
net-snmp-create-v3-user	Create SNMP V3 user for SNMP service and NMS user.

Syntax:run <executable_file_name>

scp from remote

The **scpFromRemote** command is used to copy files from a remote location to **/opt/scpfiles** directory of the Linux based Manager.

Syntax:scpFromRemote <username> <remote_machine_ip> <filepath>

For scp from remote with a key: **scpFromRemote -i <path/to/key> <user_name> <remote_machine-ip> <filepath>**

> **NOTE**
>
> Ensure the key is FIPS compatible. To make the key FIPS compatible, refer to KB article KB94844.

The parameters for **scpFromRemote** command are as follows:

Parameters	Description
<user_name>	Login username for the remote machine
<remote_machine-ip>	IP address of the remote machine

Parameters	Description
<filepath>	File path in the remote machine for the file to be copied
<path/to/key>	File path in the Linux based Manager for the key

Sample Output:

```
IPSManager> scpFromRemote root 10.2.1.1 /root/infoLogs_2018_11_26_07_29_54.tar

FIPS mode initialized root 10.2.1.1 /root/infoLogs_2018_11_26_07_29_54.tar

root@10.2.1.1's password:

infoLogs_2018_11_26_07_29_54.tar 100% 6220KB 11.1MB/s 00:00

IPSManager> show files

infoLogs_2018_11_26_07_29_54.tar
```

scp to remote

The **scpToRemote** command is used to copy files to a remote location from **/opt/scpfiles** directory of the Linux based Manager.

Syntax:scpToRemote <file_name> <user_name> <remote_machine-ip> <filepath>

For scp to remote with a key: **scpToRemote -i <path/to/key> <file_name> <user_name> <remote_machine-ip> <filepath>**

> **NOTE**
>
> Ensure the key is FIPS compatible. To make the key FIPS compatible, refer to KB article KB94844.

The following table lists the parameters for **scpToRemote** command.

Parameters	Description
file_name	Name of the file to be copied to the remote machine
user_name	Login username for the remote machine
remote_machine-ip	Enter the IP address of the remote machine
filepath	Location in the remote machine to copy the file
<path/to/key>	File path in the Linux based Manager for the key

Sample Output:

```
IPSManager> show files

infoLogs_2018_11_26_07_29_54.tar

IPSManager> scpToRemote infoLogs_2018_11_26_07_29_54.tar root 10.1.1.1 /root/
```

```
FIPS mode initialized

The authenticity of host '10.2.1.2 (10.2.1.2)' can't be established.

ECDSA key fingerprint is SHA256:tv30NNgsRMY6U+UNOEAU+/WFhFXPn4KABrMxNbHK9qY.

ECDSA key fingerprint is SHA1:heXX04NJBvbz+mv22LlSYwWN7MQ.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.2.1.2' (ECDSA) to the list of known hosts.

root@10.1.1.1's password:

infoLogs_2018_11_26_07_29_54.tar 100% 6220KB 11.2MB/s 00:00
```

semanage

You can use this command to configure elements of the SELinux policy without requiring any modification or recompilation from policy sources.

Syntax: **`semanage <parameters>`**

set

It displays commands in the Manager shell for configuring Manager and network configuration.

This command has no parameters

Syntax:`set`

Set login banner

This command is used to set the login banner in the Linux based Manager.

Syntax:`set login banner`

Sample Output:

```
IPSManager> set login banner

[sudo] password for admin:
```

> **NOTE**
>
> This command will edit the file using **`vi editor`**. Trellix recommends you to use **`vi editor`** commands to enter the message to be displayed when the user logs in to the Manager shell.

```
User should be able to see the updated message from next login onwards
```

set network

This CLI displays commands in the Manager shell for configuring network parameters.

This command has no parameters.

Syntax:set network

Sample Output:

```
IPSManager> set network

Expected one of
```

configuration	Set full network configuration
dns	Set DNS servers
domain	Set DNS domain name
gateway	Set Network Gateway
hostname	Set Network Hostname
ip dhcp	Set Network IP
ipv6	Set ipv6 network configuration
ntp <IP> [<IP> ...]	Set NTP Server(s)
route	Set Network Route

set network configuration

This command is used to configure network parameters for the Linux based Manager.

> **NOTE**
>
> Reboot the Linux based Manager machine after executing **set network configuration** command for successful configuration of the network parameters.

Syntax:set network configuration

```
Select the type of NIC configuration:

Please select one of the below option:

1 -> Configure Single NIC

2 -> Configure Both the NIC's

Input 1 or 2 based on you selection :<1/2>

Enter the NIC you want to configure with public network ip:

1 -> eth0 [NIC 1]

2 -> eth1 [NIC 2]

Input 1 or 2 based on your selection : <1/2>

Enter the DOMAIN NAME : <Manager_Domain_Name>
```

```
Enter the HOSTNAME : <Manager_Hostname>

Configuring <eth0/eth1> with public ip

Enter the IP ADDRESS : <Manager_Public_IP_Address>

Enter the NETMASK : <Netmask_IP_Address>

Enter the GATEWAY : <Gateway_IP_Address>

Enter the DNS1 : <DNS1_Server_IP_Address>

Do you want to set DNS2 ? (y/n): <y/n>

Enter the DNS2 : <DNS2_Server_IP_Address>

Configuring <eth0/eth1> with private ip

Enter the IP ADDRESS : <Manager_Private_IP_Address>
```

Parameters	Description
Manager_Domain_Name	Enter the domain name for the Manager server.
Manager_Hostname	Enter the hostname to be assigned to the Manager server.
Manager_Public_IP_Address	Enter the public IP address to be assigned to the Manager server.
Netmask_IP_Address	Enter the subnet mask for the Manager server.
Gateway_IP_Address	Enter the gateway address for the Manager server.
DNS1_Server_IP_Address	Enter primary DNS server IP address.
<y/n>	Type **y**, if you want to configure secondary DNS server IP address, or else type **n**.
DNS2_Server_IP_Address	(Optional) Enter secondary DNS server IP address.
Manager_Private_IP_Address	Enter the private IP address to be assigned to the Manager server.

Sample Output:

```
IPSManager> set network configuration

[sudo] password for admin:

*****Setting up all the required network configuration.*****

Select the type of NIC configuration:

Please select one of the below option:

1 -> Configure Single NIC

2 -> Configure Both the NIC's
```

```
Input 1 or 2 based on you selection : 2

Enter the NIC you want to configure with public network ip:

1 -> eth0 [NIC 1]

2 -> eth1 [NIC 2]

Input 1 or 2 based on your selection : 1

Enter the DOMAIN NAME : mydomain.com

Enter the HOSTNAME : mycompany

Configuring eth0 with public ip

Enter the IP ADDRESS : 10.1.1.1

Enter the NETMASK : 255.255.255.0

Enter the GATEWAY : 10.1.1.252

Enter the DNS1 : 10.1.2.11

Do you want to enter DNS2 ? (y/n): y

Enter the DNS2 : 10.2.1.3.

Configuring eth1 with private ip

Enter the IP ADDRESS : 10.1.1.7

Your mac address is 00:50:56:89:ec:83

*****Networking configuration setup complete.*****

Restarting network (via systemctl): [ OK ]
```

set network dns

This command enables users to specify IP address of DNS server for the Manager.

Syntax:`set network dns`

```
Enter the DNS1 : <DNS1_Server_IP_Address>

Do you want to set DNS2 ? (y/n): <y/n>

Enter the DNS2 : <DNS2_Server_IP_Address>
```

Parameters	Description
`DNS1_Server_IP_Address`	Enter primary DNS server IP address.
`<y/n>`	Type **y**, if you want to configure secondary DNS server IP address, or else type **n**.

Parameters	Description
DNS2_Server_IP_Address	(Optional) Enter secondary DNS server IP address.

Sample Output:

```
IPSManager> set network dns

[sudo] password for admin:

Enter the DNS1 : 10.1.2.11

Do you want to enter DNS2 ? (y/n): y

Enter the DNS2 : 10.2.1.3.

Restarting network (via systemctl): [ OK ]
```

set network domain

This command enables users to configure DNS domain name for the Manager.

Syntax:`set network domain`

```
Enter the DOMAIN NAME : <Manager_Domain_Name>
```

Parameters	Description
Manager_Domain_Name	Enter the domain name for the Manager server.

Sample Output:

```
IPSManager> set network configuration

[sudo] password for admin:

Enter the DOMAIN NAME : mydomain.com

Restarting network (via systemctl): [ OK ]
```

set network gateway

This command enables users to specify IP address of gateway for the Manager.

Syntax:`set network gateway`

```
Enter the GATEWAY : <Gateway_IP_Address>
```

Parameters	Description
Gateway_IP_Address	Enter the gateway address for the Manager server.

Sample Output:

```
IPSManager> set network gateway
```

```
[sudo] password for admin:

Enter the GATEWAY : 10.1.1.252

Restarting network (via systemctl): [ OK ]
```

set network hostname

This command enables users to specify the host name for the network.

Syntax:`set network hostname <host_name>`

Sample Output:

Syntax:`set network hostname`

```
Enter the HOSTNAME : <Manager_Hostname>
```

Parameters	Description
`Manager_Hostname`	Enter the hostname to be assigned to the Manager server.

Sample Output:

```
IPSManager> set network hostname

[sudo] password for admin:

Enter the HOSTNAME : mycompany

Restarting network (via systemctl): [ OK ]
```

set network ip

You can specify IP address for the Manager server using this command.

Syntax:`set network ip`

```
Enter the IP ADDRESS : <Manager_IP_Address>
```

Parameters	Description
`Manager_IP_Address`	Enter the IP address to be assigned to the Manager server.

Sample Output:

```
IPSManager> set network ip

[sudo] password for admin:

Enter the IP ADDRESS : 10.1.1.1

Restarting network (via systemctl): [ OK ]
```

set network ipv6

You can specify an IPv6 address for the Manager server using this command.

Syntax: `set network ipv6`

`Enter the DOMAIN NAME : <Manager_Domain_Name>`

`Enter the HOST NAME : <Manager_Hostname>`

`Enter the IPv6 ADDRESS : <Manager_IPv6_Address>/<Prefix_Length>`

`Enter the IPv6 GATEWAY : <Gateway_IP_Address>`

`Enter the DNS1 : <DNS1_Server_IP_Address>`

`Do you want to set DNS2 ? (y/n): <y/n>`

`Enter the DNS2 : <DNS2_Server_IP_Address>`

Parameters	Description
`Manager_Domain_Name`	Enter the domain name for the Manager server.
`Manager_Hostname`	Enter the hostname to be assigned to the Manager server.
`Manager_IPv6_Address/Prefix_Length`	Enter the IPv6 address to be assigned to the Manager server/Provide the prefix length. Example: **`fe80::2/64`**
`Gateway_IP_Address`	Enter the gateway address for the Manager server.
`DNS1_Server_IP_Address`	Enter the primary DNS server IP address.
`<y/n>`	Type **`y`**, if you want to configure a secondary DNS server IP address, or else type **`n`**.
`DNS2_Server_IP_Address`	(Optional) Enter the secondary DNS server IP address.

Sample Output:

```
IPSManager> set network configuration

########################## Configuring IPv6 Network ############################

#                                                                              #

# [NOTE]:                                                                      #

#       >  Only eth0 can be configured                                         #

#       >  Network service will be restarted at the end of the configuration   #

#       >  The system will reboot after complete configuration                 #

#       >  Input 'quit' at any step to quit configuration                      #

#                                                                              #
```

```
################################################################################
Enter the DOMAIN NAME : mydomain.com
Enter the HOSTNAME : mycompany
Enter the IPv6 ADDRESS : 0:0:0:fe80:0:0:1010:0101
Enter the IPv6 GATEWAY : 0:0:0:fe80:0:0:1010:001l
Enter the DNS1 : 0:0:0:0:1111
Do you want to enter DNS2 ? (y/n): y
Enter the DNS2 : 0:0:0:1111:1111
```

NOTE

- The system will automatically reboot after complete configuration.
- To confirm the configured IPv6 address, use **nmcli** or **show network ip**.

set network ntp

This command enables users to specify NTP server for the Manager.

Syntax: set network ntp <ntp_server_ip_address>

Sample Output:

```
IPSManager> set network ntp 10.1.1.3
[sudo] password for admin:
Redirecting to /bin/systemctl stop ntpd.service
Redirecting to /bin/systemctl start ntpdate.service
Created symlink from /etc/systemd/system/multi-user.target.wants/ntpd.service to /usr/lib/sys-
temd/system/ntpd.service.
```

set password

The **set passwd** command is used to change password of a user account.

This command has no parameters.

Syntax:show passwd

Sample Output:

```
IPSManager> set passwd
Changing password for user admin.
```

```
Changing password for admin.

(current) UNIX password: *************

New password: ***********

Retype new password:***********

passwd: all authentication tokens updated successfully.
```

set time

This command is used to configure date and time in the Manager.

Syntax:`set time <Year>-<Month>-<Date> <Hour>:<Minute>:<Second>`

The following table lists the parameters for **`set time`** command.

Parameters	Description
`Year`	Enter the year in 4 digits.
`Month`	Enter the month in 2 digits.
`Date`	Enter the date in 2 digits.
`Hour`	Enter the hour in 2 digits. The clock in the Manager is configured in 24 hours format.
`Minute`	Enter the minute in 2 digit.
`Second`	Enter the second on 2 digit.

Sample Output:

```
IPSManager> set time 2018-11-28 06:12:58

[sudo] password for admin:

Local time: Wed Nov 28 06:12:58 UTC 2018

UTC time: Wed Nov 28 06:12:58 UTC 2018
```

show

It displays the list of commands in Manager shell to view the Manager and network information.

This command has no parameters.

Syntax:`show`

show arp

It displays arp table information.

This command has no parameters.

Syntax:`show arp`

Sample Output:

```
IPSManager> show arp

Address HWtype HWaddress Flags Mask Iface

10.2.1.1 ether 30:f7:0d:bf:ce:bf C eth0
```

show backup log

This command lists or displays all the restored log files.

Syntax:show backup log <all>/<file_name>

Parameter	Description
<all>	This option enlists all the var log files available.
<file_name>	This option opens the log file in vi editor for user.

show clock

It displays Manager server and host machine time stamp.

This command has no parameters.

Syntax:show clock

Sample Output:

```
IPSManager> show clock

Local time: Mon Oct 15 17:45:04 UTC 2018

UTC time: Mon Oct 15 17:45:04 UTC 2018
```

show database version

It displays the version of MariaDB database used in the Manager.

This command has no parameters.

Syntax:show databaseVersion

Sample Output:

```
IPSManager> show databaseVersion

/opt/IPSManager/MariaDB/bin/mariadb Ver 15.1 Distrib 10.5.16-MariaDB, for linux-systemd (x86_64) us-
ing readline 5.1
```

show editables

This CLI command lists the files in the Linux based Manager that a user can edit.

This command has no parameters.

Syntax:show editables

Sample Output:

```
IPSManager> show editables
[sudo] password for admin:
The following files can be edited by the user
1) ems.properties
2) log4j2.xml
3) my.cnf
```

show executables

It lists the executables in **IPSManager/App/bin** folder.

This command has no parameters.

Syntax:show executables

Sample Output:

```
IPSManager> show executables
1) changeDbRootPass.sh
2) dbBackup.sh
3) dbrestore.sh
4) dbtuning.sh
5) initdb.sh
6) passwordchange.sh
7) pruning.sh
8) SolrQuery.sh
9) AlertTLVReader.sh
10) CACertsFileGen.sh
11) InfoCollector.sh
12) changeOwnerToAdmin.sh
13) MalwareDecrypter.sh
14) keytool.sh
15) auditPartEnc.sh
```

16) net-snmp-create-v3-user

show files

It lists files available in the **/opt/scpfiles** directory.

This command has no parameters.

Syntax:show files

Sample Output:

```
IPSManager> show files

infoLogs_2018_10_12_14_57_02.tar
```

show file systems

This CLI command displays file systems in the Manager.

This command has no parameters.

Syntax:show filesystems

Sample Output:

```
IPSManager> show filesystems

Filesystem Size Used Avail Use% Mounted on

/dev 8.7G 0 8.7G 0% /dev

tmpfs 8.7G 0 8.7G 0% /dev/shm

tmpfs 8.7G 9.5M 8.7G 1% /run

/dev/mapper/fs-root 32G 1.1G 29G 4% /

tmpfs 8.7G 0 8.7G 0% /sys/fs/cgroup

tmpfs 8.7G 0 8.7G 0% /dev/fs

/dev/mapper/fs-opt 123G 5.8G 111G 5% /opt

/dev/sda1 386M 40M 327M 11% /boot

tmpfs 1.8G 0 1.8G 0% /run/user/0

tmpfs 1.8G 0 1.8G 0% /run/user/500
```

show java version

It displays java version of MLOS.

This command has no parameters.

Syntax:show javaVersion

Sample Output:

```
IPSManager> show javaVersion

openjdk version "1.8.0_181"

OpenJDK Runtime Environment (Zulu 8.31.0.2-linux64) (build 1.8.0_181-b02)

OpenJDK 64-Bit Server VM (Zulu 8.31.0.2-linux64) (build 25.181-b02, mixed mode)
```

show kernel version

This CLI command displays kernel version of MLOS.

This command has no parameters.

Syntax:`show kernelVersion`

Sample Output:

```
IPSManager> show kernelVersion

4.19.176-1.mlos3.x86_64
```

show log

It lists the commands in the Manager shell to view Linux based Manager logs.

Syntax:`show log`

Sample Output:

```
IPSManager> show log

Expected one of

file Syntax -> show log file <all> OR <file_name> - 'all' option enlists all the log files availa-
ble. Where as file name argument opens the log file in vi editor for user.
```

show log file

This CLI command displays contents of the log file specified in the command.

Syntax:`show log file <file name>`

> **NOTE**
>
> For a list of log files in the Linux based Manager, execute **`show log file all`** command in the Manager shell.

Sample Output:

```
IPSManager> show log file cim.log

2022-09-26 14:53:25,795 INFO [Thread-128] [] com.intruvert.cim.ccm.core.CloudVMGroupImpl:77 - Star-
ted VM Monitoring thread [frequency = 60 sec] ...
```

```
2022-09-26 14:53:25,800 INFO [Thread-128] [] com.intruvert.cim.ccm.core.CloudClusterManagerImpl:66 -
iv.cloud.sensor.termination.monitor = true

2022-09-26 14:53:25,807 INFO [Thread-128] [] com.intruvert.cim.ccm.core.CloudClusterManagerImpl:74 -
Started Cloud Sensor Termination monitor thread [frequency= 120 secs] ...

2022-09-26 14:56:48,212 INFO [Thread-128] [] com.intruvert.cim.ccm.core.CloudVMGroupImpl:77 - Star-
ted VM Monitoring thread [frequency = 60 sec] ...
```

show mail file

This command allows the user to view and edit the mail file specified in the command.

> **NOTE**
>
> For a list of mail files in the Linux based Manager, execute **show mail file all** command in the Manager shell.

> **NOTE**
>
> The **show mail file** command will view and edit the mail file using vi-editor. Trellix recommends you to use vi_editor commands to perform operations on the files.

Syntax:show mail file <file name>

show manager version

The **show managerVersion** command displays the Manager version running on MLOS.

This command has no parameters.

Syntax:show managerVersion

Sample Output:

```
IPSManager> show managerVersion

10.1.7.xx
```

show network

This command displays the commands in Manager shell to view network information.

This command has no parameters.

Syntax:show network

Sample Output:

```
IPSManager> show network

Expected one of
```

dns Show DNS servers

domain Show DNS domain name

hostname Show Hostname

ip Show network IP

ntp Show NTP Server(s)

route Show network routing

show network dns

This CLI command, when executed, displays IP address of DNS server for the Manager.

This command has no parameters.

Syntax:show network dns

Sample Output:

```
IPSManager> show network dns

10.1.1.1

10.2.2.2
```

show network domain

This command displays DNS domain name of the host.

This command has no parameters.

Syntax:show network domain

Sample Output:

```
IPSManager> show network domain

mycompany.com
```

show network gateway

It displays IP address of gateway for the Manager.

This command has no parameters.

Syntax:show network gateway

Sample Output:

```
IPSManager> show network gateway

10.1.1.1
```

show network hostname

This command displays network hostname of the Linux machine.

This command has no parameters.

Syntax:show network hostname

Sample Output:

```
IPSManager> show network hostname

IPSManager
```

show network ip

This CLI command displays IP address of the host machine.

This command has no parameters.

Syntax:show network ip

Sample Output:

```
IPSManager> show network ip

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid_lft forever preferred_lft forever

inet6 ::1/128 scope host

valid_lft forever preferred_lft forever

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000

link/ether 00:0c:29:fc:68:ce brd ff:ff:ff:ff:ff:ff

inet 10.1.1.1/24 brd 10.208.12.255 scope global eth0

valid_lft forever preferred_lft forever

inet6 fe80::20c:29ff:fefc:68ce/64 scope link

valid_lft forever preferred_lft forever
```

show network ntp

It displays host machine NTP server information.

This command has no parameters.

Syntax:show network ntp

Sample Output:

```
IPSManager> show network ntp

utcnist2.colorado.edu

time.fu-berlin.de

ntp.nict.jp
```

show network route

This command displays network configuration information of the host machine.

This command has no parameters.

Syntax:`show network route`

Sample Output:

```
IPSManager> show network route

default via 10.208.12.252 dev eth0

10.208.12.0/24 dev eth0 proto kernel scope link src 10.208.12.138
```

show OS version

It displays MLOS version of the host machine.

This command has no parameters.

Syntax:`show osVersion`

Sample Output:

```
IPSManager> show osVersion

MLOS release 3.9.2009 (Core)
```

show process

This command displays the on-going processes in the Manager.

This command has no parameters.

Syntax:`show process`

Sample Output:

```
IPSManager> show process

USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND

root 1 0.0 0.0 194572 9216 ? Ss Oct09 0:04 /usr/lib/systemd

root 2 0.0 0.0 0 0 ? S Oct09 0:00 [kthreadd]
```

```
root 3 0.0 0.0 0 0 ? S Oct09 0:00 [ksoftirqd/0]

root 5 0.0 0.0 0 0 ? S< Oct09 0:00 [kworker/0:0H]

root 7 0.0 0.0 0 0 ? S Oct09 0:03 [rcu_sched]

root 8 0.0 0.0 0 0 ? S Oct09 0:00 [rcu_bh]

root 9 0.0 0.0 0 0 ? S Oct09 0:00 [migration/0]

root 10 0.0 0.0 0 0 ? S< Oct09 0:00 [lru-add-drain]
```

show process monitor

This command displays monitor processes in the Manager.

Syntax:`show process monitor`

Sample Output:

```
IPSManager> show process monitor

top - 22:37:52 up 6 days, 7:53, 2 users, load average: 0.01, 0.03, 0.01

Tasks: 142 total, 1 running, 141 sleeping, 0 stopped, 0 zombie

%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st

KiB Mem : 16828016 total, 10005468 free, 1061536 used, 5761012 buff/cache

KiB Swap: 4095996 total, 4095996 free, 0 used. 15378056 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND

1482 admin 20 0 56864 4036 3368 R 0.3 0.0 0:00.01 top

1961 root 20 0 219136 6644 5552 S 0.3 0.0 0:16.03 rsyslogd

1 root 20 0 194572 9216 5712 S 0.0 0.1 0:04.28 systemd

2 root 20 0 0 0 0 S 0.0 0.0 0:00.07 kthreadd

3 root 20 0 0 0 0 S 0.0 0.0 0:00.15 ksoftirqd/0

5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:+

7 root 20 0 0 0 0 S 0.0 0.0 0:03.44 rcu_sched

8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh

9 root rt 0 0 0 0 S 0.0 0.0 0:00.09 migration/0

10 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 lru-add-dr+

11 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/0

12 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/1
```

```
13 root rt 0 0 0 0 S 0.0 0.0 0:00.03 migration/1

14 root 20 0 0 0 0 S 0.0 0.0 0:00.28 ksoftirqd/1

16 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/1:+

17 root 20 0 0 0 0 S 0.0 0.0 0:00.00 cpuhp/2

18 root rt 0 0 0 0 S 0.0 0.0 0:00.01 migration/2

top - 22:38:43 up 6 days, 7:54, 2 users, load average: 0.00, 0.03, 0.00

Tasks: 142 total, 1 running, 141 sleeping, 0 stopped, 0 zombie

%Cpu(s): 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st

KiB Mem : 16828016 total, 10005060 free, 1061944 used, 5761012 buff/cache

KiB Swap: 4095996 total, 4095996 free, 0 used. 15377648 avail Mem
```

show syslogCerts

The **show syslogCerts** command enlists all syslog certificates and keys available in **/etc/syslogcerts** directory.

This command has no parameters.

Syntax:show syslogCerts

Sample Output:

```
IPSManager> show syslogCerts

[sudo] password for admin:
```

show system

It displays commands in Manager shell to view overall system information.

This command has no parameters.

Syntax:show system

Sample Output:

```
IPSManager> show system

Expected one of

info Show system info

memory Show system memory usage

uptime Show system uptime
```

show system info

The **show system info** command displays hardware and software information of the host machine.

This command has no parameters.

Syntax:show system info

Sample Output:

```
IPSManager> show system info
Static hostname: IPSManager
Pretty hostname: NSMAppliance
Icon name: computer-vm
Chassis: vm
Machine ID: 8d0fb74033784c778fb01f7489b237fd
Boot ID: 88ec7375ffec45ae86bd249614ed2b30
Virtualization: vmware
Operating System: MLOS 3.0
Kernel: Linux 4.19.245-1.mlos3.x86_64
Architecture: x86-64
```

show system memory

It displays memory usage of the host machine.

This command has no parameters.

Syntax:show system memory

Sample Output:

```
IPSManager> show system memory
MemTotal: 16828016 kB
MemFree: 10005184 kB
MemAvailable: 15377808 kB
Buffers: 292380 kB
Cached: 5187804 kB
SwapCached: 0 kB
Active: 1732468 kB
Inactive: 4721364 kB
Active(anon): 974492 kB
```

```
Inactive(anon): 8376 kB

Active(file): 757976 kB

Inactive(file): 4712988 kB

Unevictable: 0 kB

Mlocked: 0 kB

SwapTotal: 4095996 kB

SwapFree: 4095996 kB

Dirty: 84 kB

Writeback: 0 kB

AnonPages: 972204 kB

Mapped: 37964 kB

Shmem: 9220 kB

Slab: 280916 kB

SReclaimable: 241516 kB

SUnreclaim: 39400 kB

KernelStack: 2960 kB

PageTables: 5120 kB

NFS_Unstable: 0 kB

Bounce: 0 kB

WritebackTmp: 0 kB

CommitLimit: 12510004 kB

Committed_AS: 850120 kB

VmallocTotal: 34359738367 kB

VmallocUsed: 0 kB

VmallocChunk: 0 kB

HardwareCorrupted: 0 kB

AnonHugePages: 911360 kB

ShmemHugePages: 0 kB

ShmemPmdMapped: 0 kB
```

```
HugePages_Total: 0

HugePages_Free: 0

HugePages_Rsvd: 0

HugePages_Surp: 0

Hugepagesize: 2048 kB

DirectMap4k: 18368 kB

DirectMap2M: 3532800 kB

DirectMap1G: 14680064 kB
```

show system uptime

The **show system uptime** command is used to view number of users and uptime of the Manager.

This command has no parameters.

Syntax:show system uptime

Sample Output:

```
IPSManager> show system uptime

22:42:26 up 6 days, 7:57, 2 users, load average: 0.00, 0.00, 0.00
```

show upgradeHistory

This command displays the Manager upgrade history.

Syntax:show upgradeHistory

Sample Output:

```
IPSManager> show upgradeHistory

Wed Oct 09 10:21:53 UTC 2019: 10.1.7.1

Tue Oct 15 02:42:04 UTC 2019: 10.1.7.2

Thu Oct 17 14:07:39 UTC 2019: 10.1.7.3
```

show temp files

The command displays the files available in the **/temp/** directory.

Syntax:show tmpFiles

Sample Output:

```
IPSManager> show tmpFiles
```

```
total 20

-rw-r--r--. 1 root root 899 Apr 29 08:35 depmod.txt

-rw-r--r--. 1 root root 825 Apr 29 08:35 new-kern-pkg.11995

-rw-rw-r--. 1 root root 390 Apr 29 08:36 mgrinstall.log

drwxr-xr-x. 2 root root 4096 Apr 29 08:40 hsperfdata_root

drwxr-xr-x. 2 admin admin 4096 Apr 29 09:34 hsperfdata_admin

srwxrwxrwx. 1 mysql mysql 0 Apr 29 09:34 mysql.sock
```

show var log

It displays content of the system log file specified in the command.

> **NOTE**
>
> For a list of log files in **/var/log** directory in the Linux based Manager, execute **show var log all** command in the Manager shell.

Syntax:show var log <file name>

Sample Output:

```
IPSManager> show var log audit.log

type=DAEMON_START msg=audit(1566224011.274:5833): op=start ver=2.8.4 format=raw ker-
nel=4.9.124-1.mlos3.x86_64 auid=4294967295 pid=2530 uid=0 ses=4294967295 subj=system_u:system_r:au-
ditd_t:s0 res=success

type=AVC msg=audit(1566224011.259:36): avc: denied { read } for pid=2532 comm="audispd"
name="ld.so.cache" dev="dm-5" ino=785358 scontext=system_u:system_r:audisp_t:s0 tcontext=uncon-
fined_u:object_r:unlabeled_t:s0 tclass=file permissive=1
```

snmp

The SNMP service when enabled in the Linux based Manager allows administrators to view and manage the Linux machine attributes remotely.

> **NOTE**
>
> The service is disabled by default on a fresh installation of the Linux based Manager. You need to issue the **snmp enable** command to enable it.

NOTE

The default configuration present in snmpd.conf file allows you to read limited number of machine attributes. You can modify this file using the **`edit snmpd.conf`** command to view the attributes of your choice. Upon modifying the file, issue the **`snmp restart`** command for the changes to be effective.

NOTE

The default SNMP community string set in the configuration file is **`mlosnsm`**. You can use this string for authentication, or change it through snmpd.conf if you intend to use a different string. Restart the SNMP service upon changing the string.

The **`snmp`** command displays a list of commands in the Manager shell which can be used to perform actions on the SNMP service in the Linux based Manager.

This command has no parameters.

Syntax:`snmp`

Sample Output:

```
IPSManager> snmp

Expected one of

disable Disable snmpd service

enable Enable snmpd service

restart Restart snmpd service

start Start snmpd service

status Show snmpd Status

stop Stop snmpd service
```

snmp disable

This command disables the SNMP service in the Linux based Manager.

This command has no parameters.

Syntax:`snmp disable`

Sample Output:

```
IPSManager> snmp disable

[sudo] password for admin:

Removed symlink /etc/systemd/systed/multi-user.target.wants/snmpd.service
```

snmp enable

This command enables the SNMP service in the Linux based Manager and auto starts the service every time the Manager boots.

This command has no parameters.

Syntax:`snmp enable`

Sample Output:

```
IPSManager> snmp enable

Created symlink from /etc/systemd/system/multi-user.target.wants/snmpd.service to /usr/lib/sys-
temd/system/snmpd.service.
```

snmp list

This CLI command displays a list of all the SNMP commands.

This command has no parameters.

Syntax: `snmp list`

Sample Output:

```
IPSManager> snmp list

disable Disable snmpd service

enable Enable snmpd service

help List available commands with "help" or detailed help with "help cmd".

list Print Comamnd List

restart Restart snmpd service

start Start snmpd Status

status Show snmpd Status

stop Stop snmpd service
```

snmp restart

This command restarts the SNMP service in the Linux based Manager.

This command has no parameters.

Syntax: `snmp restart`

Sample Output:

```
IPSManager> snmp restart

[sudo] password for admin:
```

```
Redirecting to /bin/systemctl restart snmpd.service
```

snmp start

This CLI command starts the SNMP service in the Linux based Manager.

This command has no parameters.

Syntax:`snmp start`

Sample Output:

```
IPSManager> snmp start
[sudo] password for admin:
Redirecting to /bin/systemctl start snmpd.service
```

snmp status

This command displays whether the SNMP service is running in the Linux based Manager.

This command has no parameters.

Syntax: `snmp status`

Sample Output:

```
IPSManager> snmp status
Redirecting to /bin/systemctl status snmpd.service
 snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
Loaded: loaded (/usr/lib/systemd/system/snmpd.service; enabled; vendor preset: disabled)
Active: active (running) since Mon 2021-06-28 18:27:17 UTC; 1 weeks 1 days ago
Main PID: 3686 (snmpd)
CGroup: /system.slice/snmpd.service
3686 /usr/sbin/snmpd -LS0-6d -f
Jun 28 18:27:17 RKG101M6FT systemd[1]: Starting Simple Network Management Protocol (SNMP) Daemon....
Jun 28 18:27:17 RKG101M6FT snmpd[3686]: NET-SNMP version 5.7.2
Jun 28 18:27:17 RKG101M6FT systemd[1]: Started Simple Network Management Protocol (SNMP) Daemon..
Hint: Some lines were ellipsized, use -l to show in full.
```

snmp stop

This command stops the SNMP service in the Linux based Manager.

This command has no parameters.

Syntax:snmp stop

Sample Output:

```
IPSManager> snmp stop

[sudo] password for admin:

Redirecting to /bin/systemctl stop snmpd.service
```

shutdown

This command halts the Manager so you can turn off the Manager Appliance. You can turn off the appliance manually after a minute.

This command has no parameters.

Syntax:shutdown

ssh

This command allows user to create a secure ssh connection from the Linux based Manager to any remote machine.

Syntax:ssh <username>@<remote_machine_ip>

Sample Output:

```
IPSManager> ssh admin@10.x.x.x

FIPS mode initialized

* * *

Authorized users only. Unauthorized users will be prosecuted to the full extent of the law.

* * *

Password:

Last login: Mon Apr 1 10:26:13 2019 from 10.208.15.90

Trying 127.0.0.1...

Connected to 127.0.0.1.

Escape character is 'off'.

Hello, this is zebra (version 0.92a).

Copyright 1996-2001 Kunihiro Ishiguro.

intruShell@NS9500>
```

syslog

The **syslog** command displays the list of commands in Manager shell to perform actions on syslog service in the Linux based Manager.

This command has no parameters.

Syntax:syslog

Sample Output:

```
IPSManager> syslog

Expected one of

restart Restart Syslog service

start Start Syslog service

status Show Syslog Status

stop Stop Syslog service
```

syslog restart

The **syslog restart** is used to restart the syslog service in the Linux based Manager.

This command has no parameters.

Syntax:syslog restart

Sample output:

```
IPSManager> syslog restart

Redirecting to /bin/systemctl restart rsyslog.service
```

syslog start

The **syslog start** command is used to start the syslog service in the Linux based Manager.

This command has no parameters.

Syntax:syslog start

Sample output:

```
IPSManager> syslog start

Redirecting to /bin/systemctl start rsyslog.service
```

syslog status

This command displays whether the syslog service is running in the Linux based Manager.

This command has no parameters.

Syntax:syslog status

Sample Output:

```
IPSManager> syslog status

[sudo] password for admin:

 rsyslog.service - System Logging Service

Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)

Active: active (running) since Mon 2022-09-26 14:55:36 UTC; 1 day 5h ago

Docs: man:rsyslogd(8)

http://www.rsyslog.com/doc/

Main PID: 1544 (rsyslogd)

CGroup: /system.slice/rsyslog.service

1544 /usr/sbin/rsyslogd -n

Sep 26 14:55:36 IPSManager systemd[1]: Starting System Logging Service...

Sep 26 14:55:36 IPSManager rsyslogd[1544]: [origin software="rsyslogd" swVersion="8.24.0-57.mlos3"
x-pid="1544" x-in... start

Sep 26 14:55:36 IPSManager systemd[1]: Started System Logging Service.

Hint: Some lines were ellipsized, use -l to show in full.
```

syslog stop

The **syslog stop** command is used to turn-off the syslog service in the Linux based Manager.

This command has no parameters.

Syntax:syslog stop

Sample Output:

```
IPSManager> syslog stop

Redirecting to /bin/systemctl stop rsyslog.service
```

system config backup

This command takes the operating system configuration files, Manager configuration, and log file backup.

This command has no parameters.

Syntax:system config backup

Sample Output:

```
IPSManager> system config backup

[sudo] password for admin:
```

```
System config backup collected successfully. View the sysConfBackup tar using command 'show files'
```

system config restore

This command restores the operating system configuration files, Manager configuration, and log file backup.

Syntax:`system config restore`

Sample Output:

> **NOTE**
>
> You can either restore the backup from a remote machine or present in the current system.

To restore backup from remote machine:

```
IPSManager> system config restore

Choose one of the below options

1: scp backup tar from remote machine and restore

2: restore the backup tar present on this system

Input [1] or [2] : 1

Enter the IP of the remote machine: 10.2.1.1

Enter the user of the remote machine: admin

Enter the backup tar file's path as on remote machine: /home/admin/sysConfBack-
up_<yyyy>_<mm>_<dd>_<HH>_<MM>_<SS>.tar

FIPS mode initialized

admin@10.2.1.1's password:

sysConfBackup_<yyyy>_<mm>_<dd>_<HH>_<MM>_<SS>.tar100% 138MB 81.8MB/s 00:01

/bin/tar: Removing leading `/' from member names

Backed up logs have been successfully copied to the system. Please execute command show backup log
<all> or <filename> to view the logs

Successfully restored the system configuration
```

To restore backup present on this system:

```
IPSManager> system config restore

Choose one of the below options

1: scp backup tar from remote machine and restore

2: restore the backup tar present on this system
```

```
Input [1] or [2] : 2

Enter the path to the backup tar file: /opt/scpfiles/sysConfBack-
up__<yyyy>_<mm>_<dd>_<HH>_<MM>_<SS>.tar

/bin/tar: Removing leading `/' from member names

Backed up logs have been successfully copied to the system. Please execute command show backup log
<all> or <filename> to view the logs

Successfully restored the system configuration
```

tail

It displays last ten entries of the file specified in the command.

Syntax:`tail <filepath>`

Sample Output:

```
IPSManager> tail /opt/scpfiles/infoLogs_2019_04_02_02_07_07.tar

2019-03-29 01:57:52,582 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.insert
- Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDataFil-
lInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,identity ==> RelevancyInfo-
LookupActor)

2019-03-29 01:57:52,582 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.insert
- Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDataFil-
lInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,Setting of the Relevancy
info lookup actor reference done.)

2019-03-29 01:57:52,582 ERROR [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.ac-
tor.insert - Error(akka.event.Logging$Error$NoCause$,akka://AlertManager/user/AlertManagerSuper-
visorActor/AlertInsertSupervisorActor/AlertDataFillInActor,class com.intruvert.ext.alert.actor.in-
sert.AlertDataFillInActor,Received null Identity message for VM info lookup actor!!)

2019-03-29 01:57:52,582 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.insert
- Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDataFil-
lInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,Setting of the Executable
info lookup actor reference done.)

2019-03-29 01:57:52,582 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.insert
- Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDataFil-
lInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,Received ActorInitialized-
Message message from: VMInfoLookupActor)

2019-03-29 01:57:52,582 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.insert
- Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDataFil-
lInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,actorPath ==> akka://Alert-
Manager/user/AlertManagerSupervisorActor/AlertUpdateSupervisorActor/VMInfoLookupActor)

2019-03-29 01:57:52,582 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.insert
- Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDataFil-
```

```
lInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,identity ==> VMInfoLooku-
pActor)

2019-03-29 01:57:52,583 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.in-
sert - Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDa-
taFillInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,Setting of the TS info
lookup actor reference done.)

2019-03-29 01:57:52,583 INFO [AlertManager-akka.actor.default-dispatcher-22] [] iv.core.actor.in-
sert - Info(akka://AlertManager/user/AlertManagerSupervisorActor/AlertInsertSupervisorActor/AlertDa-
taFillInActor,class com.intruvert.ext.alert.actor.insert.AlertDataFillInActor,Setting of the VM info
lookup actor reference done.)
```

tcpdump

The **tcpdump** command lists data packets transferred and received by the Linux based Manager over the network.

This command has no parameters.

Syntax:`tcpdump`

Sample Output:

```
IPSManager> tcpdump

[sudo] password for admin:

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes

20:48:42.641766 IP IPSManager.test.com.ssh > 10.207.148.169.54517: Flags [P.], s eq
3698902508:3698902672, ack 4112560286, win 501, length 164

20:48:42.642259 IP IPSManager.test.com.45080 > bancorpdc1.corp.nai.org.domain: 1 695+ PTR?
169.148.207.10.in-addr.arpa. (45)

2 packets captured

10 packets received by filter

0 packets dropped by kernel
```

timedatectl

This command allows the user to configure timezone, time, and date.

Syntax:`timedatectl <parameter>`

> **NOTE**
>
> To get a list of parameters for the **timedatectl** command execute **timedatectl -h** command.

top

This command displays the processor activity in the Linux based Manager.

This command has no parameters.

Syntax:top

Sample Output:

```
top - 04:52:18 up 19:18, 1 user, load average: 0.10, 0.08, 0.04

Tasks: 76 total, 1 running, 38 sleeping, 0 stopped, 0 zombie

%Cpu(s): 0.7 us, 0.7 sy, 0.0 ni, 98.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st

KiB Mem : 33622928 total, 25692864 free, 5726976 used, 2203088 buff/cache

KiB Swap: 4095996 total, 4095996 free, 0 used. 27438936 avail Mem

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND

3435 admin 20 0 18.6g 4.6g 33640 S 0.7 14.4 184:09.66 java

1495 root 20 0 0 0 0 I 0.3 0.0 0:00.83 kworker/u2:1-fl

3647 mysql 20 0 1625592 670644 19204 S 0.3 2.0 3:14.48 mysqld

1 root 20 0 46056 7940 5568 S 0.0 0.0 0:10.93 systemd

.....
```

traceroute

This command traceroutes a network host.

Syntax:traceroute <ipv4 address>

Sample Output:

```
IPSManager> traceroute 10.208.15.64

traceroute to 10.208.15.64 (10.208.15.64), 30 hops max, 60 byte packets

1 * * *

2 * * 10.208.15.64 (10.208.15.64) 0.158 ms
```

unzip

This command unzips a zipped file and saves it at **/opt/scpfiles**.

Syntax: unzip <filepath_of_the_file_to_be_unzipped>

The following table lists the parameters for **unzip** command.

Parameters	Description
filepath_of_the_file_to_be_unzipped	File path of the file to be unzipped in the Linux machine

Sample Output:

```
IPSManager> unzip /opt/scpfiles/testZip.zip

Archive: /opt/scpfiles/testZip.zip

extracting: test1
```

upgrade

The **upgrade** command is used to download and install upgrade bundles.

Syntax:upgrade

```
Choose one of the below options

1: scp setup from remote machine and install

2: install the setup present on local machine

Input [1] or [2] : <Select the upgrade method>
```

If you select **1**:

```
Enter the IP of the remote machine: <remote_machine_ip>

Enter the user of the remote machine: <remote_machine_user>

Enter the setup file's path as on remote machine: <Filepath of the upgrade file in the remote machine>
```

If you select **2**:

> **NOTE**
>
> For using option 2, you must have the upgrade file readily available in the Linux based Manager server.

```
Enter the path to the setup.bin file: <upgrade_file_filepath>
```

Parameters	Description
Select the upgrade method	Enter **1** to scp the upgrade file from remote machine and install or enter **2** to install the upgrade file available on the local machine.
remote_machine_ip	Enter the IP address of the remote machine where the upgrade file is saved.
remote_machine_user	Enter the login username of the remote machine where the upgrade file is saved.

Parameters	Description
Filepath of the upgrade file in the remote machine	Enter the file path of upgrade file in the remote machine.
upgrade_file_filepath	Enter the file path of upgrade file in the Linux based Manager server.

NOTE

On execution, the **upgrade** command requests certain user input and permissions. Make sure you provide appropriate input and permissions for successful upgrade.

WARNING

Manager services will not be available during the upgrade process.

uvscan

This command is used to perform virus scans on the Linux operating system.

Syntax: uvscan [object1] [object2...] [option1] [option2...]

NOTE

To get a list of parameters for the **uvscan** command, execute **uvscan --help** command.

Sample Output:

```
IPSManager> uvscan --VERSION

McAfee VirusScan Command Line for Linux64 Version: x.x.x.x

Copyright (C) 2020 McAfee, Inc.

(xxx) xxx-xxx LICENSED COPY - January 06 2023

AV Engine version: xxxx.xxxx for Linux64.

Dat set version: xxxx created Dec 8 2020

Scanning for 668683 viruses, trojans and variants.
```

vgextend

This command helps in extending volume groups in the Linux based Manager.

Syntax:vgextened <parameters>

watchdog

It displays commands in Manager shell to perform actions on watchdog service in the Manager.

This command has no parameters.

Syntax:`watchdog`

Sample Output:

```
IPSManager> watchdog

Expected one of

restart Restart Watchdog Service

start Start Watchdog Service

status Show Watchdog Status

stop Stop Watchdog Service
```

watchdog start

The **`watchdog start`** command is used to start watchdog service in the Manager.

This command has no parameters.

Syntax:`watchdog start`

Sample Output:

```
IPSManager> watchdog start

Redirecting to /bin/systemctl start watchdog.service
```

watchdog status

The **`watchdog status`** command displays whether the watchdog service is enabled or disabled in the Manager.

This command has no parameters.

Syntax:`watchdog status`

Sample Output:

```
IPSManager> watchdog status

 watchdog.service - IPS Watchdog Daemon

Loaded: loaded (/etc/systemd/system/watchdog.service; enabled; vendor preset: disabled)

Active: active (running) since Mon 2022-09-26 14:55:36 UTC; 5h 38min ago

Process: 1539 ExecStart=/opt/IPSManager/App/bin/watchdog start (code=exited, status=0/SUCCESS)

Main PID: 1549 (sh)

CGroup: /system.slice/watchdog.service

1549 sh /opt/IPSManager/App/bin/start_watchdog.sh
```

```
1574 /opt/IPSManager/App/jre/bin/java -cp /opt/IPSManager/App/ext/ivcoresvcs.jar:/opt/IPSManag-
er/App/lib/3rdpa...

Sep 26 14:55:36 IPSManager systemd[1]: Starting IPS Watchdog Daemon...

Sep 26 14:55:36 IPSManager systemd[1]: Started IPS Watchdog Daemon.
```

watchdog stop

The **watchdog stop** command is used to stop watchdog service in the Manager.

This command has no parameters.

Syntax:`watchdog stop`

Sample Output:

```
IPSManager> watchdog stop

Redirecting to /bin/systemctl stop watchdog.service
```

Best Practices

Introduction

Trellix IPS is a combination of network appliances and software, built for the accurate detection and prevention of intrusions and network misuse.

We recommend that you follow some of the best techniques and tips to use Trellix IPS most effectively. This can save considerable time during the installation and tuning process of the system.

Following chapters outline the best practices for Trellix IPS.

Pre-installation checklist

There are some important tasks that you should consider before Trellix IPS Manager software installation. For more information, see the *Trellix Intrusion Prevention System Installation Guide*.

Manager version and its compatible Sensor software versions

Every update release consists of at least one new feature, enhancements, and fixes. It requires changes from both the Manager and Sensor components. It is recommended that the Manager software version is always higher or more recent than the Sensor Software version as the Manager manages the Sensors. The Manager handles the latest and the older Sensor software versions. This software version compatibility is maintained by segment version numbering that the Manager sends to Sensors as part of the compiled configuration. So, maintaining compatible software versions is suggested.

Refer the following table to for compatible Manager and Sensor software versions.

Release Version	Manager	NS-series	Virtual IPS
10.1	10.1.7.4	10.1.5.3, 10.1.5.5	NA
	10.1.7.7	10.1.5.41	10.1.7.1
	10.1.7.29	10.1.5.64	10.1.7.42
	10.1.7.24 (Public Cloud)	NA	10.1.7.33
	10.1.7.35	10.1.5.75	10.1.7.51
	10.1.7.25 (Public Cloud)	NA	10.1.7.34
	10.1.7.40	10.1.5.92	10.1.7.65
	10.1.7.44	10.1.5.106 (NS3x00, NS3500, NS5x00, NS7x00, NS7500, NS9x00) 10.1.5.107 (NS7x50, NS9500)	10.1.7.86
	10.1.7.50	10.1.5.116	10.1.7.96
	10.1.7.50.2	NA	NA
	10.1.7.55	10.1.5.153	10.1.7.123

Release Version	Manager	NS-series	Virtual IPS
	10.1.7.61	10.1.5.170	10.1.7.135
	10.1.7.65	10.1.5.190	10.1.7.155
	10.1.7.66 (Public Cloud)	NA	10.1.7.156
	10.1.7.66.3	NA	NA
	NA	10.1.5.202 (NS3x00, NS3500, NS5x00, NS7x00, NS7500, NS9x00) 10.1.5.204 (NS7x50, NS9500)	NA
	10.1.7.66.11	NA	NA
11.1	11.1.7.3	11.1.5.2	11.1.7.1
	11.1.7.3.5	NA	NA
	11.1.7.26	11.1.5.22	11.1.7.22
	11.1.7.41	11.1.5.44	11.1.7.44
	11.1.7.41.2	NA	NA
	11.1.7.56	11.1.5.56 (NS3x00, NS3500, NS5x00, NS7x00, NS7500, NS9x00) 11.1.5.57 (NS7x50, NS9500)	11.1.7.56
	11.1.7.71	11.1.5.72	11.1.7.72
	11.1.7.x	11.1.5.x	11.1.5.x

NOTE

IPS-VM5000 is introduced with the Virtual IPS Sensor software version 11.1.7.44. Any prior version listed in the table is associated with IPS-VM600 alone.

Cabling best practices

It is a common practice to physically cable the monitoring ports, only after the Sensor has been fully configured.

In other words, most administrators cable the console and management ports, use those connections to configure the solution, and physically introduce the Sensor into the scanning process once the proper scanning policies are in place, the monitoring ports have been configured, the latest signature set has been downloaded, and so on.

Additionally, in the most security-conscious environments, or those with congestion problems, a private network is often used to connect the Sensor management ports to the Manager. This is another best practice in terms of cabling the Sensors.

Hardening the MariaDB installation for Windows platform

This section describes methods for hardening your MariaDB installation.

Introduction

Manager implementation varies across different environments. The Manager server's positioning in the network, both physically and logically, may influence specific remote access and firewall configuration requirements.

The following best practices are intended to cover the configurable features that can impact the security of Manager. This information should be used in combination with the Trellix Intrusion Prevention System Release Notes and the rest of the documentation set.

Following are Trellix's recommendations at a high level:

- Install a desktop firewall on the server and open the proper ports.
- Harden the MariaDB installation.
- Harden the Manager host.

Install a desktop firewall

It is recommended that you operate a desktop firewall on the Manager server. Certain ports are used within Trellix IPS. Some of these required for Manager - Sensor and Manager client-server communication. All remaining unnecessary ports should be closed. The ports used by Trellix IPS are listed in Install a desktop firewall.

Harden the MariaDB installation

Complete the following steps to harden the MariaDB installation.

Ensure the command prompt used for making changes to database tables stays opened in the MariaDB shell until validation is completed.

This is necessary to enable you to rollback the changes in case you need to. Rollback procedures are shown at the end of this section.

Use another command prompt window, where necessary, to validate the hardening changes you have made.

Remove test database

Perform the following steps to remove the 'test" database from the server.

1. Log in to the MariaDB prompt and execute the command to enter the **mysql** schema.	`MariaDB [none]> use mysql;`
2. Backup db table to db_backup before changing it.	`MariaDB [mysql]> create table db_backup as select * from db;`
3. Validate that the backup table was created and row count matches that of the mysql.db table.	`MariaDB [mysql]> select count(*) from db_backup;`
4. Check all the databases on the Manager server.	`MariaDB [mysql]> show databases;`
5. Remove the test db.	`MariaDB [mysql]> drop database test;`

6. The test database should no longer be listed.	`MariaDB [mysql]> show databases;`

Remove local anonymous users

Perform the following steps to remove local anonymous users:

1. Look for blank entries for user.	`MariaDB [mysql]> select host,db,user from db;`
2. Remove anonymous access to databases.	`MariaDB [mysql]> update db set host="localhost" where user="";`
3. Remove anonymous/blank accounts.	`MariaDB [mysql]> flush privileges;`
4. Validate that "localhost" replaced % entry under the host column. You will also notice that you now need to qualify username and password on the local machine to get into MariaDB prompt.	

Remove remote anonymous users

To remove remote anonymous users, you harden CLI access for MariaDB users by forcing the requirement for a username and password to get into the MariaDB shell. The process to do so is as follows.

1. Log in to MariaDB prompt and execute the command to enter the **mysql** schema.	`MariaDB [none]> use mysql;`
2. Back up the user table to user_backup before changing it.	`MariaDB [mysql]> create table user_backup as select * from user;`
3. Validate that the backup table was created and row count matches that of the mysql.db table.	`MariaDB [mysql]> select count(*) from user_backup;`
4. List all users and hosts.	`MariaDB [mysql]> select user,host from user;`
5. Remove anonymous/blank accounts.	`MariaDB [mysql]> delete from user where user="";`
6. Validate that the rows with blank user columns have been removed.	`MariaDB [mysql]> select user,host from user;`

Secure MariaDB remote access

This section provides two options for removing remote access.

- Remove individual users' remote access.
- Remove ALL remote access (Recommended).

Removal of individual user's remote access

Do ONE of the following:

- Remove admin (Trellix IPS user) remote access.

  ```
  MariaDB [mysql]> delete from user where host!='localhost' and user='admin';
  ```

(The admin user cannot login remotely; however, Manager root can. Use the second command prompt window to validate.)

```
MariaDB [mysql]> flush privileges;
```

- Remove root remote access (Recommended minimum action).

  ```
  MariaDB [mysql]> delete from user where host!='localhost' and user='root';
  ```

  This ensures that the root user cannot login remotely. Manager user, however, can log in remotely. Use the second command prompt window to validate.

  ```
  MariaDB [mysql]> flush privileges;
  ```

Remove ALL remote access

```
MariaDB [mysql]> delete from user where host!='localhost';
```

ALL user access is disabled including Manager users from remote host(s).

Use another command prompt window to validate. You can ONLY log in to the MariaDB command prompt on the Manager server by qualifying username, password, and db. For example: **`mysql -uadmin -pXXX lf`**.

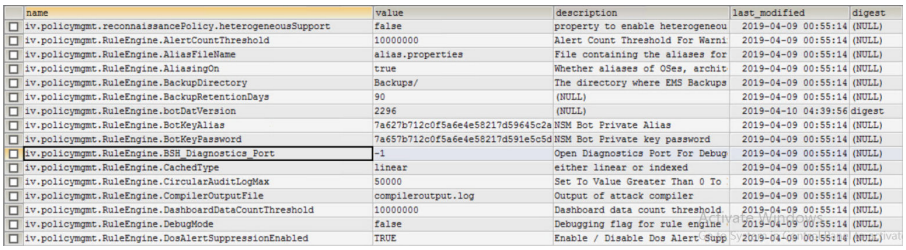
How to roll back your changes

If you need to roll back your changes, use the following commands:

- To roll back changes made to the mysql.db table from the mysql.db_backup table:
  - **`MariaDB [mysql]> rename table db to db_1;`**
  - **`MariaDB [mysql]> alter table db_backup engine=MyISAM;`**
  - **`MariaDB [mysql]> rename table db_backup to db;`**
  - **`MariaDB [mysql]> flush privileges;`**
- To roll back changes made to the "mysql.user" table from mysql.user_backup table:
  - **`MariaDB [mysql]> rename table user to user_1;`**
  - **`MariaDB [mysql]> rename table user_backup to user;`**
  - **`MariaDB [mysql]> flush privileges;`**

Removal of debug shell at port 9001

In addition to denying traffic over port 9001 and 9002 (as per Install a desktop firewall), the debugging shell that runs on port 9001 can be disabled by modifying the value of the **iv.policymgmt.RuleEngine.BSH_Diagnostics_Port** record in the **iv_emspro-perties** table. To disable the port, set the value in the field called "value" = -1



name	value	description	last_modified	digest
iv.policymgmt.reconnaissancePolicy.heterogeneousSupport	false	property to enable heterogeneou	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.AlertCountThreshold	10000000	Alert Count Threshold For Warni	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.AliasFileName	alias.properties	File containing the aliases for	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.AliasingOn	true	Whether aliases of OSes, archit	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.BackupDirectory	Backups/	The directory where EMS Backups	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.BackupRetentionDays	90	(NULL)	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.botDatVersion	2296	(NULL)	2019-04-10 04:39:56	digest
iv.policymgmt.RuleEngine.BotKeyAlias	7a627b712c0f5a6e4e58217d59645c2a	NSM Bot Private Alias	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.BotKeyPassword	7a657b712c0f5a6e4e58217d591e5c5d	NSM Bot Private key password	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.BSH_Diagnostics_Port	-1	Open Diagnostics Port For Debug	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.CachedType	linear	either linear or indexed	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.CircularAuditLogMax	50000	Set To Value Greater Than 0 To	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.CompilerOutputFile	compileroutput.log	Output of attack compiler	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.DashboardDataCountThreshold	10000000	Dashboard data count threshold	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.DebugMode	false	Debugging flag for rule engine	2019-04-09 00:55:14	(NULL)
iv.policymgmt.RuleEngine.DosAlertSuppressionEnabled	TRUE	Enable / Disable Dos Alert Supp	2019-04-09 00:55:14	(NULL)

Other best practices for securing Manager

- Use a clean, dedicated machine for the Manager server and perform a fresh installation of the Manager software, including the installation of the embedded database. No other software should be installed on the server, with the exception of a host-based firewall as described above.
- Make sure the PC is in an isolated and physically secure environment.
- Disallow access to the installation directory and its sub-directories to anyone other than authorized administrators. For more information on restricting users' folder access, refer to the Microsoft Knowledge Base article here.

Hardening the Manager Server for Windows platform

Implementation of Manager varies from environment to environment. The Manager's physical and logical position in the network influences specific remote access and firewall configuration requirements. The following best practices on managing configurable features on Manager impacts the security of Manager.

NOTE

These steps are applicable to Windows Server 2016, Windows Server 2019, and Windows Server 2022 editions.

Pre-installation

Use a dedicated machine for the Manager server and then install Manager and the embedded database. Other than the host-based firewall, no other software should be installed on the server. Before installation of Manager do the following:

- Ensure that the server is located in a physically secure environment.
- Connect the server on a protected or isolated network.
- If the hard disk is old, use fdisk (a command line utility) to remove all partitions and create new partitions.

Installation

Installation of Manager should be performed as follows:

- Install either the English or Japanese version of the Windows Server.
- Use NTFS on all partitions.

Post-installation

After installation of Manager, perform the following installations:

- Install the latest Windows Server patches, service packs, and hot fixes from Microsoft.
- Install a Virus Scanner and update the signatures.

> **NOTE**
>
> Exclude "Trellix IPS Manager" and "MariaDB" directories from being scanned.

Also keep a check on the following:

- Minimize the number of Windows roles and features that are installed.
- Uninstall applications that are not necessary.

Disable non-required services

Disable the following services:

- DHCP Client
- FTP
- Print spooler
- Remote access auto connection manager
- Remote procedure call locator
- Remote registry
- Server
- TCP/IP NetBIOS helper service
- Telephony service.

> **NOTE**
>
> Enable these services only if it is absolutely required.

Set system policies

Ensure to set the following system policies:

- Implement the System key and strong encryption of the password database by running SYSKEY.EXE
- Use Microsoft security compliance toolkit or set local security policy.
- Display legal notice at during interactive logon window.
- Do not display username that was used earlier to login.
- Disable Posix.
- Clear virtual memory page file during shutdown.
- Disable autorun.
- Disable LMHOSTS lookup while setting the advanced TCP/IP settings.

Set user policies

Make sure to set the following user policies:

- Rename the administrator account.
- Disable guest account.
- Passwords should be at least 8 ASCII characters.
- Enable locking of screensaver.

Set the desktop firewall

It is recommended that a desktop firewall operates on the Manager server. The following ports are required for Manager-Sensor communication.

NOTE

Ensure that there are no other open ports using a scanning tool.

Port	Source	Destination	Description	Comments
443	Client	Manager	HTTPS	Communication from client to Manager **NOTE** The Manager is accessible via **`https://< hostname or host-IP>`**.
443	Manager	NTBA Appliance	Command Channel (TCP)	Manager to NTBA Appliance. Communication is bidirectional
3306	Internal	Manager	Manager Database (MySQL or MariaDB)	Internal to Manager; can be used externally to connect to the database
4166	Manager	Sensor	Command Channel (UDP)	Source port for IPv6 Manager to Sensor Communication (Manager Java 1.7u45 and later). Communication between Sensor and Manager is bidirectional.
4167	Manager	Sensor	Command Channel (UDP)	Source port for IPv4 Manager to Sensor Communication. Communication between Sensor and Manager is bidirectional.
8005	Internal	Manager	Tomcat Shutdown Port (TCP)	Tomcat uses this port to listen for shutdown hook
8007	Internal	Manager	Tomcat AJP 12 Port (TCP)	Internal to Manager
8009	Internal	Manager	Tomcat AJP 13 Port (TCP)	Internal to Manager
8500	Manager	Sensor	Command Channel (UDP)	Communication between Sensor and Manager is bidirectional
8501	Sensor	Manager	Install Port/Channel (TCP)	Communication between Sensor and Manager is bidirectional

Port	Source	Destination	Description	Comments
8502	Sensor	Manager	Alert Channel (Control Channel) (TCP)	Communication between Sensor and Manager is bidirectional
8503	Sensor	Manager	Packet Log Channel (TCP)	Communication between Sensor and Manager is bidirectional
8504	Sensor	Manager	File Transfer Channel (TCP)	Communication between Sensor and Manager is bidirectional
8506	Sensor	Manager	Install channel (TCP) (2048-bit)	Communication between Sensor and Manager is bidirectional
8507	Sensor	Manager	Alert channel (TCP) (2048-bit)	Communication between Sensor and Manager is bidirectional
8508	Sensor	Manager	Packet log channel (TCP) (2048-bit)	Communication between Sensor and Manager is bidirectional
8509	Sensor	Manager	Bulk file transfer channel for 2048-bit certificates (TCP)	Communication between Sensor and Manager is bidirectional
8510	Sensor	Manager	Bulk file transfer channel for 1024-bit certificates (TCP)	Communication between Sensor and Manager is bidirectional
8551	Internal	Manager	Lumos Nameserver (TCP)	Internal to Manager (RMI/IIOP)
8552	Internal	Manager	JONAS Nameserver (TCP)	Internal to Manager (RMI)

NOTE

- Ports 8501 to 8503, 8510 use SHA256 signed 2048 bit key length Self-Signed certificate.
- Ports 8506 to 8509 use SHA256 signed 2048 bit key length CA-Signed certificate.

If you configure Email Notification or SNMP Forwarding on the Manager, and have a firewall between the Manager and SMTP or SNMP Server, allow the following ports:

Port	Description	Communication
25	SMTP port	Communication from Manager to SMTP server
162	SNMP forwarding	Communication from Manager to SNMP server

IMPORTANT

You must disable other web services before you install the Manager. The Manager server must integrate with the Apache server that's shipped with the Manager installation package. If other web services that use port 80 and 443 aren't disabled, the Manager installation fails. The failure happens because the Manager isn't able to run the Apache server.

Ports used by the Sensor

Port	Description	Communication
22	SSH	SSH connection for command-line access to Sensor and Secure Copy from the Sensor to an SCP server for a manual load image or load configuration.

Ports used for lookups and updates

Port	Source	Destination	Comments
80 TCP	Manager	download.nai.com	For downloading Botnet Detectors
443 TCP	Sensor	nsp.rest.gti.trellix.com	Trellix GTI File Reputation query
443 TCP	Manager/Sensor	nsp.repl.gti.trellix.comlist.smartfil-ter.com	Trellix GTI IP/URL reputation query
443 TCP	Manager (MLOS only)	download.nai.com	For downloading Antivirus DAT Signatures
443 TCP	Manager	nspupdate.trellix.com	IPS updates (can also be downloaded out-of-band and applied manually)
443 TCP	Manager	nsp.repl.gti.trellix.com	Trellix GTI botnet detectors update; GTI partici-pation information
443 TCP	Sensor	To view the latest hostnames/URLs, see KB65496	Gateway Anti-Malware engine (GAM) downloads
443 TCP	Manager	iam.skyhigh.cloud iam-rs.skyhigh.cloud telemetry.skyhigh.cloud telemetry.trellix.com up-cloud.fireeye.com/fenet/notifica-tion	IPS Manager Product Registration, Activation, and Telemetry
443 TCP	Manager/Sensor	feapi.marketplace.apps.fireeye.com	For IVX Cloud communication

Third-party communications

In addition to the communication channels between the components of Trellix IPS, other communications can take place with third-party systems. These third-party systems include external syslog servers, SNMP monitoring systems, and authentication services.

Port/Protocol	Source	Destination	Purpose
25 TCP	Manager	$smtp-mta-server	Email notifications
49 TCP	Sensor	$tacacs+-server	TACACS+ based authentication to Sensor for command-line interface
69 UDP	Sensor	$tftp-server	TFTP server used for loadimage/netboot to install/update Sensor soft-ware
162 UDP	Manager	$snmp-server	SNMP trap notifications

Port/Protocol	Source	Destination	Purpose
389 TCP	Manager	$ldap-server	LDAP-based authentication to IPS Manager for GUI client
514 TCP/UDP	Manager	$syslog-server	Notifications via syslog, standard UDP, or optionally TCP
636 TCP	Manager	$ldaps-server	LDAPS-based authentication to IPS Manager for GUI client
1812 UDP	Manager	$radius-server	RADIUS-based authentication to IPS Manager for GUI client

Ports used for Network Threat Behavior Analysis (NTBA) communications

NTBA Appliances are similar to Sensors. However, they provide functionality focused on analyzing network flows which support overall analysis

Port	Source	Destination	Purpose
22 TCP	Any	NTBA	SSH connection for command-line access to Sensor
22 TCP	NTBA	$netflow-exporter	Router ACL channel
53 UDP	NTBA	$dns-server	DNS queries
80 TCP	NTBA	tunnel.web.trustedsource.org list.smartfilter.com	GTO database download
111 TCP/UDP	NTBA	$backup-server	NFS (optional) portmapper, for backups
137 UDP	NTBA	<any>	NetBIOS lookups
161 UDP	NTBA	$netflow-exporter	SNMP queries (2c/3)
443 TCP	NTBA	tunnel.web.trustedsource.org	Trellix GTI IP reputation query
443 TCP	NTBA	tau-usa.mcafee.com	Gateway Anti-Malware engine (GAM) downloads
443 TCP	NTBA	tau.mcafee.com	Antimalware downloads
445 TCP	NTBA	$backup-server	CIFS backups (optional)
2049 TCP	NTBA	$backup-server	NFS (optional) for backups
8444 TCP	NTBA	ePO	For certificate signing
8501 TCP	NTBA	Manager	Install/control channel
8502 TCP	NTBA	Manager	Alert channel
8504 TCP	NTBA	Manager	File transfer channel
8505 TCP	Sensor	NTBA	IPS channel (SSL AES-128 SHA-1)
9008 UDP	EIA	NTBA	EIA service (DTLS)
9996 UDP	$netflowexporter	NTBA	NetFlow channel

NOTE

Some of the ports and protocols listed are optional; their use depends on your specific configuration.

Ports used for ePolicy Orchestrator communications

Port	Source	Destination	Comments
3306 TCP	ePO	Manager	[Manager to ePO integration] Database connection to enable Maanger-related dashboards in ePO console
8443 TCP	Manager	ePO	[ePO to Manager integration] Manager pull/query of host information from ePO; requires Trellix IPS extension installation on ePO

Ports used for Trellix IPS Central Manager communications

Port	Source	Destination	Comments
443 TCP	Manager	Central Manager	Uses HTTPS protocol
443 TCP	Central Manager	Manager	Uses HTTPS protocol

Ports used for SIEM Enterprise Security Manager (ESM) communications

Port	Source	Destination	Comments
443 TCP	ESM	Manager	Access to Manager data
3306 TCP	ESM	Manager	MariaDB queries

Ports used for Trellix Intelligent Sandbox communications

Port	Source	Destination	Comments
443 TCP	Manager	Intelligent Sandbox	REST API communication
8505 TCP	Sensor	Intelligent Sandbox	Communication channel for Sensor data

Ports used for IVX communications

Port	Source	Destination	Comments
443 TCP	Manager	IVX/IVX Cloud	IVX REST API communication
443 TCP	Sensor	IVX/IVX Cloud	IVX REST API communication

Ports used for Trellix Network Investigator communications

Port	Source	Destination	Comments
443 HTTPS	Manager	Network Investigator appliance or cluster	Export alerts to Network Investigator
443 HTTPS	Sensor	Network Investigator appliance or cluster	Export flow and metadata to Network Investigator

Ports used for TIE/DXL communications

Port	Source	Destination
443 TCP	Sensor	ePO
8081 TCP	ePO	Sensor
8443 TCP	Sensor	ePO

Port	Source	Destination
8883 TCP	Sensor	DXL Broker

NOTE

If you have multiple DXL brokers, the Sensor connects to each of them on 8883 TCP. If the DXL broker is deployed on the ePO server, the Sensor connects to the ePO server on 8883 TCP.

Ports used for Trellix Logon Collector communications

Port	Source	Destination	Comments
61641	Manager	TLC Server	JMS communications between the Logon Collector and Manager

NOTE

For more information on the ports and traffic destinations used by Trellix IPS, refer to KB59342.

Configure audit events

Set the following events to be audited:

- Audit account logon events
- Audit account management
- Audit logon events
- Audit object access (Failure)
- Audit policy change (Success)
- Audit privilege use (Failure)
- Audit system events (Success)

Configure for vulnerability issues

It is recommended that you configure your Manager server to fix the following vulnerability issues:

Vulnerability message	Port	Configuration Changes
X.509 Certificate Subject CN Does Not Match the Entity Name (certificate-common-name-mis-match)	NA	Replace self-signed SSL certificate with a CA-signed SSL certificate.

Vulnerability message	Port	Configuration Changes
SMB signing disabled (cifs-smb-signing-disabled) SMB signing not required (cifs-smb-signing-not-required)	NA	Configure SMB signing for Windows. SMB signing is enabled on the server side if the following conditions are true: • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Parameters\Enablesecuritysignature registry value is set to 1,or if the corresponding Group Policy setting is enabled. • HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanmanserver\Parameters\Requiresecuritysignature registry value is set to 0,or if the corresponding Group Policy setting is disabled.
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32) (ssl-cve-2016-2183-sweet32)	NA	• Remove the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher as it is insecure. • Disable support for TLSv1.0 & TLSv1.1
TLS/SSL Server Supports RC4 Cipher Algorithms (CVE-2013-2566) (rc4-cve-2013-2566)	NA	• Remove the TLS_RSA_WITH_RC4_128_MD5 and the TLS_RSA_WITH_RC4_128_SHA ciphers as they are insecure. • Disable support for TLSv1.0 & TLSv1.1

Vulnerability message	Port	Configuration Changes
TLS/SSL Server Supports The Use of Static Key Ciphers (ssl-static-key-ciphers)	NA	• Remove the following insecure ciphers as they are insecure. **TLS 1.0 ciphers:** • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_RSA_WITH_RC4_128_SHA **TLS 1.1 ciphers:** • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_RC4_128_MD5 • TLS_RSA_WITH_RC4_128_SHA **TLS 1.2 ciphers:** • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_RC4_128_MD5 • TLS_RSA_WITH_RC4_128_SHA • Disable support for TLSv1.0 & TLSv1.1
TLS Server Supports TLS version 1.1 (tlsv1_1-enabled)	NA	Disable support for TLSv1.0 & TLSv1.1
Diffie-Hellman group smaller than 2048 bits (tls-dh-prime-under-2048-bits)	Na	• Remove the following insecure ciphers as they are insecure. **TLS 1.0 ciphers:** • TLS_DHE_RSA_WITH_AES_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits • TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits **TLS 1.1 ciphers:** • TLS_DHE_RSA_WITH_AES_256_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits • TLS_DHE_RSA_WITH_AES_128_CBC_SHA with a Diffie-Hellman prime modulus of 1024 bits • Disable support for TLSv1.0 & TLSv1.1

Vulnerability message	Port	Configuration Changes
TLS/SSL Server Is Using Commonly Used Prime Numbers (tls-dh-primes)	NA	Disable support for TLSv1.0 & TLSv1.1
ICMP timestamp response (generic-icmp-timestamp)	443 8501 8502 8503 8506 8507 8508	Enable Windows firewall and disable the ICMP timestamp response. To do this, perform the following steps: 1. Enable the windows firewall by selecting the **on (recommended)** option. 2. Open a command prompt and enter **`netsh firewall set icmpsetting 13 disable`** 3. Allow inbound and outbound communication on port 443 and all the ports used by the Manager to communicate with outside devices like Sensors, ePO, and so on. For communicating with the Sensor, the Manager uses ports 8501-8503 and 8506-8508. **CAUTION** If you do not create firewall rules with proper port information, applying this solution might break your existing communication.
TLS/SSL Server Supports 3DES Cipher Suite (ssl-3des-ciphers)	NA	• Remove the following insecure ciphers as they are insecure. **TLS 1.0 ciphers:** • TLS_RSA_WITH_3DES_EDE_CBC_SHA **TLS 1.1 ciphers:** • TLS_RSA_WITH_3DES_EDE_CBC_SHA **TLS 1.2 ciphers:** • TLS_RSA_WITH_3DES_EDE_CBC_SHA • Disable support for TLSv1.0 & TLSv1.1
SSL Certificate Signed Using Weak Hashing Algorithm	3389	Contact the Certificate Authority to issue a certificate signed with strong hashing algorithm.

NOTE

- The exact vulnerability message might differ based on the Vulnerability Scanner you use.
- Most of the configuration changes require changes to the Windows registry and you should be careful when changing the registry values. For general information on changing the Windows registry values, see the Microsoft Knowledge Base article 310516.

Hardening the Manager Server for the Linux platform

During the Manager installation, configurational scripts are run automatically to harden the operating system as a best practice. After the configuration, only the ports required for communication between the Manager and point integrations, such as Sensor, ePolicy Orchestrator, and Alert Service, are open. The communication on the non-essential ports is disabled.

Reconfiguration of IP tables, and ports used by the Manager and Sensor, integrated products, and other third-party applications for communications

For more information on the IP Table configuration after running the reconfiguration script, ports and traffic destinations as used by the Manager and Sensor, and ports used by third-party applications and integrated products, such as NTBA, Intelligent Sandbox, ePO, and IVX, refer to the section Set the desktop firewall (page 2276).

For information on how to disable or enable firewall ports in MLOS, refer to the section *Steps to disable or enable ports on firewall in MLOS* in the *Trellix Intrusion Prevention System Manager Appliance Product Guide*.

Database maintenance best practices

Database maintenance best practices

Trellix recommends the following best practices for database backup and tuning:

- Perform regular manual backups of your database using the Backup feature in the Manager software. Your configuration tables are saved by default once a week on Sunday.
- Database backups are cumulative and the size of a backup file can become quite large. Perform regular file maintenance to prevent disk space issues.

  CAUTION

  A database left untuned can lead to performance issues over time.

- Online database tuning operation causes the creation of temporary alerts and packet log tables; if you are using an agent that queries the database, your agent may attempt to interact with these tables during tuning.

  TIP

  During tuning, the SQL query might return empty results. If this occurs, simply retry the query once the tuning is complete.

  Further information on the impact of online database tuning of the Manager database will be sent to the third-party vendors that are directly accessing this database. If you have any specific questions, contact Technical Support. Also note that there is no change in database SQL query behavior if online database tuning is disabled.

- Make a regular practice of defragmenting the disk of the Manager server, as disk fragmentation can lead to database inefficiency.

> **TIP**
>
> Ensure at any point of time the free space available in the database directory is at least one and a half times that of the maximum size occupied by a table (generally **Event Tables** and **Trend Tables**).

- When scheduling certain Manager actions (backups, file maintenance, archives, database tuning), set a time for each that is unique and is a minimum of an hour after/before other scheduled actions. Do not run scheduled actions concurrently.

Backup of data and configurations

For the back up of Trellix IPS data and configurations, following best practices are recommended:

- Back up Manager data either within the Manager server (`%programfiles%\Trellix\IPS Manager\App\Backups` folder) or preferably on any external media.
- Back up all information, including configurations, alerts, and audits.
- Implement a schedule for backups using the Backup scheduler. Backing up config tables weekly is recommended. (Be sure to schedule this at a time when other processes will not be running concurrently.)
- As the **All Tables** and **Event Tables** options can be rather large in size (depending upon the amount of alert data in the database) these types of backups should be saved off the Manager server.
- Saving the **All Tables** settings on a monthly basis is strongly recommended.
- Protect backups from tampering by creating a digital fingerprint of the file using a hash function such as MD5 or SHA-1.
- Test restoration of backups periodically to ensure that a backup was successful and valid. The best way to do this is to perform a "test" restore of the backup on a secondary, non-production Manager.
- The **Config Tables** option backs up only tabled information relating to configured tasks. This option is enabled by default to occur every Sunday night. This is set within the Backup Scheduler action.
- Save actual configurations of Sensors (not just the config tables) using the Export option under the **Sensor_Name** tab. This creates an XML file (no attempt to read this file should be made) that can be imported to any Sensor of the same type in the future. Save actual Sensor configurations once a week.

Alerts and Disk space maintenance best practices

Disk space maintenance is an important task that must be completed to ensure efficient running of the Manager.

In order to develop best practices for database maintenance, it is important to understand the lifecycle of an alert.

Archiving alerts

Archive your alerts and packet logs regularly, using the Data Archival feature. Trellix recommends that you archive your alert data monthly, and that you discard alert and packet log information from your database every 90 days to manage your database size. Note that there is currently a 4 GB size limitation for a single archive file.

Scripts for disk space maintenance

If you have a large amount of data and wish to do your tuning offline, it is a best practice to use the purge and database tuning features in the **dbadmin.bat** utility. To do this, you must stop the Manager and run the scripts.

A best practice suggestion is to wait for 97 days of data and then, on a recurring 7-day period, run the purge and the database tuning features in the **dbadmin.bat** utility.

Using File Maintenance Scheduler

Databases can be substantially overloaded with all alerts, packet logs, any incident reports that have been generated, and audit and fault logs. Maintenance of this data can be accomplished automatically using the File Maintenance scheduler.

If automatic File Maintenance is used to delete alert and packet log data it is recommended that a large value, such as 90 (as in 90 days), is entered in the "Scheduled Deletion" column for the Alert & Packet Log Data option. This allows for long-term analysis of alerts and logs without overloading your database with millions of alerts, which may affect long-term and overall database performance. By setting the value to 90 days, all alerts and packet logs older than 90 days are deleted at the weekly maintenance scheduler time.

Apart from the database data, Manager creates a group of administration files that must be maintained regularly. These include Diagnostic files, DoS files (profiles) and Data Mining files (for Trend Reporting) among others. It is a best practice to schedule the deletion of the oldest of these files on an on-going basis. This can be accomplished using the Maintenance scheduler.

Viewing Manager server disk usage statistics

When the Manager database or disk space becomes full, the Manager cannot process any new alerts or packet logs. In addition, the Manager may not be able to process any configuration changes, including policy changes and alert acknowledgment. There is also a chance that the Manager may stop functioning completely.

Trellix therefore recommends that you monitor the disk space on a continuous basis to prevent this from happening. Health checks can be performed by navigating to the **Health Check** page in Manager → <Admin Domain Name> → Troubleshooting → **Health Check**. Use the **Health Check** page to view details, such as the percentage of space used, its total capacity, and the amount of disk space used.

NOTE

A fault type warning will be generated when the Manager disk space reaches 80-90%, 90-95%, 95-100%, >100% of interval ranges. By default, the frequency is 24 hrs.

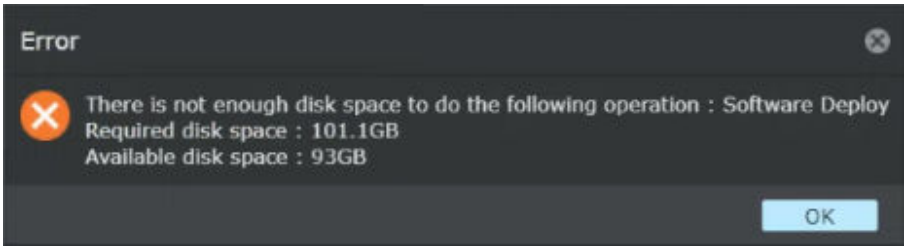
Large Sensor deployments

When you consider large or very large Sensor deployments, where the number of Sensors deployed ranges from 36 to 150, there are some important tasks which should be considered before the deployment.

If any user initiates bulk Sensor software deployment requests from the UI in an network environment with large Sensor deployments, it can considerably increase the disk space consumption in the Manager and slow down the deployment process. Inadequate disk space might also result in unpredictable software behavior and operational failures. To prevent such situations and maintain optimal performance, the Manager performs the following while handling bulk software deployment operations:

- The Manager reserves 100 GB under required free disk space for Manager operations and considers an additional file size of 1.2 GB to be generated for each software deployment request. When the Manager receives software deployment requests in bulk, it checks the number of Sensors selected and calculates the free disk space required to complete the deployment operation. If there is insufficient free disk space, the following error message is displayed in the UI.

  Figure 816. Error message displayed for device software deployment if there is insufficient disk space

  you can also check the deployment status on the **User Activities** and **Background Tasks** tabs in Manager → Troubleshooting → **Logs** page.

- Software deployments are critical operations and performed under approved/scheduled maintenance window. If the Manager receives multiple deployment requests in queue along with device software update requests, such as signature file and SSL keys deployments, it prioritizes the software deployment requests ahead of other requests. It also performs disk usage optimization for each deployment to help you perform more deployments at a faster speed, and complete the task within the approved/scheduled maintenance time.

Apart from the above-mentioned actions taken by the Manager for Sensor software deployments, Trellix recommends that you have a good understanding on the best techniques required to accomplish the tasks in your deployment scenario, prior to the deployment. Some of these include the following:

- **Sensor Software Updates** — All Sensor software updates do require a reboot. A reboot can take up to 5 minutes. You can schedule this process even though you can't reboot the Sensor automatically. But any update from the Manager Server causes the process to take place sequentially, one Sensor at a time. You can instead use the TFTP method for updating the Sensor image, which helps you to load concurrent images on the Sensor via the Sensor's CLI at a much faster rate.

  For more information, see the *Upgrading Sensor software via a TFTP server* in the *Trellix Intrusion Prevention System Installation Guide*.

- **Central Manager deployment** — If you have a large deployment of 200 Sensors, for example, that are deployed across various geographic locations, consider using a Central Manager at your organization's headquarters and deploy a dedicated Manager for each region. Each Manager will then handle the daily device operations for all Sensors configured to it. Note that when you use a Central Manager, your regional/local Managers can add their own region-specific rules, but cannot modify any configuration established by the Central Manager. Configuration updates to the Sensors must be applied through the local Managers. See Installing and Configuring Trellix IPS Central Manager (page 516) for details.

- **Usability** — Depending on the number of VIDS and Admin Domains defined in your deployment, the Manager Resource Tree can become very crowded which makes it difficult to locate the resource you require at any point of time. It can also lead to confusion if you have not provided unique, recognizable names for your Sensors and any VIDS you create. Note that the resource names appear both in the Resource Tree of the Manager as well as in Alert data and Reports. Your VIDS names should also be clear and easy for everyone maintaining the network to recognize at a glance. For example, compare a worldwide deployment where Sensors are named "4010-1" through "4010-25" as opposed to "UK-London-sens1," "India-Bangalore-sens1," and so on.

- **Alert Traffic** — Take note of the volume of alerting in your Sensors. Depending on the policies deployed on your system, there is potential to starve Manager resources since the resulting alerts are passed to the Manager. As the volume of alerting increases, more data is passed into the Manager. The Manager can handle short bursts of high alert volume, but on an average, the Manager can handle a total of 1500 alerts per minute from all the Sensors configured to it.
- **Start-up load on the Manager** — When the Manager starts, establishing connections with all Sensors can be time-consuming as Sensors continue to collect alerts. If the communication with the Manager is lost, each Sensor must pass its alert data to the Manager when connectivity is re-established. So, it is required to account for the start-up load on the Manager.
- **Concurrent processes** — Be aware of the time periods in which your scheduled processes, such as database backup or report generation, occur, and try not to attempt other tasks during that time period, as this can lead to process locking. This also includes having many users logged into the system simultaneously.

Staging Sensors prior to deployment

With large or very large deployments, if you are planning to release Sensors to various geographical regions or remote locations, you will have to consider staging your Sensors before you release them to their final destination.

For example, use the IPS Manager in a lab environment to push Sensor software to the Sensor, make sure that the Sensor is working as expected, and then box the configured Sensor and send it to its final destination. For more information, see the section *Updating the configuration of a Sensor* in the *Trellix Intrusion Prevention System Installation Guide*

Or, you can use the TFTP feature to load the Sensor image at one location, before shipping the Sensor to another location. For more information, see the section *Upgrading Sensor software via a TFTP server* in the *Trellix Intrusion Prevention System Installation Guide*.

NOTE

Very large Sensor deployments mean that the number of Sensors deployed is more than 100. Large Sensor deployments have Sensors numbering between 36 and 100+.

Recommendations for large Sensor deployment

Most Trellix IPS customers begin their deployment in their lab environment. Here they test the Sensor functionality, familiarize themselves with the Manager, and create an initial policy. Once they are comfortable with the product, they deploy the Sensor in a live environment.

Trellix provides a few recommendations for this process:

- Spend time creating *effective policies* before actual deployment. Availability of more information makes the tuning process easier. But policies, such as the Trellix IPS provided All-Inclusive policy, can overwhelm you with data, if every Sensor in a large deployment is running it without any customization.
- Stagger your Sensor deployment in *phases*. As each new batch of Sensors provides you with more data points, you can tune your policies more effectively, and become more proactive with the number of Sensors you deploy in the next phase.

Using active fail-open kits

Trellix supports the following types of passive and active fail-open kits:

- 10/100/1000 Gigabit Copper Passive Fail-Open Bypass Kit
- 1 Gigabit Optical Passive Fail-Open Bypass Kit
- 10 Gigabit Optical Passive Fail-Open Bypass Kit
- 10/100/1000 Copper Active Fail-Open Bypass Kit
- 10/100/1000 Copper Active Fail-Open Bypass Kit with SNMP monitoring
- 1 Gigabit Optical Active Fail-Open Bypass Kit
- 10 Gigabit Optical Active Fail-Open Bypass Kit
- 100 Gigabit Modular Active Fail-Open Bypass Kit Guide
- 40 Gigabit Modular Active Fail-Open Bypass Kit Guide

Fail-open kits can be deployed in production networks for the following reasons:

- Reduce the network downtime to seconds during any Sensor reboot or Sensor failure.
- Protect your network during link failure on the Sensor.
- Bypass the traffic when troubleshooting network issues. This will help you identify or eliminate the Sensor as the cause of network issues.

In the passive fail-open kit, if the Sensor goes down, the link has to be renegotiated again between the peer devices and this causes the link to go down for some time. In case of an active fail-open kit, a physical link will be established between the active fail-open kit and the two peer devices even when the Sensor is active. There would not be any link flap even when the Sensor goes down. Trellix recommends deploying active fail-open kits for protection of mission critical networks.

For Virtual IPS Sensors, only 10/100/1000 Copper Active Fail-Open Bypass Kit and 10/100/1000 Copper Active Fail-Open Bypass Kit with SNMP monitoring are supported. For more information, see *Virtual IPS Sensor deployment section* in the *Trellix Virtual Intrusion Prevention System Product Guide*.

Passive Fail-open

In passive fail-open kits, during normal Sensor in-line, fail-open operation, the Fail-Open Controller or built-in Control port (depending on which controls the Bypass Switch) supplies power and a heartbeat signal to the Bypass Switch.

If this signal is not presented within its programmed interval, the Fail-Open Bypass Switch removes the Sensor from the data path, and moves into bypass mode, providing continuous data flow with little network interruption. While the Sensor is in bypass mode, traffic passes directly through the switch, bypassing the Sensor. When normal Sensor operation resumes, you may or may not need to manually re-enable the monitoring ports from the Manager interface, depending on the activity leading up to the Sensor's failure.

Active Fail-open

In case of active fail-open kits, during normal Sensor in-line fail-open operation, the built-in monitoring sends a heartbeat signal (1 every second) to the Bypass Switch. If the Sensor does not receive 3 heart beat signals within its programmed interval, the Fail-Open Bypass Switch removes the Sensor from the data path, and moves it into the bypass mode, providing continuous data flow.

When the Bypass Switch loses power, traffic continues to flow through the network link, but is no longer routed through the Bypass Switch. This allows network devices to be removed and replaced without network downtime. Once power is restored to the Bypass Switch, network traffic is seamlessly diverted to the monitoring device, allowing it to resume its critical functions.

Considerations

This section discusses the generic requirements and notes that you need to consider with respect to active fail-open kits:

- The currently supported active fail-open kits are not plug and play devices. Initial configuration/setup is required before you begin.
- The following default options are fixed in Trellix active fail-open kits and cannot be changed:
  - LFD is set to **On**
  - Bypass Detection is set to **Off**

NOTE

Even if you change the configuration for these options using the NetOptics Web Manager or System Manager, the settings of these options on the Trellix active fail-open kit hardware cannot be changed.

- The management port on the active fail-open bypass kits cannot be configured.
- The parameters for the monitoring port must be set to Auto-Negotiate based on the speed, that is, 10/100/1000 Mbps. Trellix recommends that you set the Speed to 100 Mbps full **Duplex** with **Auto-Negotiate** enabled to improve performance.
- Unlike passive fail-open kits, an active fail-open kit moves into the bypass mode only when it does not receive the heart beat signals within its programmed interval. When the Sensor monitoring port is manually disabled or the cable is pulled out, for example, the Manager displays the port status as **AUK** (Active Unknown) under Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Physical Ports** page.
- If you are planning to use the 10/100/1000 copper active fail-open kit with SNMP monitoring, note that Trellix IPS currently supports only SNMP v1 on active fail-open kits.
- You can configure only a single SNMP Manager. The option to configure a secondary SNMP Manager is currently not available.
- The active fail-open kits do not provide any CLI option to view the serial and model numbers of the kits.
- If your network architecture is such that it requires you to remotely manage the active fail-open kits in your deployment, you can consider one of the following options:
  - Use a terminal server to connect to the system console and then connect using a remote login (interoperability issues might be seen while using UPLOGIX Terminal Server)
  - Pre-configure the kit with the required settings before shipping.

Effective policy tuning practices

All Sensors on initial deployment have the 'Default Prevention' policy loaded on all interfaces. Trellix recommends that you use the Default Prevention policy as a starting point, and then customize the policies based on your organization's requirements. The customized policies can be either cloned versions of the default pre-configured policies, or custom-built policies that employ custom rule sets. An appropriately tuned policy will reduce false positives.

Though each network environment has unique characteristics, the best practices outlined in this section can make tuning more efficient and effective. For more detailed information on IPS policy tuning, refer to the sections Trellix IPS policies (page 773) and Working with IPS policies (page 795).

NOTE

As you interact with Trellix IPS policies, you encounter the term "attack", not "signature". Trellix IPS defines an attack as being comprised of one or more signatures, thresholds, anomaly profiles, or correlation rules, where each method is used to detect an attempt to exploit a particular vulnerability in a system. These signatures and checks may contain very specific means for identifying a specific known exploit of the vulnerability, or more generic detection methods that aid in detecting unknown exploits for the vulnerability.

Analyzing high-volume attacks

Take attacks that are generating the most alerts (by using the **Attack Log** page) and investigate their legitimacy. For more information, see Attack Log (page 374).

Many of the top alerts seen on the initial deployment of a Sensor will be common false positives seen in many environments. Typically, at the beginning of the tuning process, it will be evident that your network or security policy will affect the overall level of alerts. If, for instance, AOL IM is allowed traffic on the network, there might not be a need to alert on AOL IM setup flows.

Managing ignore rules

When a particular alert is declared as a false positive, the next decision is whether to disable the corresponding attack altogether or, apply a particular ignore rule to that attack which will disable alerting for a particular IP address or range of IP addresses. In almost all cases, it is a best practice to implement the latter.

Consider some of the traffic in your network might appear as an attack. You are aware of the purpose of this traffic and you do not want the Sensor to take any response action on this traffic. However, if similar traffic is generated by any other server, you want the Sensor to treat it as an attack and respond accordingly. Trellix IPS provides various options to handle such situations.

Every ignore rule created is globally stored, so that the filter can be applied to any Exploit or Reconnaissance attack.

It is also a best practice to document all your tuning activities. The **Configuration Report** section can be used to assist the documentation process. The **Performance Monitoring - Sensor Configuration** report will deliver reports that list ignore rules that have been applied and attacks that have been otherwise customized.

NOTE

For more information, see the chapter *How to create Ignore rules for an applied IPS policy* in the *Trellix Intrusion Prevention System Product Guide*.

Learning profiles in DoS attacks

It is a best practice to let the Sensors learn the profiles of the particular segments they are monitoring, before tuning DoS attacks. This is *Learning Mode* operation. The learning process takes two days. During this period it is not unusual to see DoS alerts associated with normal traffic flows (for example, DoS SYN flood alerts reported outbound on a firewall interface to the Internet). After a profile has been learned, the particulars of the profile (number of SYNS, ACKS, and so on) can be viewed per Sensor.

DoS detection can also be implemented using the *Threshold Mode*. This involves setting thresholds manually for the type of segment characteristics that are learned in Learning Mode. Implementing this mode successfully is critically dependent on detailed knowledge of the segments that the particular Sensors are monitoring.

It is a best practice to have the Sensor re-learn the profile when there is a network change (that is, you move the Sensor from a lab or staging environment to a production environment) or a configuration change (that is, you change the CIDR block of a sub-interface) that causes a significant sudden traffic change on an interface. If the Sensor does not re-learn the new environment, it may issue false alarms or fail to detect actual attacks during a time period when it is adapting to the new network traffic conditions. There is no need to re-learn a profile when network traffic increases or decreases naturally over time (for example, an e-Commerce site that is getting more and more customers; thus its Web traffic increases in parallel), since the Sensor can automatically adapt to it.

For more information, see the section *Managing DoS Learning Mode profiles on a Sensor* in the *Trellix Intrusion Prevention System Product Guide*.

Response management

When a Sensor detects any activity which violates a configured security policy, a preset response from the Sensor is integral to the protection or prevention process. Proper configuration of responses is crucial to maintaining effective protection. Critical attacks like buffer overflows and DoS attacks require responses in real time, while scans and probes can be logged and researched to determine compromise potential and the source of the attack.

Developing a system of actions, alerts, and logs based on specific attacks or attack parameters (such as severity) is recommended for effective network security. For example, since Trellix IPS can be customized to protect any zone in a network, knowing what needs to be protected can help to determine the response type.

If the Sensor is monitoring the network outside of the firewall in inline mode, preventing DoS attacks and attacks against the firewall is crucial. Other suspicious traffic intended for the internal network, such as scans and low-impact well-known exploits, are best logged and analyzed as the impact is not immediate. In this case, a better understanding of the potential attack purpose can be determined.

Thus, if you are monitoring outside of a firewall in in-line mode, it is important not to set the policies and responses so fine that they disrupt the flow of traffic and slow down the system.

Remember that response actions are decoupled from alerting. Pay particular attention to this with the Recommended For Blocking (RFB) category of attacks, lest you enable blocking for an attack, but disable alerting, causing the attack to be blocked without your knowledge.

When there are multiple attempts to login to a specific web server from a client, the Sensor detects a reconnaissance Brute force attack (Attack ID 0x40256b00) and raises an alert. Brute force attacks are used by programs, such as password crackers, to try many different passwords in order to guess the correct one. The alerts raised are threshold-based. The Sensor may generate an alert even in scenarios, where a legitimate user keeps on retrying to login to the web server simply because he/she has forgotten the correct password. Instances of someone mistyping a password or username on the login are also common. In such cases, valid traffic flow would be blocked or subject to unnecessary responses from the Sensor, leading to a false positive. Consequently, the traffic might be dropped.

When such alerts are seen in high volume, there may be multiple reasons for it, such as a dictionary attack against the web server, or network monitoring systems (like WebSense) not updated with a user password change, and so on.

While configuring a Reconnaissance policy,Trellix IPS recommends you to edit and set optimum threshold values to suit your particular environment. This avoids unnecessary responses from the Sensor and hindrance to the traffic flow.

For example, if you have a web-server farm behind the Sensor, there are more HTTP logins seen on this segment. In such a scenario, you are required to set higher thresholds. The default values are good for most environments.

Sensor response actions

There are multiple Sensor actions that are available for configuration per attack. These include the following:

- **Dropping Alert Packets** — Only works in in-line mode. It will drop a detected attack packet and all subsequent packets in the same flow.
- **Quarantine** — Sensor will quarantine or remediate a host as per the configurations in the Manager and the Sensor monitoring ports. Quarantine can be enabled per attack in the Policy Editors.

  For more information, see Response management (page 885).

How to create rule sets

A rule set is configured based on attack category, operating system, protocol, application, severity, and benign trigger probability options. Each rule in a set is either an *include rule* or an *exclude rule*. An include rule (which should always start a rule set) is a set of parameters that encompass a broad range of well-known attacks for detection. An exclude rule removes elements from the include rule in order to focus the policy's rule set.

Proper creation of rule sets is essential for eliminating false positives and ensuring maximum protection on your network. These best practices can assist while creating rules sets in the Manager.

Best methods for rule set creation

There are two best practice methods employed for creating rule sets.

- **General-to-specific rule creation** — The first method is general-to-specific. Start with an include rule that covers a broad range of operating systems, applications and protocols. After this, create one or more exclude rules to strip away specific operating systems or protocols, thus focusing the rule set on the environment where it will be enforced. For example, start with an include rule for all Exploit category attacks. Follow this with multiple exclusion rules that strip away protocols, applications, severities, etc., that are rarely or never seen in a zone of your network.
- **Collaborative rule creation** — The second method is collaboration - Create multiple include rules within one rule set for each category, operating systems or combination that needs to be detected. Each criterion must be matched in order for an alert to be triggered. For example, create the first rule in the set with the Exploit category, Unix as the OS, Sendmail as the application, and SMTP as the protocol. Next, create another include rule for Exploit, Windows 2000, WindMail, and so forth in the same manner. Each include rule added broadens the scope of the detection.

  For more information, see How to create Ignore rules for an applied IPS policy (page 1384).

Working with firewall policies

Review the following points while working with Firewall policies:

- You cannot set explicit access rules for protocols that negotiate ports dynamically, with the exception of FTP, TFTP, and RPC services. Protocols, such as H.323 and Netmeeting, which negotiate the data channel separately from the control channel, or negotiate ports that do not follow a standard, are not supported. However, you can configure access rules to explicitly deny these protocol instances by denying the fixed control port.
- For RPC services, you can configure explicit permit and deny rules for RPC as a whole, but not its constituents, such as statd and mountd.
- Protocols or services, such as instant messaging and peer-to-peer communication that use dynamic ports, are not supported.
- An alternative option for denying protocols that use dynamic ports is to configure IDS policies to drop the attacks that are detected in such transmissions. Trellix IPS detects use of and attacks in multiple such programs as Yahoo Messenger, KaZaA, IRC, and so on.
- There is a limit on the number of access rules that can be supported by various Sensor models.

For more information, see Firewall policies (page 1216).

How to handle asymmetric networks

Traffic that uses a different path for the request vs. response is termed as asymmetric traffic. There are chances of having asymmetric traffic within a network, when networks increase in size.

If there are chances of asymmetric traffic in your network, consider the following options:

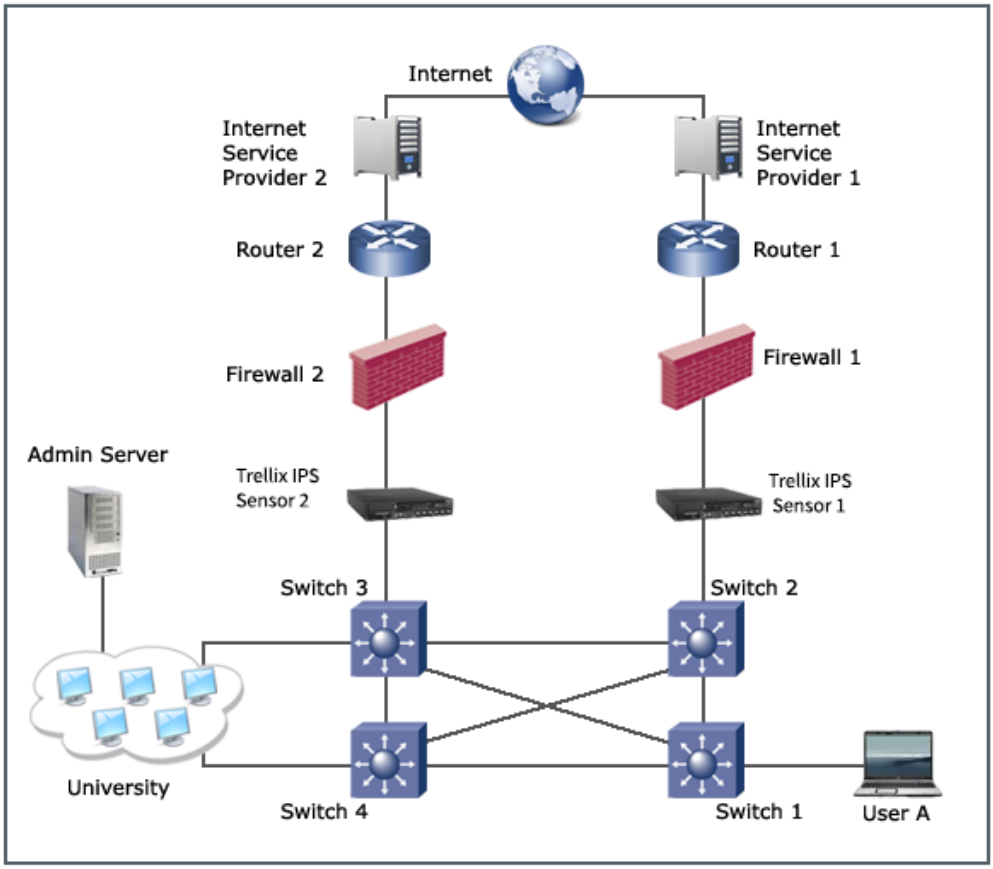
- Install IPS Sensors at a location where the traffic is symmetric.
- Implement a port clustering configuration for asymmetric traffic. Port clustering (referred to as Interface groups in the Manager) enables multiple ports on a single Sensor to be grouped together for effective traffic monitoring. Asymmetric networks are common in load balancing and active/passive configurations, and a complete transmission may be received on one segment, but depart on another. Thus, keeping state of asymmetric transmissions is essential for successfully monitoring the traffic. Interface groups normalize the impact of traffic flows split across multiple interfaces, thus maintaining state to avoid information loss.
- Place an IPS Sensor each on the request and the response path of the asymmetric traffic and create a HA pair to sync up the traffic flow between the two Sensors.
- If you are using a HA pair to monitor asymmetric traffic where the TCP traffic is going through two geographically different data centers, connect the Sensors using dark fiber. In this option, both the Sensors will have full state.
- When the distance between the two IPS Sensors is such that a HA pair cannot be created, consider enabling Stateless Inspection. In Stateless Inspection, the Sensor detects attacks without requiring a valid TCP state. This option should be used only when Sensors are placed in a network where the Sensors do not see all packets of a TCP flow like in an asymmetric network configuration.

> **NOTE**
>
> When Stateless Inspection is enabled, ACLs and syn cookie protection cannot be enabled. So, HTTP redirection to the Remediation Portal may or may not work depending on your network deployment scenario, for example, in a setup where SYN+ACK packets cannot be sent from the Sensor to the client.

The diagram below explains HTTP traffic flow in an asymmetric network between User A and the University Admin server. The outgoing connection flow from User A is through Switch 1, Switch 2, IPS Sensor 1, Router 1, Internet Service Provider 1, to the

Internet connection. The return path for the packet however, is through Internet Service Provider 2, Router 2, etc. If traffic flows by the Sensor in an asymmetric manner as described above, all packets of a TCP flow are not visible to a single Sensor.

In such a scenario, if Stateless Inspection is enabled, the Sensor will inspect packets without having the valid state for the TCP connection. Consequently, it might generate false positives that is, when a single communication flow is divided across paths, each interface will receive and analyze part of the conversation and therefore be susceptible to false positives and false negatives.



CAUTION

When you enable Stateless Inspection, there are chances of false positives, and the detection accuracy will be lower compared to when the Sensor sees all traffic. Trellix recommends that you use this feature only when network configuration does not allow the Sensor to be placed in locations where it could see all traffic.

SSL best practices

Note that there is a performance impact when using the SSL decryption feature. If there is a lot of outbound SSL traffic from the client to the internet, it consumes SSL flows. Therefore, to enable the Sensor to effectively utilize the SSL decryption feature, it is recommended to bypass these outbound SSL traffic using ACL Ignore rules.

Refer to the following sections for the SSL throughput measurements and test methodologies.

NOTE

SSL decryption feature is not supported on NS3500, NS3200, and NS3100 Sensor models.

NOTE

Proxy based SSL decryption feature is not supported on VM5000 and VM600 Sensor models.

Outbound SSL traffic best practices

The following sections describe the outbound SSL best practices.

Outbound SSL mixed traffic - throughput for proxy based SSL: NS-series Sensors

The following section contains outbound SSL best practices for mixed traffic:

NS9500 standalone - 30 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	4,500
SSL Throughput	5.0 Gbps
HTTP 1.1 Throughput	21.5 Gbps
Total Throughput	26.5 Gbps

NS9500 standalone - 20 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	3,600
SSL Throughput	4.0 Gbps
HTTP 1.1 Throughput	15.5 Gbps
Total Throughput	19.5 Gbps

NS9500 standalone - 10 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	2,250
SSL Throughput	2.5 Gbps
HTTP 1.1 Throughput	7.5 Gbps
Total Throughput	10.0 Gbps

NS9200

Parameter	Throughput
Max. SSL Connections / Sec.	5,000
SSL Throughput	3.6 Gbps
HTTP 1.1 Throughput	14.7 Gbps
Total Throughput	18.3 Gbps

NS9100

Parameter	Throughput
Max. SSL Connections / Sec.	3,000
SSL Throughput	2.5 Gbps
HTTP 1.1 Throughput	10 Gbps
Total Throughput	12.5 Gbps

NS7500 - 7.5 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	2,250
SSL Throughput	2.5 Gbps
HTTP 1.1 Throughput	3 Gbps
Total Throughput	5.5 Gbps

NS7500 - 5 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	1,125
SSL Throughput	1.25 Gbps
HTTP 1.1 Throughput	2.75 Gbps
Total Throughput	4 Gbps

NS7500 - 3 Gbps throughput

Parameter	Throughput
Max. SSL Connections / Sec.	675
SSL Throughput	750 Mbps
HTTP 1.1 Throughput	1.65 Gbps
Total Throughput	2.4 Gbps

NS7300

Parameter	Throughput
Max. SSL Connections / Sec.	2,500
SSL Throughput	2 Gbps
HTTP 1.1 Throughput	6 Gbps
Total Throughput	8 Gbps

NS7200

Parameter	Throughput
Max. SSL Connections / Sec.	800
SSL Throughput	900 Mbps
HTTP 1.1 Throughput	5 Gbps
Total Throughput	5.9 Gbps

Outbound SSL only traffic - throughput for proxy based SSL: NS-series Sensors

100 HTTPS 1.1 get page requests per TCP connection with a 128K response each and HTTP response scanning enabled.

NS9500 standalone - 30 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,500	6,200
SSL Throughput	7.9 Gbps	7.9 Gbps

NS9500 standalone - 20 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,982	4,898
SSL Throughput	6.7 Gbps	6.7 Gbps

NS9500 standalone - 10 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,022	3,700
SSL Throughput	4.5 Gbps	4.5 Gbps

NS7500 - 7.5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,250	2,250
SSL Throughput	2.5 Gbps	2.5 Gbps

NS7500 - 5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,125	1,125
SSL Throughput	1.25 Gbps	1.25 Gbps

NS7500 - 3 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	675	675
SSL Throughput	750 Mbps	750 Mbps

Inbound SSL traffic best practices

The following sections describe the inbound SSL best practices.

Inbound SSL only traffic - throughput for proxy based SSL: NS-series Sensors

100 HTTPS 1.1 get page requests per TCP connection with a 128K response each and HTTP response scanning enabled.

NS9500 standalone - 30 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,680	6,600
SSL Throughput	7.25 Gbps	7.25 Gbps

NS9500 standalone - 20 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,982	4,912
SSL Throughput	5.5 Gbps	5.5 Gbps

NS9500 standalone - 10 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,074	4,052
SSL Throughput	4.5 Gbps	4.5 Gbps

NS7500 - 7.5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,250	2,250
SSL Throughput	2.5 Gbps	2.5 Gbps

NS7500 - 5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,125	1,125
SSL Throughput	1.25 Gbps	1.25 Gbps

NS7500 - 3 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	675	675
SSL Throughput	750 Mbps	750 Mbps

Inbound SSL best practices for RSA ciphers

This section mentions inbound SSL best practices for RSA ciphers.

SSL only traffic - throughput: NS-series Sensors

Testing parameters for NS9500 and other Sensors

- Session resumption for 4 out of 5 TCP connections
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each
- (Applicable to NS9500 Sensors) 5 HTTP 1.1 get page requests per TCP connection with a 21K response each and HTTP response scanning enabled
- Cipher used: AES-128SHA

NS9500 stack - 100 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	132,000	115,200
SSL Throughput	60 Gbps	40 Gbps

NS9500 stack - 60 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	66,000	57,600
SSL Throughput	30 Gbps	20 Gbps

NS9500 stack - 40 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	52,800	43,200
SSL Throughput	22 Gbps	15 Gbps

NS9500 standalone - 30 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	33,000	28,800
SSL Throughput	15 Gbps	10 Gbps

NS9500 standalone - 20 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	26,400	21,600
SSL Throughput	11 Gbps	7.5 Gbps

NS9500 standalone - 10 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	19,800	14,400
SSL Throughput	8 Gbps	5.5 Gbps

NS9300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	44,000	30,800
SSL Throughput	20 Gbps	12 Gbps

NS9200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	22,000	15,400
SSL Throughput	10 Gbps	6 Gbps

NS9100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	17,000	13,600
SSL Throughput	8 Gbps	5.5 Gbps

NS7500 - 7.5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	13,200	13,200
SSL Throughput	6 Gbps	6 Gbps

NS7500 - 5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	8,800	8,800
SSL Throughput	4 Gbps	4 Gbps

NS7500 - 3 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	5,280	5,280
SSL Throughput	2.4 Gbps	2.4 Gbps

NS7350

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	12,000	12,000
SSL Throughput	5 Gbps	5 Gbps

NS7250

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,900	6,900
SSL Throughput	3 Gbps	3 Gbps

NS7150

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,500	3,500
SSL Throughput	1.5 Gbps	1.5 Gbps

NS7300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	12,000	12,000
SSL Throughput	5 Gbps	5 Gbps

NS7200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,900	6,900
SSL Throughput	3 Gbps	3 Gbps

NS7100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,500	3,500
SSL Throughput	1.5 Gbps	1.5 Gbps

NS5200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,000	2,000
SSL Throughput	1 Gbps	1 Gbps

NS5100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,400	1,400
SSL Throughput	600 Mbps	600 Mbps

Testing parameters for NS7600

- 1 HTTP 1.1 get page request per TCP connection with a 5K response each and HTTP response scanning enabled for Connections/Sec test
- 5 HTTP 1.1 get page request per TCP connection with a 21K response each and HTTP response scanning enabled for Throughput Test
- Cipher used for both the tests: AES-128SHA

NS7600 - 15 Gbps throughput

	2048 bit key length
Max. SSL Connections / Sec.	170,000
SSL Throughput	15 Gbps

NS7600 - 10 Gbps throughput

	2048 bit key length
Max. SSL Connections / Sec.	140,000
SSL Throughput	10 Gbps

NS7600 - 5 Gbps throughput

	2048 bit key length
Max. SSL Connections / Sec.	90,000
SSL Throughput	5 Gbps

SSL traffic mixed with HTTP 1.1 traffic: NS-series Sensors

- Session resumption for 4 out of 5 TCP connections
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each
- (Applicable to NS9500 Sensors) 5 HTTP 1.1 get page requests per TCP connection with a 21K response each and HTTP response scanning enabled
- AES-128SHA

NS9500 stack - 100 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	26,400	26,400
SSL Throughput	10 Gbps	10 Gbps
HTTP 1.1 Throughput	90 Gbps	90 Gbps
Total Throughput	100 Gbps	100 Gbps

NS9500 stack - 60 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	13,200	13,200
SSL Throughput	6 Gbps	6 Gbps
HTTP 1.1 Throughput	54 Gbps	54 Gbps
Total Throughput	60 Gbps	60 Gbps

NS9500 stack - 40 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	9,600	9,600
SSL Throughput	4 Gbps	4 Gbps
HTTP 1.1 Throughput	36 Gbps	36 Gbps
Total Throughput	40 Gbps	40 Gbps

NS9500 standalone - 30 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	6,600	6,600
SSL Throughput	2.6 Gbps	2.6Gbps
HTTP 1.1 Throughput	23.4 Gbps	23.4 Gbps
Total Throughput	26 Gbps	26 Gbps

NS9500 standalone - 20 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,800	4,800
SSL Throughput	1.8 Gbps	1.8 Gbps
HTTP 1.1 Throughput	16.2 Gbps	16.2 Gbps
Total Throughput	18 Gbps	18 Gbps

NS9500 standalone - 10 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	9 Gbps	9 Gbps
Total Throughput	10 Gbps	10 Gbps

NS9300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	9,200	9,200
SSL Throughput	4 Gbps	4 Gbps
HTTP 1.1 Throughput	36 Gbps	36 Gbps
Total Throughput	40 Gbps	40 Gbps

NS9200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	4,600	4,600
SSL Throughput	2 Gbps	2 Gbps
HTTP 1.1 Throughput	18 Gbps	18 Gbps
Total Throughput	20 Gbps	20 Gbps

NS9100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	9 Gbps	9 Gbps
Total Throughput	10 Gbps	10 Gbps

NS7500 - 7.5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,300	3,300
SSL Throughput	1.5 Gbps	1.5 Gbps
HTTP 1.1 Throughput	5.2 Gbps	5.2 Gbps
Total Throughput	6.7 Gbps	6.7 Gbps

NS7500 - 5 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,300	3,300
SSL Throughput	1.5 Gbps	1.5 Gbps
HTTP 1.1 Throughput	3 Gbps	3 Gbps
Total Throughput	4.5 Gbps	4.5 Gbps

NS7500 - 3 Gbps throughput

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	3,300	3,300
SSL Throughput	1.5 Gbps	1.5 Gbps
HTTP 1.1 Throughput	1.2 Gbps	1.2 Gbps
Total Throughput	2.7 Gbps	2.7 Gbps

NS7350

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	4 Gbps	4 Gbps
Total Throughput	5 Gbps	5 Gbps

NS7250

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	2 Gbps	2 Gbps
Total Throughput	3 Gbps	3 Gbps

NS7150

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	0.5 Gbps	0.5 Gbps
Total Throughput	1.5 Gbps	1.5 Gbps

NS7300

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	4 Gbps	4 Gbps
Total Throughput	5 Gbps	5 Gbps

NS7200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	2 Gbps	2 Gbps
Total Throughput	3 Gbps	3 Gbps

NS7100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2,500	2,500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	0.5 Gbps	0.5 Gbps
Total Throughput	1.5 Gbps	1.5 Gbps

NS5200

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,600	1,600
SSL Throughput	800 Mbps	800 Mbps
HTTP 1.1 Throughput	200 Mbps	200 Mbps
Total Throughput	1 Gbps	1 Gbps

NS5100

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1,300	1,300
SSL Throughput	500 Mbps	500 Mbps
HTTP 1.1 Throughput	100 Mbps	100 Mbps
Total Throughput	600 Mbps	600 Mbps

SSL only traffic - throughput: Virtual IPS Sensor

- Session resumption for 4 out of 5 TCP connections
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each
- AES-128SHA

IPS-VM5000

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	7500	7500
SSL Throughput on KVM	5 Gbps	4.5 Gbps
SSL Throughput on ESXi	5 Gbps	4.5 Gbps

IPS-VM600

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	1700	1700
SSL Throughput on KVM	1 Gbps	1 Gbps
SSL Throughput on ESXi	750 Mbps	750 Mbps

SSL traffic mixed with HTTP 1.1 traffic: Virtual IPS Sensor

- Session resumption for 4 out of 5 TCP connections
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each
- AES-128SHA

IPS-VM5000 (for ESXi/KVM)

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	2500	2500
SSL Throughput	1 Gbps	1 Gbps
HTTP 1.1 Throughput	3 Gbps	3 Gbps
Total Throughput	4 Gbps	4 Gbps

IPS-VM600 (for ESXi/KVM)

	1024 bit key length	2048 bit key length
Max. SSL Connections / Sec.	500	500
SSL Throughput	200 Mbps	200 Mbps
HTTP 1.1 Throughput	800 Mbps	800 Mbps
Total Throughput	1 Gbps	1 Gbps

Suricata Snort best practices

This section contains best practices for the Suricata Snort engine under the following test parameters:

- For NS-series Sensor models NS9500, NS9300, NS9200, and NS9100, the performance results are based on 2,000 simultaneous requests.
- For NS-series Sensor models NS7500, NS7300, NS7200, NS7100, NS5200, NS5100, NS3500, NS3200, and NS3100, the performance results are based on 1,000 simultaneous requests.

Sensor	Throughput
NS9500 stack - 100 Gbps throughput	40 Gbps
NS9500 stack - 60 Gbps throughput	20 Gbps
NS9500 stack - 40 Gbps throughput	13.6 Gbps
NS9500 standalone - 30 Gbps throughput	10 Gbps
NS9500 standalone - 20 Gbps throughput	6.8 Gbps
NS9500 standalone - 10 Gbps throughput	3.8 Gbps
NS9300	13.2 Gbps
NS9200	6.7 Gbps
NS9100	3.5 Gbps
NS7500 - 7.5 Gbps throughput	3.5 Gbps
NS7500 - 5 Gbps throughput	2.5 Gbps
NS7500 - 3 Gbps throughput	1.5 Gbps
NS7300	1.85 Gbps
NS7200	1.7 Gbps
NS7100	1.35 Gbps
NS5200	1.15 Gbps
NS5100	1.1 Gbps
NS3500	200 Mbps
NS3200/NS3100	200 Mbps

NOTE

The Suricata Snort engine is not available on NS7600 and NS3600 Sensors.

Sensor HTTP response processing deployment

HTTP response processing is disabled by default. You can enable it for each traffic direction on an interface pair. To minimize the potential performance impact on the Sensor, we recommend that you enable HTTP response processing on the minimum number of ports and in only the required directions to achieve your protection goals.

Some examples of HTTP response processing deployment are given below:

- You want to protect a bunch of clients on your internal network — Enable HTTP response processing for outbound traffic only.
- You are serving Web content to external clients, and do not wish to serve attacks embedded in HTTP response traffic — Enable HTTP response processing for inbound traffic only.
- You want to protect both internal clients as well as the Web content you are serving to external clients — Enable HTTP response processing in both directions.

Tests for enabling HTTP response traffic

The test results provided in the next two sections illustrate potential impact of enabling response processing traffic.

The things to note about the test are given below.

- The test involves only HTTP traffic. Changing the HTTP response processing setting does not change the Sensor performance for any other protocol. Therefore, changes in aggregate Sensor performance will depend on the proportion of HTTP traffic to other traffic on the link being monitored.
- The test sends equal HTTP request and response loads in both directions through the Sensor. Typical real-world deployments do not have equal amounts of HTTP request traffic and response traffic in both directions through the Sensor. Usually, there is significant amount of request traffic in one direction and response traffic in the opposite direction. Since HTTP requests are typically <= 1/10th of the response size, the combined HTTP request and response traffic processed by Sensors in real deployments is typically less than that shown in the tests.
- The test sends HTTP request continuously at maximum load. Real-world networks are typically loaded, occasionally peaking at maximum capacity, but typically running at significantly lower throughput. The test results reflect performance at sustained load. When not running at maximum load, the Sensor can absorb larger bursts without significant impact.
- The test environment was created to illustrate the likely worst-case performance impact, expected to occur in deployments protecting large Web server farms. In these deployments, HTTP response processing typically provides little value because all HTTP response traffic is sourced from trusted servers, which do not usually transmit hostile content due to the security measures taken. In these environments, customers can consider selectively enabling HTTP response processing to better optimize their network.

The net result of all of these factors is that, in typical networks, the impact of enabling HTTP response processing is not noticed. The exact impact is, of course, dependent on the traffic being inspected and some environments could see a reduction in performance as significant as the test results indicate.

The factors to take into account include the following:

- Proportion of HTTP traffic to other protocols
- Relative amount of HTTP requests and responses in each direction

- Size of a response page sent to the client by the sites or applications that are typically accessed

For Sensor performance numbers under the following conditions:

- HTTP response processing enabled/disabled
- 5 HTTP 1.1 get page requests per TCP connection with a 10K response each sent in one direction

HTTP response processing results for Virtual IPS Sensor

Refer to the following table for Virtual IPS Sensor (deployed on ESXi or KVM) performance numbers with HTTP response processing:

Model No.	HTTP Response Scanning Disabled	HTTP Response Scanning Enabled for outbound direction
	5 HTTP 1.1 get page requests per TCP connection with a 21K response each	5 HTTP 1.1 get page requests per TCP connection with a 21K response each
IPS-VM600	1 Gbps	1 Gbps
IPS-VM5000	5 Gbps	5 Gbps

HTTP response processing results for NS-series Sensors

Refer to the following table for NS-series Sensor performance numbers with HTTP response processing:

Model No.	HTTP Response Scanning Enabled for outbound direction
	5 HTTP 1.1 get page requests per TCP connection with a 10K response each [NS9500 and NS7600 Sensors] 5 HTTP 1.1 get page requests per TCP connection with a 21K response each and HTTP response scanning enabled
NS9500 stack - 100 Gbps throughput	100 Gbps
NS9500 stack - 60 Gbps throughput	60 Gbps
NS9500 stack - 40 Gbps throughput	40 Gbps
NS9500 stand-alone - 30 Gbps throughput	30 Gbps
NS9500 stand-alone - 20 Gbps throughput	20 Gbps
NS9500 stand-alone - 10 Gbps throughput	10 Gbps

Model No.	HTTP Response Scanning Enabled for outbound direction
NS9300	40 Gbps
NS9200	20 Gbps
NS9100	10 Gbps
NS7600 - 15 Gbps	15 Gbps
NS7600 - 10 Gbps	10 Gbps
NS7600 - 5 Gbps	5 Gbps
NS7500 - 7.5 Gbps	7.5 Gbps
NS7500 - 5 Gbps	5 Gbps
NS7500 - 3 Gbps	3 Gbps
NS7350	5 Gbps
NS7250	3 Gbps
NS7150	1.5 Gbps
NS7300	5 Gbps
NS7200	3 Gbps
NS7100	1.5 Gbps
NS5200	1 Gbps
NS5100	600 Mbps
NS3600 - 5 Gbps	5 Gbps
NS3600 - 3 Gbps	3 Gbps
NS3600 - 1 Gbps	1 Gbps
NS3500	750 Mbps
NS3200/NS3100	750 Mbps

NOTE

The NS-series performance numbers will be higher when HTTP response is disabled. For example, the NS9100 performance with HTTP response scanning disabled will be higher than 10 Gbps.

Sensor performance with Layer 7 Data Collection

Turning on the Layer 7 Data Collection feature reduces Sensor performance.

- HTTP Response Scanning setting
- Proportion of HTTP traffic to other protocols
- Relative number of HTTP requests and responses in each direction
- Size of a response page sent to the client by the sites or applications that are typically accessed

The following table provides the performance details in a test environment.

- The test environment used 5 HTTP 1.1 get page requests per TCP connection with a 10 K response, each sent in one direction.
- When Advanced Traffic Inspection is enabled, in a deployment with 90 percent of traffic without evasions and 10 percent of traffic with evasions, the overall Sensor throughput would further drop by an additional five percent approximately. For example, if you get 1 Gbps throughput with Layer 7 Data Collection enabled, you would see 950 Mbps if Advanced Traffic Inspection is also enabled.

NS-series Sensor performance with Layer 7 Data Collection

NOTE

Since the default value of L7 data collection is set to 20% of all traffic, the number of flows decreases by approximately 15%.

Table 97. NS9500 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS9500 stack - 100 Gbps throughput	Disabled	Disabled	100 Gbps
		Enabled for outbound direction	100 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	100 Gbps
		Enabled for outbound direction	100 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	100 Gbps
		Enabled for outbound direction	100 Gbps
NS9500 stack - 60 Gbps throughput	Disabled	Disabled	60 Gbps
		Enabled for outbound direction	60 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	60 Gbps
		Enabled for outbound direction	60 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	60 Gbps
		Enabled for outbound direction	60 Gbps
NS9500 stack - 40 Gbps throughput	Disabled	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
	Percentage of flows that capture L7 data: 100	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
NS9500 standalone - 30 Gbps throughput	Disabled	Disabled	30 Gbps
		Enabled for outbound direction	30 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	30 Gbps
		Enabled for outbound direction	30 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	30 Gbps
		Enabled for outbound direction	30 Gbps
NS9500 standalone - 20 Gbps throughput	Disabled	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
NS9500 standalone - 10 Gbps throughput	Disabled	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps

Table 98. NS9x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS9300	Disabled	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	40 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
		Enabled for outbound direction	40 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	40 Gbps
		Enabled for outbound direction	40 Gbps
NS9200	Disabled	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	20 Gbps
		Enabled for outbound direction	20 Gbps
NS9100	Disabled	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps

Table 99. NS7600 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7600 - 15 Gbps throughput	Disabled	Disabled	15 Gbps
		Enabled for outbound direction	15 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	15 Gbps
		Enabled for outbound direction	15 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	15 Gbps
		Enabled for outbound direction	15 Gbps
NS7600 - 10 Gbps throughput	Disabled	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	10 Gbps
		Enabled for outbound direction	10 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	10 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
		Enabled for outbound direction	10 Gbps
NS7600 - 5 Gbps throughput	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps

Table 100. NS7500 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7500 - 7.5 Gbps throughput	Disabled	Disabled	7.5 Gbps
		Enabled for outbound direction	7.5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	7.5 Gbps
		Enabled for outbound direction	7.5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	7.5 Gbps
		Enabled for outbound direction	7.5 Gbps
NS7500 - 5 Gbps throughput	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS7500 - 3 Gbps throughput	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps

Table 101. NS7x50 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7350	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS7250	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
NS7150	Disabled	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps

Table 102. NS7x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS7300	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS7200	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
NS7100	Disabled	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1.5 Gbps
		Enabled for outbound direction	1.5 Gbps

Table 103. NS5x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS5200	Disabled	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
NS5100	Disabled	Disabled	600 Mbps
		Enabled for outbound direction	600 Mbps
	Percentage of flows that capture L7 data: 5	Disabled	600 Mbps
		Enabled for outbound direction	600 Mbps
	Percentage of flows that capture L7 data: 100	Disabled	600 Mbps
		Enabled for outbound direction	600 Mbps

Table 104. NS3600 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS3600 - 5 Gbps throughput	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
NS3600 - 3 Gbps throughput	Disabled	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	3 Gbps
		Enabled for outbound direction	3 Gbps
NS3600 - 1 Gbps throughput	Disabled	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 5	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps

Table 105. NS3500 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS3500	Disabled	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 5	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
	Percentage of flows that capture L7 data: 100	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps

Table 106. NS3x00 performance details with respect to Layer 7 Data Collection

Sensor Model	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
NS3200/NS3100	Disabled	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 5	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps
	Percentage of flows that capture L7 data: 100	Disabled	750 Mbps
		Enabled for outbound direction	750 Mbps

Virtual IPS Sensor performance with Layer 7 Data Collection

Table 107. Sensor performance details with respect to Layer 7 Data Collection

Sensor model (on ESXi/KVM)	Layer 7 Data Collection setting	HTTP Response Scanning setting	Observed throughput
IPS-VM600	Disabled	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 20	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	1 Gbps
		Enabled for outbound direction	1 Gbps
IPS-VM5000	Disabled	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 100	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps
	Percentage of flows that capture L7 data: 20	Disabled	5 Gbps
		Enabled for outbound direction	5 Gbps

NS-series Sensor capacity by model number

Refer to the following considerations before changing the capacity of maximum simultaneous file scan and customized attacks for all NS-series Sensor models.

Note for Advanced Malware - Maximum simultaneous file scan

This feature is not the same as the file saving feature that is enabled through the **Save File** checkbox in the **Advanced Malware Policies** page of the Manager. It mentions the aspect of file saving that occurs temporarily within the Sensor during analysis. If the analysis result matches the severity configured in the Manager, the file is sent to the Manager to be saved.

Different outcomes based on your file saving configuration in the **Advanced Malware Policies** page are as follows:

- If you have set the **Save File** to **Disable** in the **Advanced Malware Policies** page, the scanned files are not sent to the Manager.
- If you have set the **Save File** to **Always**, all the scanned files are sent to the Manager to be archived. Before using this option ensure that you have adequate disk space.
- If you have set a severity for **Save File**, the scanned files are saved in the Sensor so that they can be analyzed by internal scanning engines like the PDF- JavaScript Engine. Once the analysis is complete and if the result is same or higher than the severity set then the file is sent to the Manager. When the Manager receives the file then it is saved in the Manager for future analysis by a security administrator.

NS9500 (stack and standalone) Sensor capacity

The following table describes the supported NS9500 (stack and standalone) Sensor capacity:

Maximum Type	NS9500 stack		NS9500 standalone			
	100 Gbps through-put	60 Gbps through-put	40 Gbps through-put	30 Gbps through-put	20 Gbps through-put	10 Gbps through-put
Aggregate HTTP Perform-ance	100 Gbps	60 Gbps	40 Gbps	30 Gbps	20 Gbps	10 Gbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	upto 120 Gbps	upto 70 Gbps	upto 50 Gbps	upto 35 Gbps	upto 25 Gbps	upto 15 Gbps
Concurrent Connections	64,000,000	32,000,000	26,000,000	16,000,000	13,000,000	10,000,000
Connections established per second	2,500,000	1,300,000	1,000,000	650,000	525,000	450,000
Latency (Average UDP per packet Latency)	20 µs	20 µs	20 µs	20 µs	20 µs	20 µs
SSL Flow Count	6,400,000	3,200,000	2,600,000	1,600,000	1,300,000	1,000,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024	1,024	1,024	1,024

Maximum Type	NS9500 stack		NS9500 standalone			
	100 Gbps through-put	**60 Gbps through-put**	**40 Gbps through-put**	**30 Gbps through-put**	**20 Gbps through-put**	**10 Gbps through-put**
Throughput with Inbound SSL Decryption (based on 10% SSL traffic) **NOTE** NS9500 Sensor throughput is with HTTP re-sponse scanning enabled.	100 Gbps	52 Gbps	36 Gbps	26 Gbps	18 Gbps	10 Gbps
Quarantine rules per Sen-sor- IPv4	7,999	7,999	7,999	7,999	7,999	7,999
Quarantine rules per Sen-sor- IPv6	500	500	500	500	500	500
Quarantine Zones per Sen-sor	50	50	50	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000	1,000	1,000	1,000
VLAN / CIDR Blocks per Sensor	3,000	3,000	3,000	3,000	3,000	3,000
VLAN / CIDR Blocks per In-terface	254	254	254	254	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000	100,000	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144	262,144	262,144	262,144
Number of attacks with ig-nore rules	128,000	128,000	128,000	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	54,000,000	27,000,000	18,000,000	13,500,000	9,000,000	5,000,000

Maximum Type	NS9500 stack		NS9500 standalone			
	100 Gbps through-put	60 Gbps through-put	40 Gbps through-put	30 Gbps through-put	20 Gbps through-put	10 Gbps through-put
Effective (Firewall) access rules	30,000	30,000	20,000	30,000	20,000	10,000
Firewall rule objects	140,000	140,000	140,000	140,000	140,000	70,000
Firewall DNS rule objects	5,000	5,000	5,000	5,000	5,000	2,500
Firewall rule object groups	1,000	1,000	1,000	1,000	1,000	500
Application on Custom Port rule objects	2,000	2,000	2,000	2,000	2,000	1,000
Firewall user-based rule objects	5,000	5,000	5,000	5,000	5,000	2,500
Firewall user groups in access rules	10,000	10,000	10,000	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	128	128	128	128	128	128
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB	100 MB	100 MB	100 MB
Passive device profile limits	100,000	100,000	100,000	100,000	100,000	100,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	4,000	2,000	2,000	1,000	1,000	1,000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	4,096	2,048	2,048	1,024	1,024	1,024
New HTTP connections per second (using 1 GET with 5000 HTTP response)	1,400,000	700,000	600,000	350,000	300,000	250,000

NS9x00 Sensor capacity

The following table describes the supported NS9x00 Sensor capacity:

Maximum Type	NS9300	NS9200	NS9100
Aggregate HTTP Performance	40 Gbps	20 Gbps	10 Gbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	up to 70 Gbps	up to 35 Gbps	up to 30 Gbps
Concurrent Connections	32,000,000	16,000,000	13,000,000
Connections established per second	1,000,000	575,000	450,000
Latency (Average UDP per packet Latency)	<100 µs	<100 µs	<100 µs
SSL Flow Count	3,200,000	1,600,000	1,200,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	40 Gbps	20 Gbps	10 Gbps
Quarantine rules per Sensor- IPv4	7,999	7,999	7,999
Quarantine rules per Sensor- IPv6	500	500	500
Quarantine Zones per Sensor	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000
VLAN / CIDR Blocks per Sensor	3,000	3,000	3,000
VLAN / CIDR Blocks per Interface	254	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144
Number of attacks with ignore rules	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	13,500,000	9,000,000	5,000,000
Effective (Firewall) access rules	20,000	20,000	10,000
Firewall rule objects	140,000	140,000	70,000
Firewall DNS rule objects	5,000	5,000	2,500
Firewall rule object groups	1,000	1,000	500
Application on Custom Port rule objects	2,000	2,000	1,000
Firewall user-based rule objects	5,000	5,000	2,500
Firewall user groups in access rules	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	128	128	128

Maximum Type	NS9300	NS9200	NS9100
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB
Passive device profile limits	100,000	100,000	100,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	1,000	1,000	1,000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	4,094	4,094	4,094
New HTTP connections per second (using 1 GET with 5000 HTTP response)	700,000	375,000	260,000

NS7600 Sensor capacity

The following table describes the supported NS7600 Sensor capacity:

Maximum Type	NS7600-15 Gbps throughput	NS7600-10 Gbps throughput	NS7600-5 Gbps throughput
Aggregate HTTP Performance	15 Gbps	10 Gbps	5 Gbps
Max Throughput with test equipment sending UDP packet size of 1518 Bytes	20 Gbps	19 Gbps	18 Gbps
Concurrent Connections	15,000,000	13,000,000	10,000,000
Connections established per second	525,000	400,000	300,000
Latency (Average UDP per packet Latency)	20 µs	20 µs	20 µs
SSL Flow Count	1,500,000	1,200,000	900,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024
Throughput with Inbound SSL Decryption (based on 100% SSL traffic)	15 Gbps	10 Gbps	5 Gbps
Quarantine rules per Sensor- IPv4	16,000	16,000	16,000
Quarantine rules per Sensor- IPv6	1,000	1,000	1,000
Quarantine Zones per Sensor	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000
VLAN/CIDR Blocks per Sensor	3,000	3,000	3,000
VLAN/CIDR Blocks per Interface	254	254	254

Maximum Type	NS7600-15 Gbps throughput	NS7600-10 Gbps throughput	NS7600-5 Gbps throughput
Customized attacks	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144
Number of attacks with ignore rules	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	7,500,000	6,500,000	5,000,000
Effective (Firewall) access rules	4,000	4,000	4,000
Firewall rule objects	35,000	35,000	35,000
Firewall DNS rule objects	1,250	1,250	1,250
Firewall rule object groups	400	400	400
Application on Custom Port rule objects	500	500	500
Firewall user-based rule objects	1,250	1,250	1,250
Firewall user groups in access rules	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	512	512	512
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB
Passive device profile limits	100,000	100,000	100,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor	1,000	1,000	1,000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor	4,094	4,094	4,094
New HTTP connections per second (using 1 GET with 5000 HTTP response)	300,000	250,000	140,000

NS7500 Sensor capacity

The following table describes the supported NS7500 Sensor capacity:

Maximum Type	NS7500-7.5 Gbps throughput	NS7500-5 Gbps throughput	NS7500-3 Gbps throughput
Aggregate HTTP Performance	7.5 Gbps	5 Gbps	3 Gbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	12 Gbps	9 Gbps	6 Gbps

Maximum Type	NS7500-7.5 Gbps throughput	NS7500-5 Gbps throughput	NS7500-3 Gbps throughput
Concurrent Connections	10,000,000	7,000,000	4,000,000
Connections established per second	250,000	225,000	200,000
Latency (Average UDP per packet Latency)	20 µs	20 µs	20 µs
SSL Flow Count	1,000,000	700,000	400,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	6.7	4.5	2.7
Quarantine rules per Sensor- IPv4	7,999	7,999	7,999
Quarantine rules per Sensor- IPv6	500	500	500
Quarantine Zones per Sensor	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000
VLAN/CIDR Blocks per Sensor	3,000	3,000	3,000
VLAN/CIDR Blocks per Interface	254	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144

Maximum Type	NS7500-7.5 Gbps throughput	NS7500-5 Gbps throughput	NS7500-3 Gbps throughput
Number of attacks with ignore rules	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	4,000,000	3,000,000	1,800,000
Effective (Firewall) access rules	4,000	4,000	4,000
Firewall rule objects	35,000	35,000	35,000
Firewall DNS rule objects	1,250	1,250	1,250
Firewall rule object groups	400	400	400
Application on Custom Port rule objects	500	500	500
Firewall user-based rule objects	1,250	1,250	1,250
Firewall user groups in access rules	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	128	128	128
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB
Passive device profile limits	100,000	100,000	100,000

Maximum Type	NS7500-7.5 Gbps throughput	NS7500-5 Gbps throughput	NS7500-3 Gbps throughput
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	1,000	1,000	1,000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	1,024	1,024	1,024
New HTTP connections per second (using 1 GET with 5000 HTTP response)	170,000	140,000	115,000

NS7x50 Sensor capacity

The following table describes the supported NS7x50 Sensor capacity:

Maximum Type	NS7350	NS7250	NS7150
Aggregate HTTP Performance	5 Gbps	3 Gbps	1.5 Gbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	up to 10 Gbps	up to 8 Gbps	up to 5 Gbps
Concurrent Connections	10,000,000	5,000,000	3,000,000
Connections established per second	225,000	200,000	135,000
Latency (Average UDP per packet Latency)	<100 µs	<100 µs	<100 µs
SSL Flow Count	500,000	400,000	250,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	5 Gbps	3 Gbps	1.5 Gbps

Maximum Type	NS7350	NS7250	NS7150
Quarantine rules per Sensor- IPv4	7,999	7,999	7,999
Quarantine rules per Sensor- IPv6	500	500	500
Quarantine Zones per Sensor	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000
VLAN/CIDR Blocks per Sensor	3,000	3,000	3,000
VLAN/CIDR Blocks per Interface	254	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144
Number of attacks with ignore rules	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	3,300,000	1,800,000	1,400,000
Effective (Firewall) access rules	4,000	3,000	3,000
Firewall rule objects	35,000	21,000	21,000
Firewall DNS rule objects	1,250	1,000	1,000
Firewall rule object groups	400	300	300

Maximum Type	NS7350	NS7250	NS7150
Application on Custom Port rule objects	500	500	500
Firewall user-based rule objects	1,250	1,000	1,000
Firewall user groups in access rules	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	128	128	128
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB
Passive device profile limits	100,000	50,000	25,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	1,000	1,000	1,000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	4,094	4,094	4,094
New HTTP connections per second (using 1 GET with 5000 HTTP response)	135,000	128,000	115,000

NS7x00 Sensor capacity

The following table describes the supported NS7x00 Sensor capacity:

Maximum Type	NS7300	NS7200	NS7100
Aggregate HTTP Performance	5 Gbps	3 Gbps	1.5 Gbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	up to 15 Gbps	up to 10 Gbps	up to 5 Gbps

Maximum Type	NS7300	NS7200	NS7100
Concurrent Connections	10,000,000	5,000,000	3,000,000
Connections established per second	225,000	200,000	135,000
Latency (Average UDP per packet Latency)	<100 µs	<100 µs	<100 µs
SSL Flow Count	500,000	400,000	250,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	5 Gbps	3 Gbps	1.5 Gbps
Quarantine rules per Sensor- IPv4	7,999	7,999	7,999
Quarantine rules per Sensor- IPv6	500	500	500
Quarantine Zones per Sensor	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000
VLAN/CIDR Blocks per Sensor	3,000	3,000	3,000
VLAN/CIDR Blocks per Interface	254	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144

Maximum Type	NS7300	NS7200	NS7100
Number of attacks with ignore rules	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	3,300,000	1,800,000	1,400,000
Effective (Firewall) access rules	5,000	3,000	3,000
Firewall rule objects	35,000	21,000	21,000
Firewall DNS rule objects	1,250	1,000	1,000
Firewall rule object groups	400	300	300
Application on Custom Port rule objects	500	500	500
Firewall user-based rule objects	1,250	1,000	1,000
Firewall user groups in access rules	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	128	128	128
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB
Passive device profile limits	100,000	50,000	25,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	1,000	1,000	1,000

Maximum Type	NS7300	NS7200	NS7100
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	4,094	4,094	4,094
New HTTP connections per second (using 1 GET with 5000 HTTP response)	135,000	128,000	115,000

NS5x00 Sensor capacity

The following table describes the supported NS5x00 Sensor capacity:

Maximum Type	NS5200	NS5100
Aggregate HTTP Performance	1 Gbps	600 Mbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	up to 3 Gbps	up to 1.5 Gbps
Concurrent Connections	1,350,000	750,000
Connections established per second	45,000	40,000
Latency (Average UDP per packet Latency)	<100 µs	<100 µs
SSL Flow Count	75,000	40,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	1 Gbps	600 Mbps
Quarantine rules per Sensor- IPv4	7,999	7,999
Quarantine rules per Sensor- IPv6	500	500
Quarantine Zones per Sensor	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	100
VLAN / CIDR Blocks per Sensor	300	300
VLAN / CIDR Blocks per Interface	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000
Ignore rules	131072	131,072
Number of attacks with ignore rules	100,000	100,000
DoS Profiles	5,000	300
SYN cookie rate (64 - byte packets per second)	1,000,000	750,000
Effective (Firewall) access rules	2,000	2,000

Maximum Type	NS5200	NS5100
Firewall rule objects	14,000	14,000
Firewall DNS rule objects	750	750
Firewall rule object groups	200	200
Application on Custom Port rule objects	250	250
Firewall user-based rule objects	750	750
Firewall user groups in access rules	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	64	64
Maximum host entries supported for Connection Limiting policies	128,000	128,000
Maximum file size during packet capture	58 MB	58 MB
Passive device profile limits	15,000	15,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	32	32
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	1,024	1,024
New HTTP connections per second(using 1 GET with 5000 HTTP response)	30,000	25,000

NS3600 Sensor capacity

The following table describes the supported NS3600 Sensor capacity:

Maximum Type	NS3600- 5 Gbps throughput	NS3600- 3 Gbps throughput	NS3600- 1 Gbps throughput
Aggregate HTTP Performance	5 Gbps	3 Gbps	1 Gbps
Max Throughput with test equipment sending UDP packet size of 1518 Bytes	15 Gbps	10 Gbps	8 Gbps
Concurrent Connections	5,000,000	4,000,000	2,000,000
Connections established per second	190,000	130,000	90,000
Latency (Average UDP per packet Latency)	< 20 µs	< 20 µs	< 20 µs
SSL Flow Count	500,000	400,000	200,000
Number of SSL certificates that can be imported into the Sensor	1,024	1,024	1,024
Throughput with Inbound SSL Decryption (based on 100% SSL traffic)	5 Gbps	3 Gbps	1 Gbps
Quarantine rules per Sensor- IPv4	8,000	8,000	8,000

Maximum Type	NS3600-5 Gbps throughput	NS3600-3 Gbps throughput	NS3600-1 Gbps throughput
Quarantine rules per Sensor- IPv6	500	500	500
Quarantine Zones per Sensor	50	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	1,000	1,000	1,000
VLAN/CIDR Blocks per Sensor	3,000	3,000	3,000
VLAN/CIDR Blocks per Interface	254	254	254
Customized attacks	100,000	100,000	100,000
Ignore rules	262,144	262,144	262,144
Number of attacks with ignore rules	128,000	128,000	128,000
DoS Profiles	5,000	5,000	5,000
SYN cookie rate (64 - byte packets per second)	2,500,000	2,000,000	1,000,000
Effective (Firewall) access rules	4,000	4,000	4,000
Firewall rule objects	35,000	35,000	35,000
Firewall DNS rule objects	1,250	1,250	1,250
Firewall rule object groups	400	400	400
Application on Custom Port rule objects	500	500	500
Firewall user-based rule objects	1,250	1,250	1,250
Firewall user groups in access rules	10,000	10,000	10,000
Number of exclusion list entries permitted for IP Reputation	512	512	512
Maximum host entries supported for Connection Limiting policies	256,000	256,000	256,000
Maximum file size during packet capture	100 MB	100 MB	100 MB
Passive device profile limits	100,000	100,000	100,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor	1,000	1,000	1,000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor	4,094	4,094	4,094
New HTTP connections per second (using 1 GET with 5000 HTTP response)	250,000	200,000	100,000

NS3500 Sensor capacity

The following table describes the supported NS3500 Sensor capacity:

Maximum Type	NS3500
Aggregate HTTP Performance	750 Mbps

Maximum Type	NS3500
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	up to 1 Gbps
Concurrent Connections	1,00,000
Connections established per second	25,000
Latency (Average UDP per packet Latency)	<100 µs
SSL Flow Count	NA
Number of SSL certificates that can be imported into the Sensor	NA
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	NA
Quarantine rules per Sensor- IPv4	7,999
Quarantine rules per Sensor- IPv6	500
Quarantine Zones per Sensor	50
Quarantine Zone ACLs per Sensor	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	32
VLAN / CIDR Blocks per Sensor	64
VLAN / CIDR Blocks per Interface	64
Customized attacks See the note below on how the number of customized attacks is affected.	100,000
Ignore rules	65,536
Number of attacks with ignore rules	40,000
DoS Profiles	128
SYN cookie rate (64 - byte packets per second)	400,000
Effective (Firewall) access rules	1,000
Firewall rule objects	7,000
Firewall DNS rule objects	500
Firewall rule object groups	100
Application on Custom Port rule objects	150
Firewall user-based rule objects	500
Firewall user groups in access rules	10,000
Number of exclusion list entries permitted for IP Reputation	32
Maximum host entries supported for Connection Limiting policies	128,000
Maximum file size during packet capture	40 MB
Passive device profile limits	10,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	16

Maximum Type	NS3500
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	255
New HTTP connections per second(using 1 GET with 5000 HTTP response)	15,000

NS3x00 Sensor capacity

The following table describes the supported NS3x00 Sensor capacity:

Maximum Type	NS3200/NS3100
Aggregate HTTP Performance	750 Mbps
Max Throughput with test equipment sending UDP packet size of 1512 Bytes	up to 1 Gbps
Concurrent Connections	1,00,000
Connections established per second	25,000
Latency (Average UDP per packet Latency)	<100 µs
SSL Flow Count	NA
Number of SSL certificates that can be imported into the Sensor	NA
Throughput with Inbound SSL Decryption (based on 10% SSL traffic)	NA
Quarantine rules per Sensor- IPv4	7,999
Quarantine rules per Sensor- IPv6	500
Quarantine Zones per Sensor	50
Quarantine Zone ACLs per Sensor	1,000
Virtual Interfaces (VIDS) per Sensor (Number of Virtual IPS Systems)	32
VLAN / CIDR Blocks per Sensor	64
VLAN / CIDR Blocks per Interface	64
Customized attacks See the note below on how the number of customized attacks is affected.	100,000
Ignore rules	65,536 **NOTE** Maximum Ignore rules supported in NS3100 Sensor model is 32,768.

Maximum Type	NS3200/NS3100
Number of attacks with ignore rules	40,000 **NOTE** Maximum number of attacks with ignore rules supported in NS3100 Sensor model is 20,000.
DoS Profiles	128
SYN cookie rate (64 - byte packets per second)	400,000
Effective (Firewall) access rules	1,000
Firewall rule objects	7,000
Firewall DNS rule objects	500
Firewall rule object groups	100
Application on Custom Port rule objects	150
Firewall user-based rule objects	500
Firewall user groups in access rules	10,000
Number of exclusion list entries permitted for IP Reputation	32
Maximum host entries supported for Connection Limiting policies	128,000
Maximum file size during packet capture	40 MB
Passive device profile limits	10,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	16
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	255
New HTTP connections per second(using 1 GET with 5000 HTTP response)	15,000

Virtual IPS Sensor capacity by model number

The following table describes the supported Virtual IPS Sensor capacity on VMware ESXi:

Maximum Type	IPS-VM600	IPS-VM5000
Aggregate Performance	1 Gbps	5 Gbps
Maximum throughput with test equipment sending UDP packet size of 1518 bytes	5 Gbps	9 Gbps
Concurrent connections	426,000	2,500,000

Maximum Type	IPS-VM600	IPS-VM5000
Connections established per second	97,000	149,000
Latency (Average UDP per packet Latency)	< 100 us	< 100 us
SSL Flow count	30,000	120,000
Number of SSL certificates that can be imported into the Sensor	256	256
Throughput with SSL Decryption (based on 10% SSL traffic)	900 Mbps	4 Gbps
Quarantine rules per Sensor - IPv4	8,000	8,000
Quarantine rules per Sensor - IPv6	500	500
Quarantine Zones per Sensor	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000
Virtual Interfaces (VIDS) per Sensor	100	100
VLAN / CIDR Blocks per Sensor	300	300
VLAN / CIDR Blocks per Interface	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000
Ignore rules	131,072	131,072
Number of attacks with ignore rules	100,000	100,000
DoS Profiles	300	300
SYN cookie rate (64-byte packets per second)	600,000	600,000
Effective (Firewall) access rules	2,000	2,000
Firewall rule objects	14,000	24,000
Firewall DNS rule objects	750	750
Firewall rule object groups	200	200
Application on Custom Port rule objects	250	250
Firewall user-based rule objects	750	750
Firewall user groups in access rules	2,000	2,000
Number of exclusion list entries permitted for IP Reputation	64	128
Maximum host entries supported for Connection Limiting policies	128,000	128,000
Passive device profile limits	15,000	15,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	32	32

Maximum Type	IPS-VM600	IPS-VM5000
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	1,024	1,024
New HTTP connections per second (using 1 GET with 5000 HTTP response)	59,000	78,000

The following table describes the supported Virtual IPS Sensor capacity on Kernel-based Virtual Machine (KVM).

Maximum Type	IPS-VM600	IPS-VM5000
Aggregate Performance	1 Gbps	5 Gbps
Maximum throughput with test equipment sending UDP packet size of 1518 bytes	5 Gbps	9 Gbps
Concurrent connections	426,000	2,500,000
Connections established per second	80,000	125,000
Latency (Average UDP per packet Latency)	< 100 us	< 100 us
SSL Flow count	30,000	120,000
Number of SSL certificates that can be imported into the Sensor	256	256
Throughput with SSL Decryption (based on 10% SSL traffic)	900 Mbps	4 Gbps
Quarantine rules per Sensor - IPv4	8,000	8,000
Quarantine rules per Sensor - IPv6	500	500
Quarantine Zones per Sensor	50	50
Quarantine Zone ACLs per Sensor	1,000	1,000
Virtual Interfaces (VIDS) per Sensor	100	100
VLAN / CIDR Blocks per Sensor	300	300
VLAN / CIDR Blocks per Interface	254	254
Customized attacks See the note below on how the number of customized attacks is affected.	100,000	100,000
Ignore rules	131,072	131,072
Number of attacks with ignore rules	100,000	100,000
DoS Profiles	300	300
SYN cookie rate (64-byte packets per second)	600,000	600,000
Effective (Firewall) access rules	2,000	2,000
Firewall rule objects	14,000	24,000
Firewall DNS rule objects	750	750
Firewall rule object groups	200	200
Application on Custom Port rule objects	250	250

Maximum Type	IPS-VM600	IPS-VM5000
Firewall user-based rule objects	750	750
Firewall user groups in access rules	2,000	2,000
Number of exclusion list entries permitted for IP Reputation	64	128
Maximum host entries supported for Connection Limiting policies	128,000	128,000
Passive device profile limits	15,000	15,000
Advanced Malware - Maximum simultaneous file scan capacity when the file is saved in the Sensor See the note below for more information.	32	32
Advanced Malware - Maximum simultaneous file scan capacity without saving files in the Sensor See the note below for more information.	1,024	1,024
New HTTP connections per second (using 1 GET with 5000 HTTP response)	47,000	83,000

Note for Advanced Malware - Maximum simultaneous file scan

The Advanced Malware - Maximum simultaneous file scan capacity with file save applies to all engines that require complete file for performing the malware analysis, such as Intelligent Sandbox, Gateway Anti-Malware, or Trellix IPS Analysis engines. It mentions the aspect of file saving that occurs temporarily within the Sensor during analysis. This feature is not the same as the file saving feature that is enabled through the **Save File** checkbox in the **Advanced Malware Policies** page of the Manager.

Different outcomes based on your file saving configuration using **Save File** checkbox in the **Advanced Malware Policies** page are below:

- If you have set the **Save File** to **Disable** in the **Advanced Malware Policies** page, the scanned files are not sent to the Manager.
- If you have set the **Save File** to **Always**, all scanned files are sent to the Manager to be archived. Before using this option, make sure that you have adequate disk space.
- If you have set a severity for **Save File**, the scanned files are temporarily saved in the Sensor for malware analysis by engines such as AIntelligent Sandbox, Gateway Anti-Malware, or Trellix IPS Analysis. If the result is same or higher than the severity configured, the file is sent to the Manager. When the Manager receives the file, it is saved in the Manager for future analysis by a security administrator.

Note for customized attacks

Customized attacks are not to be confused with custom attacks. A ***custom attack*** is a user-defined attack definition either in the Trellix IPS format or the Snort rules language. Whereas a ***customized attack*** is an attack definition (as part of the signature set), for which you modified its default settings. For example, if the default severity of an attack is 5 and you change it to 7, it is a customized attack.

The signature set push from the Manager to a Sensor fails if the number of customized attacks on the Sensor exceeds the customized attack limit.

The number of customized attacks can increase due to:

- Modifications done to attacks on a policy by users.
- Recommended for blocking (RFB) attacks.
- User created asymmetric policies.

  Example: How numerous customized attacks are created in asymmetric policies.

  1. Create a policy.
  2. Set the Inbound rule set to "File Server rule set".
  3. Set the Outbound rule set to " Default Testing rule set".

     You see that:

     - The File Server rule set has 166 exploit attacks.
     - The Default Testing rule set has 2204 exploit attacks.

  The total number of customized attacks for this policy is 2204 – 116 = 2038 customized attacks.

Troubleshooting

Troubleshooting Trellix Intrusion Prevention System

This section lists some troubleshooting tips for Trellix IPS.

Before you start troubleshooting

Before you get too deep into troubleshooting techniques, it is a good practice to consider the following questions:

- Were there physical changes to your network that occurred recently?
- If another device is placed in the Sensor's position, does that device receive traffic?
- If the Sensor is in L2 mode, are your network's services still affected?
- Are you using approved Trellix SFP, SFP+, QSFP+, or QSFP28 with your Sensor? (For a list of approved hardware, see Trellix KnowledgeBase article KB56364.

Simplifying troubleshooting

When an in-line device experiences problems, most people's instinct is to physically pull it out of the path — to disconnect the cables and let traffic flow unimpeded while the device can be examined elsewhere. Trellix recommends you first try the following techniques to troubleshoot a Sensor issue:

- All Sensors have a *Layer2 Passthru* feature. If you feel your Sensor is causing network disruption, before you remove it from the network, issue the following command:

  `layer2 mode assert`

  This pushes the Sensor into Layer2 Passthru (L2) mode, causing traffic to flow through the Sensor while bypassing the detection engine. Check to see whether your services are still affected. If they are, you have eliminated certain Sensor hardware issues and the problem could instead be a network issue or a configuration issue.

  > **NOTE**
  >
  > The **`layer2 mode deassert`** command pushes the Sensor back to detection mode.

- Trellix recommends that you configure Layer2 Passthru Mode on each Sensor. This enables you to set a threshold on the Sensor that pushes the Sensor into L2 bypass mode if the Sensor experiences a specified number of errors within a specified time frame. Traffic then continues to flow directly through the Sensor without passing to the detection engine.
- Connect a fail-open kit, which consists of a bypass switch and a controller, to any GE monitoring port pairs on the Sensor. If a kit is attached to the Sensor, disabling the Sensor ports forces traffic to flow through the bypass switch, effectively pulling the Sensor out of the path.

CAUTION

Note that the Sensor will need to reboot to move out of L2 mode only if the Sensor entered L2 mode because of internal errors. (It does not need a reboot if the **`layer2 mode assert`** command was used to put the Sensor into L2 mode).

CAUTION

A Sensor reboot breaks the link connecting the devices on either side of the Sensor and requires the renegotiation of the network link between the two devices surrounding the Sensor.

CAUTION

Depending on the network equipment, this disruption may last from a couple of seconds to more than a minute with certain vendors' devices. A very brief link disruption might occur while the links are renegotiated to place the Sensor back in in-line mode.

Issues and status checks for the Sensor

This section describes all issues and status checks specific to the Sensor.

Health check of a Sensor

To see if your Sensor is functioning correctly, do one of the following:

On the Sensor:

- At the command prompt, type **`status`**. This displays system status (such as Operational Status, system initialization, signature version, trust, channel status, alert counts, and so on). Sensor should be initialized and in good health.
- At the command prompt, type **show**. This displays configuration information (such as Sensor image version, type, name, Manager and Sensor IP addresses, and so on).

On the Manager:

- In the Manager **Dashboard** page, view the **System Faults** monitor. Manager status should be **UP**, and Sensor status should be **ACTIVE**.

NOTE

If you see system faults indicating that the Manager is down, check the **Faults** tab in **Logs** page to interpret the fault and, if necessary, take action to clear the fault.

Pinging a Sensor

The Sensor Management port responds only to 20 pings per second. This limited rate prevents the Sensor from being susceptible to a ping flood. To ping a Sensor Management port from multiple hosts, increase the time interval between pings.

Failover status check of a Sensor

To ensure that two Sensors comprising a HA pair are communicating via their interconnection cable, go to each Sensor's CLI and type **`show failover-status`**. Failover should display as enabled (YES), and the peer Sensor should display as UP.

Cable failover through a network device

Do **not** connect the heartbeat cable through an external network device.

To keep overhead low and throughput high, the Sensors do not include layer 2 or 3 headers on the packets they pass over the heartbeat connection, and they pass data larger than the standard Ethernet maximum frame size (1518 bytes).

If you attempt to place a network device, such as a switch or router, between the heartbeat ports, the heartbeat connection will fail.

Signature or software update status

To see if your Sensor successfully received a signature update or software upgrade, you can use the **`status`** command as shown in the following procedure, or the **`downloadstatus`** command, described later in this chapter.

To use the **`status`** command:

1. On the Sensor, type **`status`** at the command prompt before updating the signature set on the Sensor. Note the signature version.
2. Update the signature set on the Sensor using the Manager screens.
3. On the Sensor, again type **`status`** at the command prompt after the update from Manager is complete. Verify that the signature version number has incremented. The new signature version should match with the signature set version that has been updated from the Manager and applied to the Sensor.

Download or upload status

To see the progress of an upload or download, use the **`downloadstatus`** command.

The **`downloadstatus`** command displays the status of various download/upload operations, such as signature, software image, DoS profile downloads (from Manager to Sensor), DoS profile, and debug trace uploads (from Sensor to Manager). It also lists the number of times you have performed the operation, status of your previous attempt to perform the operation (including the cause of failure if the operation failed), and the time the command was executed.

Do the following:

On the Sensor, type **`downloadstatus`** at the command prompt.

Check the traffic status of a Sensor

Sensor Statistics can be viewed in the **Traffic Statistics** page. On the **Traffic Statistics** page, you can choose from the following tabs that display different type of Sensor statistics.

Steps:

1. For a standalone Sensor, click Devices → <Admin Domain Name> → Devices → <Device Name> → Troubleshooting → **Traffic Statistics**.

   For Sensors in a stack, click Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Troubleshooting → **Traffic Statistics**.
2. Click on a tab from the available tabs to obtain the required Sensor statistics.
3. Click **Save as CSV** to save and view the selected report in CSV format.
4. Follow a similar procedure and select other tabs for Sensor Performance to view the relevant Sensor Statistics.

   List of tabs for Sensor Statistics

   - Traffic Received/Sent: You can view the statistics of the total number of packets received (Rx) and transmitted (Tx) for a given device per port. You can select the port from the **Port** drop-down list for which you want to view the sent/received data. The **All Ports** option is selected by default and displays information for all the ports. When you hover the mouse over a port in the **Port** drop-down list, a tooltip displays the status of the port as **Link Up**, **Link Down**, or **Disabled**.
   - Flows: You can view the statistical TCP and UDP flow data processed by a device. Checking your flow rates can help you determine if your device is processing traffic normally. This also provides you with a view of statistics, such as the available flows supported, as well as the number of active TCP and UDP flows.
   - Dropped Packets: Using this tab, you can view the reason and the packet drop rate on a port for a device. The **All Ports** option is selected by default and displays information for all the ports.
   - Advanced Malware Analysis: You can view the statistics of the malware detected for a given device. The **By Malware Engine** option displays the malware detected data based on the malware engines configured for the device. The **By File type** option displays data based on the file type analyzed.
   - Advanced Callback Detection: You can view the count for number of alerts generated for various bot activities and other suspicious callback activity. This provides information on the amount of suspicious callback activity, and also communication attempts to the C&C servers.
   - SSL Decryption statistics: Using this tab, you can view the following statistics for SSL decryption:
     - **Sensor Statistics**: This tab displays the count for the following for SSL traffic:
       - Recycled SSL Flows - Total number of SSL flows that have not been recently used and have been freed by the Sensor.
       - SSL Flow Allocation Errors - Total number of SSL flows the Sensor could not allocate due to resource unavailability.
       - Skipped SSL Flows Due to Flow Allocation Errors - The Sensor could not allocate new SSL flows due to resource unavailability. This indicates total SSL flows that were skipped as the Sensor could not process them.
       - Packets Received from Unknown SSL Flows - Total number of SSL packets received that did not have a corresponding SSL flow.
       - SSL Flows Using Unsupported Diffie-Hellman Cipher Suite - Diffie Hellman cipher suite to encrypt the SSL flow. The Sensor will not be able to detect attacks in this SSL connection.

- SSL Flows Using Unsupported Export Cipher - Total flows that used SSLv3/TLS export cipher were negotiated, which the Sensor cannot decrypt due to the use of unsupported RSA cipher suite.
- SSL Flows Using Unsupported or Unknown Cipher - Total flows where unsupported or unknown cipher was used.

- **Internal Web Server Certificate Matches**: This tab displays the count for unmatched and matched certificates for inbound SSL traffic.

Conditions requiring a Sensor reboot

The following situations either cause or require a Sensor reboot. You have two options for rebooting the Sensor. You can reboot the Sensor from the Manager interface, or you can issue the **`reboot`** CLI command.

> **NOTE**
>
> A Sensor reboot can take up to five minutes.

- Issuing the following CLI commands causes an automatic reboot of the Sensor:
  - **`resetconfig`**
  - **`deletesignatures`**
  - **`factorydefaults`**

  For more information on the Sensor CLI commands, see the *CLI commands* section.
- Changing the Sensor's management port IP address (IPv4 or IPv6) requires a manual reboot of the Sensor, before the change takes into effect.
- Certain internal software errors can cause the Sensor to reboot itself. See a description of Sensor fault messages later in this chapter.
- Enabling/disabling SSL requires a Sensor reboot.
- Enabling/disabling parsing and detection of attacks in IPv6 traffic passing through the Sensor monitoring port requires a manual reboot of the Sensor.

  In the Manager user interface, you can enable/disable parsing and detection of attacks in IPv6 traffic with the Scan IPv6 traffic for attacks option from the IP Settings tab (Devices → <Device Name> → Setup → Advanced → **IP Settings**). For more information, see the topic *Configuring IP Settings for IPv4 and IPv6 traffic* in the *IPS Administration* section.
- Upgrading Sensor software requires a manual reboot of the Sensor.

Reboot a Sensor using the Manager

The **Reboot Sensor** action restarts a Sensor. You perform this action in the Manager interface.

To reboot a Sensor, do the following:

1. For a standalone Sensor, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → **Reboot**

   For Sensors in a stack, go to Devices → <Admin Domain Name> → Devices → <Device Name> → Member Sensors → <Stackname-node id> → Maintenance → **Reboot**
2. Click **Reboot**.

NOTE

You can also perform Sensor reboot from Devices → <Admin Domain Name> → Global → **Device Manager**. For a standalone Sensor, select the **Sensors** tab. For Sensors in stack, select the **Stacks** tab. From the list, choose the required Sensor and select **Reboot** from **Other Actions** drop-down. A **Warning** dialog box is displayed. Select the required reboot type.

Reboot a Sensor using the reboot command

The **reboot** command restarts a Sensor. You perform this action in the Sensor CLI.

1. Type **reboot** at the prompt.
2. Confirm reboot.

Sensor does not boot

If you cannot get the Sensor to boot, try the following:

- Check to ensure that the Sensor is powered on. Check the LEDs on the front of the Sensor.
- Check the front panel LEDs to ensure that the Sensor temperature is normal. For more information on Sensor LEDs, see the *Trellix Intrusion Prevention System NS-series Sensor Product Guide* for your Sensor model.
- If you see an error message *OS not found* in the CLI, you might have a corrupted internal flash. If you encounter this error, contact Technical Support to obtain help in recovering the Sensor.

Sensor stays in bad health

In certain instances, the Sensor stays in bad or uninitialized health state indefinitely. The bad health of the Sensor could be due to signature file download failure, or error while starting the Sensor.

You can perform the following high-level troubleshooting steps to trace the error:

1. Execute the following commands and check the output for any errors:
   - **show**
   - **status**
   - **show sensor health**
   - **show startup stats**
2. Check if the hardware is connected correctly.
3. Check the InfoCollector tool for logs and the configuration backup.
4. Check if the issue is due to signature file download failure. If it is due to the aforementioned error, contact Trellix Support for further assistance.
5. Execute **show startup stats** debug CLI command and check the output for any errors.

   ```
   IntruDbg#> show startup stats
   Controller not ready to send INIT_ACKs to datapaths and dos.
   initial READY msg : not yet received from datapaths and dos
   dos has sent INIT_DONE.
   datapath0 has not sent INIT_DONE.
   ```

```
datapath1 has sent INIT_DONE.
datapath2 has not sent INIT_DONE.
datapath3 has not sent INIT_DONE.
datapath4 has sent INIT_DONE.
datapath5 has sent INIT_DONE.
datapath6 has sent INIT_DONE.
datapath7 has sent INIT_DONE.
dos has not sent READY.
datapath0 has not sent READY.
datapath1 has not sent READY.
sb1cpu0 has not sent READY.
sb1cpu1 has not sent READY.
sb2cpu0 has not sent READY.
sb2cpu1 has not sent READY.
sb3cpu0 has not sent READY.
sb3cpu1 has not sent READY.
```

6. Try to power cycle or netboot or reload the Sensor image.
7. Check if the issue is due to a corrupt flash. Execute the **flashcheck** debug CLI command. Confirm that the output does not have any errors.

   ```
   Checking Flash may take more than 15 minutes and Sensor will go into Layer2 during command execution.
   Please enter Y to confirm:
   Checking Flash....
   Flash check successful. No errors in Flash
   ```

If the problem still persists, contact Trellix Support for further assistance.

Debugging critical Sensor issues

CLI commands in the debug mode are used to improve supportability of the Sensor for better debugging of critical issues. For more information on the CLI debugging commands, see the *CLI commands* section.

To further debug issues in Sensors, you can analyze the fault messages for process crash in Sensors. To enable logging of fault messages for process crash, set the **iv.core.device.processFailure** property to **true** in the `ems.properties` file and restart the Manager. For example:

```
iv.core.device.processFailure=true
```

From the Manager, you can view fault messages in the Manager → <Admin Domain Name> → Troubleshooting → Logs → **Faults** page.

NOTE

The **`iv.core.device.processFailure`** property is not present in the `ems.properties` file by default. Add it only if you want to enable logging of fault messages for process crash in Sensors.

Sensor response if its throughput is exceeded

Each Sensor model has a limited throughput. For example, consider the Trellix IPS NS7500 Sensor with a 3Gbps capacity license applied. The Sensor is rated at 3Gbps performance. With the Gigabit interfaces it is theoretically possible to cross the limit. What happens in this situation? Will it throttle the throughput to 3Gbps or will you just lose the IPS functionality for everything more than 3Gbps?

The answer is that the Sensor will drop packets irrespective of the TCP flow violation settings. We also have the latency monitor feature where the Sensor can inline-forward traffic without IPS inspection if it crosses the limit. There could also be false negatives and the traffic might experience high latency.

It is very important that you stay within the operating parameters of the device you deploy. If you are actually running at gigabit speeds, you should probably be running an NS9100/NS9200/NS9300/NS9500 Sensor, which all have a much higher throughput.

Sensor latency monitor management

All networks working from layer 2 through layer 7 experience some amount of latency. Latency monitor provides a means to reduce latency introduced by the Sensor, when the amount of traffic seen on the network substantially exceeds the Sensor capacity. Sensor latency can be due to various factors such as the policies configured, protocols, content, applications, type of traffic flowing through the Sensor, and so on. The **Inspection Options Policies** configured also adds to the latency. The following features consume Sensor resources which results in latency:

- HTTP Response Traffic Scanning
- Traffic Inspection
- Callback Activity
- Advanced Malware Policies
- SSL decryption

The latency can be reduced or varied, if Sensors detect the latency condition. Whenever there is a latency in the network, the Sensor performs the following functions:

- Raises an alert in the Manager whenever there is a latency in processing the packets
- Mitigates latency by switching to layer 2 mode

Latency monitor is available in all NS-series Sensor models.

Latency monitor feature configured monitors the time consumed for processing the packets. If the number of packets exceeds the threshold for which processing time is high, it is considered as a condition of latency. You can configure latency monitor as **`alert-only`** mode or layer 2 mode. When latency is detected, based on the configuration, an alert is raised in the Manager for the **`alert-only`** mode. If it is configured for mitigation, the latency is mitigated before an alert is raised in the Manager.

Latency monitor feature is disabled by default. The feature has to be enabled only when there is latency in the network introduced by the Sensor. If the feature is kept enabled, there is a possibility of some attacks not being detected by the Sensor.

To mitigate latency, the Sensor switches to layer 2 mode based on the sensitivity level configured. This takes less than a second after latency is detected. After latency is mitigated, the Sensor switches back to inline mode, depending on the time configured using the CLI command **`latency-monitor restore-inline`**. For example, if the **`latency-monitor restore-inline`** command is configured for 10 minutes, the Sensor tries to switch back to online mode (from layer 2) after 10 minutes.

NOTE

If the Sensor is not configured to return to inline mode automatically, it has to be manually restored to inline mode from layer 2 mode using the CLI command **`latency-monitor restore-inline`**.

Trellix IPS provides latency monitoring at three different sensitivity levels. The sensitivity levels configured in latency monitor checks for latency in two different stages:

Stage 1

- High sensitivity — Checks for latency in every incoming packet before processing
- Medium sensitivity — Checks for latency in every alternate packet before processing
- Low sensitivity — Does not check for latency

In the above scenarios, if latency is not detected, the packets are forwarded for further processing to stage 2.

Stage 2

Once latency is detected, the packets are processed through multiple phases taking optimized measures internally to handle high latency. If latency is mitigated by this process, the Sensor returns to normal processing. If latency is not mitigated, the Sensor switches to layer 2 mode if configured.

The time consumed for processing each packet is calculated when the packet is being processed by the Sensor. The calculations are based on the following parameters:

- Number of packets for which the latency is high
- Duration for which this latency condition persists

This duration for which the latency condition is monitored depends on the configured sensitivity level. Latency is detected based on the following sensitivity level thresholds configured:

- High latency — If latency is experienced (high) for 1/6th of a second for every 50 packets
- Medium latency – If latency is experienced for 2/6th of a second for every 100 packets
- Low latency – If latency is experienced (persists) for 3/6th of a second for every 150 packets

When latency is detected, the Sensor switches to latency management mode trying to mitigate latency by optimizing processes. During this mode, the situation is continuously monitored to check if the latency is mitigated. Optimization of processes may include turning off the attack detection and packets being forwarded without attack detection. The Sensor switches to layer 2 mode, if enabled, when latency is not mitigated even after running the optimization processes.

The following CLI commands for Oversubscription are deprecated:

- **`set oversubscription enable`**
- **`set oversubscription disable`**

- **`show oversubscription status`**

Trellix recommends that you use latency monitoring instead.

Enable latency monitor

You can use the following CLI commands to enable, set sensitivity level, and check the status of latency monitor feature.

latency-monitor enable action

This command enables latency monitoring in Sensor and also specifies the action to be performed if high latency is observed in the Sensor.

The following are the actions that can be specified in this command:

- alert-only — Generates an alert when a high latency is observed in the Sensor
- put-in-layer2 — Generates an alert and also forwards the traffic to layer 2.

Alerts that are generated can be seen in the **System faults** page in the Manager.

Syntax:

`latency-monitor enable action <alert-only | put-in-layer2>`

This command should be executed with a parameter value, else the command is treated as invalid.

> **NOTE**
>
> If layer2-forward is enabled, it is necessary to set the layer 2 mode as on. Otherwise, the layer2-forward action does not get executed.

Example:

`latency-monitor enable action alert-only`

latency-monitor sensitivity-level

This command configures the sensitivity level for latency management.

Syntax:

`latency-monitor sensitivity-level high`

`latency-monitor sensitivity-level medium`

`latency-monitor sensitivity-level low`

latency-monitor restore-inline

When a high latency is observed on the Sensor and the latency monitor is configured, the Sensor remains in layer 2 until a **`layer2 mode deassert`** is invoked or the Sensor reboots. This command allows the Sensor to come out of layer 2 mode without layer 2 deassert. The Sensor restores to inline from layer 2 if the following conditions are met:

- The latency monitor has put the Sensor in layer 2 mode.

- The Sensor is in good health. If the Sensor is in bad health, a deassert cannot be performed and the Sensor reboots.
- A substantial amount of time has lapsed, as configured using this command, when the Sensor went into layer 2 due to latency. The default time to trigger an automatic layer 2 deassert is 10 minutes.

If the latency continues to exist after the Sensor is restored to inline mode, the Sensor behaves according to the current setting of the latency monitor.

Syntax:

`latency-monitor restore-inline enable <10-60>`

`latency-monitor restore-inline disable`

Parameter	Description
<10-60>	The time in minutes to trigger the restore inline from layer 2. It is counted since the time the Sensor moved into layer 2 state due to high latency.

The **`latency-monitor status`** command displays the status of the latency monitor feature, and the status of the restore-inline feature of the latency monitor.

latency-monitor

This command disables the latency monitoring feature or displays the status of latency monitoring feature.

Syntax:

`latency-monitor <disable | status>`

Default Value:

Latency monitoring feature is disabled by default. If disabled, latency monitoring feature does not generate any alert nor forward the traffic to layer 2 when high latency is observed.

If latency monitoring is enabled, the following information is displayed.

- latency monitoring status (enable or disable)
- configured action (alert-only or layer2-forward)

Management of different types of traffic

Non-ethernet frames are forwarded without inspection.

The following are the types of special traffic:

- Jumbo Ethernet frames
- ISL frames

Jumbo ethernet frames

Sensors respond differently to jumbo frames based on which ports are receiving them. The following Sensor models support jumbo frame parsing of up to 9,216 bytes (9 KB) of IP payload:

- IPS-VM600 and IPS-VM5000 on ESXi and KVM
- NS9500, NS9300, NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS7300, NS7200, NS7100, NS5200, NS5100, and NS3600.

NOTE

1 Gigabit Sensor ports will inline forward jumbo frames that are greater than 9KB (9216 bytes) of IP payload and up to 9724 bytes. Frames with IP payload greater than 9724 bytes will be dropped on a 1 Gigabit port. However, 10 Gigabit Sensor ports will inline forward jumbo frames greater than 9KB (9216 bytes)of IP payload and up to 16KB (16384 bytes). Frames with IP payload greater than 16KB will be dropped on a 10 Gigabit port.

Jumbo frame parsing is not supported on NS3500, NS3200, NS3100.

ISL frames

All Trellix IPS Sensor models (running different Sensor software versions) pass ISL frames without IPS inspection.

Sensor failover issues

Checking the following connections and settings might resolve Sensor failover issues:

- The Sensor model and Sensor image version on both the peer Sensors should be the same.
- The Sensor license and IPv6 status should be identical on the peer Sensors.
- Identify the interconnect port for the selected model because the interconnect ports vary for different models.
- Check on the FO type setting on the Sensor. The failover creation would fail if the FO type is set on the primary Sensor.
- The Sensor health status should be good and normal.

External fail-open kit issues in connecting to the monitoring port

External fail-open kit issues can occur due to disconnection of network device cables and improper cabling or port configuration.

By having a check on the following connections might resolve the issue.

- Ensure that the cables are properly connected to both the network devices and the Bypass Switch.
- Ensure that the transmit and receive cables are properly connected to the Bypass Switch.

Fail-open kit related issues

This section discusses issues related to fail-open kit in the customer's environment.

Applicable to Sensor models: NS-series

Problem scenarios

1. Reset the password and all the parameters to factory default.
2. Passive fail-open does not bypass even though the fail-open kit Sensor is down/Sensor is rebooted.
3. Passive fail-open does not come up and continuously flaps.

4. Active fail-open does not come up and continuously flaps.
5. Active fail-open to Sensor link flaps continuously.

Data/Information Collection

1. Execute the following commands in the Sensor:
   - **`show`**
   - **`status`**
   - **`show intfport <port>`** (multiple times)
   - **`show inlinepktdropstat <port>`**
   - **`show sensor-load`**
2. Check the following details:
   - Active fail-open type (model) and configuration
   - Cables and SFP type
   - Physical connection details (network topology)
   - Peer device port configuration
3. Trace the Sensor files.
4. Check the infoCollector tool for the logs including the configuration backup (This is optional in case the issue is required to be reproduced locally.)

Following are the troubleshooting steps for the problem scenarios stated above:

Problem 1: Reset the password and all the parameters to factory default

If you have forgotten the password and do not know the correct password, perform the following steps to reset the password and all the other parameters of the Active Fail-Open kit.

1. On the fail-open switch, press the PB0 push button for three seconds to enter the main menu seen in the display panel.

2. Do a short press on the PB0 push button to move to the next submenu in the list.

> **NOTE**
>
> Perform this step till you move to the **OP** submenu.

3. Push the PB1 push button with a short press to select and view the options in the **OP** submenu.

4. Do a short press on the PB0 push button to move to the next option in the **OP** submenu.

   NOTE

   Perform this step till you move to the **DEFAULT** option.

5. Push the PB1 push button with a short press to select the **DEFAULT** option.

When the option **DEFAULT** is selected, it sets the default factory parameters.

In the display panel, you can view small lines (_ _ _ _ _) which indicates that default factory parameters are successfully set. As a result, the password is also reset to the default password.

Problem 2: Passive fail-open does not bypass even though the fail-open kit Sensor is down/Sensor is rebooted

1. Check if the Sensor is up and in good state.
2. In the **Physical Ports** page of the Manager, check the following configurations:
   - Port is configured to **Inline Fail Open - Passive**
   - **Auto-Negotiate** is selected.
3. If peer device port does not support MDIX, use an appropriate cable to bring up the link during the Sensor bypass. If it does not work, check the Passive Fail-Open Kit for any hardware issues.
4. While using Passive Fail-Open Kit, make sure to disable the STP on the peer device ports to avoid auto renegotiate.

NOTE

While using Passive Fail-Open Kit, each Sensor port individually negotiates with peer port initially when the Sensor is in inline mode. When the Sensor goes to bypass mode, the peer device port re-negotiates with each other. Make sure to enable **`Portfast`** on peer devices to minimize network outage.

Problem 3: Passive fail-open does not come up and continuously flaps

1. Check if the Sensor is up and in good state.
2. In the **Physical Ports** page of the Manager, check the following configurations:
   - Port is configured to **Inline Fail Open - Passive**
   - **Auto-Negotiate** is selected.
   - Appropriate cable is used. The cable type should be Cat5e and above for copper, and for fiber single-mode/multi-mode depending on the SFP used.
3. Check the control cable connection and the right controller port.
4. Check if the SFPs are according to Trellix's recommendations.
5. Check for bad/defective cable and SFPs.
6. Check if the peer device port is working and if the port settings are set to **Auto-Negotiate**.
7. Ensure local port testing (by connecting monitoring ports back to back).

8. Swap the working SFP and cables from another port pair.
9. If all the above steps fail, RMA the Sensor.

Problem 4: Active fail-open does not come up and continuously flaps

1. Check if the Sensor is up and in good state.
2. Use Trellix recommended transceivers (normal SFP for 1G, SPF+ for 10G, and QSP for 10G ports).
3. Check the Active Fail-Open Kit monitoring port setting (specifically **Auto-Negotiate** and speed settings). It should be the same as Sensor monitoring ports and peer device.
4. Ensure local loopback port testing (by connecting monitoring ports back to back).
5. Swap the working SFP and cables from another port pair.
6. Check the load on the Sensor.
7. If all the above steps fail, RMA the Sensor.

Steps to Configure and Debug active fail-open

When configuring the Active Fail-Open Kit, in case of flapping issues, the configuration on the network peer ports must match with the one on Active Fail-Open Kit-Sensor monitoring port pair.

1. Ensure the power to the Optical Bypass Switch is on.
2. Using a DB-9 RS232 programming cable. Connect a PC that is running the HyperTerminal to the Optical Bypass Switch.
3. Launch a terminal emulation software like HyperTerminal, and set the following communication parameters:
    - Bits per second: 19200
    - Stop bit: 1
    - Data bits: 8
    - Flow control: None
    - Parity: None
4. Click **OK**. The CLI banner and login prompt are displayed.
5. Type the default username and password. (The default username and password is **Trellix00** and is case-sensitive).
6. Once you are logged in, use the following commands in the table to configure and troubleshoot the Active Fail-Open Kit:

Com-mand	Description
a	Set the timeout value. To set the Timeout value, do the following: • Type **a** and press **Enter**. • **TimeOut period (1-254 sec)** — Type the number of seconds between each heartbeat (1-254 seconds) and press **Enter**. Default = 1. • **Retry Count (1-254)** — Type the number of missed heartbeats allowed before the Bypass Switch enters the **On** mode. Default = 3. **NOTE** The Retry Count must be greater than or equal to the Timeout period.
b	Set Switch parameters. To set speed duplex and auto-negotiation, LFD, bypass detect: • **1**= Turn On. • **0** = Turn Off. • **Fail Mode Open/Close**= 1 **NOTE** The LFD and Bypass detecting mode settings cannot be changed.
c	Set TAP mode. • Type **c** and press **Enter**. • Type **1** to set the tap mode **On**, or **0** to set the tap mode **Off**. Default = Off.
d	Show configuration. Type **d** and press **Enter**. The following is displayed: • **LFD** = On • **Timeout Period**= 1 • **Bypass Detect**= Off • **Retry Count**= 3 • **Fail Mode**= Open • **Bypass State**= Off • **TAP Mode**= Off

Com-mand	Description
e	Show port status. Type **e** and press **Enter**. The following is displayed: • **Port A**= Up/Down • **Port B**= Up/Down • **Port 1**= Up/Down • **Port 2**= Up/Down
f	Set Switch name. • Type **f** and press **Enter**. • At the prompt, type the Switch name, which can be 8 characters long.
z	Reset to Factory Defaults.

Problem 5: Active fail-open to Sensor link flaps continuously

1. Check if the Sensor is up and in a good state.
2. Use Trellix recommended transceivers (normal SFP for 1G, SPF+ for 10G, QSFP+ for 40G, and QSP28 for 100G ports).
3. Check the Active Fail-Open Kit monitoring port setting (specifically **Auto-Negotiate** and speed settings). It should be the same as Sensor monitoring ports and peer device.
4. Check the Sensor ports (by connecting monitoring ports back to back).
5. Swap the working SFPs and cables from the other working port pair.
6. Swap the working Active Fail-Open Kit to confirm whether a hardware problem exists.
7. Check the load on the Sensor to make sure that Sitera is dropping the HB packets from the Active Fail-Open Kit. To test if the Sitera is dropping the HB packets, contact Trellix Support for further assistance.

Debugging issues with Connection Limiting policies

Connection Limiting policies consist of a set of rules that enable the Sensors to limit the number of connections a host can establish or a connection rate. This section provides troubleshooting steps to resolve few issues with Connection Limiting policies.

Prerequisites:

Check that the Connection Limiting policy is correctly configured.

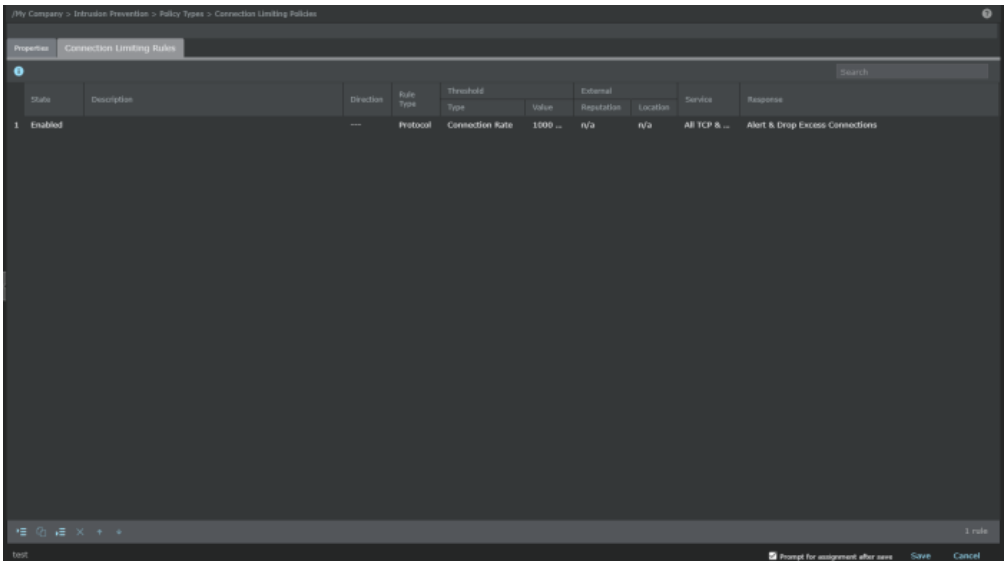
- You can configure the Connection Limiting policy with the monitoring ports in SPAN, tap, or inline modes. The response actions differ for SPAN and tap modes. In these modes, the Sensor cannot block the connections or quarantine the hosts.
- The connections are limited based on the predefined threshold value. The threshold value is defined as connections per second or active connections. For example, if you define 1 connection per second as the threshold value, then, 10 connections are allowed per 10 seconds. So, if there are 10 connections in the first second, all other connections from the second to the tenth second are dropped. On the other hand, if you have 1 connection for each second, all the 10 connections until the tenth second are allowed.

- Connection Limiting rule based on **Protocol** applies to both IPv4 and IPv6 traffic. Connection limiting rule based on **Trellix GTI** applies to only IPv4 traffic. GTI does not support IPv6 traffic.
- The Connection Limiting alert raised is [IP: Too many TCP/UDP/ICMP sessions]. This alert is present in the **IPS Policies**.

Perform these steps to configure a basic Connection Limiting policy:

1. Go to Policy → <Admin Domain> → Intrusion Prevention → Policy Types → **Connection Limiting Policies**.
2. Click **New** and configure the rule properties like description and visibility.
3. Click **Next**, in **Connection Limiting Rules** page, set the parameters like state, direction, and response.

Figure 817. Connection Limiting Rule



4. Go to Policy → Intrusion Prevention → **Policy Manager** to apply the Connection Limiting policy on the Sensor interface.

> **NOTE**
>
> Make sure the [IP: Too many TCP/UDP/ICMP sessions] alert is enabled in the IPS policy that is applied on the Sensor interface.

Troubleshooting Connection Limiting issues

After Connection Limiting policies are configured, you might come across issues like the following:

- No alerts are raised in the Manager.
- Excess packets are not dropped or denied.
- Hosts are not quarantined.

Connection Limiting rules can be configured with protocol types **Alert only**, **Alert & Drop Excess Connections**, **Alert & Deny Excess Connections**, and **Alert & Quarantine**.

Perform these steps to troubleshoot issues such as alerts not raised in the Manager, excess packets not dropped or denied, or hosts not quarantined after reaching the threshold value.

1. Make sure that the Connection Limiting policy rules are configured and applied to the Sensor interface.
2. From the Sensor CLI, run the **`show inlinepktdropstat all`** command and check if the **`Conn Limiting Pkt Drop Count`** is 0. This means that the configured threshold value is not reached. Only when the count reaches a threshold value, alerts are triggered in the Manager.
3. Check whether the incoming traffic rate to the Sensor meets the Connection Limiting rule's threshold value. If it does not meet the threshold value, send the corresponding traffic rate.
4. Set a lower threshold value and check the active connections or connections per second.
5. Check if there is any firewall ignore rule for the source IP address configured in the Connection Limiting rule.
    a. Go to Policy → Intrusion Prevension → Policy Types → Firewall Policies → <Firewall Policy> → **Access Rules.**
    b. Select a policy and click **Edit** to view the rules of that policy or double-click on the row of the policy.
    c. On the Access Rules tab, check if a source IP address's **Response** is set as **Stateless Ignore** or **Ignore**.
6. Check if the source IP address configured in the Connection Limiting rule is part of the **Quarantine Exceptions** list. Go to Devices → Global → IPS Device Settings → Quarantine → **Default Port Settings** to if source IP address is quarantined.

Considerations for GTI connection limiting and XFF feature

When you configure GTI and XFF for a connection limiting rule:

- The Sensor cannot perform GTI lookup on the XFF IP address. The GTI-based connection limiting does not work when the XFF feature is enabled.
- When the XFF feature is enabled, the Sensor expects that all HTTP flows should have XFF data in the HTTP header.
- The Sensor supports connection limiting on XFF based on protocol-based connection limiting.

Alert Detection Matrix

The table briefs how alerts are detected based on the connection limiting type and XFF feature configuration.

Connection limiting type	XFF configuration	XFF or Non XFF tag traffic sent to Sensor	Proxy IP reputation	XFF IP	Alert detection
Protocol	Disabled	Without XFF	-		Yes
Protocol	Enabled	With XFF	-		Yes
Protocol	Enabled	Without XFF	-		No
GTI	Disabled	Without XFF	-		Yes
GTI	Enabled	With XFF	Low risk	High risk	No
GTI	Enabled	With XFF	High risk	Low risk	No
GTI	Enabled	Without XFF	-	-	No

Issues with Quarantine

Trellix IPS enables you to quarantine your network hosts when required.

There are two ways to quarantine hosts:

- Configure the Sensor to quarantine hosts automatically when they generate specific attacks.
- Manually quarantine specific hosts that are listed in the **Attack Log** page.
- You can manually add endpoints to quarantine from the **Quarantine** page.

You might see the following issues while quarantining:

- When you quarantine a host from attack log but the host is not listed in the quarantine page, and the host is stuck.
- Quarantine page has a host that is not deleted after the expiry time. You might also see an error when manually deleting a host from the Quarantine page.

To confirm if it is a quarantine issue, put the Sensor in Layer 2 or add the host IP address to the **Quarantine Exceptions** list and check if the issue is resolved. If the issue is not resolved, contact Trellix Support.

Internal switch port configuration and packet forwarding issues

The following CLI commands provide insight into the Sensor internal switch port configuration. It also helps troubleshoot packet forwarding issues.

- Use **`bcmcli "<string input of the bcm>"`** command to retrieve bcm process output from the primary unit.

  For example: **`bcmcli "ps"`**

  > **NOTE**
  >
  > This command is applicable to NS-series Sensors.

- Use **`bcmcli-sec "<string input from the secondary unit bcm>"`** command to retrieve the bcm process output of secondary unit on primary unit. This command is applicable for primary unit alone.

  For example: **`bcmcli-sec "ps"`**

  > **NOTE**
  >
  > This command is applicable to NS9300 Sensors only.

Trellix recommends you not to execute these commands without the help of Trellix Support as it might cause Sensor issues based on the parameter given. In case you encounter a problem, contact Trellix Support for further assistance.

Issues and status checks for the Manager

This section describes issues and status checks specific to the Manager.

The Manager connectivity to the database

In the event that the Manager loses connectivity to the database (i.e. the database goes down) the alerts are stored in a flat file on the Manager server. When the database connectivity is restored, the alerts are stored in the database.

The Manager database is full

We recommend that you monitor the disk space continually to prevent this from happening.

If the Manager database or disk space is full, the Manager will unable to process any new alerts or packet logs. In addition, the Manager might not be able to process any configuration changes, including policy changes and alert acknowledgement. In fact, the Manager might stop functioning completely.

To rectify this situation, please perform maintenance operations on the database, including deleting unnecessary alerts and packet logs. Furthermore, please reevaluate database capacity planning and sizing, and monitor free space proactively. The Manager is designed with various file and disk maintenance functions. You can archive alert and packetlog data and then delete the data to free up disk space. It also provides a standalone tool for creating database backups that can be archived for emergency restoration.

The Manager also provides disk maintenance alerts, which send proactive system fault messages when the Manager disk space reaches a threshold of 51%. The Manager generates the disk space warning fault for disk space utilization. The severity of this fault changes with respect to the percentage of increase in the disk space utilization.

The Manager database fails to start

Below are some of the reasons for the Manager database failing to start on a Windows system.

- The Manager database process is already running. This can be verified by opening Windows Task Manager and looking for mariadbd.exe with Memory foot print of hundreds of MB.
- Start the service "Trellix IPS Manager Database" from services window. If the service has not started, check for the reason of failure in **<DB_Install_Dir>\data\<hostname>.err** file.

  NOTE

  The default Manager database directory is `%programfiles%\Trellix\IPS Manager\MariaDB`.

- In the command prompt, navigate to **<DB_Install_Dir>\bin** and run "mariadbd --version" manually. If the service has started, the message is displayed as shown below:

  ```
  mariadbd Ver 10.5.15-MariaDB-log for Win64 on AMD64 (mariadb.org binary distribution)
  ```

  NOTE

  The version number and commercial license definition vary across Manager versions.

If unexpected database service shutdown occurs, check the **<DB_Install_Dir>\data\<hostname>.err** file for possible reason. Also, during this unexpected shutdown, MariaDB creates a minidump that is, mariadbd.dmp in the data directory. If necessary, this file can be used for further analysis.

Below are some of the reasons for the Manager database failing to start on a Linux system.

- The Manager database process is already running. This can be verified by executing **database status** on CLI.
- Start the service by executing **database start** on CLI. If the service has not started, then, check for the reason of failure in **<hostname>.err** file. Execute the command **show log file <hostname>.err** to open the file.

- Execute **show databaseVersion** on CLI. If the service has started, the message is displayed as shown below:

```
Manager@USER> show databaseVersion

/opt/IPSManager/MariaDB/bin/mariadb Ver 15.1 Distrib 10.5.15-MariaDB, for Linux-systemd (x86_64) us-
ing readline 5.1
```

> **NOTE**
>
> The version number and commercial license definition vary across Manager versions.

If unexpected database service shutdown occurs, check the **<hostname>.err** file for possible reason. Also, during this unexpected shutdown, MariaDB creates a minidump named mariadbd.dmp in the data directory. If necessary, this file can be used for further analysis.

MariaDB issues

The common symptoms that occur if your database tables become corrupt:

- Inability to acknowledge or delete faults in **System Faults**.
- When trying to view packet log from **Attack log**, you receive an error message:

  ```
  No Packet log available for this alert at this time
  ```

If you think that your MariaDB database tables have become corrupt, follow the instructions on verifying your tables, which is available in Trellix KnowledgeBase article KB60660. (Go to https://thrive.trellix.com/s/customknowledge, login to the portal, enter the KB Article number in **Search Knowledge...** search field and press **Enter**.)

Sensor not displayed in the resource tree

After adding the Sensor and establishing trust, if the Sensor is not displayed in the resource tree, perform the following steps for troubleshooting:

1. Capture traffic using Wireshark in the Manager.
2. Verify if the Manager is receiving UDP response packets from the Sensor.
3. Configure the firewall to allow UDP traffic if response packets are not coming.
4. Verify if the Manager system has multiple NIC cards. If yes:
   - For Windows-based Manager, open **<Manager_Install_Dir>\bin\tms.bat**.

     > **NOTE**
     >
     > The default installation path for Windows-based Manager is **%programfiles%\Trellix\IPS Manager\App**.

   - For Linux-based Manager, open **open tms.sh** by executing the command **edit tms.sh**
5. Later, modify the following line to assign the relevant IP address that is also used in the Sensor configuration: **Set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPIPaddress=""restart Manager**

   You can enable detailed debugging messages by modifying the following file:

- For Windows-based Manager, **<Manager_Install_Dir>\config\log4j2.xml** file
- For Linux-based Manager, **log4j2.xml** file. To open this file, execute **edit log4j2.xml**

Find out and modify the following lines in the **log4j2.xml** file:

- ```
  <Logger name="iv.core.DiscoveryService" additivity="false" level="debug">
      <appender-ref ref="DEVICE_CONFIG_LOG"/>
  </Logger>
  ```
- ```
  <Logger name="iv.core.SensorConfiguration" additivity="false" level="debug">
      <appender-ref ref="DEVICE_CONFIG_LOG"/>
  </Logger>
  ```

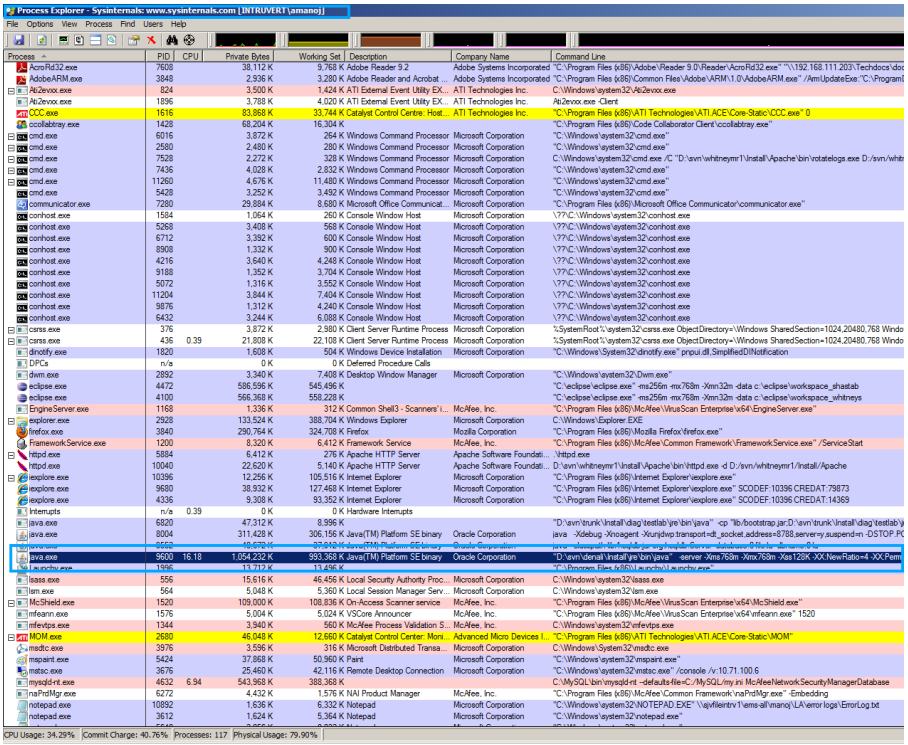
The modified logs will be available in **<Manager_Install_Dir>\logs\device_config.log** file.

The Manager fails to start

Below are some of the common reasons for the Manager failing to start:

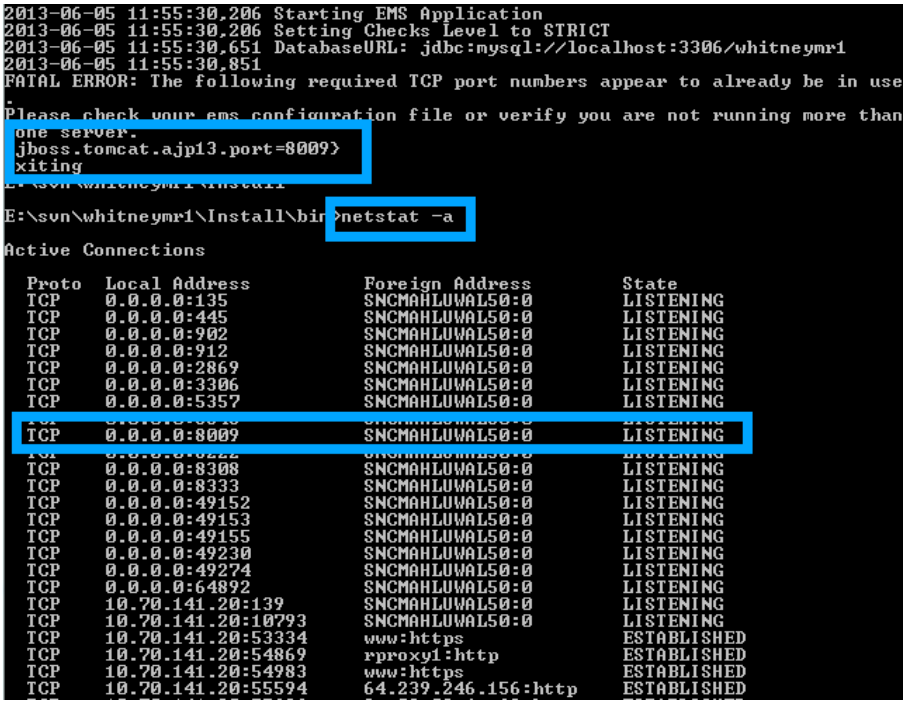
- The Manager Java process is already running. This can be checked by opening Windows Task Manager and looking for a java.exe with Memory foot print of hundreds of MB. Alternatively, install sysinternals' Process Explorer from HTTP://TECHNET.MICROSOFT.COM/EN-US/SYSINTERNALS/BB896653 to locate the java process. If found, as indicated in the following image, it should be removed.

Figure 818. Check if Manager Java process is already running



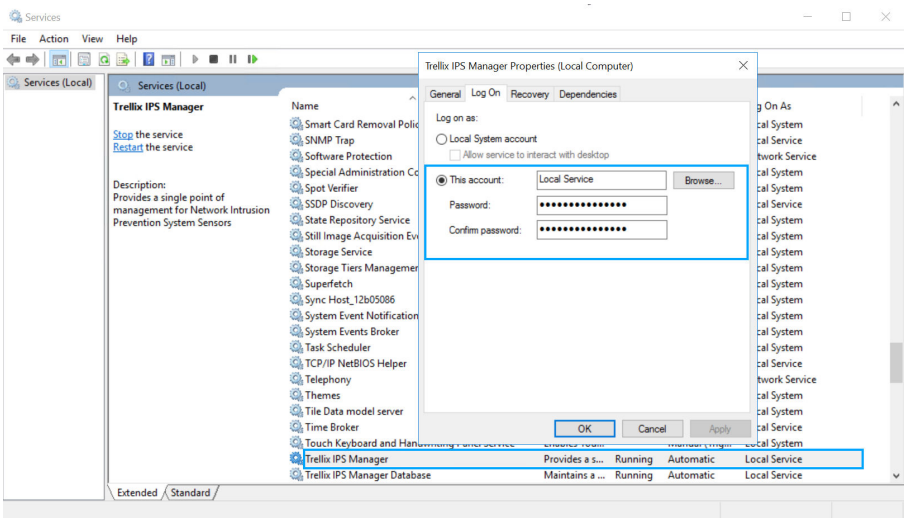
- In the command prompt, navigate to **%programfiles%\Trellix\IPS Manager\App\bin** and run **tms.bat** manually. Then check for below conditions.
  - One of the TCP ports that Manager binds to is in use. Use **netstat -nab** to list out all ports in use. These netstat options also identify the executable that is binding to the port and the executable should be stopped.

Figure 819. Check netstats



- Check whether the logged user on the server has permissions to launch Trellix IPS Manager service. This can be found by right clicking on the service, selecting **Properties** and then **Log On** tab. So, if the logged user doesn't have permission to run local service, the Manager does not start.

Figure 820. Check user permissions



- The server does not have enough RAM. The **`tms.bat`** file has a -Xmx<MaxHeap> setting in MB specifying Java heap in MB that needs to be allocated to the process. If the server does not have that much RAM, then process will not start.
- Sometimes, especially on 32-bit machines, when there are instances of heap exhaustion, you may try to increase the maximum heap setting to a larger volume assuming to be having full 2000MB available. However stack space and native libraries share memory in the same 2000MB space and java heap cannot be higher than 1170MB. So, ensure that -Xmx setting is not greater than 1170MB if it is a 32 bit machine.

- The process fails to start with a classloader exception such as ClassNotFound. This typically indicates issues with the Manager installation. A fresh installation or upgrade as appropriate should resolve the issue.

Analyze memory-related issues

Memory-related issues occur in the Manager when the amount of the heap space allocated by the Operating System, based on JVM options (-Xms, -Xmx) specified in **`tms.bat`** for Windows-based system and **`tms.sh`** for Linux-based system, is not enough for the application to continue to behave an expected manner.

Typical symptoms include the following:

- Application not being responsive — CPU usage of the Java process being high
- Application crashing — terminating
- Communication channel(s) flap between the Manager and the device — channel connections being reset frequently
- Application not being able to start

The following logs are required for analysis:

- Infocollector logs (mainly ems, emsmem, acqount, slowquery, and DB err file).
  - Threads stack trace and CPU usage using stack trace and collect live objects in heap memory space using the heap dump tool.

> **NOTE**
>
> These logs are required before restarting the application, which is usually done to restore the application, unless it is recurring issue. Heap dump tool or stack trace doesn't require a restart as, in most cases, memory leak might not be reproduced. And without these logs, an RCA would be extremely challenging.

Steps:

1. Establish that JVM has experienced memory overload. This can be determined by searching the info collector log with string OutOfMemoryError. The most preferred way is to perform a global search in all the files of InfoCollector whose file name starts with ems* - with wildcard, and this can be done using text editors like TextPad. If there are no search results, it signifies that JVM does not experience any memory issue because of the Manager application, but it could be caused by other applications or some operating System dlls - check JVM crash files.
2. If there is an exception as mentioned above, check the emsmem logs to know the time of memory and frequency; usually, most cases exhibit either slow memory over a period of days or months, or sudden decrease in memory.
3. After establishing the time of memory leak, check alert rate in aqcount logs. The recommended value is maximum 60alert/sec; any value above this value over a period of time can cause memory issues. Alert Rate can be calculated from aqcount logs using the following method:
   - Look for an entry similar to **2012-07-31 13:27:52,012 AltQ:EPR-RCD: 6178500 0 112**.Three important information, as mentioned below, need to be extracted:
     - (t1)timestamp(2012-07-31 13:27:52,012)
     - Alert received string(AltQ:EPR-RCD)
     - alert count(6178500).

- Now, look for next immediately occurring entry which contains "AltQ:EPR-RCD". This entry will have an alert count greater by 300. So, if the above example is considered, the alert count will be 6178800. Note the (t2)timestamp of this entry.

Alert Rate = 300/(t2-t1)

4. Check the MariaDB errors logs to find if there are any errors messages.
5. Check Slowquery logs to find out if there are any queries that are being called repeatedly and taking considerable amount time to execute (that is, more than 5-10 minutes).
6. Search for all the error messages in ems logs using string "error" as similar to the first step. Observe for the error messages that have occurred during the time interval of memory leak.
7. If a heap dump — .bin file with prefixes 850heap, 1500heap — is available, it can be used in the heap dump analyzer tools such as MAT and VisualVM, which will identify the suspects causing memory leak.

The Manager keeps on loading at startup

Problem/Symptom: The Manager keeps on loading and does not startup properly even after several minutes.

Potential Cause:

- The Manager server (Java) tries to establish connections to the web server. If any of the server communication are not established, the Manager will not startup properly. The problem might be due to the following reasons:
  - Java process not running on serverClient.
  - The client cannot talk to server (blocked ports).
  - Database is not running on the server.
- The Manager server process is not running on the appliance or on the Manager software.

Remedy:

For Windows-based Manager, verify that the service is started and running properly.

1. From the Start Menu search bar, type **cmd** and open the command prompt with elevated privileges.
2. Run the command **`IMAGENAME eq java.exe`** to verify if Java is running on the server.
3. Check the output for java.exe on the server to ensure that the mem usage is above 500MB. If there is nothing listed, the Manager service is not running.
4. Run the following commands on a command prompt to verify that ports 8501 to 8505 are open and actively listening.
   - **`netstat -an | find "LISTENING" | find "8501"`**
   - **`netstat -an | find "LISTENING" | find "8502"`**
   - **`netstat -an | find "LISTENING" | find "8503"`**
   - **`netstat -an | find "LISTENING" | find "8504"`**
   - **`netstat -an | find "LISTENING" | find "8505"`**
5. Verify if MariaDB is running by executing the command **`netstat -an | find "LISTENING" | find "3306"`**
6. Try to start the Manager manually by running **`tms.bat`** from **`<Manager_Install_Dir>\App\bin\`**. Look for error messages at the bottom of this output.

7. Check the bottom of the **emsout.log** file in **<Manager_Install_Dir>\App\logs** for errors.

> **NOTE**
>
> The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

For Linux-based Manager, verify that the service is started and running properly.

- Check if manager service is up by executing the **manager status** command.
- Check if database service is up by executing the **database status** command.
- Check the bottom of the **emsout.log** file for errors by executing the **show log file emsout.log** command.

Unable to log on to the Manager after typing credentials

Problem/Symptom: The Manager application does not open after typing the user name and password from the logon page. It displays only a blank page.

Potential Cause:

The Manager requires the window's pop-up capability to be disabled or have an exclusion configured.

Remedy:

Disable the pop-up blocker functionality.

or,

Create an exception for the Manager server IP addresses.

Table 108. Internet Explorer

To disable pop-up blocker	To add exception to pop-up blocker list
1. From the command prompt, execute the command **Inetcpl.cpl.** The **Internet Properties** window is displayed. 2. In the **Privacy** tab, deselect the check-box option **Turn on Pop-up Blocker**.	1. From the command prompt, execute the command **Inetcpl.cpl.** The **Internet Properties** window is displayed. 2. On the **Privacy** tab, select the **Turn on Pop-up Blocker** check-box. 3. Click **Settings**. The **Pop-up Blocker Settings** window is displayed. 4. In the **Address of website to allow** field, add the IP address or host name of the Manager to the list of websites to be allowed.

Table 109. Mozilla Firefox

To disable pop-up blocker	To add exception to pop-up blocker list
1. In the Firefox browser,select Tools → **Options** and click the **Content** tab. 2. Deselect the, **Block pop-up windows** checkbox.	1. In the Firefox browser, select to Tools → **Options** and click on the **Content** tab. 2. Select the **Block pop-up windows** checkbox. 3. Click **Exceptions**. The **Allowed sites Pop-ups** window is displayed. 4. In the **Address of website** text field, add the IP address or host name of the Manager to the list of web sites to be allowed.

Table 110. Google Chrome

To disable pop-up blocker	To add exception to pop-up blocker list
1. In the Google Chrome browser, type the following in the address bar: chrome://chrome/settings/content. The **Content Settings** window is displayed. 2. Select **Allow all sites to show pop-ups**.	1. In the Google Chrome browser, type the following in the address bar: chrome://settings/contentExceptions#popups. The **Content Settings** window is displayed. 2. In the **Hostname pattern** field, add the IP address or host name of the Manager to the list of exceptions.

Login button does not work

Problem/Symptom: The **Login** button does not work.

Potential Cause: Internet options are too restrictive.

Remedy:

Verify the following Internet Explorer browser settings by executing the **`Inetcpl.cpl`** command from the command prompt.

The Manager IP address or host name can be added to the trusted sites.

Or,

Modify the security zone's settings to allow the required changes. To modify the settings:

1. Click the **Security** tab.
2. Click **Custom Level** and enable the following entries:
   - Run ActiveX Controls & Plugins
   - Script ActiveX Controls mark safe for scripting
   - Downloads: File Download
   - Scripting: Active Scripting
3. Click the **Advanced** tab and scroll down to the **Security** section.
4. Verify that the option **Do not save encrypted page to disk** is deselected.

Automatic Windows update fails in the Manager

Problem/Symptom: The automatic Windows update fails and the Windows update log has the following error:

Handler WARNING: DPX failed with 0x80070570.

Potential Cause: Proxy or firewall settings do not allow range request.

Remedy:

In the proxy server that you use, change the setting to allow a range request and ensure that the range value is wide.

> **NOTE**
>
> The DPX (Delta Package eXpander) is a Windows setting and is pre-set by default. It is recommended not to change or disable the DPX setting to fix this problem.

Alerts do not show up in Attack Log or on dashboards after upgrading the Manager

Problem/Symptom: Alerts do not appear in the **Attack Log** page or on dashboards after upgrading the Manager.

Potential Cause and Remedy: If the alerts are missing in the **Attack Log** page, or you see a blank dashboard after upgrading the Manager, you need to run the Apache Solr scripts which ensures the previous alerts and other events are displayed in the Manager GUI. For more information on the alerts processing scripts and Apache Solr scripts, refer to the section *Run the Apache Solr scripts* in the *Trellix Intrusion Prevention System Installation Guide*.

> **NOTE**
>
> For detailed information on synchronizing IPS alerts in the Solr Database in Manager version 9.1.7.77 till 10.1.7.40, refer to KB86158.

From software version 10.1.7.44 or above, the Manager should automatically import the Solr data. If the alerts are missing from the **Attack Log** or on Manager dashboards after the installation, it indicates that the automatic import of Solr data has not been successful. In such a case, a critical fault is displayed in the Manager → <Admin Domain Name> → Troubleshooting → Logs → **Faults** to notify you regarding the failure in import of Solr data.

You need to run SolrDB import manually in the Manager to troubleshoot this issue. To do so, perform the following steps.

For Windows-based Manager:

Steps:

1. Stop the Manager Service and Manager Watchdog Service.
2. Navigate to `<Manager_Install_dir>\Solr\server\solr\alerts` and take a backup of the *data* folder. Keep this folder outside the Manager installation folder.
3. Delete the *data* folder present in `<Manager_Install_dir>\Solr\server\solr\alerts`.
4. Set the Database flag to initiate import using the following SQL query:

   ```
   UPDATE iv_emsproperties SET VALUE="true" WHERE NAME="iv.core.solr.importenabled";
   ```

5. Now, start the Manager Service and Manager Watchdog Service.
6. Wait till the Manager GUI is up and running. Then, check for the alerts in **Attack Log** and information on Manager dashboards.

For Linux-based manager:

Steps:

1. Stop the Manager service using **`manager stop`** command.
2. Stop the Manager Watchdog service using **`watchdog stop`** command.
3. Login to the Manager via SFTP window.
4. Navigate to the directory `/opt/IPSManager/Solr/server/solr/alerts`. Locate the *data* folder inside `opt/IPSManager/Solr/server/solr/alerts` directory and take a backup of that folder by copying it to the local machine.

   > **NOTE**
   >
   > If you are using Manager version 10.1.7.44 - 10.1.7.61, the directory path would be `/opt/NetworkSecurityManager/Solr/server/alerts`.

5. After the backup has been taken, delete the *data* folder inside the`/opt/IPSManager/Solr/server/solr/alerts` directory.
6. Open a terminal and run the **`dbshell`** command. Enter the DB username and password, when prompted.
7. Set the database flag to initiate import using the following SQL query:

   ```
   UPDATE iv_emsproperties SET VALUE="true" WHERE NAME="iv.core.solr.importenabled";
   ```

8. Start the Manager service using **`manager start`** command.
9. Start the Manager Watchdog service using **`watchdog start`** command.
10. Wait till the Manager GUI is up and running. Then, check for the alerts in **Attack Log** and information on Manager dashboards.

How to terminate signature set deployment in the Trellix IPS Manager

This section details the steps to terminate signature set deployment in the Manager.

Terminate signature set deployment in a Windows-based Manager

Steps:

1. Stop the Trellix IPS Manager Watchdog service.
2. Stop the Trellix IPS Manager service.
3. Open command prompt, navigate to **`%programfiles%\Trellix\IPS Manager\MariaDB\bin`**.
4. Execute the following command block to enter the database shell. Enter the database password when prompted.

   ```
   mysql -u <Database_username> -p
   ```

Field name	Description
<Database_username>	Username of the Trellix IPS Manager database, for example, **admin**.

5. Execute the following command block:

```
use lf;
```

6. Execute the following command block:

```
Select * from iv_sensor where name = '<Sensor_Name>'
```

Field name	Description
<Sensor_Name>	Name of the Sensor you want to terminate the signature set deployment in the Manager.

7. Execute the following command block:

```
UPDATE iv_sensor SET config_flags = 801 WHERE name = '<Sensor_Name>'
```

Field name	Description
<Sensor_Name>	Name of the Sensor you want to terminate the signature set deployment in the Manager.

8. Start the Trellix IPS Manager service.
9. Start the Trellix IPS Manager Watchdog service.

Terminate signature set deployment in a Linux-based Manager

Steps:

1. Log in to the Manager shell.
2. Stop the Trellix IPS Manager service using the **watchdog stop** command.
3. Stop the Trellix IPS Manager Watchdog service using the **manager stop** command.
4. Execute **dbShell** command to log in to the database shell.
5. Execute the following command block:

```
use lf;
```

6. Execute the following command block:

```
Select * from iv_sensor where name = '<Sensor_Name>';
```

Field name	Description
<Sensor_Name>	Name of the Sensor you want to terminate the signature set deployment in the Manager.

7. Execute the following command block:

```
UPDATE iv_sensor SET config_flags = 801 WHERE name = '<Sensor_Name>';
```

Field name	Description
<Sensor_Name>	Name of the Sensor you want to terminate the signature set deployment in the Manager.

8. Exit the database shell using the **exit** command.

9. Start the Trellix IPS Manager service using **`manager start`** command.
10. Start the Trellix IPS Manager Watchdog service using **`watchdog start`** command.

MDR pair creation fails when using CA signed certificates with ECDSA algorithm

Problem/Symptom: Creation of an MDR pair fails with the following error log in the **`ems.log`** file.

`javax.net.ssl.SSLHandshakeException:Certificates do not conform to algorithm constraints`

Potential Cause: This issue occurs when the Managers in the MDR pair use CA signed certificates with ECDSA algorithm.

Remedy:

Perform the following steps when this error occurs in the **`ems.log`** file:

1. Login to the Manager server.
2. Navigate to **`<Manager_Install_Dir>\jre\lib\security`**.

   > **NOTE**
   >
   > The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

3. Open the **`java.security`** file.
4. Remove the ECDSA value from the **`jdk.tls.disabledAlgorithms`** parameter.
5. Close the **`java.security`** file.
6. Restart the Manager server.

Issues and status checks for the Sensor and Manager in combination

This section describes issues and status checks when the Sensor and Manager are connected.

Difficulties connecting Sensor and Manager

If you experience problems getting the Trellix IPS Manager and Sensor to communicate, see if one of the following situations might be the cause.

Network connectivity

- Ensure that the Sensor and Manager server have power and are appropriately connected to the network.
- Verify the link indicator lights on both devices to indicate they have an active link.
- Ping the Sensor and Manager server to ensure that they are available on the network.

Inconsistency in Sensor and Manager configuration

- Verify that the Sensor name that was entered in the CLI is identical to that entered in the Manager. Ensure the same for the shared secret key value. If these values do not match, the two cannot communicate.

NOTE

The Sensor name is case sensitive.

- Check the network addresses for the Manager, the Manager's gateway, and the Sensor to ensure everything is configured correctly by typing **show** at the Sensor CLI command prompt.

Software or signature set incompatibility

Verify that the Sensor software image, Manager software version, and signature set version are compatible. This information is provided in the release notes that accompany each product release. The Manager version must be higher than the Sensor software version. Recommend that you refer to the release notes of both the Manager and Sensor software to verify compatibility.

Consider that your Manager version is 10.1.7.61 and the Sensor is an NS-series Sensor on software version 10.1.5.190. Version 10.1.5.190 for NS-series Sensors was released after Manager version 10.1.7.61. By referring to the release notes of Manager 10.1.7.61, you can verify whether Manager 10.1.7.61 can manage an NS-series Sensor on 10.1.5.190.

Firewall between the devices

If there is a firewall between the Sensor and the Manager server, make sure the devices are able to communicate by opening the appropriate ports.

NOTE

Ports used by the Manager server are listed in the *Trellix Intrusion Prevention System Installation Guide*.

Management port configuration

If you experience problems getting your Sensor and Manager to communicate, it might be a communication issue between the Sensor's Management port and the network device to which it is connected. Check the Management Port Link indicator lights on the Sensor. If the link is down, see if any of the following suggestions enable connectivity.

- Check that the network device is online.
- Check the cable connecting the Sensor to the network device.
- Ensure that the port on the device to which the Management port is connected is enabled and active.
- The port speed and duplex mode of the two devices must match. For example, if the device connecting to the Sensor is not set to auto-negotiate, you must configure the Management port to use the same settings as those of the device connecting to the Management port. To troubleshoot this, use the **`set mgmtport`** command.

NOTE

Check the link LEDs on the devices to see if communication is established, or use the **`show mgmtport`** command to show the link's status.

Try each of these configuration options to see if one establishes a link:

1. If possible, set the other device's port configuration to auto-negotiate. (The Sensor is set to auto-negotiate by default.)
2. Using the **`set mgmtport`** command as described below in *Setting the management port speed and duplex mode*, try setting the speed and port of the Sensor to **`speed 100`** and **`duplex half or full`**.
3. If no link is established, try **`speed 10`** and **`duplex half or full`**.
4. If none of these attempts creates a link, try setting the port on the other device to a speed of 100, duplex half or full, and try step 2 again.
5. If this does not establish a link, you can then do the same, setting the other device to a speed of 10, duplex half or full, and try step 3 again.
6. If you are still experiencing difficulties, contact Trellix technical support.

Set the management port speed and the duplex mode

- Set the speed of the Management port and determine whether the port should be set to half-duplex or full-duplex. At the prompt, type:

  `set mgmtport speed <10 | 100 | 1000 | 10000> duplex <half | full>`

  where< **`10`**> indicates 10 Mbps, < **`100`**> indicates 100 Mbps, < **`1000`**> indicates 1000 Mbps, < **`10000`**> indicates 10000 Mbps, < **`half`**> indicates half-duplex, and < **`full`** > indicates full-duplex.

  Example: **`set mgmtport speed 100 duplex half`**

  > **NOTE**
  >
  > Management port speed settings vary depending on the Sensor model used. Availability of half duplex option depends on the management port speed you set.

  > **NOTE**
  >
  > This command is not applicable for NS9500, NS7600, NS7500, and NS3600 Sensors. Duplex option is not available in 9100, 9200, and 9300 Sensors.

Loss of connectivity between the Sensor and Manager

If you have previously established a connection between the Sensor and the Manager and the connection fails, try the following:

- Check network connectivity.
- View the system status on both the Manager and the Sensor.
- Check to ensure the Management port on the Sensor is configured with the proper speed and duplex mode as described in *Management port configuration*.
- Has the time been reset on the Manager server? The connection between the Sensor and Manager server is secure, and this secure communication is time-sensitive; so the time on the devices should remain synchronized. You must set the time on the Manager server before you install the Manager software and never change the time on that machine. If the

time changes on the Manager server, the Manager will lose its connectivity with the Sensor and the Update Server. A time change could ultimately cause serious database errors.

For more information, see the KnowledgeBase article KB55587.

How Sensor handles new alerts during connectivity loss

The Sensor stores alerts internally until connection is restored. Trellix IPS classifies events and prioritizes to ensure the buffer is filled with the most meaningful events to an analyst.

The following table lists the number of alerts that can be stored locally on the Sensor.

Number	Alert Type
100000	Signature based alerts
2500	Throttled alerts (with source and destination IP information)
2500	Compressed throttled alerts (alerts with no source and destination IP information)
2500	Statistical or anomaly DoS
2500	Throttled DoS alerts
1000	Host sweep alerts
1000	Port scan alerts

Once the connection from the Sensor to the Manager has been re-established, the queued alerts are forwarded up to the Manager. So the customer will retain them even in the event that connectivity is disrupted for some time.

If the buffer fills up before connectivity is restored, the Sensor will drop new alerts, but if blocking is enabled, the Sensor will continue to block irrespective of the Sensor's connectivity with the Manager.

DoS troubleshooting

This section lists issues related to DoS alerts.

Applicable to Sensor models: NS-series

Problem scenario

DoS alerts raised in Trellix IPS Manager.

Data/Information Collection

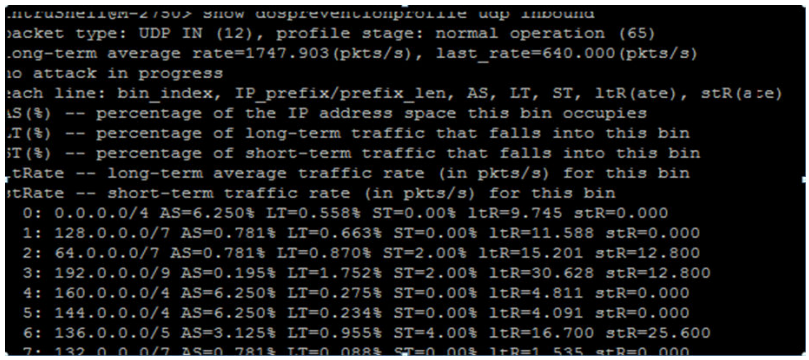
1. Execute **`show dospreventionprofile <dos-measure-name> <inbound/outbound>`** in the Sensor.
2. Trace the Sensor files.

Troubleshooting Steps

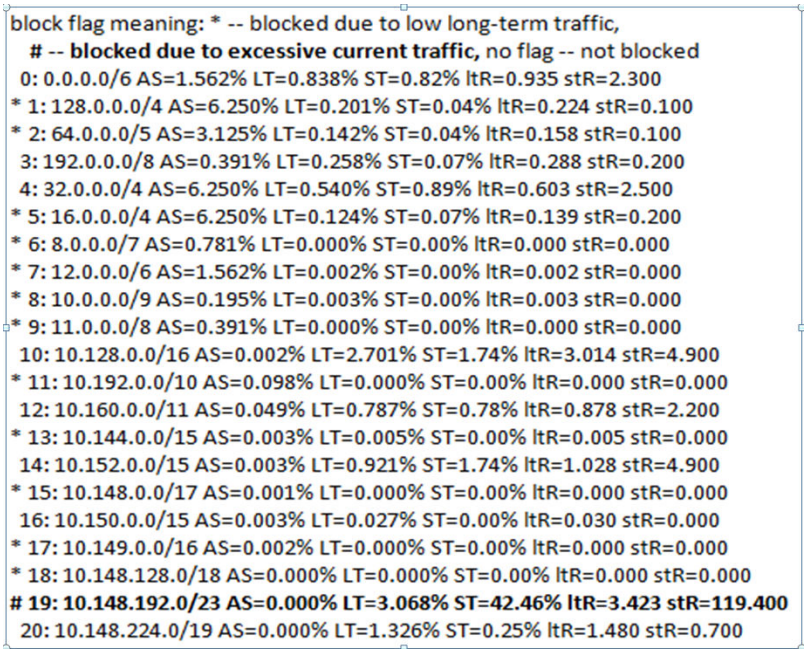
1. Check for the source IP of the profile learning each of the packet types. Execute the following commands:
   - **`show dospreventionprofile tcp-syn inbound/outbound`**
   - **`show dospreventionprofile tcp-syn-ack inbound/outbound`**
   - **`show dospreventionprofile tcp-rst inbound/outbound`**

- **show dospreventionprofile udp inbound/outbound**
- **show dospreventionprofile icmp-echo inbound/outbound**
- **show dospreventionprofile icmp-echo-reply inbound/outbound**
- **show dospreventionprofile icmp-non-echo-echoreply inbound/outbound**
- **show dospreventionprofile ip-fragment inbound/outbound**
- **show dospreventionprofile non-tcp-udp-icmp inbound/outbound**

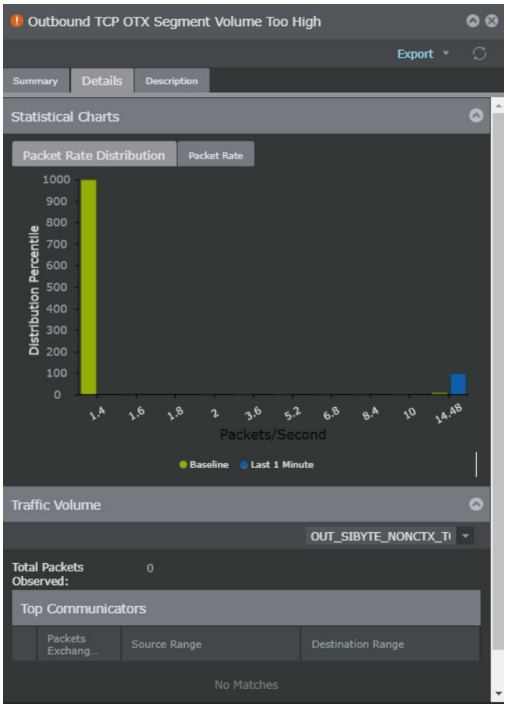
Check the bins for long-term average traffic rate and short-term average traffic rate values. An alert is raised when the short-term traffic rate is higher than the long-term traffic rate.



2. Check bins that are blocked. A sample of the source IP profile during the detection stage which indicates the blocked bins is shown in the figure.



3. If many DoS alerts are raised frequently for a particular IP, it could be false positive. The reason could be due to the profile of that IP not studied properly.
4. For volume related alerts (for example, if the inbound UDP volume is too high), check if the IP is missing in the alert details. To check the alert details, navigate to Analysis → <Admin Domain Name> → **Attack Log** and select the alert by clicking on it twice.



Solution

Rebuild the DoS profile to resolve the issue. To rebuild the DoS profile, perform the following steps:

1. Click Devices → <Domain Name> → Devices → <Device Name> → Troubleshooting → Denial of Service → **Data Management**.
2. In the **DoS Profile Learning** section, select **Rebuild the DoS Profiles**.
3. Click **Update**.

Validation errors and troubleshooting scenarios for CA-signed certificate chain

Validation errors while importing the CA-signed certificate chain

This section lists the validation errors that may appear while importing the CA-signed certificate chain.

Error	Description	Solution
Invalid CA Certificate Chain with Client Certificate	Client certificate is invalid in the certificate chain.	Request for a certificate chain from the CA with a valid client certificate.
Validity Expired for the certificate provided	Validity period for the certificate has expired.	Request for a certificate chain from the CA with the validity period set to a future date.
Signature Algo NOT SHA256with-RSA	Signature algorithm used in the certificate chain is not SHA256 with RSA 2048 bit encryption.	Request for a certificate chain from the CA sine with SHA256 with RSA 2048 bit encryption.
Invalid Serial Number in Certificate	Invalid serial number present in the certificate chain.	Request for a certificate chain from the CA with a valid serial number.

Error	Description	Solution
Certificate Issuer Not Present	Certificate issuer name is not present in the certificate chain.	Request for a certificate chain from the CA with a valid issuer name.
Some Certificate or Key file missing in import	Files missing in the certificate chain.	Request for the complete certificate chain from the CA.
Signing issue. Verification failed for root with leaf certs	Signature issue with the root and leaf certificates.	Request for a certificate chain from the CA with a valid signature.
Certificate Algorithm is not RSA or more	Signature algorithm used in the certificate chain is not using RSA encryption.	Request for a certificate chain encrypted using RSA from the CA.
Certificate Key size is not 2048 or more	Certificate public key size is not 2048 bit.	Request for a certificate chain with public key having 2048 bit from the CA.
Total certificates in chain should be at least 2 and maximum 6	Total number of certificates in the chain is not between 2 and 6.	Request for a certificate chain from the CA with correct number of certificates.
Certificate basic constraints are missing	**Basic Constraints** flag is missing in the certificate chain.	Request for a certificate chain from the CA with valid **Basic Constraints** flags.
Leaf Certificate Extended Keys are either invalid or missing	**Extended Keys** parameters are invalid or missing in the certificate.	Request for a certificate chain from the CA with valid **Extended Keys** parameters.
Leaf Certificate Extended keys are not valid for client	**Extended Keys** parameters are invalid in the certificate for the client.	Request for a certificate chain from the CA with valid **Extended Keys** parameters.
Leaf Certificate Extended keys are not valid for server	**Extended Keys** parameters are invalid in the certificate for the server.	Request for a certificate chain from the CA with valid **Extended Keys** parameters.
Certificate Chain Root CA not present	Root certificate is missing in the certificate chain.	Request for the complete certificate chain from the CA.

Troubleshooting scenarios

This section lists some troubleshooting tips for migrating Manager and Sensor from self-signed to CA-signed certificate.

Remove Manager CA-signed certificate when the Sensor is offline indefinitely

If a Sensor is offline indefinitely, remove the device from the Manager. Once the device is removed successfully, ensure that all the devices connected to the Manager are using self-signed certificate. You can then remove the CA-signed certificate chain from the Manager.

For steps to remove the CA-signed certificate chain from the Manager, see the *Manager Administration* section.

Remove Manager CA-signed certificate when the Sensor is offline temporarily

If a Sensor is offline temporarily, wait for the device to come online. Once the device is online, change the active certificate to self-signed. Ensure that all the devices connected to the Manager are using self-signed certificate. You can then remove the CA-signed certificate chain from the Manager.

For steps to remove the CA-signed certificate chain from the Manager, see the *Manager Administration* section.

Import CA-signed certificate to a Manager

To import a new CA-signed certificate to the Manager which already has a CA-signed certificate, change the active certificate of all the Sensors connected to the Manager to self-signed certificate. You can then import the new CA-signed certificate to the Manager.

For steps to import the CA-signed certificate chain to the Manager, see the *Manager Administration* section.

Import a new CA-signed certificate to a Sensor

To import a new CA-signed certificate to the Sensor which already has a CA-signed certificate, first you have to change the active certificate of the Sensor to self-signed. You can then import the new CA-signed certificate to the Sensor.

For steps to import the CA-signed certificate chain to the Manager, see the *Manager Administration* section.

Manager CA-signed certificate validation fails during Sensor trust establishment

1. Check the system faults in the Manager to see the reason for failure. Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** to see the system faults.
2. If it is a certificate error, correct the error in the certificate and replace the certificate in the Manager.
3. Establish trust with Manager using one of the methods:
    a. If self-signed certificate is present in the Sensor:
        i. Change the active to the self-signed certificate for the Sensor from the Manager.

        For steps to change active certificate, see the *Manager Administration* section.

        ii. Run the **`deinstall`** command while retaining the CA-signed certificate.

        iii. Run the **`set sensor sharedsecretkey`** command to establish trust with the Manager.

    b. If the trust is not established, run the **`set sensor sharedsecretkey`** command to establish trust with the Manager using a self-signed certificate.

Sensor CA-signed certificate validation fails during trust establishment with the Manager

1. Check the system faults in the Manager to see the reason for failure. Go to Manager → <Admin Domain Name> → Troubleshooting → **Logs** to see the system faults.
2. If a self-signed certificate is present in the Sensor, run the **`deinstall`** command without retaining the CA-signed certificate.
3. If the trust is still not established, run the **`resetconfig`** command without retaining the CA-signed certificate.
4. Run the **`set sensor sharedsecretkey`** command to reestablish trust with the Manager using self-signed certificate.
5. Import the corrected CA-signed certificate from the Manager to Sensor.
6. Change the active certificate for the Sensor in the Manager from self-signed to CA signed.

    For steps to change the active certificate, see the *Manager Administration* section.

Trust establishment fails due to Sensor errors

Migration of Manager-Sensor trust establishment from self-signed to CA-signed certificate may be caused due to one of the following issues:

- Control channel process restarts
- Sensor reboots or autorecovers
- Sensor loses connectivity with the Manager
- Network connectivity issue

In case of any issue, perform the following steps:

1. Initiate Manager-Sensor trust once the Sensor autorecovery is complete.
2. If the self-signed certificate is present in the Sensor, change the active certificate to self-signed certificate for the Sensor from the Manager.

   For steps to change the active certificate, see the *Manager Administration* section.
3. Run the **`deinstall`** command while retaining the CA-signed certificate.
4. Run the **`set sensor sharedsecretkey`** command to reestablish trust with the Manager.
5. If the trust is not established, run the **`set sensor sharedsecretkey`**command to reestablish trust with the Manager using the self-signed certificate.

Issues and status checks for the Sensor and other devices in combination

This section describes issues and status checks that involve a Sensor and any other devices, including third-party devices, that can be added.

Connectivity issues between the Sensor and other network devices

The most common Sensor problems relate to configuration of the speed and duplex settings. Speed determination issues can result in no connectivity between the Sensor and the switch.

Duplex mismatches

A duplex mismatch (for example, one end of the link in full-duplex and the other in half-duplex) can result in performance issues, intermittent connectivity, and loss of communication. It can also create subtle problems in applications. For example, if a web server is communicating to a database server through an Ethernet switch with a duplex mismatch, small database queries might succeed while large ones fail due to a timeout.

Manually setting the speed and duplex to full-duplex on only one link partner generally results in a mismatch. This common issue results from disabling auto-negotiation on one link partner and having the other link partner default to a half-duplex configuration, creating a mismatch. This is the reason why speed and duplex cannot be hard-coded on only one link partner. If your intent is not to use auto-negotiation, you must manually set both link partners' speed and duplex settings to full-duplex.

Valid auto-negotiation and speed configurations

The table below summarizes all possible settings of speed and duplex for Sensors and Cisco catalyst switch ports.

Table 111. Speed Configurations

Trellix IPS Configuration 10/100/1000 port (Speed/Duplex)	Configuration of Switch (Speed/Duplex)	Resulting Sensor (Speed/Duplex)	Resulting Catalyst (Speed/Duplex)	Comments
100 Mbps Full-duplex	1000 Mbps Full-duplex	No Link	No Link	Neither side establishes link due to speed mismatch
100 Mbps Full-duplex	AUTO	100 Mbps Full-duplex	100 Mbps Full-duplex	Correct configuration
100 Mbps Full-duplex	1000 Mbps Full-duplex	100 Mbps Full-duplex	100 Mbps Full-duplex	Correct Manual Configuration
100 Mbps Half-duplex	AUTO	100 Mbps Half-duplex	100 Mbps Half-duplex	Link is established, but switch does not see any auto-negotiation information from Trellix Intrusion Prevention System and defaults to half-duplex when operating at 10/100 Mbps.
10 Mbps Half-duplex	AUTO	100 Mbps Half-duplex	100 Mbps Half-duplex	Link is established, but switch does not see Fast Link Pulse (FLP) and defaults to 10 Mbps half-duplex.
10 Mbps Half-duplex	1000 Mbps Half-duplex	No Link	No Link	Neither side establishes link due to speed mismatch.

Gigabit auto-negotiation (no link to connected device)

Gigabit Ethernet has an auto-negotiation procedure that is more extensive than that of 10/100 Mbps Ethernet (per Gigabit auto-negotiation specification IEEE 802.3z-1998). The Gigabit auto-negotiation negotiates flow control, duplex mode, and remote fault information. You must either enable or disable link negotiation on both ends of the link. Both ends of the link must be set to the same value or the link will not connect.

If either device does not support Gigabit auto-negotiation, disabling Gigabit auto-negotiation forces the link up.

Troubleshooting a Duplex Mismatch with Cisco Devices

When troubleshooting connectivity issues with Cisco switches or routers, verify that the Sensor and the switch/routers are using a valid configuration. The **`show intfport <port>`** command on the Sensor CLI will help reveal errors.

Sometimes, there are duplex inconsistencies between Trellix IPS and the switch port. Symptoms include poor port performance and frame check sequence (FCS) errors that increment on the switch port. To troubleshoot this issue, manually configure the switchport to 100 Mbps, half-duplex. If this action resolves the connectivity problems, you might be running into this issue. Contact Cisco's TAC for assistance.

Use the following commands to verify fixed interface settings on some Cisco devices that connect to Sensors:

Cisco PIX® Firewall

- **`interface ethernet0 100full`**.

Cisco CSS 11000

- **`interface ethernet-3`**
- **`phy 100Mbits-FD`**

Cisco catalyst 4000, 5000, 6000 series (native)

- **`set port speed 1/1 100`**
- **`set port duplex 1/1 full`**

Connectivity issues with Cisco 3750-12S switch

Use the following ports when connecting a Cisco 3750-12s switch to your Sensor: 3, 4, 7, 8, 11, or 12. Connections using ports 1, 2, 5, 6, 9, or 10 might cause network issues, which is an inconsistent delay of packets.

Cisco CSS 11000

- **`interface ethernet-3`**
- **`phy 100Mbits-FD`**

Explanation of CatOS show port command counters

Counter	Description	Possible causes
Alignment Errors	Alignment errors are a count of the number of frames received that do not end with an even number of octets and have a bad CRC.	These are the result of collisions at half-duplex, duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames that do not end with on an octet and have a bad FCS.
FCS	FCS error count is the number of frames that were transmitted or received with a bad checksum (CRC value) in the Ethernet frame. These frames are dropped and not propagated onto other ports.	These are the result of collisions at half-duplex, duplex mismatch, bad hardware (NIC, cable, or port), or a connected device generating frames with bad FCS.

Counter	Description	Possible causes
Xmit-Err	This is an indication that the internal transmit buffer is full.	This is an indication of excessive input rates of traffic. This is also an indication of transmit buffer being full. The counter should only increment in situations in which the switch is unable to forward out the port at a desired rate. Situations, such as excessive collisions and 10 Mb ports, cause the transmit buffer to become full. Increasing speed and moving the link partner to full-duplex should minimize this occurrence.
Rcv-Err	This is an indication that the receive buffer is full.	This is an indication of excessive output rates of traffic. This is also an indication of the receive buffer being full. This counter should be zero unless there is excessive traffic through the switch. In some switches, the Out-Lost counter has a direct correlation to the Rcv-Err.
Under-Size	These are frames that are smaller than 64 bytes (including FCS) and have a good FCS value.	This is an indication of a bad frame generated by the connected device.
Single Collisions	Single collisions are the number of times the transmitting port had one collision before successfully transmitting the frame to the media.	This is an indication of a half-duplex configuration.
Multiple Collisions	Multiple collisions are the number of times the transmitting port had more than one collision before successfully transmitting the frame to the media.	This is an indication of a half-duplex configuration.
Late Collisions	A late collision occurs when two devices transmit at the same time and neither side of the connection detects a collision. The reason for this occurrence is that the time to propagate the signal from one end of the network to another is longer than the time to put the entire packet on the network. The two devices that cause the late collision never see that the other is sending until after it puts the entire packet on the network. Late collisions are detected by the transmitter after the first time slot of the 64-byte transmit time occurs. They are only detected during transmissions of packets longer than 64 bytes. Its detection is exactly the same as it is for a normal collision; it just happens later than it does for a normal collision.	This is an indication of faulty hardware (NIC, cable, or switch port) or a duplex mismatch.
Excessive Collisions	Excessive collisions are the number of frames that are dropped after 16 attempts to send the packet resulted in 16 collisions.	This is an indication of over utilization of the switch port at half-duplex or duplex mismatch.
Carrier Sense	Carrier sense occurs every time an Ethernet controller wants to send data and the counter is incremented when there is an error in the process.	This is an indication of faulty hardware (NIC, cable, or switch port).

Counter	Description	Possible causes
Runts	These are frames smaller than 64 bytes with a bad FCS value.	This is an indication of the result of collisions, duplex mismatch, IEEE 802.1Q (dot1q), or an Inter-Switch Link Protocol (ISL) configuration issue.
Giants	These are frames that are greater than 1518 bytes and have a bad FCS value.	This is an indication of faulty hardware, dot1q, or an ISL configuration issue.

Auto-negotiation

Auto-negotiation issues typically do not result in link establishment issues. Instead, auto-negotiation issues mainly result in a loss of performance. When auto-negotiation leaves one end of the link in, for example, full-duplex mode and the other in half-duplex (also known as a duplex mismatch), errors and re-transmissions can cause unpredictable behavior in the network causing performance issues, intermittent connectivity, and loss of communication. Generally these errors are not fatal-traffic still makes it through, but locating and fixing them is a time waster.

Situations that might lead to auto-negotiation issues

Auto-negotiation issues with the Sensor might result from nonconforming implementation, hardware incapability, or software defects.

Generally, if the switch used with the Sensor adheres to IEEE 802.3u auto-negotiation specifications and all additional features are disabled, auto-negotiation should properly negotiate speed and duplex, and no operational issues should exist.

- Problems might arise when vendor switches/routers do not conform exactly to the IEEE specification 802.3u.
- Vendor-specific advanced features that are not described in IEEE 802.3u for 10/100 Mbps auto-negotiation (such as auto-polarity or cabling integrity) can also lead to hardware incompatibility and other issues.

DNS connectivity and reputation issues

DNS connectivity

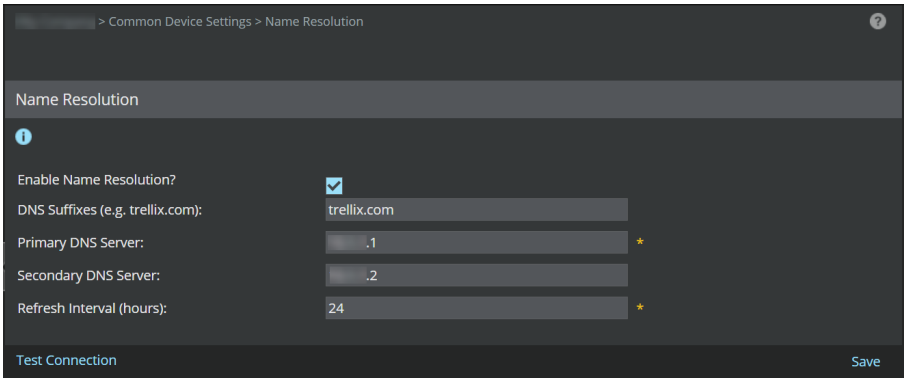
DNS connectivity to the Sensor sometimes has issues due to incorrect configuration or incorrect DNS server IP address. You can view the DNS connectivity fault on the **Faults** tab page in the Manager. The **Device DNS server connectivity status** faults are generated by the Sensor whenever there is an issue in DNS connectivity.

Figure 821. DNS server connectivity warning fault

You can perform the following high-level troubleshooting steps to solve the connectivity problem:

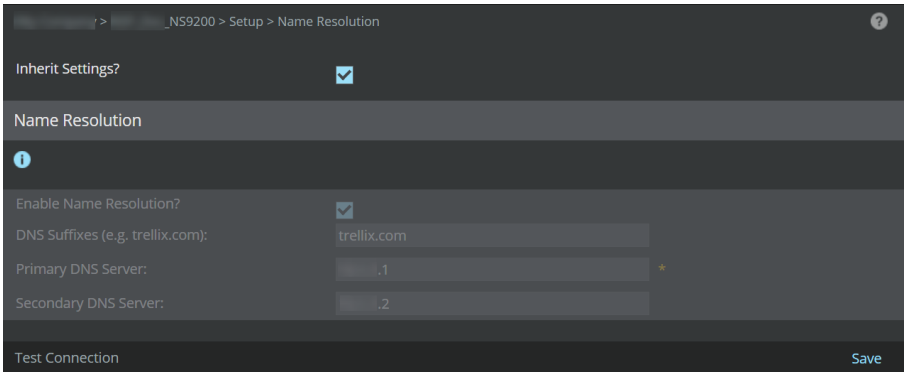
1. Check the Devices → <Admin Domain Name> → Global → Common Device Settings → **Name Resolution** for the global level setting in the Manager to see if the parent domain has the primary and secondary DNS server information entered correctly.

Figure 822. Global-level DNS server setting



2. If the global setting has the correct information, check the Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → **Name Resolution** device level setting to see if it inherits the global settings. Make sure that the **Inherit Settings?** is selected and also check if the inherited information is correct.

Figure 823. Device-level DNS server setting



If the connectivity problem still persists contact Trellix Support for further assistance.

GTI file reputation

In case of any errors for file reputation analysis, you can perform the following high-level troubleshooting steps:

1. Check if the malware detection is enabled in Policy → <Admin Domain Name> → Intrusion Prevention → Policy Types → **Advanced Malware Policies**.
2. In case of file reputation, the request is sent for bad file reputation. The file is sent as an MD5 checksum in DNS requests. If there is no response from the DNS, check the DNS connectivity. If the DNS connectivity has any issues, perform the high-level steps mentioned under **DNS connectivity** to solve the problem.

   If the DNS connectivity is working correctly, there will be a response for the file reputation request. Confirm the connectivity by executing and checking the output of **`show malwareenginestats`** CLI command.

Check the output of malware statistics for GTI file reputation engine. The **`Number of files sent`** and **`Number of response Received`** should show an increase in comparison with the number of files sent/received before sending the reputation request.

```
Malware Statistics for GTI File Reputation Engine
Number of files sent: 11132
Number of response Received: 9377
Number of files ignored: 1755
Number of files with malware score clean: 0
Number of alerts with malware score very low: 37
Number of alerts with malware score low: 0
Number of alerts with malware score medium: 0
Number of alerts with malware score high: 0
Number of alerts with malware score very high: 1233
Number of alerts with malware score unknown: 8051
Total number of alerts sent: 1233
Total number of attacks blocked: 1233
Total number of TCP resets sent: 1233
```

If the connectivity problem still persists contact Trellix Support for further assistance.

GTI IP reputation

When a syn packet is seen, the Sensor checks to see if IP reputation is enabled for that port/protocol. When enabled, the Sensor sends a query to the management process. The first flow is always allowed to pass through since the reputation score is not available. After a reputation score is assigned to the packet, the score is updated to the Sensor. The subsequent flows from the same IP address is marked with the reputation score in the header for lookup in datapath processor. Source IP is checked for inbound flows, and destination IP is checked for outbound flows, even though the entire 5-tuple is passed in the query.

The **Sensor connectivity status with GTI server** critical fault is generated by the Sensor in the Manager whenever the GTI server has connectivity issues to the Sensor.

You can perform the following high-level troubleshooting steps to solve the connectivity problem:

1. Check if proxy configuration is required. If the organization has a firewall/proxy between the Sensor management port and the cloud, the proxy has to be configured with username/password, if required. You can configure the proxy server under Manager → <Admin Domain Name> → Setup → **Proxy Server**.
2. Port 443 should not be blocked on the management port network.
3. Check the Devices → <Admin Domain Name> → Global → Common Device Settings → **Name Resolution** for the global level setting in the Manager to see if the parent domain has the primary and secondary DNS server information entered correctly.

If the connectivity problem still persists, contact Trellix Support for further assistance.

Issues and status checks for 10G/40G Active Fail-Open Bypass Kit

This section describes all issues and status checks specific to the 10G/40G Active Fail-Open Bypass Kit.

Unable to login to the system due to credential related issue

To reset the login credentials, perform the following steps:

1. Connect RS232 (RJ45) cable to the console port of the Active Fail-Open kit chassis.
2. Press the **M1** and **M3** buttons on the chassis for 10 seconds. This resets the parameters to default settings.
3. Login to the Active Fail-Open kit using the default username and password.

   NOTE

   The default **Username** and **Password** are **`Trellix00`**.

4. Configure the basic settings like IP address, network mask, gateway, and web connectivity.

Active Fail-Open kit does not work after login

After the initial installation, you might face the following issues with the Active Fail-Open kit:

- The network or monitor link does not come up.
- Active Fail-Open kit does not go to inline or bypass mode.

In such cases, reset the Active Fail-Open kit to factory default settings using the following steps:

1. Check the fiber cables and transceivers connections.
2. If the connections are correct, connect the RS232 (RJ45) cable to the console port of the Active Fail-Open kit chassis.
3. In the CLI, execute the **`set_default`** CLI command. This resets the parameters to default settings.
4. Login to the Active Fail-Open kit using the default username and password.

   NOTE

   The default **Username** and **Password** are **`Trellix00`**.

5. Configure the basic settings like IP address, network mask, gateway, and web connectivity.
6. Confirm if the links are up, or run the command **`get_dev_state`** in the CLI to check if the Active Fail-Open kit is functioning properly.
7. If resetting the Active Fail-Open kit does not fix the issue, RMA the module.

Packets getting dropped or network latency issues

Troubleshoot the issue by performing the following steps:

1. Force the Sensor into **Bypass** mode from the web interface:

a. Log in to the web interface.

b. Go to the **Bypass** page.

c. In the **Bypass** page, set **HB active mode** to **OFF**.

d. Set **Active Bypass** to **Bypass** mode.

e. Click **Apply**.

Monitor the network traffic. If the issue persists, troubleshoot the Network in your environment to resolve the issue.

If the issue does not persist, go to the next step.

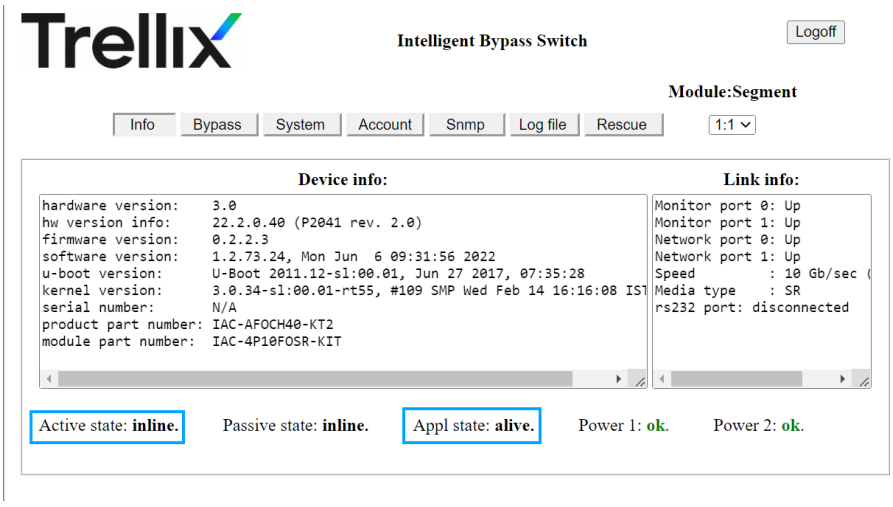
2. In the **Bypass** page, set **HB active mode** to **ON**.
3. Put the Sensor in layer 2 mode using the **`layer2 mode assert`** command from the Sensor CLI.
4. Monitor the network traffic. If the issue does not persist, issue is with the Sensor.

Active Fail-Open kit module is stuck in bypass mode

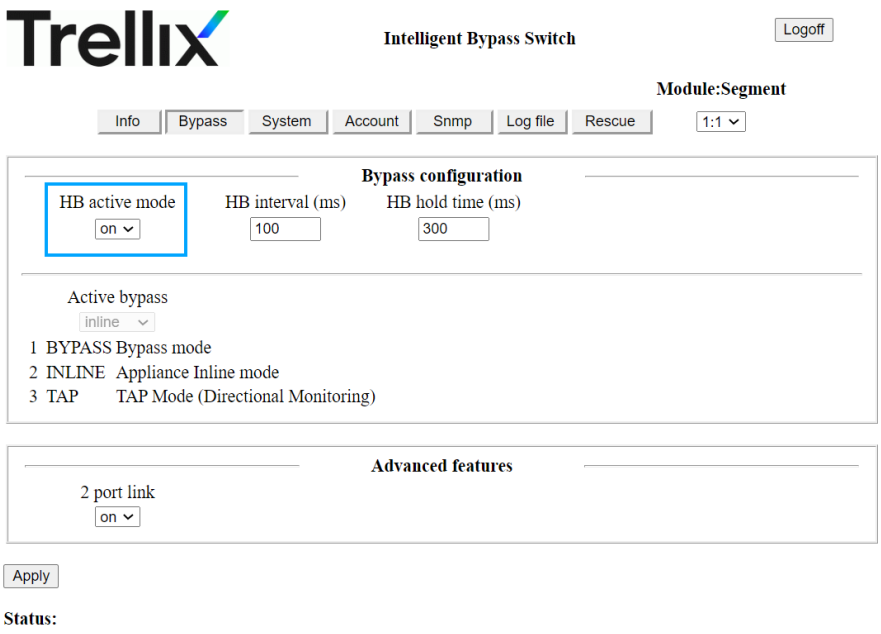
Links between Sensor and Active Fail-Open module Mon0/Mon1 are up but the Sensor is not receiving any traffic from the Active Fail-Open module. When this occurs, the **BYP/TAP/DISC** LED is **Amber** and **INLINE** LED is **OFF**.

You can troubleshoot the issue using the following two methods:

- At the CLI, run the following commands:
  1. **`get_hb_act_mode`** - If **`HB active mode`** is **`off`**, enter the next command.
  2. **`get_bypass_mode`** - If **`Active state`** is **`bypass`**, enter the next command.
  3. **`set_hb_act_mode on`**
- From the web interface:
  1. Check if the **Active State** is in **Inline** or **Bypass** or **Tap**.



2. Check if the **Appl State** is **unknown**. This means that the module in forced bypass state.
3. In the **Bypass** page, confirm that **HB active mode** is set to **ON**.



ALM LED is stuck on RED

To reset the **ALM** LED, do the following:

1. Confirm that all the faults have been cleared.
2. At the CLI, run the following commands:
   - **`get_dev_state`** — Displays the current state of the device
   - **`get_power_state`** — Displays the current state of the power supply
   - **`reset_err`** — Resets the **ALM** LED
   - **`get_log`** — Displays the faults that are triggered or are being triggered

Monitoring ports flap consistently due to heavy traffic load

Due to heavy traffic load, the monitoring ports MON0/MON1 flap between bypass/inline state consistently. To resolve the flapping issue, change the heartbeat interval and heartbeat hold time from default settings of 100 ms and 300 ms respectively to a higher setting.

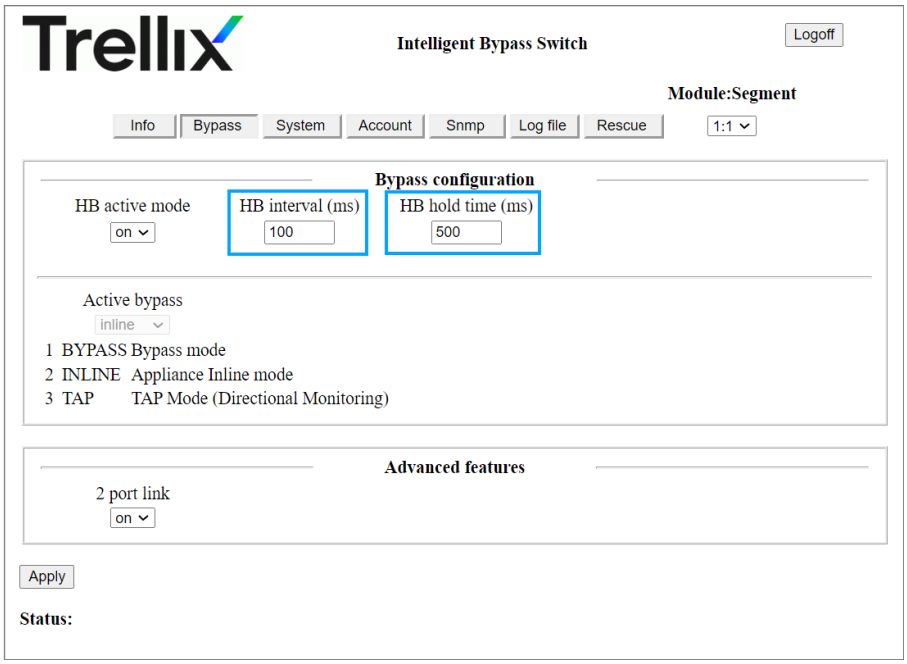
- Heartbeat interval - The frequency of heartbeat packets sent out of monitoring ports MON0 and MON1.
- Heartbeat hold time - Time for the Active Fail Open kit to go to bypass mode if no heartbeat packets are received within the defined time.

This means that if no heartbeat packets are received within 300 ms, the Active Fail Open kit goes into bypass mode. To prevent false positives being triggered, we send 3 heartbeats within the hold time.

> **NOTE**
>
> The thumb rule is that the heartbeat hold time has to be 3 times greater than the heartbeat interval.

Perform the following steps to troubleshoot the issue:

1. Login to the web interface, and go to the **Bypass** tab.
2. By default, the heartbeat interval is 100 ms. Set the heartbeat hold time to 500 ms.



3. Continue to increase the heartbeat hold time 100 ms at a time until the flapping is resolved under heavy traffic load.

Network ports flap consistently due to routing protocol interval

If the two-port link is enabled by default and the two-port link timeout has a value lower than the routing protocol hello interval in the network devices, the network ports flap consistently.

> **NOTE**
>
> To view this issue, login to the web interface and select the **Log file** tab. Under **Log file view**, click **>|**.

Perform the following steps in the CLI to troubleshoot the issue:

1. Change the 2pl timeout to a higher value than routing protocol hello interval.

   ```
   set_2pl_link_timeout <4-25>sec
   ```

2. If problem persists after changing the 2pl timeout to the highest value (25 seconds), turn off 2pl.

   ```
   set_2pl off
   ```

   > **NOTE**
   >
   > Setting the two-port link off disables the LFD feature on the network side. That is, if one side of the network goes down, the peer side stays up which results in routing issue and network traffic outages.

Additional troubleshooting tips

Power settings

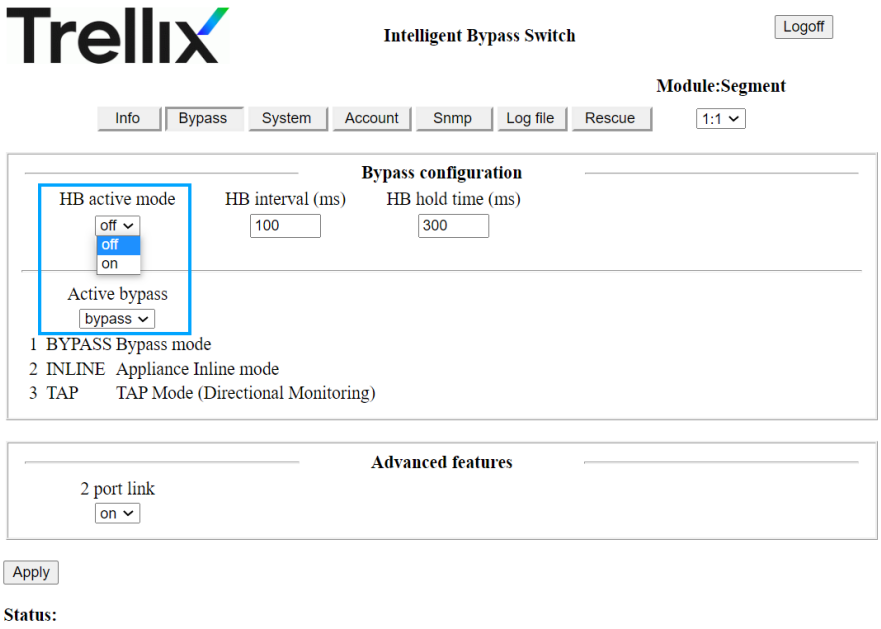
- Press and hold the **PWR** button for at least 4 seconds to do a power cycle.
- Press and hold the **PWR** button for at least 8 seconds to do a power shutdown.

System reset

- Press and hold the **RST** button for at least 1 second, to do a system reset.

Force active fail-open bypass Kit module to Bypass or Tap mode

1. From the web interface, go to **Bypass** tab.
2. Click the **HB active mode** drop-down and select **off**.
3. Click the **Active Bypass** drop-down and select **bypass** or **tap**.
4. Click **Apply**.



CLI attributes

After logging into the active fail-open bypass Kit CLI, depending on your access level, you will see one of the two login prompts:

- **`Info.m1s1.40g: AFO$`**
- **`Ctrl.m1s1.40g: AFO$`**

The description of each parameter is given below:

Parameter	Definition
Info	Read-only mode
Ctrl	Read/write mode
m1s1	Module 1 - Segment 1 is being accessed. This is the default module at log on. **NOTE** The value for the Segment is always **1**.
40g	Type of active fail-open bypass kit
AFO	Active fail-open bypass kit. This value will always remain the same

Disconnecting an active session

- Type **exit** from the CLI.
- From the web client, click **Logoff** in the upper right-hand corner.

Changing the active fail-open bypass Kit module slot

- From the CLI, type **set_seg <module_number> 1**. The <module_number> parameter can have value of either 1, 2 or 3.

List all get commands

- Type **get help** from the CLI. The command displays the list of all supported get commands.

List all set commands

- Type **set help** from the CLI. The command displays the list of all supported set commands.

Technical support information

- Type **get_support_info** from the CLI. The command displays information needed for the Technical Support team to help resolve technical problems.

Display sessions logged into the system

- Type **display_sessions** from the CLI.

CLI commands for troubleshooting

The following CLI commands are applicable for 10G/40G Active Fail-Open Bypass Kit:

Command	Description
display_sessions	Displays details of the active CLI sessions
exit	Ends current session. Once the sessions ends, the user who logged in after this session started will have read/write access.
get_dev_prop	Displays device properties

Command	Description
`get_dev_state`	Displays state of the device
`get_seg`	Displays details of the module and segment that are being used

`get_support_info <parameter> <number_of_lines>`	Displays information needed for the Technical Support team to help resolve technical problems. This command takes the following parameters:
	• **<parameter>** — Can be one of the following values:
	  • **swd_log** — Displays lines of swdaemon log file
	  • **kern_log** — Displays lines of kernel
	  • **snmp_log** — Displays lines of snmp log file
	• **<number_of_lines>** — Number of lines to be displayed

`power_off`	Shuts down the chassis
`reboot`	Reboots the chassis **NOTE** The chassis needs to be rebooted when a new module is inserted or if an old module is reseated.
`reset_err`	Clears the **ALM** LED once error condition is corrected
`set_default`	Resets parameters to factory default
`set_psw <old_password> <new_password>`	Changes the current password
`set_seg <module> <segment>`	Changes the module and the segment to a different active fail-open module in a different slot (either 1 or 2 or 3) **NOTE** The value for the **** parameter will always be **1**.
`set_session_exp_time <seconds>`	Sets the CLI and web sessions to timeout in seconds. The default value is **900** seconds. The maximum allowed value is **86400** seconds.
`set_time`	Sets the time to user-specific time zone. Coordinated Universal Time (UTC) is the default time zone.
`get help`	Displays all supported get commands
`set help`	Displays all supported set commands

Integration Scenarios

This section explains about the troubleshooting in integration scenarios and the required steps for troubleshooting.

Global Threat Intelligence - API Overload

When the Manager integrates with Global Threat Intelligence to obtain the reputation scores on hosts and geo-locations, the API is used to send back the feature usage data to Trellix and there is a possibility of the API getting overloaded.

Perform the following steps for troubleshooting:

1. If the proxy server is enabled, verify that "tunnel.web.trustedsource.org" is allowed by proxy server ACLs.
2. In the Manager, select Manager → Integration → **GTI** and check if the **Alert Data Details** option is enabled.
3. Check if SDK boot straps to Global Threat Intelligence cloud successfully by checking for below in ems.log.
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - Major version:
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - 2
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - Minor version:
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - 0
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - Version description:
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - TrustedSource SDK 2.0.5.02 (Build 1117)
    - 2011-12-06 15:55:01,510 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - Version:
    - 2011-12-06 15:55:01,511 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - 2.0.5.02-1117
    - 2011-12-06 15:55:01,672 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - Using Proxy Server:1.1.1.1, port: 20
    - 2011-12-06 15:55:01,780 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - Device Id: 9b11e1c4-069e-4195-8dd1-c2842ba338f6
    - 2011-12-06 15:55:01,780 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - MIICZjCCAc+gAwIBAgICEFIwDQYJKoZIhvcNAQEFBQAwNjEZMBcGA1UEAxQQVHJ1c3RlZFNvdXJjZV9DQTEMMAoGA1UEChMDU0NDMQswCQYDVQQGEwJVUzAe
    - 2011-12-06 15:55:01,780 INFO [http-0.0.0.0-9999-3] com.intruvert.ts.helper.TSRatingLookupHelper - MIICXQIBAAKBgQDegOtxL2JHaGLwU6RTQKPfGtzMp3zxiKRc4yPqgPtIgZqReQj7yw6pqvpBmpcx/OobEjs0hA8v0abE3BFwEX0Mezre2B9NpPhuJnNHhe4c/cGdxtC53

ePO - Connection failure

If there is a connection failure between the Manager and the Trellix ePO - On-prem server, perform the following steps for troubleshooting.

In the Manager:

Steps:

1. Ensure that the provided configurations such as IP address, port numbers, user name, and the password to the ePO server are correct.
2. Ping or try to access ePO server directly from the Manager server. If it is not accessible, check the firewall configuration and follow other regular network troubleshooting steps.

3. Ensure that the required permissions are given to the configured user name. To isolate the permission issue, use global administrator user name or password for testing the connection. If the connection is successful with global administrator credentials, then it could be a problem with configured user name.
4. Check the ems.log files for any errors:
5. Manager uses the following URLs. Try accessing them from the Manager server through a browser:https://EPO_SERVER_IP:8443/remote/ISExtension.HostForensicsCommand.do?command=getHostDetails&ip=[specify_IP]

   Check the logs files.

   Following denotes is a successful "TestConnection":

   011-11-22 15:09:51,500 INFO [ajp-127.0.0.1-8009-3] iv.common.HttpClient.ApacheGetImpl - doGET(), succesfully made the request to http client, url is https://172.16.101.37/remote/ISExtension.HostForensicsCommand.do?command=getHostDetails&ip=127.0.0.1&orion.user.security.token=tpc5pvsNVHxo3fiS

   The following denotes an error in connection:

   ems.log.3:2011-11-17 12:15:10,914 ERROR [ajp-127.0.0.1-8009-5] iv.common.HttpClient.ApacheGetImpl - doGET:Error while doing the http get function for the url https://172.17.94.80/remote/ISExtension.HostForensicsCommand.do?command=getHostDetails&ip=127.0.0.1&orion.user.security.token=kSffjTChbZRcE0IJ the error isjava.net.SocketTimeoutException: Read timed out

   ems.log.3:2011-11-17 12:48:21,435 ERROR [ajp-127.0.0.1-8009-4] iv.common.HttpClient.ApacheGetImpl - doGET:Error while doing the http get function for the url

In the ePO

Steps:

1. Ensure that the ePO server has the latest Trellix IPS Extension installed.

   > **NOTE**
   >
   > The Trellix IPS Extension file needs to be installed on the ePO server to help establish communication between Trellix Intrusion Prevention System and ePO.

2. Ensure that the required permissions are given to the configured username. Check if user has sufficient permission to access Trellix IPS Extension.
   - In Menu → User Management → Users → **desired User**, note down "Permissions Sets".
   - In Menu → User Management → **Permission sets**, select the permission that is assigned to this user. Check if **Trellix Intrusion Prevention System** has view and change settings.
3. To test the connection to the Manager server, manually run the NSP:Dashboard Data Pull Task. If connection fails, ping or try to access the Manager server directly from the ePO server. If connection fails, check the firewall and follow regular network troubleshooting steps.
4. Check orion.log file for any error messages at `<ePO_Install_Dir>\Server\Logs`. .

> **NOTE**
>
> If test connection is carried out from child admin domain, create test connection for parent admin domain by following above troubleshooting steps.

Trellix Logon Collector - Integration issues

To ensure connectivity between the Trellix Logon Collector and Manager, the following configurations are mandatory.

- Ensure that the Active Directory services are up and running. If the Active Directory (AD) is not configured correctly or down, the Manager does not receive Logon Collector updates and test connectivity does not get verified.
- Add the domain that needs to be monitored in the Logon Collector server. If the domain is not added, test connection fails and the Manager does not receive Logon Collector updates.
- Ensure that all Logon Collector components of the Logon Collector server are running.
- While exchanging Logon Collector certificate with the Manager by pasting, ensure that you copy the certificate content to Notepad to remove any inadvertent spaces that might cause certificate exchange failure during connectivity.
- To verify that Manager is receiving Logon Collector updates, create a Firewall and then double-click the **Source User** field to verify that the Groups are configured in the AD.

As a part of the Manager-Sensor and Logon Collector Integration, the Manager sends IP User mapping and User-Group mapping periodically on certain well defined events. The Sensor receives the Logon Collector updates from the Manager only when user-based Firewall policies are assigned to Sensors. Manager notifies the following two faults related to this integration which will be available in the **System Fault** page:

- Number of user configured in AD is more than 75000 or IP-user mapping is more than 100,000.
- TLC bulk update file exceeds 25mb limit which is a critical fault and user intervention is needed.

Performance issues

Most performance issues are related to switch port configuration, duplex mismatches, link up/down situations, and data link errors.

Sniffer trace

A Sniffer details packet transfer, and thus, a Sniffer trace analysis can help pinpoint switch and Trellix IPS performance or connectivity issues when those persist after you have exhausted the other suggestions in this document. Sniffer trace analysis reveals every packet on the wire and pinpoints the exact problem.

Note that it may be important to obtain several Sniffer traces from different ports on different switches, and that it is useful to monitor ("span") ports rather than spanning VLANs when troubleshooting switch connectivity issues.

Data link errors

Many performance issues may be related to data link errors. Excessive errors usually indicate a problem. For more information, refer to the *Configuration of Speed and Duplex settings*.

Half-duplex setting

When operating with a duplex setting of half-duplex, some data link errors, such as FCS, alignment, runts, and collisions are normal. Generally, a one percent ratio of errors to total traffic is acceptable for half-duplex connections. If the ratio of errors to input packets is greater than two or three percent, performance degradation may be noticeable.

In half-duplex environments, it is possible for both the switch and the connected device to sense the wire and transmit exactly at the same time, resulting in a collision. Collisions can cause runts, FCS, and alignment errors, which are caused when the frame is not completely copied to the wire, resulting in fragmented frames.

Full-duplex setting

When operating at full-duplex, FCS, cyclic redundancy checks (CRC), alignment errors, and runt counters should be minimal. If the link is operating at full-duplex, the collision counter is not active. If the FCS, CRC, alignment, or runt counters are incrementing, check for a duplex mismatch. Duplex mismatch is a situation in which the switch is operating at full-duplex and the connected device is operating at half-duplex, or vice versa. The result of a duplex mismatch is extremely slow performance, intermittent connectivity issues, and loss of connection. Other possible causes of data link errors at full-duplex are bad cables, a faulty switch port, or software and/or hardware issues.

Determine false positives

This section lists methods for determining and reducing false positives.

Reduce false positives

Your policy determines what traffic analysis your Sensor will perform. Trellix IPS provides a number of policy templates to get you started toward your ultimate goal — prevent attacks from damaging your network, and limit the alerts displayed in the **Attack Log** page to those which are valid and useful for your analysis.

There are two stages to this process — initial policy configuration and policy tuning. Though these are tedious tasks, Trellix has extended its blocking options to include SmartBlocking, which only activates blocking when high confidence signatures are matched, thus minimizing the possibility of false positives. Trellix IPS is replacing its present Recommended for Blocking (RFB) designation with Recommended for SmartBlocking (RFSB) because this new level of granularity enables Trellix to recommend many more attacks – the list of RFB attacks is a subset of the list of RFSB attacks.

The ultimate goal of policy tuning is to eliminate false positives and noise, and avoid overwhelming quantities of legitimate, but anticipated alerts.

Tune your policies

The default Trellix IPS policy templates are provided as a generic starting point; you will want to customize one of these policies for your needs. So the first step in tuning is to clone the most appropriate policy for your network and your goals, and then customize it. (You can also modify a policy directly rather than modifying a copy.)

Some things to remember when tuning your policies:

- We ask that you set your expectations appropriately regarding the elimination of false positives and noise. A proper Trellix IPS implementation includes multiple tuning phases. False positives and excess noise are routine for the first 3 to 4 weeks. Once properly tuned, however, they can be reduced to a rare occurrence.
- When initially deployed, Trellix IPS frequently exposes unexpected conditions in the existing network and application configuration. What may at first seem like a false positive might actually be the manifestation of a mis-configured router or Web application, for example.
- Before you begin, be aware of the network topology and the hosts in your network, so that you can enable the policy to detect the correct set of attacks for your environment.

- Take steps to reduce false positives and noise from the start. If you allow a large number of "noisy" alerts to continue to sound on a very busy network, parsing and pruning the database can quickly become a cumbersome task. It is preferable to all parties involved to put energy into preventing false positives than working around them. Exception objects are also an option where you can have custom rule sets specific to your environment. You can disable all alerts that are obviously not applicable to the hosts that you protect. For example, if you use only Apache web servers, you can disable IIS-related attacks.

False positives and noise

The mere mention of false positives always causes concern in the mind of any security analyst. However, false positives may mean quite differently things to different people. In order to better manage the security risks using any IDS/IPS devices, it's very important to understand the exact meanings of different types of alerts so that appropriate response can be applied.

With Trellix IPS, there are three types of alerts which are often taken as false positives:

- incorrectly identified events
- correctly identified events subject to interpretation by usage policy
- correctly identified events uninteresting to the user

Incorrect identification

These alerts typically result from overly aggressive signature design, special characteristics of the user environment, or system bugs. For example, typical users will never use nested file folders with a path more than 256 characters long; however, a particular user may push the Windows' free-style naming to the extreme and create files with path names more than 1024 characters. Issues in this category are rare. They can be fixed by signature modifications or software bug fixes.

Correct identification — significance subject to usage policy

Events of this type include those alerting on activities associated with Instant Messaging (IM), Internet Relay chat (IRC), and Peer to Peer programs (P2P). Some security policies forbid such traffic on their network, for example, within a corporate common operation environment (COE); others may allow them to various degrees. Universities, for example, typically have a totally open policy for running these applications. Trellix IPS provides two means by which to tune out such events if your policies deem these events uninteresting. First, you can define a customized policy in which these events are disabled. In doing so, the Sensor will not even look for these events in the traffic stream to which the policy is applied. If these events are of interest for most of the hosts except a few, creating exception objects to suppress alerts for the few hosts is an alternative approach.

Correct identification — significance subject to user sensitivity (also known as noise)

There is another type of event which you may not be interested in, due to the perceived severity of the event. For example, Trellix IPS will detect a UDP-based host sweep when a given host sends UDP packets to a certain number of distinct destinations within a given time interval. Although you can tune this detection by configuring the threshold and the interval according to their sensitivity, it's still possible that some or all of the host IPs being scanned are actually not live. Some users will consider these alerts as *noise*, others will take notice because it indicates possible reconnaissance activity. Another example of noise would be if someone attempted an IIS-based attack against your Apache Web server. This is a hostile act, but it will not actually harm anything except wasting some network bandwidth. But the attack attempted can help a would-be attacker to learn something new that they can use against your network (for Example, an attack failed can help zero in on the type of web server you use). Relevance analysis involves the analysis of the vulnerability relevance of real-time alerts, using the vulnerability data imported to Manager database. The imported vulnerability data can be from supported vulnerability scanners such as Nessus. You can better manage this type of events through policy customization or installing attack filters.

The noise-to-incorrect-identification ratio can be fairly high, particularly in the following conditions:

- The configured policy includes a lot of Informational alerts or scan alerts which are based on request activities (such as the All Inclusive policy).
- Deployment links where there is a lot of hostile traffic, such as in front of a firewall
- overly coarse traffic VIDS definition that contains very disparate applications, for example, a highly aggregated link in dedicated interface mode

Users can effectively manage the noise level by defining appropriate VIDS and customize the policy accordingly. For dealing with exceptional hosts, such as a dedicated pentest machine, alert filters can also be used.

Determine a false positive versus noise

Below are provided some troubleshooting tips for gathering the proper data to determine whether you are dealing with a false positive or uninteresting event:

- What did you expect to see? What is the vulnerability, if applicable, that the attack indicated by the alert is supposed to exploit?
- Ensure that you capture valid traffic dumps that are captured from the attack attempt (for example, have packet logging enabled and can view the resulting packet log).
- Determine whether any applications are suspected of triggering the alert — identify which type of applications, their versions, and the specific configurations.

If you intend to work with Trellix Technical Support on the issue, we ask that you provide the following information to assist in troubleshooting:

- If this occurred in a lab using testing tools rather than live traffic, please provide detailed information of the attack/test tool used, including its name, version, configuration and where the traffic originated.
- If this is a testing environment using a traffic dump relay, make sure that the traffic dumps are valid, TCP traffic follows a proper 3-way handshake, and so on.
- Also, please provide detailed information of the test configuration in the form of a network diagram.
- Export **Alert Details** and **Packet Capture** (within **Attack Log**).
- Be ready to tell Technical Support how often you are seeing the alerts and whether they are ongoing.

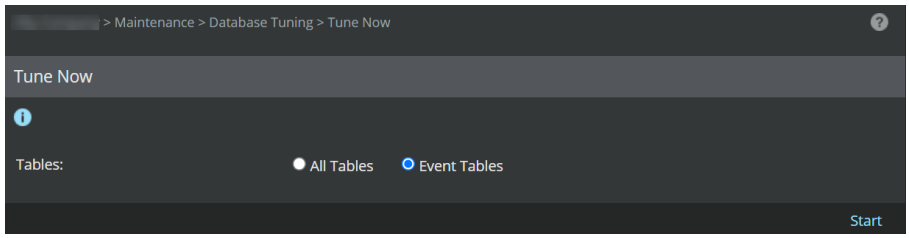
System Log Files

This section lists all log files available in the Manager that can be used for troubleshooting.

The log file contains all activities specific to its module. The size of each log file is smaller than 4 MB. To accommodate all logs when the log file reaches its maximum value, it automatically increments and the data from the current log file is moved to the incremented log file. Each log file can be incremented 13 times, and once all files are loaded, the data from the oldest log file is deleted. For instance, if ems.log file reaches its maximum limit, the file is automatically incremented to ems.log.1. The data from ems.log is moved to ems.log.1, and the new data into ems.log. This operation is executed incrementally in log files that are created further till the log files reach ems.log.13. This results in the latest logs available in ems.log and the oldest logs in ems.log.13.

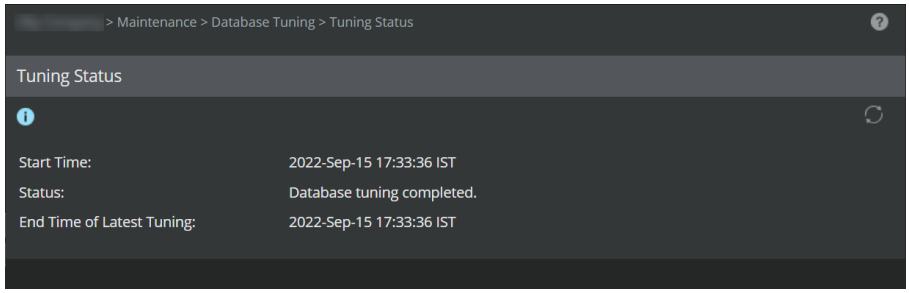
For example, you choose to tune your database:

1. Go to Manager → < Admin Domain Name > → Maintenance → Database Tuning → **Tune Now**.
2. Click **Start**.



> **NOTE**
>
> When the tuning is in progress, the message *Database tuning has started. Please consult the Tuning Status page for details* appears.

3. Go to Manager → < Admin Domain Name > → Maintenance → Database Tuning → **Tuning Status**.



4. To view the logs related to database tuning operation, see the **dbtuning.log** file.
   - On a Linux system, you can view the **dbtuning.log** file by running the **`show log file dbtuning.log`** command on the Manager CLI.

     > **NOTE**
     >
     > Similarly, to view other log files, execute **`show log file <log file name>`**.

   - On a Windows system, the **dbtuning.log** file will be available in the `<Manager_Install_Dir>\logs` directory.

> **NOTE**
>
> The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

The log file is copied to your system that contains all messages in the log from the start time of database tuning until the end.

For more information about system logs, see the section [System Files] in the *Manager Administration* section.

Manager Modules	Log Files	Description
ACM	sent.log	Logs related to ACM server

Manager Modules	Log Files	Description
Alert Processing	acltlv.log	Logs related to firewall events that are forwarded from the Manager to the Sensor
	acm.log	Logs related to alerts generated in Manager to know the alert rate
	akka_actors.log	Logs alerts from the Sensor through alert processing module
	alertCounts.log	Logs related to alert counts received from the Manager
	alertInstCounts.log	Logs related to alert inserts
	alertL7Counts.log	Logs related to processing of layer7 data
	alertpktcorrelation.log	Logs related to alerts packets
	alert_process.log	Logs related to the process of traffic detection/prevention at the Sensor level, and the alerts getting generated on Manager
	alertthrottling.log	Logs related to alert traffic information from the Sensor to the Manager
	alertthrottled.log	Logs related to alert traffic information for multiple attacks that are combined into a single event
	appatlv.log	Logs related to application alert events
	aqcollector.log	Logs related to alert queue collector
	aqcount.log	Logs related to alert queues
	aquptprocessor.log	Logs related to alert queue update events from the Sensor
	alt_chnl_event_cnt.log	Logs related to alert channel information
	altupdatecount.log	Log alerts related to update count of layer7, Endpoint Intelligence Agent, Logon Collector, etc.
	atlv.log	Logs byte data sent from the Sensor to the Manager
	bandwidth_savings.log	Logs related to bandwidth traffic information for multiple attacks that are combined into a single event
	BulkFileTransfer.log	Logs related to malware policies that are forwarded from the Sensor to the Manager
	bwatlv.log	Logs related to bandwidth alert events that are forwarded from the Manager to the Sensor
	epo.log	Logs related to ePO service post integration with the Manager
	insertActors.log	Logs new alerts from the Sensor through alert processing module

Manager Modules	Log Files	Description
	updateActors.log	Logs the existing alerts from the Sensor through alert processing module
	wacm.log	Logs related to Attack Log of the Central Manager
	vips.log	Logs related to Virtual Machine and Intel Security Controller Manager
Central Manager-Manager	emssync.log	Logs that are synced between Central Manager and the local Manager
	nacm.log	Logs related to communication between the Manager and the Central Manager
	nscm.log	Logs related to all activities within the Central Manager
Cloud	cim.log	Logs related to cloud activity within the Manager
	cimweb.log	Logs related to connections between the Manager, Controller, and Sensors
Compiler	compileroutput.log	Logs related to signature set compilation by the Manager
Dashboard	tcc_debug.log	Logs related to dashboard debug logs of the Manager
	tcc_query.log	Log queries related to the **Dashboard** page of the Manager
Database	dbbackup.log	Logs related to database backup files
	dbcheck.log	Logs created while upgrading the Manager to check database availability or consistency
	dbconsistency.log	Logs related to inconsistency during Manager upgrade
	dbtuning.log	Logs related to database tuning
	pruning.log	Logs related to deletion of alert data from MariaDB
Device Management	appviz.log	Logs related to application visualization
	dpinfo_epo.log	Logs information like the device type, operating system, and the source of the profile when Trellix ePO - On-prem is integrated with the Manager
	dpinfo_ips.log	Logs information like the device type, operating system, and the source of the profile that is extracted from the IPS Sensor and is forwarded to the Manager
	dpinfo_ntba.log	Logs information like the device type, operating system, and the source of the profile when the NTBA is integrated with the Manager
	emsKS, emsKS2048, emsKSStrong2048	Logs related to certificates imported from the Manager to the Sensor
	emsperfstats.log	Logs related to performance statistics of a device that are attached to the Manager
	nbaalertquey.log	Logs related to alerts of the NTBA Appliance

Manager Modules	Log Files	Description
	perfmon.log	Logs related to performance monitoring
	vmidcactivities.log	Logs related to cache, resources, and database entries of virtualization
Device Performance Monitoring	pefrmonatlv.log	Logs related to Sensor performance alerts
High Risk Endpoints	risk_score.log	Logs related to high risk endpoints based on their risk score
Installation	Initdb.log	Logs related to initialization of database after the installation of the Manager
Java Virtual Machine	crash.log	Logs related to crash related activities that are created using Java virtual machine
Malware	malware.log	Logs related to all malware activities
Manager APIs	sdkpayload.log	Logs related to the request and responses with the payload of the Manager
Manager Disaster Recovery	mdr.log	Logs related to the communication, synchronization, and switchover of the Manager Disaster Recovery pair
Manager Memory	emsmem.log	Logs related to memory management in the Manager (Total memory, used memory, and free memory)
Manager Startup Checks	checks.log	Logs that are checked when the Manager is restarted manually
TLC Integration	mlcSensor.log	Logs related to TLC integration where the information of users, groups, etc. from the Active Directory is sent to the Manager
Network Investigator Integration	niinteg.log	Logs related to Network Investigator integration and communication among the Manager, the Sensor and Trellix NI
NTBA Appliance	ntba.log	Logs related to the integration and communication between the Manager and NTBA
	nbaatlv.log	Logs related to NTBA-Manager queries
Overall Manager Logs and Console Logs	audit.log	All logs related to user interactions in the Manager and CLI
	ems.log	All logs related to the Manager
	emsout.log	Logs related to the console output of the Manager
Packet Channel	pkt_chnl_event_cnt.log	Logs related to packet log channel events
Policy	ips_policy.log	Logs related to the addition, modification, and deletion of IPS policy
Quarantine	hitask.log	Logs related to the attack log of the quarantine module
	hostevent.log	Logs related to the quarantine host events that are added, updated, and deleted

Manager Modules	Log Files	Description
	host_isolation.log	Logs all cache information of the quarantine host from the Sensor
Report Generation	reportgen.log	Logs related to report generation
Scheduler	scheduler.log	Logs related to schedulers running in the Manager
Signature Set	sigfile.log	Logs related to signature file deploy/compilation activity
	sigset.log	Logs related to signature set download from update server/local system.
	sigperf.log	Logs related to signature file deploy/compilation duration for the following processes: • Test compile start and end time for Manager Installation/Upgrade/Restart • Test compile start and end time for manual import of a signature set • Test compilation of snort or UDS attacks • Deploy the signature set to the Sensors • HA pair Sensor software upgrade using the Manager GUI
Solr Database	high_risk_solr.log	Logs related to Solr based details in Threat Explorer about high risk threats
	initdbSolr	Logs related to initialization activity occurring in Solr database
	solr.log	Logs related to configuration and startup details of Solr database
	solr_nsm.log	Logs the communication between the Solr database and the Manager
SSL Decryption	ssl_decryption.log	Logs related to SSL key information
Troubleshooting	health_check.log	Logs related to health checks of the Manager
Watchdog	watchdog.log	Logs the unrecoverable failure that is detected in the Manager

System fault messages

This section lists the system fault messages visible in the Manager Operational Status viewer, organized by severity, with Critical messages first, followed by Errors, Warnings, and Informational messages.

You can view the faults from the **Operational Status** menu in Manager.

The fault messages you might encounter, their severity, and a description, including information on what action clears the fault, are briefed. In many cases, the fault clears itself if the condition causing the fault is resolved. In cases where the fault does not clear, you must acknowledge or delete it to dismiss it.

For Sensor faults, go through Manager and Sensor faults. Similarly for NTBA issues, refer to Manager and NTBA faults.

NOTE

Many of the fault descriptions have information within a flower bracket**{}**. The value within these brackets will be displayed at run-time based on the context and type of the fault. For example, in case of a Sensor fault, if the description text is **`{0} temperature is {1}.`**, at run-time **`{0}`** will be replaced by name of the Sensor and **`{1}`** will be replaced by temperature value.

Manager faults

The Manager faults can be classified into critical, error, warning, and informational. The **Action** column provides you with troubleshooting tips.

Manager critical faults

These are the critical faults for a Manager and Central Manager.

Fault	Severity	Description/Cause	Action
Deployment Error	Critical	The device has detected an error on signature segment {0}. The segment error cause is {2}, and the download type is {3} (The Manager will automatically make another attempt to deploy changes to the device).	Ensure the device is connected to the Manager and in good health.
MDR Status Conflict	Critical	Detected MDR Status: Manager IP address / MDR Status as {0} / {1} and {2} / {3}	Review the mode, status, and configuration from each Manager console for accuracy. If needed, reset and recreate the MDR pair.
MDR Mode Conflict	Critical	MDR Mode: Manager IP address / MDR mode as {0} / {1} and {2} / {3}	Review the mode, status and configuration from each Manager console for accuracy. If needed, reset and recreate the MDR pair.
MDR Pair IP Address Conflict	Critical	Device detected a conflict with MDR pair IP address: Manager-IP address / MDR action as {0} / {1}	Review the mode, status, and configuration from each Manager console for accuracy. If needed, reset and recreate the MDR pair.
MDR IP Address Type Conflict	Critical	Device detected a conflict with MDR IP address type as {0} instead of type {1}.	Review the mode, status, and configuration from each Manager console for accuracy. If needed, reset and recreate the MDR pair.
Cluster Software Mismatch Status	Critical	Device software versions between primary cluster and secondary cluster is {0}.	

Fault	Severity	Description/Cause	Action
SSL Decryption Certificate Deployment Failure	Critical	Deployment of SSL decryption certificates to the device {0} by the Manager failed. This could result from a network connectivity issue. (The Manager will continue to attempt deployment until it is successful.)	Consult the system log for details.
Private GTI Cloud Certificate Deployment Failure	Critical	The Manager could not deploy the certificate required for communication with the private GTI cloud to device {0}. This error is due to a connectivity error between the Manager and the device. The Manager will automatically try to re-deploy the certificate to the device.	If the problem persists, consult the system log for details.
Callback Detectors Deployment Failure	Critical	Deployment of Callback Detectors to the device {0} by the Manager failed. This could be due to a network connectivity issue.	If the problem persists, consult the system log for details.
NTBA Public Key Deployment Failure	Critical	Deployment of NTBA public key to the device {0} by the Manager failed. This could be due to a network connectivity issue.	If the problem persists, consult the system log for details.
Packet Capture Rule Deployment Failure	Critical	Deployment of packet capture rules to the device {0} by the Manager failed. This could be due to a network connectivity issue.	If the problem persists, consult the system log for details.
Alert Storage Capacity Threshold Exceeded	Critical	Alert capacity: {0}. Current alert count: {1}	Prune and tune the database.
Dropped Alerts and Packet Captures	Critical	{0}% capacity. Dropping alerts and packet captures.	Prune and tune the database.
Update Server Connectivity Error	Critical	The Manager is unable to connect to the Trellix IPS Update Server.	Consult the system log for details and confirm that the Manager can resolve names and communicate with its default gateway and proxy server, as applicable.
Proxy Server Connectivity Error	Critical	The Manager is unable to connect to the configured proxy server {1}.	Consult the system log for details and confirm that the Manager can reach the proxy server and is using the proper proxy port. (Tip: You can test Manager connectivity through its proxy server on the Proxy Server page in the Manager GUI)

Fault	Severity	Description/Cause	Action
Attack Packet Capture Save Error	Critical	The Manager is unable to save packet captures from attacks to the database. Error Message: {0}.	Ensure that the disk space allocated to the database is sufficient.
Packet Log limit exceeded	Critical	Entries in packet log table has exceeded the current threshold [{0}] in database.	To recover the Manager from this state, Kindly fine tune the packet logging settings in your IPS policy. Also delete the old alerts and fine tune scheduled alert pruning settings.
Alert Save Error	Critical	The Manager is unable to save alerts to the database. Error Message: {0}.	Ensure that the disk space allocated to the database is sufficient.
Database Backup Error	Critical	The attempt to back up the Manager database failed. Error Message: {0}.	Check available disk space and that the necessary permissions to the directory have been given to the Manager application.
Expired License Detected	Critical	A license has expired.	Replace expired and expiring licenses.
Incompatible Custom Attacks	Critical	One or more custom attack is incompatible with the attacks in the current signature set. (Incompatibility often results from attack or signature definition overlap.) The following custom attack ids are in COMPILE FAILED state. {0} Please Check the CAE log for more details.	Update the custom attacks that show as having failed the Test Compile on the Custom Attacks window.
Central Manager Custom Attack Synchronization Error	Critical	Port conflict detected during attempt to synchronize custom attack definitions from the Central Manager. Port {0} is already in use.	Free the port and restart the synchronization.
Low JVM Memory	Critical	The Manager is experiencing high memory usage. Available system memory is low. Total memory (M): {0}, Free memory (M): {1}.	Reboot the host on which the Manager is running.
Audit Failure and Manager Shutting Down	Critical	The Manager is unable to log an audit event and is therefore shutting down.	Consult the system log for the reason for audit failure.
Signature Set Import Error	Critical	Sigset processing has failed in the Manager. This could be due to improper format or other technical reasons. Active sigset is empty, hence certain functionalities may not work fine.	Please download or import a valid sigset. If the issue persists, please contact the system administrator.
Signature Set Download Failed due to tampered sigset	Critical	Signature set was tampered and the download failed from the Trellix IPS Update Server to the Manager.	N/A

Fault	Severity	Description/Cause	Action
GTI Server Connectivity Error	Critical	The Manager is unable to communicate with the Trellix GTI Server.	Consult the system log for details and confirm that the Manager can resolve names and communicate with its default gateway and proxy server, as applicable.
MDR - System Time Synchronization Error	Critical	The two Managers in an MDR Pair must have the same operating system time. Otherwise, the device communication channels will experience disconnects.	Ensure both Managers are using the same time source and are synchronized with it.
The MDR Connection is Down	Critical	The communication from {0} to {1} is down.	Confirm SSL (TCP 443) connectivity between the Managers (in both directions).
Database Connectivity Error	Critical	The Manager is having trouble communicating with its database. Error Message: {0}.	Consult the database logs for errors and run the Manager Health Check to confirm the database is in good standing.
Database Connectivity Lost	Critical	The Manager has lost connectivity with its database. Error Message: {0}	Check the status of the database service and consult its logs for errors.
Database Integrity Error	Critical	Unable to locate index file for table: {0}.	Tune the database.
Database Tuning Error	Critical	Database tuning failure. Error Message: {0}.	Run the Manager Health Check to confirm there is sufficient free disk space.
Manager {0} Unreachable	Critical	Connectivity with Manager {0} has been lost.	Run the Manager Health Check on each Manager to check status and confirm basic connectivity. Then check connectivity between the Managers.
Manager {0} MDR Error	Critical	Manager {0} detected in standby mode. The peer Manager {1} is either not reachable or does not have {2} data.	If the above Managers are Trellix IPS Central Managers, make the Central Manager with the Trellix IPS Manager data active or recreate the MDR Pair. If the Managers are Trellix IPS Managers, make the Manager with the Trellix IPS Central Manager data active.
Manager {0} MDR Error	Critical	Manager {0} used to be the {1}/{2} MDR configuration and is now the {3}/{4} MDR configuration, and the primary Manager {5} is not active and its peer {6} does not have {7} configured.	If the above Managers are Trellix IPS Central Managers, make the Central Manager with the Trellix IPS Manager data active or recreate the MDR Pair. If the Managers are Trellix IPS Managers, make the Manager with the Trellix IPS Central Manager data active.
MDR Configuration Conflict for Manager {0}	Critical	Manager {0} is in {1} mode, and its peer Manager {2} is in {3} mode.	Recreate the MDR Pair.
MDR Pair Status Changed {0}	Critical	The {0} Manager is {1}/{2} and now primary and secondary are {3}/{4}.	Correct the MDR Pair status. If needed, recreate the MDR Pair.

Fault	Severity	Description/Cause	Action
Vulnerability Data Import Error	Critical	{0}	Consult the system log for details and contact Trellix Technical Support if the problem continues.
Simultaneous FIPS Role Login	Critical	Users from all three FIPS mode roles (Audit Administrator, Crypto Administrator and Security Administrator) have logged onto the Manager at the same time.	
AD Groups Size Exceeded	Critical	Currently TLC integration supports only {0} AD groups. This has been exceeded, so the Sensor behavior cannot be guaranteed until these numbers are brought down from "{1}".	Reduce the number of groups in Active Directory.
AD Groups Size Limitation	Critical	Currently TLC integration supports only {0} AD groups. Sensor version {1} cannot accommodate {2} AD groups" .	Reduce the number of groups in Active Directory.
Malware File Archive Disk Usage ({0})	Critical	The disk usage for archived "{0}" has reached {1} of the maximum allowed ({2}). New files of this type will no longer be saved to the disk.	Prune/delete unwanted files, increase the maximum disk space, or both.
Insightix LDAP Server Communication Error	Critical	The link between the NAC Sensor and the Insightix LDAP Server is down.	
Communication Error with Trellix Intelligent Sandbox Device ({0})	Critical	The Manager is unable to establish connectivity with the Trellix Intelligent Sandbox device "{0}".	Confirm connectivity between the devices, port, and credentials used to send Intelligent Sandbox files.
Solr Alert Core Indexing Error	Critical	Solr indexing failed for core: "{0}" due to error - "{1}".	The Solr index may need to be recreated from the database.
Solr AppAlert Core Indexing Error	Critical	Solr indexing failed for core: "{0}" due to error - "{1}".	The Solr index may be corrupted.
Solr Directory Backup Error	Critical	Backing up Solr core {0} encountered an error.	Check available disk space and Solr directory settings.
Database Backup File Creation Error	Critical	Creation of the backup file encountered an error.	Check the available disk space on backup drive.
Solr Directory Backup Error	Critical	Backing up Solr core {0} encountered an error.	Check the available disk space and Solr directory settings.
Importing alert data to Solr failed	Critical	Importing data to solr post Trellix IPS upgrade failed.	Please contact Trellix Technical Support.
Cloud Provider Access Error	Critical	An activity with the cloud provider failed due to access credentials.	Confirm/edit the access credentials and check connectivity to the cloud.

Fault	Severity	Description/Cause	Action
Trellix Virtual IPS Controller disconnected	Critical	The Manager is unable to communicate with Trellix Virtual IPS Controller: {0} ({1})	Confirm that the Controller instance is running and that it is using the proper Manager IP address ({2}) in its user data. Also ensure that the Controller is allowed to connect to the Manager over TCP 443. (Check both local/remote firewall and cloud access rules.) Finally, consult controller.log on the Controller and cim_web.log on the Manager for more details.
Trellix Virtual IPS Controller Connectivity Error	Critical	An activity with the Controller failed due to connectivity problems.	Confirm connectivity between the Manager and the Controller. (Tip: Connectivity issues are often due to lack of access. To isolate the issue, temporarily remove all access restrictions to see if the problem is resolved)
AWS Cloud Access Error	Critical	An activity with the AWS cloud failed because of access credentials.	Confirm/edit the access credentials used for AWS connectivity.
Trellix Virtual IPS Controller Upgrade Error	Critical	An activity with the Controller failed because of {0}	Confirm connectivity between the Manager and the Controller. (Tip: Connectivity issues are often due to lack of access. To isolate the issue, temporarily remove all access restrictions to see if the problem is resolved)
Outbound Decryption - Re-Signing Certificate Deployment Error	Critical	The re-signing SSL certificate could not be deployed to one or more devices. This is due to the addition of the device to the Manager after importing a custom re-signing certificate (The Manager no longer has the re-signing certificate from which it can generate a copy for the new device). Outbound decryption will not function as intended.	Re-import the custom re-signing certificate.
Manager CSR File Generation Error	Critical	An error occurred while generating a CSR file for the Manager. (The CSR file is used to create a CA-signed certificate, which is in turn used by the Manager when the devices establish trust with it using their own CA-signed certificates)	Confirm that the App/CCMigration folder has been created on the Manager file system and the NSMks.ks file has been created inside it. If missing, confirm that the Manager has proper permissions to the file system. Use of special characters when creating the CSR may also lead to an error. If using special characters, try to generate the CSR again without them. Otherwise, consult the system log for details.

Fault	Severity	Description/Cause	Action
Manager Trust Establishment Ports Error	Critical	An error occurred while the Manager was attempting to close the ports on which it had been listening to establish trust with the device using CA-signed certificates.	Confirm that CA-signed channel ports 8506/8507/8508 are open on the Manager and try again.
Trust Establishment Error	Critical	The trust request has failed. Error message: {0}.	Please verify reachability between Trellix IPS Central Manager and Trellix IPS Manager
Trust Establishment Error	Critical	The trust request has failed because Trellix IPS Manager {0} may not be reachable.	Confirm the Trellix IPS Manager IP address and that its service is up and running.
Trust Establishment Error	Critical	The trust request has failed because Trellix IPS Manager {0} has not yet configured.	Configure Trellix IPS Manager with Trellix IPS Central Manager.
Trust Establishment Error	Critical	The trust request has failed because the {0} already has a trust using the configured name. The previous trust with {1} may represent the Trellix IPS Manager or another.	Delete and re-add the configuration with Trellix IPS Central Manager.
Trust Establishment Error	Critical	The trust request has failed because the configured Trellix IPS Manager is in MDR mode, and no active {0} Trellix IPS Manager has been detected with which to establish the trust.	Please make one of the Trellix IPS Managers as Active in case of MDR prior to configure with Trellix IPS Central Manager.
Disk Space Warning	Critical	The drive on which the Manager database is installed ({1}) is {0} full.	Prune and tune the database.
NI Connectivity Failed	Critical	Connectivity to NI server {0} with group name {1} from Trellix IPS Manager failed.	Please check authorization token input is correct.
NI Connectivity Failed	Critical	Connectivity to NI server {0} with group name {1} from Trellix IPS Manager failed due to missing Application ID.	Please check request to NI contains Application Identifier.
NI Connectivity Failed	Critical	Connectivity to NI server {0} with group name {1} from Trellix IPS Manager failed.	Please check network connection and reachability of NI server from Trellix IPS Manager.

Manager error faults

These are the error faults for a Manager and Central Manager.

Fault	Severity	Description/Cause	Action
GAM Updating Error	Error	Device is detecting an error on av-dat file segment {0}. The segment error cause is {2}, and the download type is {3}. (The Manager will automatically make another attempt to deploy the update to the device.)	Ensure the device is connected to the Manager and in good health.
Deployment Failure	Error	The attempt by the Manager to deploy changes to device {0} failed during device re-initialization. The device configuration is now out-of-sync with the Manager settings and may be down. This can also occur when a failed device is replaced with a new unit, and the new unit is unable to discover its configuration information.	Consult the system log for details.
Interface/Sub-Interface Creation Failure	Error	Device {0} could not generate an interface or sub-interface. This fault generally occurs in situations in which the port configuration is incorrect. For example, when a port pair is configured to run in different operating modes (1 is in-line mode while 2 is in SPAN mode).	Reconfigure the physical port settings and consult the system log for details.
Deployment Failure	Error	The attempt by the Manager to deploy pending changes to device {0} failed. This could be due to a network connectivity issue. (The Manager will continue to attempt deployment until it is successful)	Consult the system log for details.
Geolocation Database Deployment Failure	Error	Deployment of geolocation database to the device {0} by the Manager failed. This could be due to a network connectivity issue.	If the problem persists, consult the system log for details.
Guest Portal Certificate Deployment Failure	Error	Deployment of guest portal certificate to the device {0} by the Manager failed. This could be due to a network connectivity issue.	If the problem persists, consult the system log for details.
E-mail Server Unreachable	Error	The connection attempt to e-mail server {0} failed. Error: {1}. This fault occurs when the Manager fails to send an email notification or a scheduled report.	Confirm connectivity with the server and that the proper ports are open.
Syslog Server Unreachable	Error	The connection attempt to syslog server {0} failed. Error: {1}. This fault occurs when the Manager fails to send a syslog notification.	Confirm connectivity with the server and that the proper ports are open.
Alert Processing Error	Error	The Manager alert queue has reached its maximum size of {0} alerts. ({1} alerts dropped) Alerts are being received at a higher rate than the Manager can process. The Manager will not accept additional alerts until it is done processing the existing ones.	Reduce the alert rate by tuning your IPS policies. For example, disable/remove informational alerts.

Fault	Severity	Description/Cause	Action
SNMP Notification Error	Error	The Manager's SNMP forwarder queue has reached its maximum size of {0} alerts. ({1} alerts dropped) Notifications are being sent at a higher rate than the Manager can process. The Manager will not send additional notifications until it is done sending the existing ones.	Reduce the number of notifications sent by applying a more restrictive filter. For example, only send notifications for high-severity attacks or explicitly selected attacks.
Alert Processing Error	Error	The Manager has reached its limit ({0}) for alerts that can be queued for storage in the database. ({1} alerts dropped) Alerts are being received at a higher rate than the Manager can process. The Manager will not accept additional alerts until it is done processing the existing ones.	Reduce the alert rate by tuning your IPS policies. For example, disable/remove informational attacks.
Packet Capture Processing Error	Error	The Manager packet capture queue has reached its maximum size of {0} packets captures. ({1} packet captures dropped) Packet captures are being received at a higher rate than the Manager can process. The Manager will not accept additional packet captures until it is done processing the existing ones.	Reduce the packet capture rate by ensuring tuning your IPS policies. Tuning may achieved by reduing the number of attacks, such as informational alerts, as well as reducing the packet capturing per attack. For example, disable post-attack packet captures. Tip: Run the Manager Health Check to see which policies have one or more attack definition with post-attack packet capturing enabled.
Automatic Signature Set Download Error	Error	The Manager was unable to download the latest signature set from the Trellix IPS Update Server as scheduled. Error Message: {0}.	Consult the system log for details and confirm that the Manager can resolve names and communicate with its default gateway and proxy server, as applicable.
Automatic Callback Detectors Download Error	Error	The Manager was unable to download the latest Callback Detectors from the Trellix IPS Update Server as scheduled. Error Message: {0}.	Consult the system log for details and confirm that the Manager can resolve names and communicate with its default gateway and proxy server, as applicable.
Automatic Deployment Error	Error	The Manager was unable to deploy signature sets and configuration changes as scheduled. Error Message: {0}.	Consult the system log for errors while generating the signature file (compilation errors, signature set validity or compatibility errors) and confirm connectivity between the Manager and its device.

Fault	Severity	Description/Cause	Action
Automatic Callback Detectors Deployment failure	Error	The Manager was unable to deploy Callback Detectors as scheduled. Error Message: {0}.	Consult the system log for Callback Detector errors and confirm connectivity between the Manager and its device.
Incident Update Failure	Error	The Manager is unable to accept more incidents from the Incident Generator. Error message: {0}.	Delete old incidents to make room for incoming incidents.
MDR Synchronization Error	Error	There was an error retrieving data from the peer Manager - aborting the synchronization process.	Confirm SSL (TCP 443) connectivity between the Managers (in both directions). If the secondary Manager is online, review its logs (both Manager and OS) for errors that might be preventing it from receiving the data transfer.
Alert Pruning Error	Error	The Manager was unable to prune alerts and attack packet captures during its routine maintenance. Error Message: {0}.	Consult the database logs for errors and run the Manager Health Check to confirm the database is in good standing.
Too Many Virtual NTBA Appliances	Error	NTBA Appliance {0} could not be discovered because the supported number of virtual NTBA Appliances has already been reached.	Remove the device.
TLC Server Connection Error	Error	Manager has no connection to configured TLC server.	Confirm connectivity to the TLC server and that the correct TLC certificate has been imported into the Manager.
TLC Bulk Update File Size Exceeds Limit	Error	The Sensor has a limit for the TLC-Bulk-Update-File size that it can process. As this has exceeded, update to the Sensor is aborted.	Check the TLC server configured in this Manager for the number of users, groups and IP user mappings. Make sure they do not exceed the limits specified in the TLC integration guide.
ePO Server Connection Error	Error	The Manager has no connection to configure ePO server {0}.	Confirm connectivity between the devices and the credentials used for ePO integration.
NMS Authentication Key Decryption Error	Error	NMS user authentication key decryption failed for user "{0}".	Delete and re-add the NMS user with valid credentials.
NMS Privacy Key Decryption Error	Error	NMS user privacy key decryption failed for user "{0}".	Delete and re-add the NMS user with valid credentials.
CA-Signed Certificate Error	Error	Error: {0}. Error: {0}. Certificate Fingerprint: {1}	Consult the system logs for details.

Fault	Severity	Description/Cause	Action
RuleObjects file Deployment Failure	Error	Deployment of RuleObjects file to the device {0} by the Manager failed. There could be a connectivity issue between Manager and device.	To resolve this failure, kindly perform a manual sigfile deploy to this Sensor from the **Deploy Pending Changes** page. If the problem persists, consult the system log for details.
Error while uploading daily telemetry data into Titan F telemetry server	Error	Telemetry data must be sent to Titan F telemetry server to help Trellix stay ahead of threats. However, the Manager is not able to upload data at the moment. Manager will re-attempt to upload the data in 5 minutes.	Check ems.log to know more about upload failure.
Error while uploading hourly telemetry data into Titan F telemetry server	Error	Telemetry data must be sent to Titan F telemetry server to help Trellix stay ahead of threats. However, the Manager is not able to upload data at the moment. Manager will re-attempt to upload the data in 5 minutes.	Check ems.log to know more about upload failure.
Error while uploading corporate telemetry data into Titan F telemetry server	Error	Telemetry data must be sent to Titan F telemetry server to help Trellix stay ahead of threats. However, the Manager is not able to upload data at the moment. Manager will re-attempt to upload the data in 5 minutes.	Check ems.log to know more about upload failure.
Error while uploading threat telemetry data into Titan F telemetry server	Error	Telemetry data must be sent to Titan F telemetry server to help Trellix stay ahead of threats. However, the Manager is not able to upload data at the moment. Manager will re-attempt to upload the data in 5 minutes.	Check ems.log to know more about upload failure.
Error while saving telemetry data into the Manager database	Error	Telemetry data saved in Manager database will be used by customers to check the historic data sent to Titan F telemetry server. Due to this error, Default-Telemetry (Trellix Titan F telemetry server) next generation report will have data missing.	Check ems.log to know more about telemetry data save failure.

Manager warning faults

These are the warning faults for a Manager and Central Manager.

Fault	Severity	Description/Cause	Action
GTI URL Reputation Services Disabled	Warning	The Manager has disabled the GTI URL reputation services on device {0} because one or more prerequisite has not been met. The Manager must have telemetry enabled for alert data details (unless using a private GTI cloud), and name resolution must be enabled on the device.	Enable telemetry and name resolution. Re-deploy the changes to the device.
Alert Storage Capacity Threshold Warning	Warning	Alert capacity: {0}. Current alert count: {1}.	Prune and tune the database.
Database Size Warning	Warning	Current database size: {1} GB. Disk capacity: {0}.	Prune and tune the database.
Automatic Database Backup Error	Warning	The Manager was unable to back up its database as scheduled. Error Message: {0}	Check available disk space and that the necessary permissions to the directory have been given to the Manager application.
Pending License Expiration	Warning	Your license is going to expire in less than 7 days.	Replace expiring licenses.
Ungraceful Manager Shutdown	Warning	The Manager service was not shut down gracefully.	Tune the database to fix any errors caused by the previous shutdown. To ensure a graceful shutdown, explicitly stop the Manager service before shutting down the host on which it is running.
Deprecated Application Detected in Firewall Policies	Warning	The Manager has detected the following use of deprecated applications in firewall policies: {0}	Remove these applications from firewall policies.
Missing Syslog Server	Warning	Firewall logging has been enabled, yet no syslog server is currently defined/enabled for admin domain {0}.	Define and enable a syslog server for forwarding firewall access events.
Database Tuning Recommended	Warning	{0} days have passed since the last database tuning.	Tune the database.
Automated MDR Switchover Detected	Warning	An automatic MDR switchover has completed without error. (The secondary {0} will take control of the {1}.)	Check the MDR log and the Manager system log on both Managers to understand if the primary is down or simply disconnected from the secondary.
MDR - {0} Version Mismatch (current {1} has newer version)	Warning	The two {0}s in an MDR configuration must have the same {0} software version installed. The current {0} server software is more recent than that of the peer {0}.	Ensure both Managers are running the same Manager software version.

Fault	Severity	Description/Cause	Action
MDR - {0} Version Mismatch (peer {1} has newer version)	Warning	The two {0}s in an MDR configuration must have the same {0} software version installed. The peer {0} server software is more recent than that of the current {0}.	Ensure both Managers are running the same Manager software version.
MDR - Manager Type Mismatch	Warning	The two Managers in an MDR pair must be of the same type (Manager versus Central Manager).	Ensure both Managers are of same Type (Trellix IPS Central Manager versusTrellix IPS Manager).
MDR - Invalid Request	Warning	The {0} request is not from a trusted IP address.	Ensure the Peer Manager is not already in MDR with another Manager.
MDR - Device-to-Manager IP Mismatch	Warning	The device-to-Manager communication IP {0} does not match with the peer Manager IP {1}.	Ensure the Device-to-Manager communication IP matches with the peer Manager peer IP in the MDR configuration.
MDR - IPv4 and IPv6 Address Warning	Warning	You have specified only the peer Manager {0} address. So you cannot add any {1} devices to the current Manager, nor will the existing {2} devices be able to communicate to the peer Manager.	If devices need to communicate with the Manager over IPv6 and the Manager is part of an MDR Pair, MDR must be reconfigured to include the IPv6 address of the peer Manager.
Internet Connectivity Required for Trellix Virtual IPS Cluster Usage	Warning	Trellix Virtual IPS cluster usage data must be sent to Trellix for proper Trellix Virtual IPS Cluster function, however, this Manager is currently unable to send the usage data to Trellix. Deployment of pending changes to Trellix Virtual IPS Clusters will be prevented until connectivity has been restored. Tip: The Manager will automatically attempt to contact Trellix again in one hour. If you believe connectivity has been restored sooner, use the Test Connection button on the GTI Integration page to confirm and reset the ability to deploy pending changes.	Check Internet connectivity, including proxy settings and name resolution.
License Required for Trellix Virtual IPS Sensor/Probe	Warning	A valid license is required to manage Trellix Virtual IPS Sensors/Probes, however, no license currently exists on the Manager. Without at least one license, deployment of pending changes to Trellix Virtual IPS Sensors will be prevented.	Add a license.
Scheduled Reports Error	Warning	Report generation failed for report template {0} because one or more of the selected resources in its definition is no longer available.	Edit and save the updated template.

Fault	Severity	Description/Cause	Action
Manager Deleted	Warning	The Manager information {0} has been deleted. Reason: {1}.	View related-faults and consult the system log for details.
Policy Synchronization Terminated	Warning	Policy synchronization has been terminated because concurrent processes are running on the Manager.	Consult the background tasks log to view running tasks and try again.
Deleted Trellix IPS Central Manager Policy in Use	Warning	Policy {0} is currently assigned to one or more resource. Creating copy {1} before deletion.	
Deleted Trellix IPS Central Manager Attack Filter in Use	Warning	Attack filter {0} is currently assigned to one or more resource. Creating copy {1} before deletion.	
Deleted Trellix IPS Central Manager Attack Set Profile in Use	Warning	Attack set profile {0} is currently assigned to one or more resource. Creating copy {1} before deletion.	
IPS Policy Backup Error	Warning	Failed to back up policy {0}.	Consult the system log for details.
IPS Policy Backup Error	Warning	Failed to back up policy {0}. The maximum limit of {1} has been reached.	Delete previous backups.
Reconnaissance Policy Backup Error	Warning	Failed to back up policy {0}.	Consult the system log for details.
Reconnaissance Policy Backup Error	Warning	Failed to back up policy {0}. The maximum limit of {1} has been reached.	Delete previous backups.
TLC IP-User Mapping Count Exceeds Limit	Warning	Currently, Trellix IPS Manager-TLC integration supports only 100,000 IP-user mapping.This has exceeded, so the Sensor behavior cannot be guaranteed until these numbers are brought down.	Consider reducing the number of computers TLC is monitoring.
TLC User Count Exceeds Limit	Warning	Currently, Trellix IPS Manager-TLC integration supports only 75,000 users. This has exceeded, so the Sensor behavior cannot be guaranteed until these numbers are brought down.	Consider reducing the number of users TLC is monitoring.
TLC Bulk Update File Transfer Error	Warning	TLC bulk update failed on sensor {0}.	There is no explicit action required. The Manager will retry to send the bulk update again automatically.
Policy Update Error	Warning	Failed to update policy "{0}" during signature set import.	Edit the policy to fix the issue.
Invalid Malware File Archive Storage Settings	Warning	The available free disk space on the Manager ({0}) is less than the disk space required to support the current malware storage settings ({1}).	Reduce the maximum disk space allowed for one or more file type.

Fault	Severity	Description/Cause	Action
Vulnerability Assessment Report Import Error	Warning	{0}	Confirm the existence of the file and its format.
Vulnerability Assessment Report Import Complete with Warnings	Warning	{0}	If the timestamp on the newly-imported report is the same as or older than the previously imported report, confirm that your process to copy new report files to the Manager file system is functioning properly.
MDR - Manager {0} Switched from {1} to {2} Mode	Warning	Manager {0} is taking the control.	The Manager "{0}" is "{1}" and its peer Manager, "{2}" is "{3}.
Trellix Virtual IPS Probe disconnected	Warning	Virtual machine {0} ({1}) is running, but its Controller has not received one or more heartbeat from its Probe at the expected interval. Its Probe may be stopped. Its Controller is listening for heartbeats on {2}:{3}.	Check the Probe's status directly from the virtual machine's console and ensure that the proper ports are open between the virtual machine and its Controller. Tip: If the Probe fails to connect to one of its components, an error will be written to its operating system's event log (Event Viewer in Windows and /var/log/messages in Linux).
Unregistered Manager	Warning	The Manager will not be able to download updates directly from the Trellix IPS Update Server until it has been registered.	Register the Manager with Trellix from the Summary page.

Manager informational faults

These are the informational faults of a Manager and Central Manager. These messages are only for your information and there is no specific action to be taken.

Fault	Severity	Description/Cause
System Startup and Alert Restoration in Process	Informational	The Manager is starting up and restoring its alerts. (Not all alerts may be visible until the Manager is fully operational.)
Database Backup Started	Informational	A database backup is in progress.
Database Backup Complete	Informational	The database was successfully backed up.
Custom Attack Save in Progress	Informational	One or more custom attack definition is in the process of being saved to the Manager.
Custom Attack Save Complete	Informational	One or more custom attack definition has been successfully saved to the Manager.

Fault	Severity	Description/Cause
Audit Logs Rotated	Informational	The audit log capacity on the Manager is 50000 records. When this maximum number of records is reached, the Manager overwrites the oldest records with the newest records (i.e. first in, first out). This fault indicates that <number> new records have been written to the audit log and that the oldest audit log records have been overwritten. This fault will be raised every <number> record(s) written.
License Auto Assignment Success	Informational	Successfully auto assigned license with keys {00-XX-00-00} to device.
Manual Import Started	Informational	A device software image, IPS signature set, Callback Detectors file or GAM update is being imported into the Manager.
Callback Detectors Import Started	Informational	A Callback Detectors file is being imported into the Manager.
Contacting Update Server	Informational	The Manager is connecting to the Trellix IPS Update server to download an update.
Deployment Started	Informational	The Manager is in the process of deploying updates to its devices. This can include configuration changes, signature sets, Callback Detectors, GAM updates and SSL decryption certificates, as applicable.
Deployment Complete	Informational	The Manager successfully deployed updates to device {0}. This can include configuration changes, signature sets, Callback Detectors, GAM updates and SSL decryption certificates, as applicable.
Signature Set Download Started	Informational	A signature set is being downloaded from the Trellix IPS Update Server to the Manager.
Signature Set Download Complete	Informational	A signature set was successfully downloaded from the Trellix IPS Update Server to the Manager.
Automatic Signature Set Download Started	Informational	The scheduled signature set download from the Trellix IPS Update Server to the Manager is in progress.
Automatic Signature Set Download Complete	Informational	The scheduled signature set download from the Trellix IPS Update Server to the Manager was successful.
Automatic Callback Detectors Download Started	Informational	The scheduled Callback Detectors download from the Trellix IPS Update Server to the Manager is in progress.
Automatic Callback Detectors Download Complete	Informational	The scheduled Callback Detectors download from the Trellix IPS Update Server to the Manager was successful.
Update Started	Informational	The Manager is connecting to the Trellix IPS Update Server.
Update Complete	Informational	The Manager has successfully connected to the Trellix IPS Update Server for updates.
Automatic Signature Set Deployment Started	Informational	A new signature set has recently been downloaded by the Manager and is being deployed to its devices.
Automatic Signature Set Deployment Complete	Informational	A new signature set has recently been downloaded by the Manager and successfully deployed to its devices.
Automatic Callback Detectors Deployment Started	Informational	A new Callback Detectors version has recently been downloaded by the Manager and is being deployed to its devices.

Fault	Severity	Description/Cause
Automatic Callback Detectors Deployment Complete	Informational	A new Callback Detectors version has recently been downloaded by the Manager and successfully deployed to its devices.
Scheduled Signature Set Deployment Started	Informational	A new signature is being deployed by the Manager to its devices, as scheduled.
Scheduled Signature Set Deployment Complete	Informational	A new signature was successfully deployed by the Manager to its devices, as scheduled.
Scheduled Signature Set Deployment Complete	Informational	A new signature set was successfully deployed by the Manager to its NTBA devices, as scheduled.
Callback Detectors Deployment Started	Informational	A new Callback Detectors version has recently been downloaded by the Manager and is being deployed to its devices.
Scheduled Callback Detectors Deployment Complete	Informational	A new Callback Detectors version has recently been downloaded by the Manager and is being deployed to its devices.
Database Tuning Started	Informational	The Manager database is currently being tuned.
Database Tuning Complete	Informational	The Manager database was successfully tuned.
Alert Archival Started	Informational	Alerts are currently being archived. Do not attempt to tune, back up or restore the database until the archival process is complete.
Alert Archival Complete	Informational	The alert archival completed successfully.
Device Discovery Started ({0}, {1})	Informational	The Manager is in the process of discovering a new device.
MDR Synchronization Started	Informational	The synchronization from the peer Manager is in progress.
MDR Synchronization Complete	Informational	Synchronization from the peer Manager has completed successfully.
MDR Pair Reset to Standalone	Informational	The MDR pair has been reset to standalone Managers. This {0} is standalone and will take control of the {1}.
MDR Pair Reset to Standalone	Informational	The MDR pair has been reset to standalone Managers. The peer {0} is standalone and will take control of the {1}.
MDR Pair Created	Informational	Manager Disaster Recovery (MDR) has been successfully configured.
MDR Pair Creation Canceled	Informational	Manager Disaster Recovery (MDR) creation has been canceled.
Manual MDR Switchover Started	Informational	The administrator has initiated an MDR switchover. (The secondary {0} will take control of the {1}.)
Manual MDR Switchover Complete	Informational	The administrator-initiated MDR switchover has completed without error. (The secondary {0} will take control of the {1}.)
MDR Switchback Complete	Informational	The MDR switchback has completed without error. (The primary {0} will take control of the {1}.)
Successful MDR Synchronization	Informational	The secondary {0} has successfully retrieved configuration information from the primary {0}.
MDR Suspended	Informational	Manager Disaster Recovery has been administratively suspended. (No switchover will take place while MDR is suspended.)

Fault	Severity	Description/Cause
MDR Resumed	Informational	Manager Disaster Recovery functionality has been resumed by the administrator after previous suspension. Failover functionality is again available.
Alert Archival Started	Informational	The Manager is archiving alerts.
Attack Packet Capture Archival Started	Informational	The Manager is archiving attack packet captures.
Telemetry Enabled for Trellix Virtual IPS Cluster Usage	Informational	Telemetry for Trellix Virtual IPS cluster usage data has been automatically enabled because one or more Trellix Virtual IPS Cluster is defined on this Manager. You can view the details of what is being sent to Trellix on the GTI Integration page. (The telemetry data will be sent as long as one or more Trellix Virtual IPS Cluster is defined.)
Vulnerability Data Import Complete	Informational	{0}
Vulnerability Assessment Report Import Complete	Informational	{0}
Custom Attack Incorporated into Signature Set	Informational	One or more custom attack definition has been incorporated into the published Trellix signature set and therefore removed as a custom attack. Removed custom attacks: {0}
Importing alert data to Solr started	Informational	Upgrade of Trellix IPS requires reindexing data. Reindexing of data in progress. Attack Log and Dashboard will not have all the data during reindexing.
Importing alert data to Solr completed	Informational	Upgrade of Trellix IPS requires reindexing data. Reindexing of data completed.

Sensor faults

The Sensor faults can be classified into critical, error, warning, and informational. The **Action** column provides you with troubleshooting tips.

Sensor critical faults

These are the critical faults for a Sensor device.

Fault	Severity	Description/Cause	Action
Temperature Error	Critical	Device temperature is outside its normal range.	Check the fan LEDs to ensure all internal fans are functioning and contact Trellix Technical Support if it persists.
Fan Error	Critical	{0} is {1}. The fan has failed.	Check the fan LEDs to confirm fan status. Switch off the device and contact Trellix Technical Support.

Fault	Severity	Description/Cause	Action
Power Supply Error	Critical	The {0} power supply to the device {1}	Confirm that the power supply is connected to a working outlet. If the outlet is working, replace the power supply.
Link Error on {0}	Critical	The link on {0} is {1}	Confirm that the device to which this port is connected is online and the cable connecting them is secure. If this port is not actually being used, disable it on the Physical Ports page.
Generic Memory Error	Critical	A generic, memory-related error has been detected.	A device reboot may resolve the issue. Check device logs for additional details and contact Trellix Technical Support if it persists.
Generic Hardware Error	Critical	A generic, hardware-related error has been detected.	A device reboot may resolve the issue. Check device logs for additional details and contact Trellix Technical Support if it persists.
Device Software Error	Critical	A recoverable software error has occurred within the device.	A device reboot may resolve the issue. Check device logs for additional details and contact Trellix Technical Support if it persists.
GAM Engine Process Failure	Critical	Device {0} has detected a failure in the GAM engine process, which may impact GAM file analysis.	Run the "status" CLI command. If the system health status is good, the device has likely recovered on its own. If the system health status is bad, a reboot may be required to recover from the failure. Also consult the layer 2 status and auto-recovery settings because repeated failures may cause the device to move into bypass mode or reboot automatically (as configured).
Malware Server Process Failure	Critical	Device {0} has detected a failure in the malware server process, which may impact all advanced malware file analysis.	Run the "status" CLI command. If the system health status is good, the device has likely recovered on its own. If the system health status is bad, a reboot may be required to recover from the failure. Also consult the layer 2 status and auto-recovery settings because repeated failures may cause the device to move into bypass mode or reboot automatically (as configured).

Fault	Severity	Description/Cause	Action
Datapath Process Failure	Critical	Device {0} has detected a failure in the datapath process, which may impact datapath inspection.	Run the "status" CLI command. If the system health status is good, the device has likely recovered on its own. If the system health status is bad, a reboot may be required to recover from the failure. Also consult the layer 2 status and auto-recovery settings because repeated failures may cause the device to move into bypass mode or reboot automatically (as configured).
GTI Engine Process Failure	Critical	Device {0} has detected a failure in the GTI file reputation lookup process, which may impact GTI file analysis.	Run the "status" CLI command. If the system health status is good, the device has likely recovered on its own. If the system health status is bad, a reboot may be required to recover from the failure. Also consult the layer 2 status and auto-recovery settings because repeated failures may cause the device to move into bypass mode or reboot automatically (as configured).
Frontend Datapath Process Failure	Critical	Device {0} has detected a failure in the frontend datapath process, which may impact datapath inspection.	Run the "status" CLI command. If the system health status is good, the device has likely recovered on its own. If the system health status is bad, a reboot may be required to recover from the failure. Also consult the layer 2 status and auto-recovery settings because repeated failures may cause the device to move into bypass mode or reboot automatically (as configured).
Packet Buffer Overflow	Critical	A packet buffer overflow has been detected.	A device reboot may resolve the issue. Check device logs for additional details and contact Trellix Technical Support if it persists.
Generic Error	Critical	A generic error has been detected	A device reboot may resolve the issue. Check device logs for additional details and contact Trellix Technical Support if it persists.
Firewall Connectivity Failure	Critical	The connectivity between the device and the firewall is down.	This fault can occur in situations where, for example, the firewall machine is down or the network is experiencing problems. Ping the firewall to see if the firewall is available. Contact your IT department to troubleshoot connectivity issues.
Late Collision of {0}	Critical	The link on {0} detects {1}.	Check both, the device and the one to which it is connected for compatible ethernet settings.

Fault	Severity	Description/Cause	Action
Port Pair {0} in Bypass Mode	Critical	Device {0} is configured in in-line, fail-open mode, but it is in bypass mode. The port pair is not inspecting traffic.	Confirm that the port is connected properly and operational. Additionally disable and re-enable the port. Check if the traffic rate is above the supported port throughput (this forces the device into bypass mode).
Port Pair {0} in In-Line, Fail-Open Mode	Critical	{0} has returned from bypass mode to in-line, fail-open mode.	Confirm if the traffic statistics are incrementing and traffic is being inspected.
Fail-Open Bypass Switch Timeout	Critical	The device is not able to communicate with the fail-open bypass switch.	Run the CLI command "show intfport all" to confirm connectivity. If disconnected, disable and re-enable the port.
Invalid Fail-Open Configuration: {0}	Critical	An invalid configuration has been applied to {0} (The device requires appropriate hardware to support in-line, fail-open configuration on its gigabit ports).	Ensure that hardware is available and correct ports are configured to run in in-line mode.
Inspection Disabled	Critical	The device is operating in layer 2 bypass mode. Inspection is disabled. The device has either been explicitly placed into bypass mode via the CLI/GUI, or it has experienced multiple errors, surpassing the configured threshold, and switched to bypass mode as a precaution.	Check for faults and the device status. Use the "layer2 mode deassert" CLI command to re-enable inspection. On GUI, Navigate to Device → Troubleshooting → **Layer 2 Bypass** & Update layer 2 mode to Deassert.
Invalid SSL Decryption Certificate	Critical	The device has detected an invalid SSL decryption certificate: {0}	Re-import the SSL decryption certificate.
Generic Device Error	Critical	{0}	Review the device status.
Port Media Type Mismatch	Critical	{0}: Configured media type is {1}. Inserted media type is {2}	Ensure the configured media type matches with the media inserted.
Port Certification Mismatch	Critical	{0}: Trellix Certified pluggable interface. Trellix certification status is {1}.	Replace the non-certified transceiver with a Trellix-certified one or update the physical port's settings to allow a non-certified connector type.
Temperature Status	Critical	{0} temperature is {1}.	
Bootloader Upgrade Failure	Critical	Bootloader upgrade status is {1}.	
Temperature Error	Critical	Chassis temperature (device index {0}) is {1}.	Check the Fan LEDs to ensure all internal chassis fans are functioning and contact Trellix Technical Support if the problem persists.

Fault	Severity	Description/Cause	Action
Device Dropping Packets Internally	Critical	Device front end is overloaded.	If this problem is an ongoing occurrence, a model with a higher system capacity should be considered. (Tip: Multiple capacities are supported on some models with a license change to increase the capacity)
Device Dropping Packets Internally	Critical	Device capacity has been reached.	If this problem is an ongoing occurrence, a model with a higher system capacity should be considered. (Tip: Multiple capacities are supported on some models with a license change to increase the capacity)
Incompatible Device Model Detected	Critical	Device {0} has been replaced by a model ({2}) that is not the same as the original model. The alert channel cannot establish a connection.	Ensure you replace the device with another device of the same model.
Device Disconnected	Critical	The Manager cannot communicate with the device {0} through its command channel. The connection between the device and the Manager is down.	Check the device status using the "status" CLI command. Make sure the device can ping its default gateway and the Manager. Make sure any firewalls between the devices have the proper ports open.
Load Balancer Disconnected	Critical	The Manager cannot communicate with load balancer {0} through its command channel. The connection between the load balancer and the Manager is down.	Check load balancer status. Make sure the load balancer can ping its default gateway and the Manager. Make sure any firewall between the devices and the Manager have proper ports open.
Device in Bad Health	Critical	Device {0} is reporting bad health. This fault occurs due to device software failure. (It usually occurs in conjunction with a software error fault.)	If this fault persists, refer the system log and contact Trellix Technical Support.
Uninitialized Device	Critical	Device {0} is not initialized properly and is therefore not passing traffic. If the device is newly added, this is expected until it receives its initial configuration from the Manager.	If this is a new device, it will start passing traffic once it receives its initial configuration from the Manager, once it establishes trust with it. If the device has rebooted, it normally auto recovers once the device has finished its boot process. If the problem persists, check the device status using the "status" CLI command to ensure that a signature set is present. If no signature set is available, re-deploy the settings from the Manager.
Trellix Intelligent Sandbox Certificate Deployment Failure	Critical	Deployment of the Trellix Intelligent Sandbox certificate to the device {0} by the Manager failed. This could be due to a network connectivity issue.	If the problem persists, consult the system log for details.

Fault	Severity	Description/Cause	Action
Device Discovered without License	Critical	Device {0} was discovered without a license.	Add a license.
Device Discovered with Cluster Secondary License	Critical	Device {0} was discovered with a cluster secondary license. This device should not be connected to the Manager directly.	To obtain a standard license now, please contact Technical Support or your local reseller.
Device License Expired	Critical	Device {0} ({1}) license expired.	Add a license.
Device Support License Expired	Critical	Device {0} (support {1}) license expired.	Add a license.
Expired Device License	Critical	Device {0} ({1}) license expired.	Add a license.
Expired Device Support License	Critical	Device {0} (support {1}) license expired.	Add a license.
No Valid License Detected for {0} of Type {1}	Critical	A license is required.	Add a license.
Pending Support License Expiration for {0} of Type {1}	Critical	Support license for this device expires in {0} days.	Renew the license.
Expired License for {0} of Type {1}	Critical	A license is required.	Add a license.
Expired Support License for {0} of Type {1}	Critical	A license is required.	Add a license.
Insufficient Licenses Detected	Critical	The Manager does not have enough licenses to support the number of Trellix Virtual IPS sensors and/or Virtual Probes it is currently managing. Additional licenses are required to become compliant. Virtual Sensors: {0} in use ({1} allowed) Additional Virtual Sensor Licenses Required: {2}	Add enough licenses to become compliant.

Fault	Severity	Description/Cause	Action
Expired License	Critical	Proxy Decryption License with key {0} has expired. Updates to the Sensor to which it is assigned will be prevented until a valid license is assigned. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
Expired License	Critical	The system license with key {0} has expired and 30 days passed beyond expiry. Updates to the Sensor to which it is assigned will be prevented until a valid license is assigned. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
Expired License	Critical	The system license with key {0} has expired. Post 30 days from expiry, Updates to the Sensor to which it is assigned will be prevented until a valid license is assigned. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
Expired License	Critical	The evaluation system license with key {0} has expired. Updates to the Sensor to which it is assigned will be prevented until a valid license is assigned. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
GTI File Reputation DNS Error	Critical	{1}.	Confirm that the device has name resolution enabled, and properly configured, and that it can communicate with the configured DNS servers.
Port Pair {0} Fail-Open Kit Status	Critical	Device {0} is configured to run in-line and to fail open, but it is in {1} mode. This fault indicates that some failure has occurred, causing the fail-open control module to switch operation to {1} Mode. No traffic is flowing through the device.	Consult the system log for details. If the problem persists, remove and re-add the fail-open kit.

Fault	Severity	Description/Cause	Action
CLI Login After Device Initialization	Critical	Device reports user "{0}" login via CLI after device initialization. This is a FIPS 140-2 Level 3 violation.	
Link Error on {1}	Critical	The link on port {1} is {2}	Confirm that the device to which this port is connected is online and the cable connecting them is secure. If this port is not actually being used, disable it on the Physical Ports page.
Load Balancer HA Configuration Mismatch	Critical	Load Balancer "{0}" reports HA peer configuration is not matching.	Verify the load balancer configuration and recreate the HA Pair if needed. (Both load balancers in the HA Pair are expected to have the same configuration.)
FFP File Update Error	Critical	Failed to send FFP file update to device.	Check sensor connectivity and consult the device system logs for details.
Device Reboot Required	Critical	The device requires a manual reboot due to "{1}".	Reboot the device.
Solid State Drive ({0}) Error	Critical	The Solid State Drive {0} is "{1}". Restore the SSD to clear this fault.	Check the SSD status. On failure, replace the failed SSD.
GTI Connectivity Error	Critical	The device is {1} to communicate with GTI server.	Confirm device connectivity and name resolution.
Trellix Intelligent Sandbox Connectivity Error	Critical	The device is {0} to communicate with the Trellix Intelligent Sandbox appliance due to {1}.	Confirm connectivity between the devices, port, and credentials used to send Intelligent Sandbox files.
Attack Detection Error	Critical	IPS device attack detection has stopped on one or more engine.	Consult the device system logs for details. A reboot may be required to resolve the issue.
Invalid Device Trust Certificate Detected	Critical	Device {0} tried to establish trust with the Manager using an invalid CA-signed certificate. Validation error: {1}.	Replace the invalid certificate with a valid one.
Device CSR File Generation Error	Critical	An error occurred while the device {0} was attempting to upload the CSR file to the Manager. (The CSR file is used to create a CA-signed certificate, which is in turn used by the device to establish trust with the Manager)	The use of special characters when creating the CSR may lead to an error. If using special characters, try to generate the CSR again without them. Otherwise, consult the system log for details.
Device Trust Certificate Deployment Error	Critical	An error occurred while attempting to deploy a CA-signed certificate to device {0}. (The CA-signed certificate is used by the device to establish trust with the Manager)	Check the connectivity between the Manager and the device, and then consult their system logs for details.

Fault	Severity	Description/Cause	Action
Internal Configuration Error	Critical	Unsupported configuration detected after upgrade/downgrade. The device is restored to default configuration. An internal application communication error occurred in the device during {0}. Unsupported Callback Detectors configuration detected after upgrade/downgrade. The device is restored to default configuration. Image downgrade detected. Execute "resetconfig" on the device CLI to complete the downgrade.	This is an internal error. Check the device status to ensure the device is connected to the Manager and in good health.
NI Connectivity from Sensor Failed	Critical	Connectivity to NI server from Sensor {0} failed.	Please check authorization token input is correct.
NI Connectivity from Sensor Failed	Critical	Connectivity to NI server from Sensor {0} failed.	Please check network connection and reachability of NI server from Trellix IPS Manager.

Sensor error faults

These are the error faults for a Sensor device.

Fault	Severity	Description/Cause	Action
Firewall Filter Application Error	Error	Error applying firewall filter "{0}." An attempt to apply this firewall filter from the device to the firewall has failed. Failure reason: {1}.	Check your firewall configuration. If possible, increase the maximum number of available filters. Ensure connectivity between the device and the firewall.
NMS User Authentication Key Decryption Failure	Error	NMS user authentication key decryption failed for {0}	Delete and re-add the NMS user.
NMS User Privacy Key Decryption Failure	Error	NMS user privacy key decryption failed for {0}	Delete and re-add the NMS user.
SSL Decryption Engine Down	Error	The SSL decryption service is down on the device {0}. HTTPS traffic cannot be inspected.	Check the device logs for additional details and contact Trellix Technical Support if it persists.
SSL Decryption Update Error	Error	The SSL decryption configuration update failed for component {0}	Check the device status using the "status" CLI command and re-attempt to deploy the changes from the Manager.

Fault	Severity	Description/Cause	Action
Internal Packet Drop Error	Error	The device is dropping packets due to high traffic load.	Review the number and duration of performance-related faults for this device and refer its performance charts to determine if high usage is an on-going occurrence. If yes, a model with a higher system capacity should be considered. (Tip: Multiple capacities are supported on some models with a license change to increase the capacity)
IPS to NTBA Communication Error	Error	The IPS device cannot communicate with its NTBA appliance. Reason: {0}	This problem may exist for a few minutes after the initial connection but is cleared once complete. If the problem persists, check for interference from external devices, such as a firewall that may be dropping the traffic.
Cannot Start Control Channel Service	Error	Cannot obtain the Manager certificate (Size {0}).	Database tuning may fix the problem. Else, a database restore is required.
Cannot Start Control Channel Service	Error	Unable to load the Manager key store.	Database tuning may fix this problem. Else, a database restore is required.
Failed to Create Command Channel Association	Error	Command channel association creation failed for device {0}. A secure connection could not be established between the Manager and the device. This could be caused due to loss of time during synchronization between the Manager and device, or when the device is not completely online after a reboot.	Restart the Manager and/or check the device status to ensure that the device is connected to the Manager and in good health.
{0} Discovery Failure	Error	{0}, {1} failed to discover configuration information. The device is not initialized properly and may not be displayed in the Manager UI. This error is typically due to incompatible software versions between the device and the Manager.	Check the Trellix Download Portal to ensure you are running compatible Manager and device software versions. If required, upgrade the device software via SCP or TFTP.

Fault	Severity	Description/Cause	Action
Peer DoS Profile Retrieval Failure	Error	Peer DoS profile retrieval request from device {0} failed. No DoS profile for peer {1} is available. The Manager cannot obtain the requested profile from the peer device, nor can it obtain a valid saved profile.	Consult the system log for details.
Peer DoS Profile Retrieval Failure	Error	Peer DoS profile retrieval request from device {0} failed as the profile cannot be pushed from the Manager to the device that requested it.	Consult the system log for details.
Invalid Internal Web Server Certificate Detected	Error	An invalid internal web server certificate ({0}) has been detected on device {1} and needs to be re-imported. Reason: {2}	Re-import the internal web server certificate.
Device Discovery Failure	Error	The Manager could not obtain configuration details for device {0}. The device is not properly initialized and may not be displayed in the Manager UI. This error is typically due to incompatible software versions between the device and the Manager.	Check the Trellix Download Portal to ensure you are running compatible Manager and device software versions. If required, upgrade the device software via SCP or TFTP.
Alert Channel Down	Error	The Manager cannot communicate with the device {0} over the channel on which it receives alerts. Reason: {1}.	Check the device status using the "status" CLI command. Disconnect and re-connect the channel using the "disconnectalertandpktlogchannels" and "reconnectalertandpktlogchannels" CLI commands.
Packet Capture Channel Down	Error	The Manager cannot communicate with the device {0} over the channel on which it receives the attack packet captures. Reason: {1}.	Check the device status using the "status" CLI command. Disconnect and re-connect the channel using the "disconnectalertandpktlogchannels" and "reconnectalertandpktlogchannels" CLI commands.
Packet Capture Channel Down	Error	The packet capture channel for the device {0} is down, but the physical link is up. Details: {1}	The device normally auto recovers from this issue. If your device is otherwise functioning normally, you can ignore this message.
Out-of-Range Configuration	Error	Device {0} has detected an out-of-range SNMP configuration value.	If the problem persists, contact Trellix Technical Support.

Fault	Severity	Description/Cause	Action
License Required for SSL Proxy Decryption	Error	Sensor {0} was added to admin domain {1}, which has SSL proxy decryption enabled, yet there is no SSL proxy decryption license available for its model type {2}. Inheritance and the feature have therefore been disabled on Sensor {0}.	Add the missing license and re-enable SSL proxy decryption on the Sensor.
Trust Establishment Error	Error	Device {0} could not be added to the Manager as there is mismatch in the shared secret defined in the Manager.	Make sure the shared secret entered on the device CLI matches exactly with the one defined within the Manager GUI. (Tip: You can edit the one in the GUI if needed)
Trust Establishment Error	Error	Device {0} is attempting to establish a trust with the Manager, but it has not been defined on the Manager.	Make sure the device you would like to add to the Manager has been defined within the Manager GUI before trying to add it via the device CLI. Tip: The Manager definition is case sensitive, so make sure the device name and shared secret key match exactly.
SSL Decryption Certificate File Update Error	Error	The SSL certificate with key ID "{0}" error in "{1}".	Re-deploy the certificate file.
Suricata Rule Load Failure	Error	Device "{0}" failed to load one or more Suricata Snort rule. A log for this has been created in: INSTALL_DIR/App/temp/ftpin/{0}/{1}.	Consult the log for failure details.

Fault	Severity	Description/Cause	Action
Packet Capture Error	Error	The device detected an error connecting to the SCP server while attempting to transfer a packet capture file. The device is unable to send the packet capture file via SCP. The device has stopped capturing packets due to insufficient internal memory. The device experienced an internal error while performing the packet capture. The device is unable to authenticate with the target server to transfer the packet capture file.	The device will attempt to recover automatically. Confirm the packet capture configuration.
GAM Engine Update Status	Error	Sensor {0} has a status of: {1}.	Please check the connectivity of the Trellix IPS sensor with external network. If connection is fine, please attempt a manual GAM update from the Trellix IPS Manager. If the issue still persists, please contact the support team.
PKCS cert processing error	Error	Device {0} faced an error while processing the pkcs cert store.	Consult the system logs for details.

Sensor warning faults

These are the warning faults for a Sensor device.

Fault	Severity	Description/Cause	Action
Device Startup Detected	Warning	The device has powered up or rebooted.	If the device rebooted, confirm that the reboot was intentional. If not, consult the system log for details.
Voltage Error	Warning	Device voltage is outside its normal range	Ensure that all cables are connected correctly. Check connections on the fans and HDDs. Replace the CMOS battery. Remove all, but minimum components for operation and check sensor. If the issue follows a particular component, swap it, otherwise, replace the board. If the issue remains, replace the power supplies.

Fault	Severity	Description/Cause	Action
Fan Error	Warning	Device fan is not performing at expected capacity	Swap the fans round to see whether the problem stays with the location or follows the fan. Replace the fan or fan wiring/housing depending on the previous outcome. If the system has been in this use for a while, the event may be a sign of impending fan failure. Replace the fan.
Power Supply Error	Warning	Device power supply is outside its normal range	Remove and reapply AC. If the power supply still fails, replace it.
Processor Error	Warning	Device processor error	**Internal Error:** Swap processors and test. Replace the processors depending on the results of the test. **Thermal Issues:** Verify heatsink is properly attached and has thermal grease. If the system has a heatsink fan, ensure the fan is spinning. Check all system fans are operating properly. Check that the air used to cool the system is within limits.
Memory Error	Warning	Device memory error	• Review and confirm memory stick (RAM) population rules for environment. • Swap suspect memory for known working memory within system. • Observe for any error messages that might clarify whether the error is limited to the memory or the socket/location on the server board. • If error travels with memory, replace memory. • If error remains localized to the same memory socket, replace server board.

Fault	Severity	Description/Cause	Action
Physical Security Error	Warning	Device physical security error	**Chassis intrusion:** Use the Quick Start Guide and the Service Guide to determine whether the chassis intrusion switch is connected properly. If this is the case, make sure it makes proper contact when the chassis is closed. **LAN Leash lost:** Could be most likely due to unplugging the cable but can also happen if there is an issue with the cable or switch. Check the LAN cable and connector for issues. Investigate switch logs where possible. If this is also the case, someone has opened the chassis. Ensure nobody has access to the system that should not.
Physical Interrupt Error	Warning	Physical Interrupt error.	PCI related Issue: • Refer Intel SEL Troubleshooting guide to decode the bus, device, and function to identify the card. • If this is an add-in card: 1. Verify the card is inserted properly. 2. Install the card in another slot and check whether the error follows the card or stays with the slot. 3. Update all firmware and drivers, including non-Intel components. • If this is an on-board device: 1. Update all BIOS, firmware, and drivers. 2. Replace the board.
		FP (NMI) Interrupt (Frontend Panel Non-Maskable Interrupt)	• If this button was not actually pressed, ensure there is no physical fault with the front panel. • This event creates a memory dump to preserve state of Sensors for further inspections. • This event only gets logged if a user pressed the NMI button or sent an IPMI Chassis Control command requesting this action and, although it causes the OS to crash, is not an error.

Fault	Severity	Description/Cause	Action
System Firmware Error	Warning	Device system firmware error	If this is a serious error, there is typically also a corresponding System Event Log entry logged for whatever was the cause of the error; this event may contain more information about what happened.
Watchdog Error	Warning	Device watchdog error	Capture a System BMC Debug Log as soon as possible after the failure. OS event logs need to be investigated to determine what may have caused this.
Logging Error	Warning	Device logging disabled error	The BMC logs an SEL clear event. This is an informational event only. This is only ever the first event in the SEL. The cause of this event is either a manual SEL clear or some other IPMI-aware utility or is done in the factory as one of the last steps in the manufacturing process.
Generic Hardware Error	Warning	Device General Hardware error	Caused by another event. System event logs would be cleared manually. Platform event Filters were triggered to send alerts of system event logs. Inspect system event logs that are found around the time of event.
Operating System Shutdown Error	Warning	Operating system shutdown error	These events are usually found along with several other events. Examine System event log entries found around the event timestamp. Events come along with reason code. Refer Intel SEL troubleshooting guide to decode them.
Sensor Health Changed	Warning	Health of sensor {0} changed from {1} to {2}	Please visit Devices → Sensor Health → **Health Status** to more about the health of the sensor
HA Peer Status Change	Warning	High-availability device {0} is {1}	A status of Incompatible indicates that the HA member Sensors are not running the same Sensor software version, which is required for proper HA function. A status of Down indicates that the peer Sensor cannot be reached. In this case, check the HA interconnect port's status as well as the peer Sensor's health.
Device Reboot Required	Warning	The jumbo frame parsing setting on this device has been updated and a reboot is required for the change to take effect.	Reboot the device to make the change take effect.
Pluggable Interface Certification Status	Warning	Pluggable interface in port {0} is {1}	Replace the non-certified transceiver with a Trellix-certified one or update the physical port's settings to allow a non-certified connector type.

Fault	Severity	Description/Cause	Action
Device performance - {0}	Warning	{0}{1} {2} detected on {3}. ({4} Threshold: {5}{6}).	Review the number and duration of performance-related faults for this device and refer its performance charts to determine if high usage is an ongoing occurrence. If yes, a model with a higher system capacity should be considered. (Tip: Multiple capacities are supported on some models with a license change to increase the capacity)
Alert Channel Down	Warning	The alert channel for device {0} is down, but the physical link is up. Details: {1}	The device normally auto recovers from this issue. If your device is otherwise behaving normally, you can ignore this message.
Device Configuration Change Detected	Warning	A change in the physical configuration for device {0} has been detected. A new configuration has been discovered.	Refer the physical ports and confirm if the configuration change is intended.
Failed to Dismantle HA Pair	Warning	The HA pair could not be dismantled as device {0} is disconnected from the Manager. (The Manager will try to dismantle once the device reconnects.)	Ensure that both member devices in the HA pair are connected to the Manager.
HA pair Configuration Out-of-Sync	Warning	Pending changes could not be deployed to the device {0} in a HA pair {1}. Configuration will be out-of-sync until pending changes are deployed to both devices in the pair. (The Manager will continue to deploy changes until the deployment is successful.)	Ensure that the device is connected to the Manager and is in good health.
HA pair Configuration Out-of-Sync	Warning	The firewall connection status for the devices in the HA pair {0} is inconsistent. This results in inconsistent functioning of firewall in the pair.	Ensure that both devices in a HA pair are connected to the firewall and the devices are online in good health.
HA Pair Decryption Certificates Out-of-Sync	Warning	SSL decryption certificates could not be deployed to device {0} in HA pair {1}. The certificates will be out-of-sync until they are deployed to both devices in the pair. (The Manager will continue to attempt to deploy them until deployment is successful.)	Ensure that the device is connected to the Manager and in good health.

Fault	Severity	Description/Cause	Action
Callback Detectors Out-of-Sync	Warning	The deployment of Callback Detectors to the device {0} failed. The Callback Detectors on the HA pair {1} are out-of-sync as a result. (The Manager will automatically make another attempt to deploy them.)	Ensure that the device is connected to the Manager and in good health.
Device Discovered with Expiring License	Warning	Device {1} was discovered with a license that will expire on {0}.	Renew the expiring license.
Pending Device License Expiration	Warning	Device {0} ({1}) license expires in less than {2} days.	Renew the expiring license.
Pending Device Support License Expiration	Warning	Device {0} (support {1}) license expires in less than {2} days.	Renew the expiring license.
Pending Device Add-On License Expiration	Warning	Device {0} (device {1}) license expires in less than {2} days.	Renew the expiring license.
Pending Device Support Add-On License Expiration	Warning	Device {0} (support {1}) license expired in less than {2} days.	Renew the expiring license.
License Detected for {0} of Type {1}	Warning	License valid until {0}.	Renew the license before it expires.
Pending License Expiration for {0} of Type {1}	Warning	License for this device expires in {0} days.	Renew the license.
Expiring License	Warning	The SSL proxy decryption license key {0} will expire on {1}. Updates to the Sensor to which it is assigned will be prevented once the license has expired. License details - Model:{2}, Capacity:{3}, Required Devices:{4}, Grant ID:{5}, Customer Name:{6}, Expiration:{7}, Assigned To:{8}	Renew the license.

Fault	Severity	Description/Cause	Action
Expiring License	Warning	The SSL proxy decryption license key {0} will expire on {1}. License details - Model:{2}, Capacity:{3}, Required Devices:{4}, Grant ID:{5}, Customer Name:{6}, Expiration:{7}, Assigned To:{8}	Renew the license.
Expired License	Warning	Proxy Decryption License with key {0} has expired. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
System License Required	Warning	Sensor {0}, which was added to admin domain {1}, is running without a valid system license. Updates to the Sensor will be prevented until a valid license is assigned.	Assign the device a valid system license.
Expired License	Warning	The system license with key {0} has expired and 30 days passed beyond expiry. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
Expired License	Warning	The system license with key {0} has expired. Post 30 days of expiry the license cannot be used. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
Expired License	Warning	The evaluation system license with key {0} has expired. License details - Model:{1}, Capacity:{2}, Required Devices:{3}, Grant ID:{4}, Customer Name:{5}, Expiration:{6}, Assigned To:{7}	Replace the expired license with a valid one.
Expiring License	Warning	The system License with key {0} will expire on {1}. Post 30 days of expiry, license cannot be used. License details - Model:{2}, Capacity:{3}, Required Devices:{4}, Grant ID:{5}, Customer Name:{6}, Expiration:{7}, Assigned To:{8}	Renew the license.

Fault	Severity	Description/Cause	Action
Expiring License	Warning	The system License with key {0} will expire on {1}. Post 30 days of expiry, updates to the Sensor to which it is assigned will be prevented. License details - Model:{2}, Capacity:{3}, Required Devices:{4}, Grant ID:{5}, Customer Name:{6}, Expiration:{7}, Assigned To:{8}	Renew the license.
Console Login Failure	Warning	{3} login failure threshold of 3 attempts is exceeded for user name {0} from remote IP Address {1} on remote port {2}.	
Device Packet Capturing Terminated	Warning	Packet capturing has been stopped during device re-initialization.	Restart the packet capture, as required.
Packet Capture Complete	Warning	The device is near capacity. Packet captures might not capture all packets.	Verify the packet capture configuration and restart the packet capture, as required.
Device DNS Server Connectivity Status	Warning	DNS server is {0} from the device.	Confirm the status of, and connectivity with, the configured DNS servers, and update the name resolution settings, as needed.
SNMP Trap Received from Load Balancer	Warning	Load balancer "{0}" reported trap type "{1}".	
Load Balancer Port Mode Change for {1}	Warning	Load balancer "{0}" reports operating mode for port "{1}" changed to "{2}".	
Load Balancer Port HA Mode Change for {1}	Warning	Load balancer "{0}" reports port "{1}" HA mode changed.	
Load Balancer HA Mode Change	Warning	Load balancer "{0}" reports HA mode change to "{1}".	
Load Balancer HA Status Change	Warning	Load balancer "{0}" reports HA status change to "{1}".	
Load Balancer Peer HA Status Change	Warning	Load balancer "{0}" reports peer HA status change to "{1}".	

Fault	Severity	Description/Cause	Action
Load Balancer Port Load Balancing Mode Change for {1}	Warning	Load balancer "{0}" reports port "{1}" load balancing mode changed to "{3}"	
I/O Module {0} Status Change	Warning	A {1} I/O module has been inserted into slot {0} on the device. A (full) Device reboot is required to make the new I/O module active. An I/O module has been removed from slot {0} on the device. Device reports I/O module {2} in slot {0}.	
Hitless Reboot Status	Warning	The device was unable to complete a hitless reboot. It will perform a full reboot instead.	
Device Auto-Recovery Status	Warning	The device was unable to complete auto-recovery. It will perform a full reboot instead.	
Monitoring Configuration Mismatch	Warning	Device latency monitoring configuration requires Layer 2 pass-through monitoring to be enabled.	Disable moving device to Layer 2 bypass mode on high latency or enable Layer 2 pass-through monitoring.
Device in High Latency Mode	Warning	Device high latency mode is currently {1}. Device high latency mode and Layer 2 bypass mode are currently {1}.	No explicit action is required. The device will attempt to automatically recover from the high latency condition.
Device Reboot Required	Warning	The SSL decryption state and/or the number of flows allocated for decryption has changed on device {0}. (New flow value = {1}). A device reboot is required for the configuration to be updated.	Reboot the device for the configuration to be updated.
Temperature Error	Warning	Device temperature is outside its normal range.	Check the cooling of your server room. Ensure there are no fan failures. Ensure the air used to cool the system is within the thermal specifications for the system (typically below 35°C).

Sensor informational faults

These are the informational faults for a Sensor device. These messages are only for your information and there is no specific action to be taken.

Fault	Severity	Description/Cause
FIPS Violation Detected - User Login	Informational	The device reports a user login to its CLI after device initialization. This is a FIPS 140-2 Level 3 violation.
Device Reset for FIPS Mode Change	Informational	{0}
Cluster Software Initialization Status	Informational	{0} device software has been initialized correctly.
Pluggable Interface Absent {0}	Informational	Pluggable interface in {0} is {1}.
Device Download Started	Informational	A download has been initiated from the device CLI.
FIPS Mode Change	Informational	An upgrade or downgrade between FIPS and non-FIPS software images has been detected. This resets the device configuration and restores the default login password.
Load Balancer Power Up	Informational	Load Balancer "{0}" has completed booting and is online.
Packet Capture File Transfer Status	Informational	The device has started sending the packet capture file via SCP. The device has completed sending the packet capture file via SCP. The device has stopped capturing packets because it has reached the configured maximum capture file size. The device has stopped capturing packets because it has reached the configured maximum duration. The device is ready to transfer the packet capture file to the Manager.
Hitless Reboot Status	Informational	The device successfully completed a hitless reboot.
Device Auto-Recovery Status	Informational	The device successfully completed auto-recovery.
Device Download Complete	Informational	Device download initiated from the device CLI has completed with status {2}. Download type={4}, Time={3}, Filename={5}
Sensor Health Changed	Informational	Health of sensor {0} changed from {1} to {2}. This fault is raised in the event of Sensor's **Overall Health** status change.

NTBA faults

The NTBA faults can be classified into critical, error, warning, and informational. The **Action** column provides you with troubleshooting tips.

NTBA critical faults

These are the critical faults for a NTBA device.

Fault	Severity	Description/Cause	Action
GAM Initialization Error	Critical	The Gateway Anti-Malware engine failed to initialize due to an internal error.	Consult the system log for details.
GAM Initialization Error	Critical	The Gateway Anti-Malware engine failed to initialize because the required update files are not available.	Enable automatic GAM updating or download the updates manually using the CLI or via the Manager.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because the update file import failed.	Consult the system log for details. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because the update file is not available.	Confirm connectivity and consult the system log for details. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because NTBA cannot connect to the Trellix IPS Update Server.	Confirm connectivity and consult the system log for details. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because the update file validation failed.	Consult the system log for details and attempt another update. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because NTBA cannot connect to the Trellix IPS Update Server.	Confirm connectivity and consult the system log for details. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because NTBA cannot resolve the name of the Trellix IPS Update Server.	Confirm proper name resolution settings for the NBTA Appliance. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because NTBA cannot communicate with the configured proxy server.	Confirm connectivity between the NTBA Appliance and the configured proxy server. If the problem persists, contact Trellix Technical Support.
GAM Update Failure	Critical	The Gateway Anti-Malware update failed because NTBA failed to authenticate with the configured proxy server.	Confirm proper proxy server settings for the NTBA Appliance. If the problem persists, contact Trellix Technical Support.
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because the ePO server is unreachable.	Confirm that the ePO server is up and reachable to NTBA.
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because the ePO extension does not support the auto-signing service.	Confirm that the ePO server supports the ePO auto-signing service (Change on Name confirmation).
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because of an authentication error while connecting to the ePO server.	Edit EIA integration and update the ePO server credentials.

Fault	Severity	Description/Cause	Action
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because of an internal error on the ePO server.	Consult ePO for errors.
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because of unexpected errors.	Consult the NTBA logs for errors.
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because of a corrupt ePO certificate.	Update the ePO certificate from within the EIA integration settings.
EIA Service Stopped	Critical	Endpoint Intelligence Service has stopped because the configured port for Endpoint Intelligence Service is already in use.	Review and potentially update the listening port from within the EIA integration settings.
Link Error on {0}	Critical	The link on {0} is {1}	Confirm that the device to which this port is connected is online and the cable connecting them is secure. If this port is not actually being used, disable it on the Physical Ports page.
NTBA Appliance Disconnected	Critical	A command channel ping failed to NTBA Appliance {0}. The device is unreachable through its command channel.	Check the device status using the "status" CLI command, and confirm basic network connectivity between the device and the Manager.

NTBA error faults

These are the error faults for a NTBA device.

Fault	Severity	Description/Cause	Action
NTBA Deployment Error	Error	{0}	Re-try the deployment.
NTBA Signature Set Mismatch Error	Error	There has been a mismatch between the NTBA version {0} and the signature set version {1}. The Manager will automatically try to deploy changes again.	Consult the system log for details.
NTBA Zone Configuration Event	Error	Invalid interface or zone configuration. All the zones configured are {0}. {1}.	Consult the system log for details and review the zone definition.
NTBA {0}	Error	{0}	Check connectivity between NTBA and GTI.
NTBA {0}	Error	{0}	Check the NTBA storage configuration.
NTBA {0}	Error	{0}	Check the NTBA GAM configuration.
DXL Service Offline	Error	Failed to connect to the ePolicy Orchestrator server.	Consult the system logs and check connectivity between the device and Trellix ePO - On-prem.

Fault	Severity	Description/Cause	Action
DXL Service Offline	Error	Failed to connect to the Data Exchange Layer service.	Consult the system logs.
DXL Service Offline	Error	Failed to start the Trellix Agent service.	Consult the system logs.
DXL Service Offline	Error	Failed to start the Data Exchange Layer service.	Consult the system logs.

NTBA informational faults

These are the informational faults for a NTBA device. These messages are only for your information and there is no specific action to be taken.

Fault	Severity	Description/Cause
{0}	Informational	{0}
{0}	Informational	The NTBA interfaces were changed from {0} to {1}
{0}	Informational	The NTBA resource {0} was changed to {1} {2}. Recommended is {3} {4}.
NTBA Database Pruning	Informational	Current database usage: {0}%
NTBA Network Forensics Data Pruning	Informational	Current Network Forensic data usage: {0}%

Troubleshooting scenarios

Network outage due to unresolved ARP traffic

Scenario

Sudden outage in the network due to unresolved ARP traffic

Applicable to Sensor models: NS-series and Virtual IPS Sensors.

Sensor software version:10.1, 11.1

Problem type to be solved

Resolve the ARP traffic which is dropped by the Sensor due to heuristic web application server protection configuration setting.

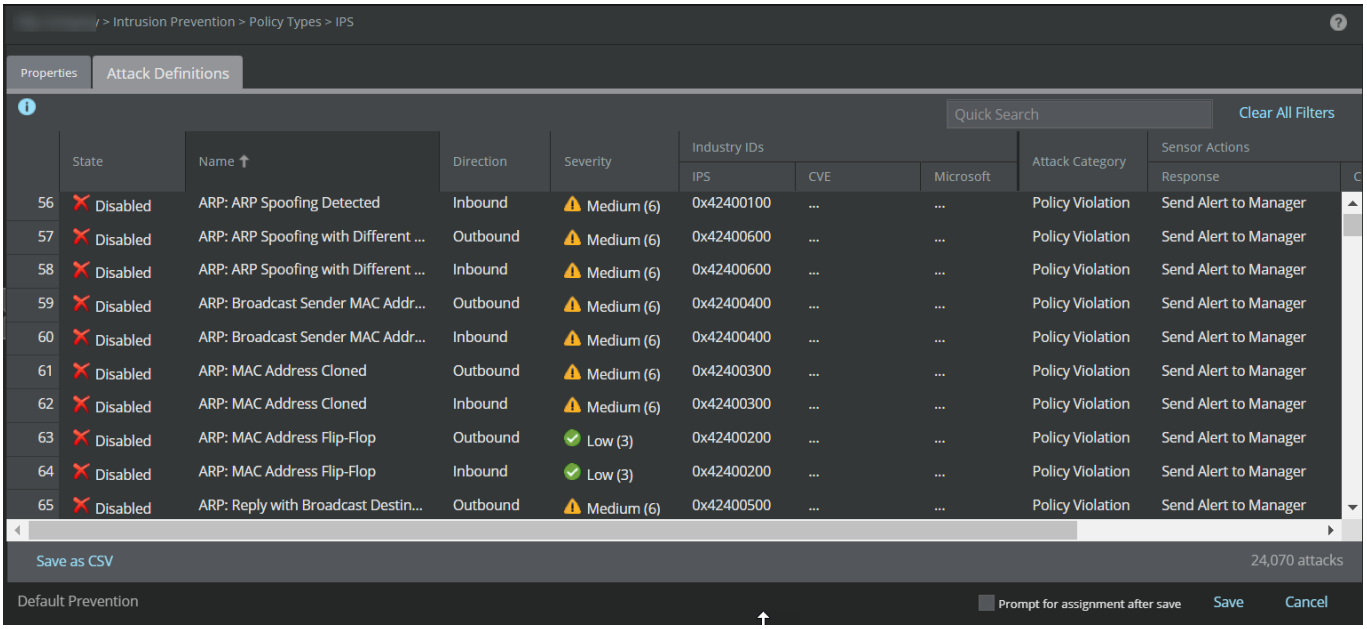
Data/Information Collection

Steps:

1. Check if the attack **ARP MAC Address Flip-Flop** is disabled from the policy.

   Go to Policy → Intrusion Prevention → Policy Types → **IPS**. Double-click **Default Prevention** listed in **IPS** name column.

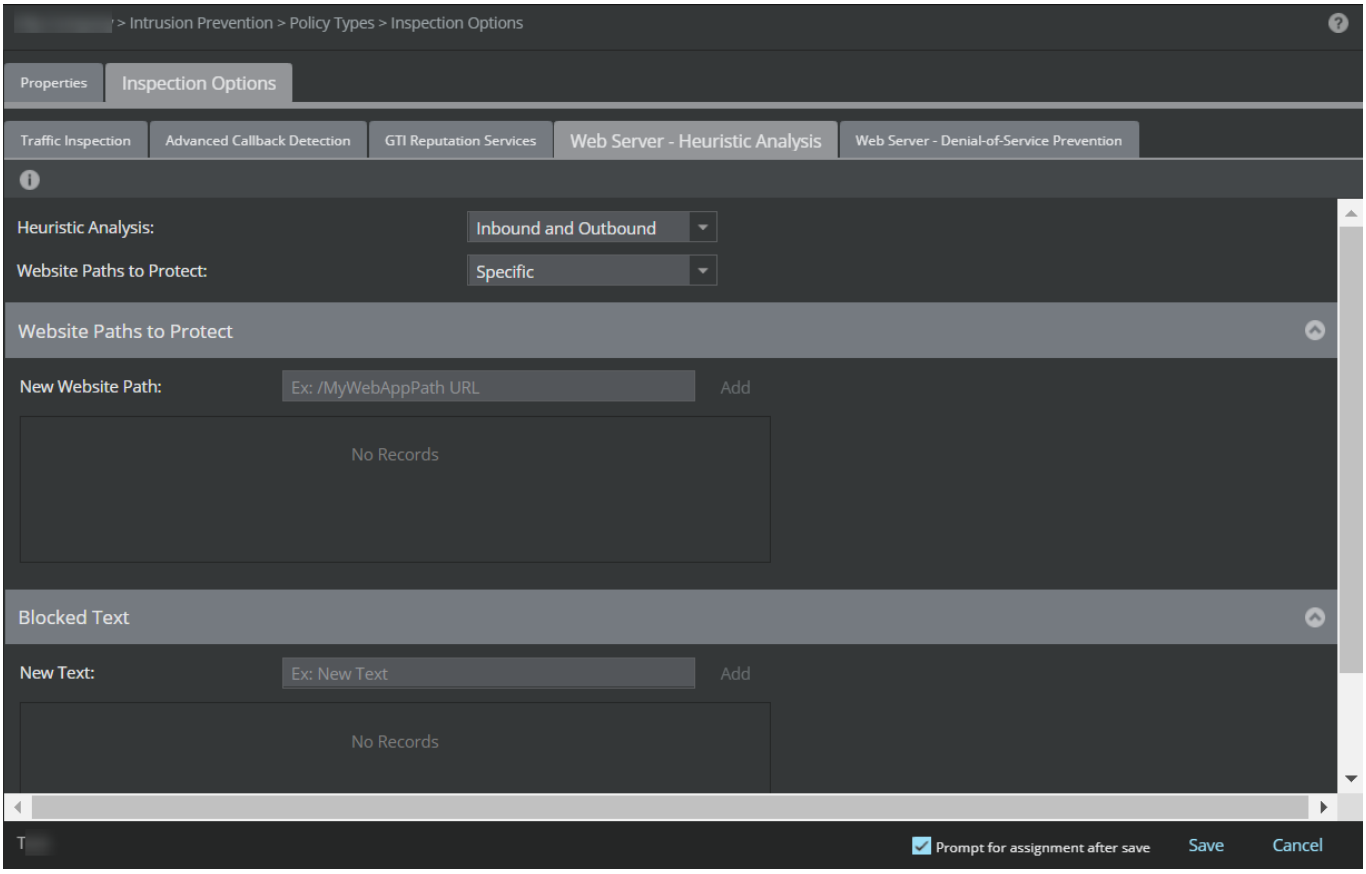
   Check the policy on the entire device interfaces and make sure ARP flip flop alert is either disabled or not included in the policy on the entire device interfaces.



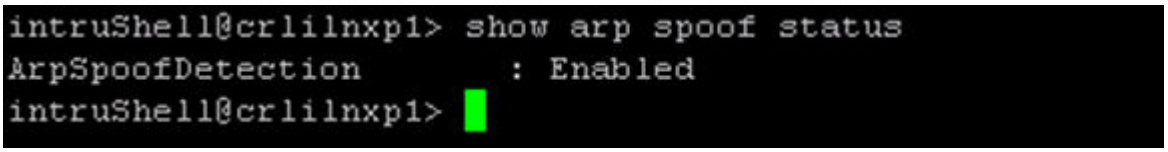
2. Check if the **Heuristic Web Application Server Protection** is enabled.

   Go to Policy → Intrusion Prevention → Policy Types → **Inspection Options**. Double-click **<Policy Name>** listed in **Inspection Options** page.

> **NOTE**
>
> Check each interface of the device individually.



3. Check if ARP spoofing is enabled on the Sensor. Use the command **`show arp spoof status`**.



Explanation

When heuristic web application server protection is enabled, the Manager caching is disabled and only selected attacks are pushed to the Sensor. If the MAC Flip-Flop attack is not part of the attacks chosen by the user, the Sensor drops the ARP packets. This happens in scenarios such as the following:

- Assignment of dynamic MAC address in the network (vmac)
- For the firewall in failover mode which uses the Virtual MAC address, the IP address remains the same but the MAC address will change

Troubleshooting Steps

1. Disable ARP spoofing on the Sensor. Use the command **`arp spoof`** to disable ARP spoofing.
2. Disable **Heuristic Web Application Server Protection** on the device's individual interfaces.

   If the problem still persists, contact Trellix Support for further assistance.

Delay in alerts between the Sensor and Manager

Scenario

Delay in receiving the Sensor alerts on the Manager

Applicable to Sensor models: NS-series and Virtual IPS Sensors

Sensor software versions: 10.1, 11.1

Problem type to be solved

- Delay in the Sensor alerts being sent to the Manager
- Sensor alerts are not seen in real time on the Manager
- Time lag in sending the Sensor alerts to the Manager

Data/Information Collection

Steps:

1. Execute the following commands on the Sensor :
   - **`status`** (Execute 5 times in 10 seconds duration.)
   - **`show sensor-load`** (Execute 5 times in 10 seconds duration.)
   - **`getccstats`** (Enter debug mode and execute this command 5 times in 10 seconds duration.)

   > **NOTE**
   >
   > Also execute the same commands on a similar model Sensor, which does not have the issue.
2. Collect graphs for Sensor throughput utilization and port utilization.
3. Collect the attack csv file for this Sensor from the **Attack Log** page.
4. Collect the alert archival for the last 24 hour time duration.
5. Retrieve the configuration backup of the Manager.
6. Create/collect the network diagram that clearly indicates where the Sensor and the Manager are located.

Troubleshooting steps

1. Check if there are any network connectivity issues or any delay in the network. If there is a delay in the network between the Sensor and the Manager, it can lead to low alert rates.
2. Verify that the entire link between the Sensor management port and the Manager is 1G auto, and they are using the correct CAT6 cables.
3. Check if the other Sensors connected to the same Manager are also facing this issue. If yes, it is a Manager issue.
4. Check the Sensor policy being used. If the **Default Testing** or **Default Exclude Informational** is used, the Sensor processes more alerts and alert generation rate increases. Switching to **Default Prevention** policy can help resolve the delay issue sometimes.
5. Check if there are any saved alerts/packetlogs on the Sensor.

Command: **`show savedalertinfo`**

6. Check if there is any specific category of alerts, which is delayed or all the alerts are delayed. Also check if the system events that are being raised, are also delayed.
7. Check if the alerts are seen in the **Attack Log** page as the alerts are restored here from the database. This check will confirm if the issue is on the database or cache. Check the database size and if it is very high, purge and tune the database.
8. Check the time on the Sensor and whether it matches with the Manager system time. If there is any issue with the time stamp, the Manager may show the wrong timestamp in the **Attack Log** page, which can incorrectly appear as alerts being delayed.
9. Check the rate of alert generated/detected by the Sensor using the following command in debug mode:

   `getccstats`

   The command displays the following statistics:

   - The status of trust between the Manager and Sensor, Sensor installation, alert channel, peer alert channel, etc.
   - The alert suppression/throttling configuration status and suppression intervals
   - The sensor failover action (1 = Enabled, 2 = Disabled) and failover status (1 = Active, 2 = Standby, 3 = Init/Not Applicable), failover peer status (1 = Up, 2 = Down, 3 = Incompatible, 4 = Compatible, 5 = Init/Not Applicable), fail-open status (1 = Enabled, 2 = Disabled)
   - The count of detected alerts (signature-based, scan/recon, DoS) sent to management port and peer Manager (in case of MDR)
   - The count of throttled alerts
   - The count of alerts sent to and received from Correlation Engine and alert correlation counts
   - The count of alerts in ring buffer, queued to be sent to the Manager
   - The ACL alerts' throttling configuration status (throttling interval and threshold)
   - The count of throttled ACL alerts (IPS)
   - The Sensor reboot count and/or alert wrap count

   For example, consider the following statistics from **`getccstats`** command that indicate that many alerts are still pending in ring buffer:

   `AlertsInRngBufPriCount = 83621`

   `AlertsInRngBufSecCount = 83606`

   `PutAlertInRngBufErrCount = 6499317`

   The alert rate could be so high that the Manager may not be able to handle. Subsequently, it introduces a delay that is similar to backoff (with the delay reaching a max of 30 seconds per alert) and this causes the alerts to be queued up in ring buffer. Once this condition is reached, the alerts delay will increase with time. To recover, check the type of attacks and then try to create an exception rule to filter the attack, and see if the Manager recovers.
10. Collect the packet captures at the Sensor and the Manager side to identify whether the issue is at the Sensor/Manager side or network side.

    On the Manager, use Wireshark or equivalent to collect packet captures on the Manager port 8502.

    Sample packet capture on the Sensor:

15	2014-06-02 16:53:32.401608	10.50.3.201	10.94.203.90	TCP	192 51112 > 8502 [PSH, ACK] Seq=671 Ack=297 Win=9600 Len=138
16	2014-06-02 16:53:32.642158	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=297 Ack=809 Win=63166 Len=74
17	2014-06-02 16:53:32.676184	10.50.3.201	10.94.203.90	TCP	54 51112 > 8502 [ACK] Seq=809 Ack=371 Win=9600 Len=0
18	2014-06-02 16:53:32.708442	10.50.3.201	10.94.203.90	TCP	192 51112 > 8502 [PSH, ACK] Seq=809 Ack=371 Win=9600 Len=138
19	2014-06-02 16:53:32.949113	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=371 Ack=947 Win=63028 Len=74
20	2014-06-02 16:53:32.949769	10.50.3.201	10.94.203.90	TCP	54 51112 > 8502 [ACK] Seq=947 Ack=445 Win=9600 Len=0
21	2014-06-02 16:53:32.986336	10.50.3.201	10.94.203.90	TCP	320 51112 > 8502 [PSH, ACK] Seq=947 Ack=445 Win=9600 Len=266
22	2014-06-02 16:53:33.422152	10.94.203.90	10.50.3.201	TCP	60 8502 > 51112 [ACK] Seq=445 Ack=1213 Win=64240 Len=0
23	2014-06-02 16:53:33.592803	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=445 Ack=1213 Win=64240 Len=74
24	2014-06-02 16:53:33.593007	10.50.3.201	10.94.203.90	TCP	54 51112 > 8502 [ACK] Seq=1213 Ack=519 Win=9600 Len=0

Sample packet capture on the Manager:

18	2014-06-02 16:53:40.723166000	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=223 Ack=617 Win=63470 Len=74
21	2014-06-02 16:53:40.963183000	10.50.3.201	10.94.203.90	TCP	208 51112 > 8502 [PSH, ACK] Seq=617 Ack=297 Win=9600 Len=154
22	2014-06-02 16:53:40.968161000	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=297 Ack=771 Win=63316 Len=74
26	2014-06-02 16:53:41.224796000	10.50.3.201	10.94.203.90	TCP	208 51112 > 8502 [PSH, ACK] Seq=771 Ack=371 Win=9600 Len=154
27	2014-06-02 16:53:41.229829000	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=371 Ack=925 Win=63162 Len=74
31	2014-06-02 16:53:41.480835000	10.50.3.201	10.94.203.90	TCP	192 51112 > 8502 [PSH, ACK] Seq=925 Ack=445 Win=9600 Len=138
34	2014-06-02 16:53:41.486328000	10.94.203.90	10.50.3.201	TCP	128 8502 > 51112 [PSH, ACK] Seq=445 Ack=1063 Win=63024 Len=74

Using packet captures from the Sensor and the Manager, which are taken simultaneously, you can identify if there is a delay in the Sensor sending the alert to the Manager, or there is a delay in the Manager sending the alert acknowledgment to the Sensor, or both are happening which indicate a potential network issue.

11. Check if Layer 7 Data Collection is enabled on the Sensor. There is a known issue when Layer 7 Data Collection is enabled, where the alerts in the **Attack Log** page are no longer received in real time.

    ```
    IntruDbg#> show l7dcap-usage
    Layer-7 Dcap Buffers Allocated at Init 16000
    Layer-7 Dcap Buffers Available now 16000
    Layer-7 Dcap Buffers Alloc Errors 0
    Layer-7 Dcap Alert Buffers Allocated 40960
    Layer-7 Dcap Alert Buffers Available 40960
    Layer-7 Dcap Alert Buffers Allocate Error 0
    Layer-7 Dcap Regular Alert's Sent 0
    Layer-7 Dcap Special Alert's sent 0
    Layer-7 Dcap Context End Alert's Sent 0
    Layer-7 Dcap CB InActive when DCAP Called 0
    Layer-7 Dcap Ring Buffer Errors 0
    Alert Ring Buffer Full Cnt 0
    Num Alerts Dropped at Sensors 0
    Layer-7 Dcap Fifo Check Seen 0
    ```

12. On the Manager database, use SQL queries output to check the frequency of alerts going to the Manager. This can be done by logging into MariaDB on the Manager server and executing the following command:

    a. Get Sensor ID from database:

    ```
    select sensor_id, name from iv_sensor;
    ```

    b. Input the time range for which the alert generation rate needs to be checked:

    ```
    SELECT "2014-05-29 18:39:47", "2014-05-30 18:39:47" INTO @stdate, @enddate;
    ```

    c. Total Attacks for Sensor ID and the time range:

```
SELECT sensorid,COUNT(*) atcount FROM iv_alert WHERE creationtime BETWEEN @stdate AND
@enddate GROUP BY sensorid ORDER BY atcount;
```

d. Total packetlog for Sensor ID and time range:

```
SELECT sensorid,COUNT(*) pktcount FROM iv_packetlog WHERE (creationtime BETWEEN @stdate
AND @enddate) AND sensorid=<id of problematic sensor> GROUP BY sensorid ORDER BY
pktcount;
```

If the problem still persists, contact Trellix Support for further assistance.

Sensor-Manager Connectivity Issues

Scenario

Connectivity issues between the Sensor and Manager

Applicable to Sensor models: NS-series and Virtual IPS Sensors

Sensor software versions: 10.1, 11.1

Problems type to be solved

Sensor is not detected on the Manager.

Trust establishment does not happen between the Sensor and Manager.

Data/Information Collection

Steps:

1. Execute the following commands on the Sensor:
   - **`status`**
   - **`show`**
   - **`show sbcfg`**
   - **`show mgmtcfg`**
   - **`show doscfg`**
   - **`show mgmtport`**
   - **`getccstats`**
   - **`show netstat`**
   - **`checkmanagerconnectivity`**
2. Collect the Manager infocollector logs. If possible, perform the following:

   For Windows-based Manager, enable detailed debugging messages by modifying **`<Manager_Install_Dir>\config\log4j2.xml`** file.

   NOTE

   The default Manager installation directory is `%programfiles%\Trellix\IPS Manager\App`.

For Linux-based Manager, enable detailed debugging messages by modifying **log4j2.xml** file. To open the file, execute **edit log4j2.xml**.

Find out and modify the following lines in the **log4j2.xml** file:

- `<Logger name="iv.core.DiscoveryService" additivity="false" level="debug">`
  `<appender-ref ref="DEVICE_CONFIG_LOG"/>`
  `</Logger>`
- `<Logger name="iv.core.SensorConfiguration" additivity="false" level="debug">`
  `<appender-ref ref="DEVICE_CONFIG_LOG"/>`
  `</Logger>`

The modified logs will be available in **<Manager_Install_Dir>\logs\device_config.log** file.

3. Collect the Sensor trace files.
4. Collect packet capture at the Manager (for the problematic Sensor).
5. Network diagrams clearly mentioning where the Sensor and Manager are located.

Troubleshooting Steps

1. Check if there is any network connectivity issue such as conflicting IP address of the Sensor. This can result in alert/pktlog channel flaps.
2. Verify that the Management Interface speed and duplex settings are configured correctly on the Manager and Sensor and that they are hard-coded. If this fails, change one link to auto and change the other side's duplex and speed settings until communications are established or combinations are exhausted.
3. Ping from the Sensor to Manager and Manager to Sensor, and make sure the ping is successful.
4. Check if the other Sensors connected to the same Manager are also facing this issue.

   If yes, it is a Manager issue.
5. Check the IP address of the system on which the Manager is installed. Make sure the correct IP address is provided in the **set manager ip** command at Sensor CLI.
6. Try a **deinstall** and establish the trust again with the Manager.
7. Check if the Manager machine has multiple NIC cards. If yes, do the following:
   - For Windows-based Manager, open **<Manager_Install_Dir>\bin\tms.bat** file.
   - For Linux-based Manager, open **tms.sh** file. To open the file, execute **edit tms.sh**.

   Later, modify the following line to assign the relevant IP address that is also used in the Sensor configuration: **set JAVA_OPTS=%JAVA_OPTS% -Dlumos.fixedManagerSNMPIPaddress=""restart Manager**
8. Check the Sensor name, which is given on the Manager while adding the Sensor using the **Add New Device** wizard. Sensor name is case-sensitive. So make sure it exactly matches the one given on the Manager.
9. Check that the device type is selected as **IPS Sensor** while adding the Sensor using **Add New Device**. Selecting incorrect device type can also lead to connectivity issues.
10. Make sure that firewall is not blocking traffic between the Manager and Sensor for the following ports:

    Manager:4167 -> Sensor:8500 (UDP)

    Sensor:Any -> Manager:8501-8504,8510 (TCP) for 1024-bit trusts

    Sensor:Any -> Manager:8504,8506-8509 (TCP) for 2048-bit trusts

11. If using the malware policy, check if the file save option is enabled. Make sure firewall is not blocking ports 8509 and 8510, which are used for saving malware files.
12. Check that UDP port 8500 is open and allows the Manager to Sensor SNMP communication.
13. Use the **`netstat -na`** command to verify that ports 8501 - ,8505 are listening on the Manager. Click Start → **Run** type **`cmd`**, press **Enter**, then type **`netstat -na`** at the command prompt.
14. Make sure large UDP and/or fragmented UDP packets are not dropped between the Sensor and Manager communication. This can lead to SNMP timeout. Look for the following logs in ems.log:

    `Ems log`

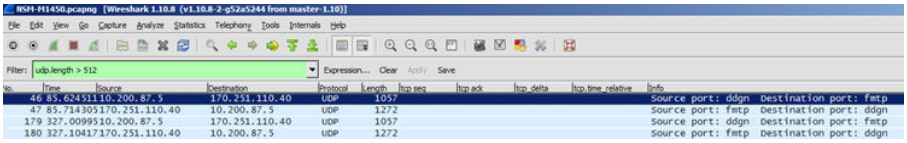
    `******`

    `014-06-27 15:47:29,150 INFO [Thread-135] iv.core.SensorConfiguration - M1450 Experience a SNMP error during set/get, Change the STATUS to DISCCONECTED`

    `2014-06-27 15:47:29,163 ERROR [Thread-135] iv.core.SensorConfiguration - Fail to process SNMP return node:`

    `com.intruvert.ext.sensorconfig.leap.SensorConfigException: Time Out`
15. Capture UDP traffic using Wireshark on the Manager. Check if the Manager is receiving UDP response packets from the Sensor.

    Sample capture on the Manager:



16. Check the time on the Sensor, and if it matches with the Manager system time.
17. Check if there are any **Out Of Memory** related logs in the Manager. This can lead to connectivity issues between the Sensor and Manager.
18. Check if the Manager is an MDR pair. If yes, verify that the IP of primary Manager in the sensor matches the IP of the active Manager. Also check whether the Sensor is treating the standby Manager as the primary Manager. This might lead to connectivity issues.

    If the problem still persists, contact Trellix Support for further assistance.

Wrong country name in IPS alerts

Scenario

To find the root cause of cases for IPS alerts in the **Attack Log** page that shows wrong country name for Attacker and Target.

Problems type to be solved

The **Attack Log** page displays wrong country name for source or destination IP address for an IPS alert.

Troubleshooting Steps

Applicable to Sensor models: NS-series and Virtual IPS Sensors

Sensor software versions: 10.1.5.116 and later for NS-series Sensors, and 10.1.7.86 and later for Virtual IPS Sensors

1. Download the latest signature set and deploy it to the Sensor.

   This ensures that the Sensor has the latest Digital Envoy database and country-to-CIDRs mapping information.
2. Login to the Sensor with “admin” ID.
3. In the Sensor CLI, issue the **debug** command to enter Debug mode.
4. In Debug mode, type the following command and press **Enter**:

   `show geoloc ipv4 <IP Address>`
5. The Sensor CLI returns the latest country information for the specified IP address. If you think the information is incorrect, contact Support for further assistance.

> **NOTE**
>
> If the Manager and Sensor are on software versions prior to 10.1 Update 7, it is recommended to upgrade them to later versions to continue receiving the updated geolocation databases. For more information, refer to KB95636. Always ensure to maintain the latest software versions of the Manager, Sensor, and Signature Sets.

Wrong country name in ACL alerts

Scenario

Wrong country name appears in ACL alerts/ACL logs

Applicable to Sensor models: NS-series and Virtual IPS Sensors

Sensor software version: 10.1, 11.1

Problem type to be solved

Wrong country name is displayed in the ACL alerts/ACL logs when forwarded to third-party software either from the Sensor or from the Manager.

Data/Information Collection

Execute **`show acl stats`** in the Sensor CLI.

Troubleshooting Steps

Execute the **`show acl stats`** command in the Sensor CLI to fetch the following data from the management process:

- Number of ACL alerts sent by the datapath processor to the management processor
- Number of ACL alerts sent from the management processor to the Manager or third-party software tool.

If there is difference between the received and sent/sent directly count by a large value but within 10,000, it indicates that the buffer to keep the ACL alerts at management processor is full. This might potentially be the cause for the issue.

```
intruShell@mil-ips-01> show acl stats

[Acl Alerts]

Received : 0

Suppressed : 0
```

```
Sent : 0

Sent Direct : 0

Stateless ACL Fwd count : 0
```

The buffer kept for receiving the ACL alerts from datapath processor is full, and is not flushed in an event like ACL alert suppression disabled/enabled. In this type of scenario, if the ACL alert buffer is not flushed, the country name for the old ACL alert is mixed with the new ACL alert, which results in the wrong country name in the ACL logs.

NOTE

If the country name is displayed wrong in the ACL alert, for either source IP address or destination IP address, there is an issue with the Sensor. If you are not able to solve the problem even after repeating the steps explained in troubleshooting, or the problem is not understood, contact Trellix Support for further assistance.

Using the InfoCollector tool

This section describes the following aspects of using the Infocollector tool in the Windows based Manager.

Introduction

InfoCollector is an information collection tool, bundled with Manager that allows you to easily provide Trellix with Trellix IPS-related log information. Trellix can use this information to investigate and diagnose issues you may be experiencing with the Manager.

InfoCollector can collect information from the following sources within Trellix IPS:

Information Type	Description
Ems.log Files	Configurable logs containing information from various components of the Manager. The current ems.log file is renamed when its size reaches 3MB, using the current timestamp. Another ems.log is created to collect the latest log information.
Configuration backup	A collection of database information containing all Trellix IPS configuration information
Configuration files	XML and property files within the Trellix IPS config directory
Fault log	A table in the Trellix IPS database that contains generated fault log messages
Sensor Trace	A file containing various Sensor-related log files
Compiled Signature	A file containing signature information and policy configuration for a given Sensor

InfoCollector is a tool that can be used both by you and by Trellix.

Trellix systems engineers can use the InfoCollector tool to provide you with a definition (.def) file via email. This file is configured by Trellix to automatically choose information that Trellix needs from your installation of Trellix IPS. You simply open the definition file within the InfoCollector and it will automatically select the information that Trellix needs from your installation of the Manager.

Alternatively, a manual approach can also be used with InfoCollector, and you can select information yourself to provide to Trellix. For example, Trellix may ask you to select checkboxes that correspond to different sets of information available within Trellix IPS.

How to run the InfoCollector tool in Windows based Manager

To run InfoCollector in Windows based Manager, follow the steps given below:

1. Access the following location :

   `<Manager_Install_Dir>\diag\InfoCollector`

   > **NOTE**
   >
   > The default Manager installation directory is **`%programfiles%\Trellix\IPS Manager\App`**.

2. Run the `InfoCollector.bat` file.

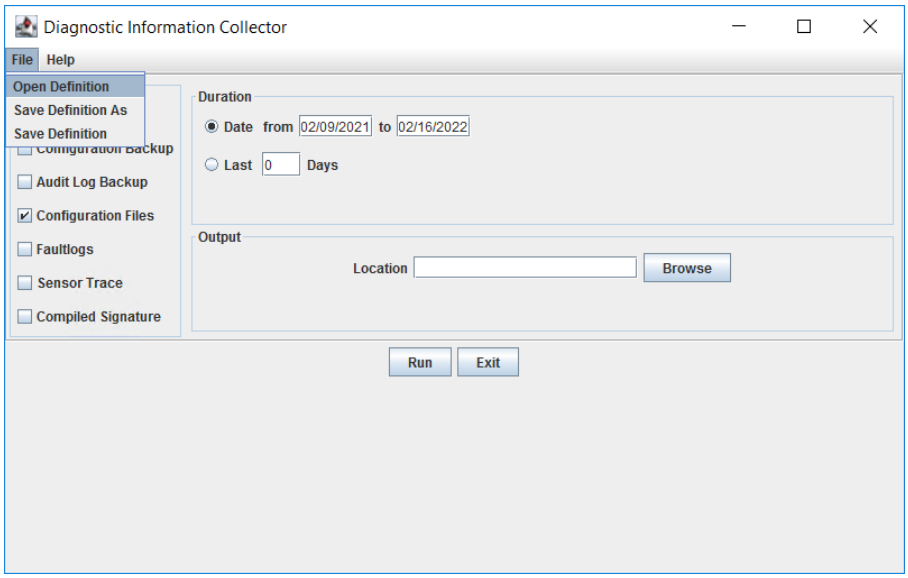
Using InfoCollector tool

To use InfoCollector, follow these steps:

1. After you run InfoCollector, do one of the following:
   - If Trellix provides you with a definition file:

   a. After you run InfoCollector, open the **File** menu and click **Open Definition**.

   Figure 824. Navigating to Open Definition option

   b. Select the definition file that Trellix sent you via email and click **Select**.

   - If Trellix instructs you to select InfoCollector checkboxes:

   a. After you run InfoCollector, select the checkboxes as instructed by Trellix.

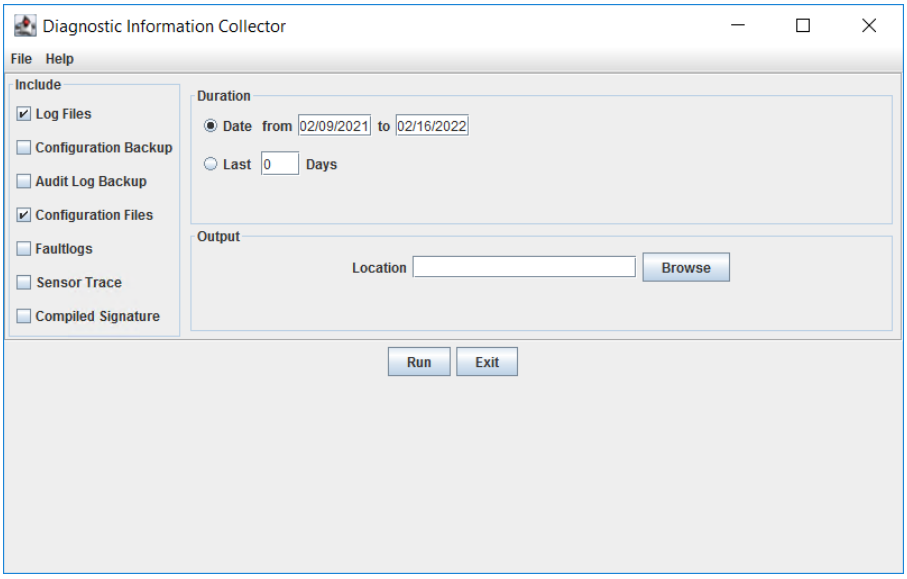
   b. Select a **Duration**. Select **Date** to specify a start and end date, or select Last X Days.

c. Select the number of days from which InfoCollector should gather information.

d. Click **Browse** and select the path and filename of the output ZIP file.

2. Click **Run**.

Figure 825. Running selected files



3. Provide the output ZIP file to Trellix as recommended by Trellix Technical Support. You can send the file via email or through FTP.

> **CAUTION**
>
> The output ZIP file contains the toolconfig.txt file, which lists the information that you have chosen to provide Trellix.

How to run InfoCollector in Linux based Manager

To run InfoCollector in a Linux based Manager, do the following:

1. Log in to the Manager shell using SSH.
2. Execute **`run InfoCollector.sh`** command to collect info logs.

   For collecting info logs by masking the sensitive information, execute **`run InfoCollector.sh -anon`** command.
3. (For InfoCollector in anonymous mode only) Select **`Update configuration`** in the operation menu and click **Enter**.
4. (For InfoCollector in anonymous mode only) Type **y** and click **Enter** when the following question is prompted:

   ```
   Do you want to procced with info collector bundle creation? [y/n]
   ```
5. Specify the log collection start date in the format [MM/DD/YYYY] and press **Enter**. Alternatively, just press **Enter** to choose the default start date (date preceding the current date).
6. Specify the log collection end date in the format [MM/DD/YYYY] and press **Enter**. Alternatively, just press **Enter** to choose the default end date (date preceding the current date).

Select the type of log files to be collected. By default, InfoCollector collects Manager and Manager Configuration files only. However, you can control which items are collected as shown below:

1. For default log file, specify **y** at Collect Default Items only prompt. The log bundle will be created with the filename in the format **`InfoLogs<Date><time>.zip`** along with success message.

   TIP

   You can view the generated InfoCollector bundle (zip file) by executing **`show files`** command.

   NOTE

   By default, InfoCollector collects Manager logs and Manager configuration files only; however, you can control which items are collected.

2. For manually selecting custom sets of logs, specify **n** at the Collect Default Items only prompt. Now, select the log files to be included in the bundle by specifying **y** or **n** one by one for each type of log.

   The available log types are as follows:

   - Manager Logs
   - Configuration Backups
   - Audit Log Backups
   - Manager Configuration Files
   - Compiled 'Sigfiles' (Sensor Deployment Binaries)
   - System Faults
   - Sensor Logs

NOTE

You can collect the Configuration Backups only when the InfoCollector utility is run in the normal mode.

A success message is displayed after the creation of InfoCollector bundle is completed.

NOTE

The InfoCollector bundle will be available at the following locations in the Manager:

- **`/opt/IPSManager/App/diag/InfoCollector/InfoCollectorData/`**
- **`/opt/scpfiles/`**

Automatically restarting a failed Manager with Manager Watchdog

This section provides information on how the Manager Watchdog works, installing the Manager Watchdog, starting the Manager Watchdog, using the Manager Watchdog in an MDR configuration, and tracking the Manager Watchdog activities.

Introduction

The Manager Watchdog feature is designed to restart the Manager if the Manager crashes, potentially bringing the Manager back online before MDR enables.

The Manager Watchdog monitors the Manager process on the Manager server periodically for availability. If Manager Watchdog detects that the Manager has gone down unexpectedly, it restarts the service automatically. (It does not restart the Manager if the Manager has been shut down intentionally.)

How the Manager Watchdog works

Manager Watchdog runs as a separate process and monitors Manager through the Windows OS Services model. Manager Watchdog polls Manager every 10 seconds. If the Manager Watchdog does not detect the Manager during a polling period, it waits for 30 seconds and then restarts the Manager service automatically. Manager Watchdog will make five attempts to restart the Manager and then, if it has not succeeded, it will exit.

Manager Watchdog, by default, is a manual service; you must explicitly start it.

> ⚠ **CAUTION**
>
> You can instead change this setting to be automatic if you wish the service to start automatically after a system reboot.

> ⚠ **CAUTION**
>
> If you have chosen to change the Manager service setting from its default (Auto) to "Manual" (during a troubleshooting session, for example), consider doing the same for Manager Watchdog as well. This will prevent the Manager Watchdog from restarting Manager automatically.

Install the Manager Watchdog

Manager Watchdog is installed automatically during Manager installation, and a new OS service called "Trellix IPS Manager Watchdog" is created to enable you to start and stop the Manager Watchdog service. When you first install the Manager, this service is started automatically. However, the default Windows **Startup Type** for this service is manual.

> ⚠ **CAUTION**
>
> Manager Watchdog monitors only the "Trellix IPS Manager" service; it does not monitor services like MariaDB or Apache.

Start the Manager Watchdog

The Manager watchdog process is, by default, not started after installation; you must start the Manager watchdog process manually.

To start/stop Manager Watchdog:

1. Select Start → Settings → **Control Panel**. Double-click Administrative Tools, and then double-click Services.
2. Click **Trellix IPS Manager Watchdog Service**.
3. Do one of the following:
   - To start the service, select Action → **Start**.
   - To stop the service, select Action → **Stop**.

   Alternatively, you can also use the Manager icon in the Windows system tray to start or stop Manager Watchdog. Right-click on the Manager icon at the bottom-right corner of your server and select **Start Watchdog** or **Stop Watchdog** as required.

Use the Manager Watchdog with Manager in an MDR configuration

When using Manager Watchdog on an Manager that is part of an MDR configuration, consider whether you want the Manager Watchdog to restart the Manager before failover can occur. If so, you must ensure that the value set for the MDR setting "Downtime Before Switchover" is greater than the Manager Watchdog setting of 30 seconds. This prevents the initiation of MDR, wherein the peer Manager takes over if the primary Manager fails. Trellix suggests retaining the default value of 5 minutes or greater to allow the Manager Watchdog time to restart the Manager.

If the Manager Watchdog brings up a primary Manager after MDR has initiated, note that the primary Manager does not come back Active; it checks first to determine whether the secondary is Active and if so, remains as standby.

Track the Manager Watchdog activities

The Manager Watchdog logs all controlled activities in a log file. For Windows-based Manager, log files can be found at **`<Manager_Install_Dir>\logs\wdout_<time stamp>.log`**

> **NOTE**
>
> The default installation path for Windows-based Manager is **`%programfiles%\Trellix\IPS Manager\App`**.

A sample log file entry follows:

Sample Manager Watchdog Log

```
Restarting server at Mon Jun 09 14:48:53 GMT+05:30 2022

SERVER STDOUT: The Trellix IPS Manager Service is starting.

SERVER STDOUT: The Trellix IPS Manager Service was started successfully.

SERVER STDOUT:

SERVER STDOUT:
```

If the Manager Watchdog fails after five attempts to restart Manager, the following line appears in the log file:

```
SERVER STDOUT: Failed to restart Manager after five attempts. Exiting. [kl]
```

For Linux-based Manager, log files can be found by executing **`show log file wdout_<time stamp>.log`** command.

Utilization of the Trellix Knowledge Base

The Trellix Knowledge Base (KB) contains a large number of useful articles designed to answer specific questions that might not have been addressed elsewhere in the documentation set. We suggest checking to see if a question you have is answered in a KB article.

To access Trellix Knowledge Base, perform the following steps:

1. Access https://thrive.trellix.com/s/customknowledge on your browser. Login to the portal.

   The **Trellix Knowledge Portal** page opens.

   > **NOTE**
   >
   > Alternatively, you can login to the Trellix Support Portal and click the **Knowledge** tab to access the **Knowledge Portal**.

2. Enter the product name or KB Article number in **Search knowledge...** text field and click **Search** or press **Enter**.

The following list contains some of the more commonly accessed KB articles.

New Number	Topic
KB94845	Manager Attack log page doesn't show new alerts (Exclude manager Installation, MariaDB, and SolrDB folders from antimalware scanning)
KB94844	How to create a FIPS compatible cloud public key for SSH and SCP operations in a cloud environment
KB94843	Offline utility to download the latest Signature Sets
KB87848	How to reset the Active Fail-Open kit to Factory Default
KB86247	SNMP MIB files for Trellix IPS Active Fail-Open Kit
KB86228	How to enable Solr debugging for Trellix IPS Manager
KB86227	Solr Exception seen during Pruning or Purging the Trellix IPS Manager
KB86216	How to verify that alerts are sent to the Manager Solr database
KB86158	After upgrading, you see a blank dashboard and attack log (Importing data from MySQL into the Manager Solr database)
KB85202	IP addresses are reversed for Bot/Malware attacks
KB79462	How to troubleshoot and replace an NS-9x00 Sensor fan
KB79461	How to troubleshoot and replace the NS-9x00 Sensor PSU
KB77287	Collecting information to troubleshoot high use of CPU or memory
KB75269	FAQs for Trellix Intrusion Prevention System
KB73355	Alternative method to upgrade Trellix IPS Sensor Appliance software in a failover pair
KB71628	Trellix IPS DoS profile - learning and detection modes

New Number	Topic
KB71562	How to configure SNMP for the Trellix IPS Sensor
KB70861	How to troubleshoot Sensor latency issues
KB67501	Port indexes for Trellix IPS Sensors
KB60660	How to verify the Trellix IPS Manager database tables for corruption
KB59344	How to reset the Trellix IPS Manager password
KB59342	Ports and traffic destinations used by Trellix Intrusion Prevention System
KB56364	Third-party connectors for Trellix IPS Sensors
KB55743	How to submit Trellix IPS false-positives and incorrect detections to Technical Support
KB55549	How to collect a diagnostics trace from the Trellix IPS Sensor (Trace.log)
KB55450	How to request a User Defined Signature for a new threat, worm, virus, or vulnerability
KB55448	Trellix Intrusion Prevention System release information
KB55446	Trellix Intrusion Prevention System Signature Set Updates **NOTE** This is a restricted article and requires the user to log into Trellix Support Service Portal.
KB55447	Trellix Intrusion Prevention System User-Defined Signature Releases **NOTE** This is a restricted article and requires the user to log into Trellix Support Service Portal.
KB54928	How to check Trellix IPS Manager database tables from a command-line session