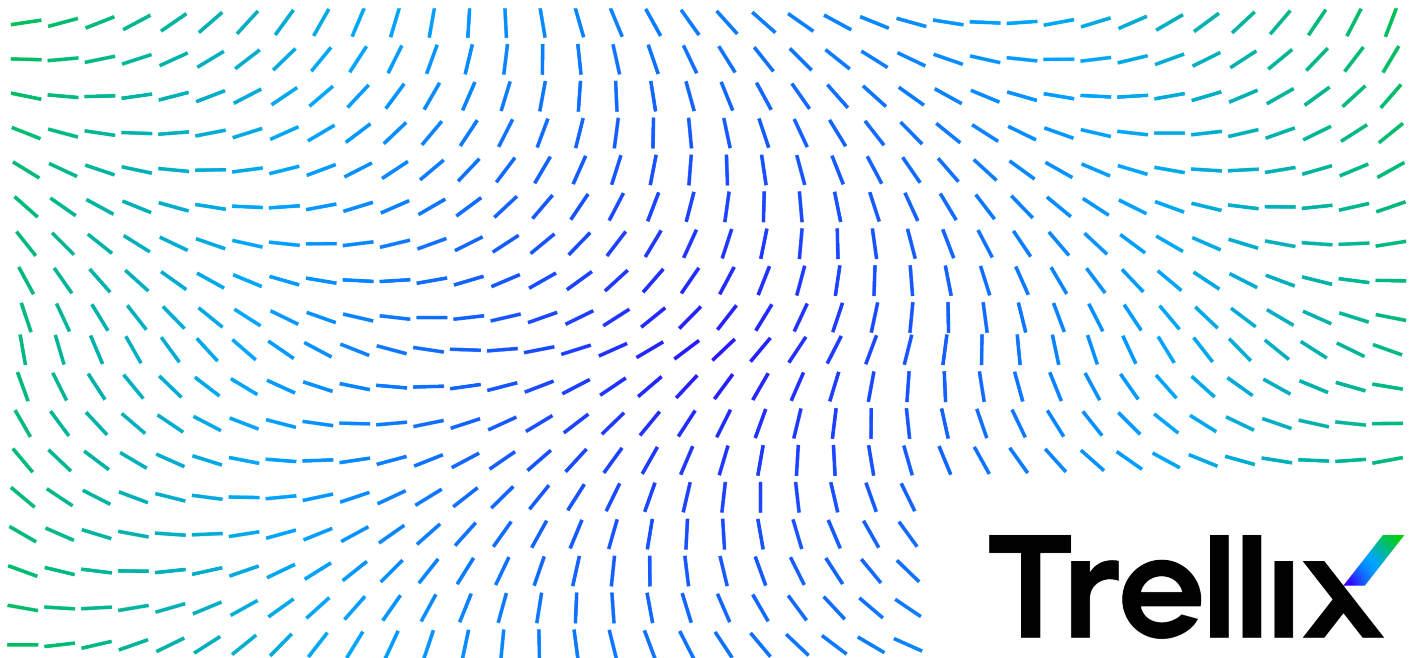


# Trellix Intrusion Prevention System

## 11.1 FIPS and CC Certification Guide



---

# Table of Contents

<b>An overview of Trellix Intrusion Prevention System</b> .....	<b>4</b>
Overview .....	4
Sensor features in FIPS compliant images .....	4
Key destruction (zeroization) mechanism details and exceptions .....	6
Protocol features in the certified evaluated configuration .....	6
Device bootup processing .....	7
Verification of authenticity of the software images .....	7
<b>Upgrade Paths</b> .....	<b>8</b>
Upgrade paths for Manager software versions .....	8
Upgrade paths for Sensor software versions .....	8
<b>Configuration of Trellix IPS for Certification</b> .....	<b>10</b>
Install the Manager .....	10
Install an IPS Sensor with a FIPS mode software image .....	10
<b>Sensor CLI for Certification</b> .....	<b>11</b>
SSH public key based authentication for Sensor .....	11
Sensor as the SSH server .....	11
Sensor as the SSH client .....	11
Sensor CLI commands related to Certification .....	12
auditlogupload .....	12
auditlog remove .....	13
deinstall .....	13
loadconfiguration .....	14
loadimage .....	15
resetconfig .....	15
sshlogupload .....	16
set auditlog .....	18
set fips sharedkey .....	18
set password age .....	19
set password length .....	19
set sensor sharedsecretkey .....	19
set sshlog .....	20
show .....	20
show fips mode status .....	22
show firmware version .....	22
show ssh config .....	23
status .....	23
traceupload .....	25

---

<b>Manager configuration for Certification</b> .....	<b>26</b>
SSH public key based authentication for Manager Appliance (Linux) .....	26
FIPS-related Manager user interfaces .....	26
TACACS+ authentication .....	26
Importing a Sensor's configuration .....	26
Sensor Failover .....	26
Sensor Report .....	26
Certificate Expiration Fault .....	26
View Details .....	27
Logon History .....	27
Shutdown on audit failure .....	27
<b>Handling user password between FIPS and non-FIPS Sensor images</b> .....	<b>28</b>
Upgrade or downgrade from non-FIPS to FIPS images .....	28
Upgrade or downgrade from FIPS images to non-FIPS .....	28
<b>Password requirements for Manager CLI and GUI</b> .....	<b>29</b>
<b>Trellix Threat Intelligence Exchange (TIE) broker configuration</b> .....	<b>30</b>
<b>Product Functionality not Included in the Scope of the Evaluation</b> .....	<b>32</b>
<b>Security Functions Provided by the TOE</b> .....	<b>33</b>
<b>Appendix: Trellix Intrusion Prevention System Documentation List</b> .....	<b>35</b>
<b>Appendix: Audit Log Records</b> .....	<b>37</b>
.....	37

# An overview of Trellix Intrusion Prevention System

Trellix Intrusion Prevention System combines Trellix Intrusion Prevention System Sensor and Trellix Intrusion Prevention System Manager for the accurate detection and prevention of attacks using signature detection, zero-day attacks using anomaly detection, denial of service (DoS) attacks, and distributed denial of service (DDoS) attacks.

Sensors can be deployed in a variety of topologies such as SPAN or Hub, Tap, In-line fail-closed, and In-line fail-open. Additionally, Sensors support features like interface groups or port clustering where multiple ports on a single Sensor can be grouped together for effective traffic monitoring, particularly useful for asymmetrically routed networks. Trellix IPS also provides high-availability; 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.

The following are the currently available NS-series Sensor models for IPS/IDS: NS9500(1.10), NS9500(1.00), NS9300(P & S), NS9200, NS9100, NS7600, NS7500, NS7350, NS7250, NS7150, NS5200, NS5100, NS3600, NS3200, and NS3100.

## Overview

The information in this document supplements that released in the Trellix Intrusion Prevention System 11.1 user documentation.

This document covers new features and enhancements that are supported in the following versions of Trellix IPS software:

- Manager software version: 11.1.19.x
- Signature set: 11.x.x.x
- NS-series Sensor software version: 11.1.17.x

The Manager in this release can be run using two modes:

- Non-FIPS mode: All Manager features up to 11.1 are supported in the non-FIPS mode.
- FIPS mode: All features supported in this mode are FIPS compliant:
- The Manager and Sensor versions support features that are mandatory requirements for FIPS and Common Criteria certification.
- The new features are certified for FIPS and Common Criteria for Manager Appliance Linux and NS-series Sensors.

### NOTE

Do not use the Manager to set the inactivity option under Account Lockout via GUI. This way of managing account lockouts has not been evaluated for use in the Common Criteria configuration.


## Sensor features in FIPS compliant images

The algorithms implemented in the Sensor image are FIPS 140-3 compliant. Make note of the following features when FIPS compliant images are enabled in the Sensor:

### NOTE


For a list of Sensor features that do not specifically relate to FIPS mode, refer to [Trellix Intrusion Prevention System 11.1.x Product Guide].

- The Sensor version supports features that are mandatory requirement for Common Criteria certification.
- This FIPS Sensor image permits loading only SHA-256 signed images. You must **netboot** the Sensor to load a non-FIPS image signed with a weaker algorithm.
- All critical security parameters (CSPs)/Sensitive security parameters (SSPs) are zeroized, in compliance with FIPS 140-3.
- The following channels operate with algorithms approved by FIPS 140-3:
  - Install channel (8501)
  - Alert channel (8502)
  - Packet Log channel (8503)
  - Authentication channel (8502)
  - Malware file upload channel (8510)

 **NOTE**


The SNMPv3 channel between the Manager and Sensor uses AES128 encryption, SHA authentication, and is RFC3414 and RFC3826 compliant. All CSP/SSP information on this channel is additionally encrypted by the Manager using the Sensor 2048-bit RSA public key and can be decrypted only by the Sensor private key.

- Common Criteria compliance requires the use of specific secure protocols. Hence, SNMPv3 is further encapsulated within TLS (TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384). The Sensor will use port 18500 as a TLS server for this service.

 **NOTE**

If the trust between the Manager and Sensor is established using a self-signed certificate, the Sensor will use port 8500 to service SNMPv3 as a TCP/UDP server. If the trust between the Manager and Sensor is established using a CA-signed certificate, the Sensor will use port 18500 to service SNMPv3 as a TLS server.

- The Sensor supports read-only access to third party SNMPv3 clients. Third party SNMPv3 clients can only be configured at the Manager. The Sensor retains the use of port 8500 for SNMPv3 service to these clients.
- The Sensor install, alert, packet log, authentication, and malware file upload channels use TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384.
- TACACS+ authentication configuration is disabled at the Sensor level.
- Stronger authentication for user login is enforced.
- The Manager version that supports FIPS can manage Sensors that are not FIPS compliant. In the Common Criteria (CC) evaluated configuration, all Sensors must be in FIPS mode.
- When a Sensor of a fail-over pair is running a FIPS image, it is mandatory for the peer Sensor to also be FIPS compliant.

 **NOTE**

Before you upgrade, convert the Sensors in the fail-over pair to standalone Sensors. If you do not do this, trust will not be re-established after the upgrade.

- The channels use RSA certificates based on 2048-bit RSA keys.
- Use SCP for file transfers. The use of TFTP is not permitted.

- Cryptographic support is provided by Trellix modified OpenSSL-FIPS-Object-Module v2.0 and OpenSSL 1.0.2zh-fips.
- Trellix modified OpenSSH v7.8p1 is configured to support only the following:

**SSH Client Configuration:**

- Ciphers: aes256-gcm@openssh.com and aes128-gcm@openssh.com
- MACs: Implicit
- KexAlgorithms: ecdh-sha2-nistp256
- HostKeyAlgorithms: ecdsa-sha2-nistp256

**SSH Server Configuration:**

- Ciphers: aes256-gcm@openssh.com and aes128-gcm@openssh.com
- MACs: Implicit
- KexAlgorithms: ecdh-sha2-nistp256
- HostKeyAlgorithms: ecdsa-sha2-nistp256

**User authentication:**

- Password, ssh-rsa, rsa-sha2-256, rsa-sha2-512 and ecdsa-sha2-nistp256
- SSH in 11.1 FIPS Sensor image is restricted to AES128 and AES256 GCM Mode cipher only. The use of AES CBC or CTR mode is not permitted.
- This requires that an external SSH client or server must support AES128 and AES256 GCM mode ciphers. Some popular clients (like PuTTY) may not support them currently. In such scenarios, you must migrate to an alternative SSH client or server approved by your local administrator.
- The external SSH client is used to log into a Sensor running 11.1 FIPS image.
- The external SSH server is used to host a remote Sensor image, that you can SCP into the Sensor running a 11.1 FIPS image using the **loadimage** CLI command.

## Key destruction (zeroization) mechanism details and exceptions

There are no exceptions to the Sensor and Manager. For more details, refer to the tables **Manager Key zeroisation** and **Sensor Key zeroisation** under the topic [Cryptographic Key Destruction] within the [Trellix IPS Sensor and Manager Appliances version 11.1 Security Target] document.


## Protocol features in the certified evaluated configuration

Usage of NTP is not permitted. The system time may be configured by authorized administrators via the "**timedatectl**" command of the Manager CLI.

The TLS functionality of the Trellix IPS components is pre-configured and fixed with the following behaviors:

- Only TLS v1.2 is supported
- The reference identifier is the IPv4 address or fully qualified domain name of the configured endpoint (matching the type used to configure the endpoint) and may be found in the SAN or CN fields of the presented certificate.
- The management GUI interface on the Manager supports the following cipher suite:
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- The management GUI interface on the Manager supports the secp256r1 Elliptic Curve Extension.
- Between Sensors and the Manager, the cipher suite used to perform mutual authentication are TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384. The systems must use CA-signed RSA certificates with key size 2048 bits.
- The syslog server interface on the Manager supports the following cipher suites:
  - TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5289
  - TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5289
- The syslog server interface on the Manager supports the secp256r1 and secp384r1 Elliptic Curve Extensions.
- The TOE uses HMAC-SHA-256 and HMAC-SHA-384 for TLS KDF and TLS message authentication.

 **NOTE**

The Target of Evaluation (TOE) supports session resumption using session ID, which does not require any separate configuration.

## Device bootup processing

- The FIPS Sensor boot-up executes all the FIPS compliant algorithms, as part of the pre-operational self-tests, firmware integrity tests, and known answer tests (KAT).
- If a self-test fails, the Sensor enters into error state and reboots continuously. User needs to netboot the Sensor with a valid firmware to come out of the error state. A user can refer to the console log to view which self-test has failed.
- Similarly, Manager executes power-up self tests and software integrity tests. Failure of self-tests will cause the module to transition to an error state. Logical components will shut-down and no data output will be provided during error states. User needs to install a valid software image to come out of the error state. Users can refer to the console log to view which self-test has failed. Additionally, users can refer to ems.log for more details.
- The Random Number Generation (RNG) functionality does not require any manual configuration and is initialized on startup.

## Verification of authenticity of the software images

### IPS Sensor and Manager:

The modules perform firmware integrity check using RSA 2048 with SHA2-256. If the integrity check fails, the new image is not accepted and an error message is thrown to the user. Users are expected to re-attempt with a valid image.

## Upgrade Paths

This section mentions the various upgrade paths available to the latest FIPS and CC Intrusion Prevention System. It takes into consideration several scenarios to migrate to a FIPS and CC supported version of Trellix IPS 11.1. For a list of upgrade paths not related to FIPS and CC refer to the [Trellix Intrusion Prevention System 11.1.x Installation Guide].

### Upgrade paths for Manager software versions

This section shows you different scenarios of deployment from which you can upgrade/migrate to the latest version of the Manager.

#### NOTE

You can log in to the [Trellix Download Server](#) using your Grant ID to verify the file hash for the software build.

#### NOTE

When you migrate the Manager to a FIPS image, the installation validates certain files to make sure they have not been tampered with. For example, if you change tms.bat, you can regenerate the FIPS hash by running initdb.bat update.

#### NOTE

Windows based Manager is not supported for FIPS and CC.

Linux based Manager:

**Table 1. Linux based Manager upgrade paths**

Manager version	Recommended Manager version
10.1.19.17, 10.1.19.30, 10.1.19.33, 10.1.19.38, 10.1.19.47, 10.1.19.53	11.1.19.x

### Upgrade paths for Sensor software versions

This section shows you different scenarios of deployment from which you can upgrade to the latest version of the Sensors.

**Table 2. Sensor upgrade paths**

Sensor model	Current Sensor software (FIPS and CC)	Upgrade path to latest FIPS and CC compliant Sensor software
NS3100, NS3200, NS3500, NS5100, NS5200, NS7100, NS7200, NS7300, NS9100, NS9200, NS9300,	10.1.17.15, 10.1.17.26, 10.1.17.36, 10.1.17.47, 10.1.17.63, 10.1.17.75	11.1.17.x




Sensor model	Current Sensor software (FIPS and CC)	Upgrade path to latest FIPS and CC compliant Sensor software
NS7150, NS7250, NS7350, N9500	10.1.17.15, 10.1.17.26, 10.1.17.36, 10.1.17.50, 10.1.17.63, 10.1.17.75	11.1.17.x
NS7500	10.1.17.15, 10.1.17.36, 10.1.17.47, 10.1.17.63, 10.1.17.75	11.1.17.x

The following applies for FIPS software running on NS-series Sensors:

- The user must synchronize a symmetric key, specified from the CLI using the `set fips sharedkey` command, on both the Primary and Secondary Sensors of an NS9300. The Sensor bootloaders are automatically upgraded to allow verification of subsequent image downloads signed with SHA256.

# Configuration of Trellix IPS for Certification

 **NOTE**

This section is not applicable for Common Criteria evaluated configuration.


This section provides guidelines to set up the product in a manner that meets certification configuration requirements. The guidelines and requirements listed below are in addition to the instructions written in the generic documentation of Trellix IPS. For a complete list of documentation, refer to the appendix.

Note the following:


- If a feature or service is listed below, you must configure the mentioned item as described in this section.
- If a feature or service is not listed below, configure it as written in the reference documentation.

## Install the Manager

Follow the directions in the [Manager Appliance (Linux) Installation] section within [Trellix Intrusion Prevention System Manager Appliance Product Guide]. When installing the virtual Manager, follow the directions in the [Trellix Intrusion Prevention System Installation Guide].

 **NOTE**


Trellix recommends you to change the Manager shell password immediately. The new password must be compliant with the site's password requirements.

 **NOTE**

For Manager shell, the default user name is **admin** and password is **ML0SnsmApp**.

## Install an IPS Sensor with a FIPS mode software image

When installing a Sensor with a FIPS mode image, perform the initial Sensor setup using the serial console interface but do not enter the shared secret key to avoid a FIPS mode violation. Connect and log onto the Sensor using an SSH client, such as Tera Term, and enter the shared secret key. Wait for the Sensor initialization to complete and the trust to be established with the Manager.

 **CAUTION**

Using the serial console interface for configuring shared secret key will cause a FIPS mode violation.

# Sensor CLI for Certification

## SSH public key based authentication for Sensor

You can use SSH public key authentication or password based authentication to login to the Sensor/remote machine using SSH. Use of public key authentication allows administrators and users to access the Sensor or the remote machine without the use of password based authentication.

### Sensor as the SSH server

You can access the Sensor remotely using SSH from a remote machine. The SSH public key from the remote machine has to be configured in the Sensor. Since the Sensor does not permit any key to be exported by the remote client, you must import the key explicitly for every user.

The steps to access Sensor through SSH from a remote machine is as follows:

1. Generate the key pair (SSH public and private keys) for a user accessing the Sensor through a remote machine.
2. Add the user to the Sensor using **adduser** CLI command.
3. Set SCP server IP address from where the SSH public key is to be imported to the Sensor to login.
4. Import your SSH public key to the Sensor using the **importsshpublickey** CLI command.
5. Sensor updates the SSH local repository with the SSH public key.
6. When you login to the Sensor using the SSH key, the Sensor authenticates the user with the SSH public key stored in the local repository.

#### NOTE

The sensor accepts both RSA and ECDSA public keys for user authentication. DSA is not supported.

### Sensor as the SSH client


You can SCP files to a remote machine serving as a SCP server from the Sensor. This requires the Sensor SSH public key to be configured on the remote SCP server for the user. The Sensor exports this key to the remote SCP server if permitted to do so.

The steps to configure Sensor's ssh public key on remote machine are as follows:

1. The Sensor generates a public-private key (ECDSA) pair using the SSH utility "ssh-keygen".
2. The Sensor retains the private-key and exports the SSH public key to the remote machine using **exportsshpublickey** CLI command.

#### NOTE

The **exportsshpublickey** CLI command exports the Sensor's SSH public key to the configured SCP server.

 **NOTE**

The `exportsshpublickey` CLI command exports the Sensor's SSH public key to the remote machine only by password based authentication.

There are two outcomes while executing `exportsshpublickey` CLI command:

- When the public key of the Sensor is directly configured on the remote machine:

```
intruShell@ips-ns9500#> exportsshpublickey <path>
```

```
Please enter the SCP User Name : emb-demo
```

```
Please enter the SCP User Password :
```

```
Public Key configured on the remote machine
```

In this scenario, the Sensor successfully configures the SSH public key on the remote machine.

- When the public key is not configured but just copied on the remote machine:

```
intruShell@ips-ns9500#> exportsshpublickey <path>
```

```
Please enter the SCP User Name : emb-demo
```

```
Please enter the SCP User Password :
```

```
Transfer Successful through scp, User need to configure the public key manually on the remote machine.
```

In this scenario, the Sensor fails to configure the SSH public key on the remote machine, but a copy of it is saved in the file path provided (`<path>`) in the remote machine. You need to manually configure the SSH public key on the remote machine's `authorized_keys` file.

 **NOTE**

If the SSH public key authentication fails, the Sensor will use password based authentication method.

 **WARNING**

The SSH public key authentication could fail due to incorrect permission of authorized keys; change the mode of `authorized_keys` file to 600 and try again.

## Sensor CLI commands related to Certification

The following CLI commands support the mandated requirements for FIPS and Common Criteria and can be used on a FIPS and Common Criteria compliant Sensor. However, for a list of commands that can be used in other modes of operation and their availability for different roles, refer to the [Trellix Intrusion Prevention System 11.1.x Product Guide].

### auditlogupload

This command uploads the audit log file to the configured SCP server.

#### Syntax:

```
auditlogupload scp WORD
```

where **WORD** stands for the name of the audit file on the server as per the CLI command.

Note the following:

- For NS-series Sensors, when loading the audit log file to the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor will use password based authentication.

#### NOTE

For NS-series Sensors, even if the public key authentication is not configured on the Sensor, the first login attempt will be using the public key. If the SSH public key is not present, a warning message will be displayed and the Sensor will then use password based authentication.

- When loading an audit log file on the SCP server, you are prompted for the SCP server credentials. The command succeeds only on providing the correct SCP server credentials.

#### NOTE

If the Sensor's SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

- When loading an audit log file on the SCP server, the pathname of the file should be absolute.

## auditlog remove

It removes auditlog file on the Sensor.

### Syntax

```
auditlog remove
```

## deinstall

This command clears the Manager-Sensor trust data (the certificates 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 if the Sensor has CA-signed certificate:

```
Do you want to retain the current CA signed certificate chain ?
```

```
Enter Y/y(for yes) or N/n(for no): Y
```


 **NOTE**

If you enter **Y**, the CA-signed certificate chain for the Sensor is retained. If you enter **N**, both the current Sensor CA-signed certificate and self-signed certificate will be removed along with the trust.

Pressing **Y** displays the following message:

```
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. If you enter **N**, the Manager-Sensor trust remains intact and you exit the deinstall prompt.


```
deinstall in progress ...
```

```
this will take a couple of seconds, please check status on CLI
```

On executing the command, the following messages are displayed if the Sensor has self-signed certificate:

```
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. If you enter **N**, the Manager-Sensor trust remains intact and you exit the deinstall prompt.

Entering **Y** displays the following message:

```
deinstall in progress ...
```

```
this will take a couple of seconds, please check status on CLI
```

## loadconfiguration

This command loads the Sensor configuration from the configured SCP server. The SCP server IP is specified in the Sensor. When the Sensor is added to the Manager, the configuration type should be specified as offline.


### Syntax:

```
loadconfiguration scp WORD
```

where **WORD** stands for the name of the configuration file on the SCP server.

Note the following:

- For NS-series Sensors, when loading Sensor configuration from the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor uses password authentication.
- 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.

 **NOTE**

If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

- When loading Sensor configuration from the SCP server, the pathname of the file should be absolute.

## loadimage

Upon execution, this command loads a Sensor image file from the configured SCP server.


### Syntax:

**loadimage scp WORD**

where **WORD** stands for the name of the image file on the SCP server.

Note the following:

- For NS-series Sensors, when loading a Sensor image file from the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor uses password authentication.
- 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.

 **NOTE**

If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

- When loading a Sensor image file from the SCP server, the pathname of the file should be absolute.

## resetconfig

This command resets all configuration values to their default values. It deletes or resets values as described below. This command causes an automatic reboot of the Sensor.

Deleted Values	Values Reset to Defaults
<ul style="list-style-type: none"> <li>• Manager IP addresses (and secondary interface's IP address, if configured). This can be IPv4 or IPv6 address.</li> </ul>	<ul style="list-style-type: none"> <li>• Monitoring and Response port settings</li> </ul>
<ul style="list-style-type: none"> <li>• Certificates establishing trust between Sensor and Manager</li> </ul>	<ul style="list-style-type: none"> <li>• Management port settings</li> </ul>
<ul style="list-style-type: none"> <li>• Shared secret key</li> </ul>	<ul style="list-style-type: none"> <li>• Manager Install port value</li> </ul>
<ul style="list-style-type: none"> <li>• Signatures</li> </ul>	<ul style="list-style-type: none"> <li>• Manager Alert port value</li> </ul>
<ul style="list-style-type: none"> <li>• TFTP server IP address (IPv4 or IPv6 address)</li> </ul>	<ul style="list-style-type: none"> <li>• Manager Log port value</li> </ul>

• SCP server IP address (IPv4 or IPv6 address)
• DoS profile files (learned DoS behavior)
• SSL Keys
• Exception Object
• ACL
• Advanced Setting
• SSH Host Public/Private Key (Client/Server)
• SSH Session Key
• Administrator Passwords
• Sensor User Passwords (Users created by admin using "adduser" CLI)
• 3rd Party SNMP Client Privacy and Authentication Keys
• Manager SNMP Client Privacy and Authentication Keys

On executing the command, the following messages are displayed:

```
Reset other configurations and reboot? Please enter Y to confirm: Y
```

#### NOTE

If you enter **Y**, the Manager-Sensor trust is removed. If you enter **N**, the Manager-Sensor trust remains intact and you come out of the deinstall prompt.

Pressing **Y** displays the following message:

```
resetting the configuration and rebooting the sensor
```

On executing the command, the following messages are displayed if the CA signed certificate is present:

```
CA cert detected, will be deleted on resetconfig
```

```
reset the configuration and reboot the sensor? Please enter Y to confirm: Y
```

Entering **Y** displays the following message:

```
resetting the configuration and rebooting the sensor
```

#### Syntax:

```
resetconfig
```

## sshlogupload

Use this command to upload the SSH log file to the SCP Server.

Ensure the following before using this command:

- The SCP server IP address must be set using the command `set scpserver ip <server_ip>`.



The file uploaded on the SCP server is the TAR file containing one or more zipped 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.
- For NS-series Sensors, when loading the SSH log file to the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor will fall back to the password authentication. If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

## Syntax

`sshlogupload scp word`

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
```

### NOTE

SSH log only contains entries for SSH accept or SSH drop from a particular client IP address.

Log Message Fields	Description
SSHD_DROP	The Log prefix. It can be SSHD_DROP or SSHD_ACCEPT.
IN=eth0	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: <ul style="list-style-type: none"> <li>• <b>Dest MAC= 00:06:92:25:9d:80</b> - The destination MAC address</li> <li>• <b>Src MAC=00:0b:bf:a1:b7:fc</b> - The source MAC address</li> <li>• <b>Type=08:00</b> - Ethernet frame carrying an IPv4 datagram</li> </ul>
SRC=172.16.232.47	Source IP address
DST=172.16.199.89	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.

Log Message Fields	Description
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 which is only exchanged at TCP connection establishment
URGP=0	The urgent flag

## set auditlog

This command helps in configuring the Sensor to begin or stop archival of audit logs.

### Syntax:

```
set auditlog <enable | disable>
```

where <enable> allows the audit log feature to record system events and <disable> stops the audit log feature from recording system events

### Default Value:

enable

### Example:

```
set auditlog enable
```

## set fips sharedkey

This command is used to authenticate the Primary and the Secondary Sensors in FIPS mode. The Primary and the Secondary Sensors exchange the shared key (user configured keys) for authentication. Any difference in key specifications will result in authentication failure.

The shared key can be created only in FIPS mode.

### Syntax:

```
set fips sharedkey
```

The shared key must be entered once from the Primary Sensor and once from the Secondary Sensor.

### Applicable to:

NS9300 Sensors

## set password age

This command allows you to set a limit on password validity period.

### Syntax

```
set password age <days>
```

Where days can be between 10-99 days.

## set password length

This command allows you to set the length of the password.

### Syntax

```
set password length <number of characters>
```

Where number of characters can be between 15-255.

## set sensor sharedsecretkey

Use this command to set the shared secret key value that the Manager and Sensor use to establish trust.

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 enter in the CLI to identify the Sensor must match the shared secret key entered in the Manager GUI. If the shared secret keys between the Manager GUI and Sensor CLI do not match, the Manager and Sensor cannot communicate. If you want to change the shared secret key, you must change the value in the CLI as well as the Manager GUI.

### 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. The shared secret key value is case-sensitive (for example, IPSkey123.)

### 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 deinstalled -
  - ```
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

#### NOTE

If the Sensor and Manager already have a CA-signed certificate chain, the Sensor will try to establish trust with the Manager using the CA-signed certificate chain. If the CA-signed certificate does not exist in the Manager, the Sensor uses the self-signed certificate chain.

## set sshlog

Use this command to enable or disable SSH logging (archiving SSH activity into log files).

### Syntax

```
set sshlog <enable/disable>
```

It is disabled by default.

## show

Upon execution, this command displays all the current configuration settings on the Sensor, such as the 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]

- System Name
- Date
- System Uptime
- System Type
- System serial number (displays the primary, secondary and master/system serial numbers separately in case of NS9300)
- Software Version
- Hardware Version
- MGMT Ethernet Port
- MGMT port Link Status

[Sensor Network Config]

- IP Address
- Netmask

- Default Gateway
- SSH Remote Logins

[Manager Config]

Self Signed cert support

- Install TCP Port
- Alert TCP Port
- Logging TCP Port

CA Signed cert support

- Install TCP Port
- Alert TCP Port
- Logging TCP Port
- FIPS Mode
- Admin SSH/Console Access

### Sample Output:

For Sensor, the output is as shown:

```
intruShell@NS3200_FIPS> show
```

```
[Sensor Info] System Name : NS3200_FIPS
```

```
Date : 1/15/2024 - 16:1:3 UTC
```

```
System Uptime : 41 days 21 hrs 34 min 46 secs
```

```
System Type : IPS-NS3200
```

```
System Mode : Standalone
```

```
Serial Number : 0123456789
```

```
Software Version : 11.1.17.x
```

```
Hardware Version : 1.10
```

```
MGMT Ethernet port : auto negotiated
```

```
MGMT port Link Status : link up
```

```
[Sensor Network Config]
```

```
IP Address : 10.x.x.x
```

```
Netmask : 255.255.255.0
```

```
Default Gateway : 10.x.x.x
```

Default SCPserver : 10.x.x.x

SSH Remote Logins : enabled

[Manager Config]

Manager IP addr : 10.x.x.x (primary intf)

Install TCP Port : 8501

Alert TCP Port : 8502

Logging TCP Port : 8503

FIPS Mode : Enabled

Admin SSH/Console Access: Enabled

## show fips mode status

This command displays the status of the FIPS mode.

### Syntax

```
show fips mode status
```

This command displays the following information:

- FIPS mode status - Displays the status as enabled
- The admin SSH/console access status

## show firmware version

This command shows the current bootloader version information running on the Sensor.

### Syntax

```
show firmware version
```

### Sample Output

For Sensor, the output is as shown:

```
IntruDbg#> show firmware version
```

```
Bootloader Version: GRUB 2.01 - Production
```

```
Group 0: 0x32 - 2-SFP+ On-board Controller ; FPGA version 01; Working image
```

```
Group 1: Module not installed
```

```
Group 2: Module not installed
```

```
Group 3: 0x32 - 8-1GBE On-board Controller ; FPGA version 01; Working image
```

CPLD Device ID: 0x31; Version: 0x01; Revision: 0x01

#### NOTE

You can append the `a11` parameter in the command to fetch additional details such as the BIOS version, BMC version, IPMI version, and Linux version.

## show ssh config

This command displays the SSH version, client configuration, and sever configuration information.

#### Syntax:

```
show ssh config
```

#### Sample output:

```
intruShell@NS7500_FIPS> show ssh config

SSH Version: OpenSSH_7.8p1, OpenSSL 1.0.2zh-fips 30 May 2023

SSH Client Configuration :

Ciphers : aes256-gcm@openssh.com,aes128-gcm@openssh.com

MACs : hmac-sha2-256,hmac-sha2-512

KexAlgorithms : ecdh-sha2-nistp256

SSH Server Configuration :

Ciphers : aes256-gcm@openssh.com,aes128-gcm@openssh.com

MACs : hmac-sha2-256,hmac-sha2-512

KexAlgorithms : ecdh-sha2-nistp256

PublicKeyAuthentication : Enabled

PasswordAuthentication : Enabled
```

## status

The `status` command shows 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:

```
intruShell@NS3200_FIPS> status
```

```
[Sensor]
```

```
System Initialized : yes
```

```
System Health Status : good
```

```
Layer 2 Status : normal (IDS/IPS)
```

```
Installation Status : complete
```

```
IPv6 Status : Dont Parse and Allow Inline
```

```
Reboot Status : Not Required
```

```
Guest Portal Status : up
```

```
Hitless Reboot : Available
```

```
Last Reboot reason : unknown
```

```
[Signature Status]
```

```
Present : yes
```

```
Version : 11.10.10.5
```

```
Power up signature : good
```

```
Geo Location database : Present
```

```
DAT file : Present
```

```
DAT file Version : 3756.0
```

```
[Manager Communications]
```

```
Trust Established : yes (Self Signed cert support)
```

```
Alert Channel : up
```

```
Log Channel : up
```

```
Authentication Channel : up
```

```
Last Error : None
```

```
Alerts Sent : 14
```

```
Logs Sent : 42
```

```
[Alerts Detected]
```



```
Signature : 0
Alerts Suppressed : 0
Scan : 0
Denial of Service : 0
Malware : 14
```

```
[TIS Communication]
```

```
Status : down
```

```
IP : 0.0.0.0
```

```
Port(Secure) : 8505
```

```
FIPS Mode : Enabled
```

```
Admin SSH/Console Access: Enabled
```

#### NOTE

If there is a failure in establishing trust relationship 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.

## traceupload

This command uploads an encoded diagnostic trace file to the configured SCP server from which you can send it to Trellix Technical Support for diagnosing a problem with the Sensor. A trace upload facility is also available on the Manager GUI.

### Syntax:

```
traceupload scp WORD
```

where **WORD** stands for the file name to which the trace must be written.

For NS-series Sensors, when loading an encoded diagnostic trace file to the SCP server, the first attempt will be based on SSH public key authentication. If that fails, the Sensor will use password authentication. If SSH public key authentication is successful, you will not be prompted for the SCP server credentials.

#### NOTE

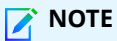
As part of traceupload, additional information is collected using logstat. Due to this, additional time is required to collect logs from the Sensor, and can take around 10-30 minutes based on the Sensor model.

# Manager configuration for Certification

For information about all other Manager user interfaces, refer to the [Trellix Intrusion Prevention System 11.1.x Product Guide].

## SSH public key based authentication for Manager Appliance (Linux)

For information about SSH public key based authentication, refer to the [Trellix Intrusion Prevention System Manager Appliance Product Guide].



### NOTE

Manager supports both RSA and ECDSA based public key authentication.

## FIPS-related Manager user interfaces

### TACACS+ authentication

Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Setup → Remote Access → **TACACS+**.

When FIPS mode is enabled in the Sensor, configuration for TACACS+ authentication is disabled.

### Importing a Sensor's configuration

Go to Devices → <Admin Domain Name> → Devices → <Device Name> → Maintenance → Import Configuration.

While importing a Sensor configuration file from a non-FIPS-enabled Sensor to a FIPS-enabled Sensor, the configurations that are not supported in the FIPS mode are ignored.

### Sensor Failover

Go to Devices → <Admin Domain Name> → Global → **Failover Pairs**.

When one of the Sensors in a failover pair is FIPS-enabled, it is required that the peer Sensor is also FIPS-enabled.

### Sensor Report

Go to Manager → <Admin Domain Name> → Reporting → Configuration Reports → **IPS Sensor**.

The Sensor report displays the **FIPS Mode** field with the status of the configuration. The Sensor Information table displays whether the FIPS mode is enabled, disabled, or not supported in the Sensor.

### Certificate Expiration Fault

To view the fault information, select Manager → <Admin Domain Name> → Troubleshooting → Logs → **Faults**.

The Manager raises a fault if a certificate has either expired or is approaching expiration. This check is done as part of scheduled file pruning and will not be done during Manager start-up.

## View Details

You should update the **ems.properties** file for various settings explained in the sections below. This file is available at `/opt/IPSEManager/App/config/`.

Go to Devices → <Admin Domain Name> → Devices → <Device Name> → **Summary**.

The details includes a field called **FIPS Mode** that displays FIPS compliance information for an installed Sensor. The **FIPS Mode** field displays whether FIPS is enabled, disabled or not supported in the Sensor.

## Logon History

This feature is enabled by setting this property in **ems.properties** file:

```
iv.access.control.authentication.loginHistoryTimePeriodLastNumberOfDays=30
```

To view **Recent Logon History** window, click **Login History** link in the header bar located on top of the menu bar.

The **Recent Logon History** window displays failed and successful logon attempts for a number of days set in **ems.properties**.

The period of time is set by assigning a value to the `loginHistoryTimePeriodLastNumberOfDays` property in the **ems.properties** file. If this property is not defined or set to -1 in the **ems.properties** file, then the **Recent Logon History** page will display failed logon attempts.

**Figure 1. Logon history**

| Recent Logon History - Administrator             |                                          |
|--------------------------------------------------|------------------------------------------|
| Previous Session:                                | 2020-Feb-20 18:57:13 IST(10.208.224.109) |
| Failed Logon Attempts Since Previous Session (2) |                                          |
| Time                                             | Location                                 |
| 2020-Feb-20 19:20:13 IST                         | 10.208.224.109                           |
| 2020-Feb-20 19:20:22 IST                         | 10.208.224.109                           |
| Close                                            |                                          |

## Shutdown on audit failure

This feature is enabled by setting this property in **ems.properties** file:

```
iv.core.audit.ShutDownOnAuditFailureEnabled=true
```

The Manager must invoke a system shutdown in the event of an audit failure. If the audit system detects an exception while attempting to audit to database or audit to file, it shuts down the Manager. Note since audit failure forcibly shuts down the Manager, it requires the Manager to be manually restarted. Server logs contain the root cause of audit failure. Also, system fault is listed after the Manager is successfully restarted.

# Handling user password between FIPS and non-FIPS Sensor images

The MD5/SHA1 algorithm standards are used by non-FIPS sensor images to verify a user password. FIPS capable Sensor images use the SHA-512 algorithm standard to verify the user password.

FIPS images require passwords to satisfy the following criterion:

- Password length should be of minimum 15 characters.
- Password should at the least contain 2 lower case, 2 upper case letters, 2 numeric, and 2 of the following special characters: !@#%&^\*()
- New password must differ from the previous password by at least 4 characters.
- Password must not be reused from the last 10 passwords.
- Password expire in 45 days.

There can be issues during upgrade or downgrade between FIPS and non-FIPS Sensor images as mentioned below:

- **The default admin password has not changed:** If there is no change in the default password, no conflict arises during upgrade/downgrade.
- **The default admin password has changed with FIPS capable image:** If there is a change in the FIPS capable image, the password is reset to default. The initial bootup script of the FIPS capable image detects the password format to be of MD5 format and deletes it. The password is then reset to default SHA-512 supported format.
- **The default admin password has changed with non-FIPS capable image:** Any change to a non-FIPS capable image will result in the password being reset to default. This process of resetting the password is done when the image is downloaded. The newly downloaded image version is compared to a tag, and if the newly downloaded image is non-FIPS capable, the password is deleted. The password is then reset to default MD5 supported format.

## Upgrade or downgrade from non-FIPS to FIPS images

On a transition from non-FIPS to FIPS image, you can only login with default admin password. Since this default admin password is not FIPS compliant, you will be prompted to change the default admin password.

### NOTE

If you had previously changed your password in a non-FIPS image, logging into the FIPS Sensor requires the default admin password for a FIPS images. The automatic configuration reset enforces the FIPS default password. The Manager notifies about this reset.

## Upgrade or downgrade from FIPS images to non-FIPS

A transition from FIPS to non-FIPS will result in password being reset to default. You can only login using the default passwords for admin of the non FIPS image.

## Password requirements for Manager CLI and GUI

The Linux based Manager CLI requires passwords to satisfy the following criterion:

- Password length should be of minimum 15 characters.
- Password should at the least contain 1 lowercase, 1 upper case letter, 1 numeric, and 1 of the following special characters: !@#\$%^&\*()
- Must differ from the previous password by at least 4 characters.
- Must not be reused from the last 5 passwords.
- Must not contain same type of character more than four times consecutively.
- Must not be a palindrome.
- Must not contain the username.
- Must not be similar to the previous password.
- Password expires in 60 days.

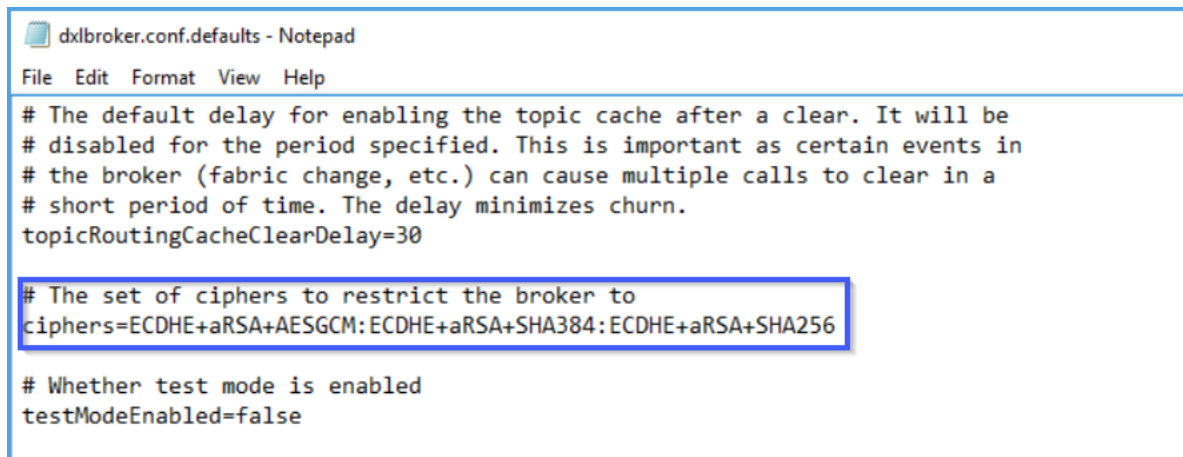
For Manager GUI password requirements, refer to the section [Add users] in [Trellix Intrusion Prevention System 11.1.x Product Guide].

# Trellix Threat Intelligence Exchange (TIE) broker configuration

By default, Threat Intelligence Exchange/Trellix Agent with integrated Trellix Data Exchange Layer broker uses RSA based ciphers. Follow these steps to switch from weak cipher (RSA) to strong cipher (ECDHE):

## Windows based setup

1. Navigate to `<Install_Dir>\McAfee\dxlbroker` and open **dxlbroker.conf.defaults** in a text editor.
2. Scroll down to the section where you can edit the ciphers that the broker can be restricted to. Ensure that the broker is restricted only to the cipher - **ECDHE+aRSA+AESGCM:ECDHE+aRSA+SHA384:ECDHE+aRSA+SHA256**. A sample screenshot is shown below:



```

dxlbroker.conf.defaults - Notepad
File Edit Format View Help
# The default delay for enabling the topic cache after a clear. It will be
# disabled for the period specified. This is important as certain events in
# the broker (fabric change, etc.) can cause multiple calls to clear in a
# short period of time. The delay minimizes churn.
topicRoutingCacheClearDelay=30

# The set of ciphers to restrict the broker to
ciphers=ECDHE+aRSA+AESGCM:ECDHE+aRSA+SHA384:ECDHE+aRSA+SHA256

# Whether test mode is enabled
testModeEnabled=false

```

3. Save the text file and close it.
4. Restart the TIE server and the ePO service to effectively use this cipher.

## Linux based setup

1. Open **dxlbroker.conf.defaults** file located in `/opt/Mcafee/dxlbroker/conf` using a text editor.

### NOTE

You need to open the file as a root user to be able to edit the file and save changes.

2. Scroll down to the section where you can edit the ciphers that the broker can be restricted to. Ensure that the broker is restricted only to the cipher - **ECDHE+aRSA+AESGCM:ECDHE+aRSA+SHA384:ECDHE+aRSA+SHA256**. A sample screenshot is shown below:

```
- Bitwise xterm - @tieserver:/opt/McAfee/dxlbroker/conf
# The default delay for enabling the topic cache after a clear. It will be
# disabled for the period specified. This is important as certain events in
# the broker (fabric change, etc.) can cause multiple calls to clear in a
# short period of time. The delay minimizes churn.
topicRoutingCacheClearDelay=30

# The set of ciphers to restrict the broker to
ciphers=ECDHE+aRSA+AESGCM:ECDHE+aRSA+SHA384:ECDHE+aRSA+SHA256

# Whether test mode is enabled
testModeEnabled=false

# Whether to validate certificates against the connection identifier
certIdentityValidationEnabled=false

# Whether to restrict the fabric to a single instance of each
# unique client identifier
uniqueClientIdPerFabricEnabled=false

# Whether to utilize managed certificates when in unmanaged mode. This value
# will always be true when ePO managed.
managedCerts=false

#####
# Settings that are only applicable when the broker is managed by ePO/MA
#####

# Whether the broker is managed by ePO/MA
epoManaged=true
-- INSERT --
```

3. Save the changes.
4. Restart the TIE server and the ePO service to effectively use this cipher.

## Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:

- Trellix Intrusion Prevention System can be configured to maintain accurate time via NTP. NTP must be disabled in the evaluated configuration.
- The Manager can manage Sensors that are not FIPS compliant. All Sensors must be in FIPS mode in the evaluated configuration.
- The Manager can manage Sensors that are using self-signed X.509 certificates. In the evaluated configurations, all Sensors must use CA-signed certificates.
- Trellix IPS can be configured to authenticate users via an LDAP server (rather than relying solely on internal user accounts). This optional functionality was not evaluated.



# Security Functions Provided by the TOE

- **Security Audit:**

The TOE generates audit records related to TOE operation and administration. These audit records are stored on the IPS Manager (and stored in a local database) and are also forwarded to an external audit server. The database stores 50,000 audit records. When the database reaches capacity, the oldest audit records are overwritten.

The Sensor generates audit records and forwards the audit records to the IPS Manager, the Sensor caches audit records in a local file. The audit file can be uploaded to Manager (or any other SCP server using the `auditlogupload` CLI command). If the file reaches capacity, new events are dropped.

Only authenticated users can view audit records.

- **Cryptographic Support:**

The TOE uses symmetric key cryptography to secure communication between the Sensors and the Manager for the following functionality:

- Exchange of configuration information (including IPS policies)
- Time/date synchronization from the Manager to Sensors
- Transfer of IPS data to the Manager
- Transfer of audit records to the Manager
- Distribution of TOE updates to Sensors

Connections between the Manager and Sensors are secured using TLS.

Connections between the Manager and the Audit Server (for audit record upload) are secured using TLS.

Connections between the Manager and the SCP Server is secured using SSH.

Sessions between the Management Workstation and the TOE are secured using SSH or HTTPS and authenticated using username and password. Local console connections between the Console Workstation and the TOE are physically secured. The Sensors also use SSH to securely copy a new image to update the Sensor.

- **Identification and Authentication:**

Administrators connecting to the TOE are required to enter an IPS administrator username and password to authenticate the administrative connection prior to access being granted.

The Manager and Sensors authenticate to one another through a shared secret that is configured during the initial installation and setup process of the TOE. Although in the evaluated configuration, the Manager supports use of a default self-signed certificate for trust establishment with the sensor, such a channel is out of scope for this evaluation. The sensor-Manager channel must be established using CA-signed certificates.

- **Security Management:**

An administrative CLI can be accessed via the Console port or SSH connection, and an administrative GUI can be accessed via HTTPS. These interfaces are used for administration of the TOE, including audit log configuration, upgrade of firmware and signatures, administration of users, configuration of SSH and TLS connections.

Only administrators authenticated to the **admin** role are considered to be authorized administrators.

- **Protection of the TSF:**

The presence of the Sensors' components on the network is transparent (other than network packets sent as reactions to be configured IPS conditions). The Sensors are protected from the monitored networks as the system is configured to not accept any management requests or input via the monitored interfaces.

The TOE users must authenticate to the TOE before any administrative operations can be performed on the system.

The TOE ensures consistent timestamps are used by synchronizing time information on the Sensors with the Manager, so that all parts of the IPS system share the same relative time information.

Synchronization occurs over a secure communications channel. Time on the Manager may be configured by an administrator.

The administrator can query the currently installed versions of software on the Sensor using the `show` command, which returns details about the software and hardware version. A trusted update of the TOE software can be performed from the Manager UI, which is then pushed out to the Sensors.

A suite of self-tests is performed by the TOE at power on, and conditional self-tests are performed continuously.

- **TOE Access:**

The TOE monitors local and remote administrative sessions for inactivity and terminates the session when a threshold time is reached. An advisory notice is displayed at the start of each session.

Trusted Path/Channels:

The TSF provides the following trusted communication channels:

- TLS for an audit server
- TLS for communication between Manager and Sensors
- SSH for communication with an SCP Server for updates

The TOE implements TLS/HTTPS and SSH for protection of communications between itself and the administrators.

# Appendix: Trellix Intrusion Prevention System Documentation List

To find Trellix IPS product documentation:

1. Go to Trellix Documentation Portal (<https://docs.trellix.com>).
2. Click **Intrusion Prevention System** from the **Network Security** tile under the **Featured Content** section.



#### TIP

You can alternatively scroll down the page and click **Intrusion Prevention System** from the **Products A-Z** section.

The **Intrusion Prevention System** documentation landing page appears displaying the list of documents categorized under various tiles.



#### NOTE

The documentation category tiles primarily list the latest 11.1 documents. If you plan to access 10.1.10 or older documents, you can click the version specific links provided under the **Older Product Documents** tile.

**Table 3. Trellix Intrusion Prevention System Software Documentation**

| Software Documentation      |
|-----------------------------|
| Certification Guide         |
| Installation Guide          |
| Product Guide               |
| Integration Guide           |
| Manager API Reference Guide |

**Table 4. Trellix Intrusion Prevention System Hardware Documentation**

| Guide                           | Models                                                                                                                                                                                |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manager Appliance Product Guide | MLOS                                                                                                                                                                                  |
| NS-series Sensor Product Guide  | NS9500, NS9x00, NS7600, NS7500, NS7x50, NS7x00, NS5x00, NS3600, NS3500, and NS3x00                                                                                                    |
| NS-series Reference Guide       | <ol style="list-style-type: none"> <li>1. NS-series Interface Modules</li> <li>2. NS-series Transceiver Modules</li> <li>3. NS-series Sensors DC Power Supply Installation</li> </ol> |

| Guide                       | Models                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fail-Open Kit Product Guide | <ul style="list-style-type: none"><li>• 100 Gigabit Modular Active Fail-Open Bypass Kit</li><li>• 10/40 Gigabit Modular Active Fail-Open Bypass Kit</li><li>• 1/10 Gigabit Modular Active Fail-Open Kit</li><li>• 1/10 Gigabit Modular Passive Fail-Open Kit</li><li>• 40 Gigabit Active Fail-Open Bypass Kit</li></ul> |

## Appendix: Audit Log Records

This section describes the audit log records in relation to a user's activities. The general format of audit records is:

Time, Results, Category, Summary, Details, Domain, UserDate, Admin Domain, User, Attack Category, Action, Result, Description

An example of an audit record displayed in the GUI is:

The screenshot shows a 'Logs' window with tabs for 'Faults', 'System Files', 'Background Tasks', 'User Activities', and 'MDR Events'. The 'User Activities' tab is selected. The log table has columns for Time, Activity (Result, Category, Summary), Details, Domain, and User. Two records are visible:

| Time                  | Activity Result | Category | Summary                | Details                                                                                                                                                                                    | Domain      | User          |
|-----------------------|-----------------|----------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|---------------|
| Jan 17, 2024 20:05:03 | Success         | User     | Manager Console Login  | User "Administrator" with login id "admin" successfully logged into the Manager from "10. (10. )": Login URI: /intruvert/jsp/module/Login.jsp , URI referrer : null , protocol : HTTP/1.1. | /My Company | Administrator |
| Jan 17, 2024 20:04:56 | Success         | User     | Manager Console Logout | User "Administrator" with login id "admin" logged out of the Manager from "10. (10. )".                                                                                                    | /My Company | Administrator |

The following table documents the messages within audit log records generated by Trellix Intrusion Prevention System.

**Table 5. Audit Log Records**

| Action                                         | Log Message                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Changes to the system time by an Administrator | Time has been changed                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Communication between the Manager and Sensors  | <ul style="list-style-type: none"> <li>• <b>Enabling:</b> Successfully added sensor "<i>sensor_name</i>"</li> <li>• <b>Disabling:</b> Successfully deleted sensor "<i>sensor_name</i>"</li> </ul>                                                                                                                                                                                                                                                 |
| Failure to establish a TLS Session             | <ul style="list-style-type: none"> <li>• Certificate having missing Extended keys</li> <li>• Mismatch between configured Server Name and Subject Alt Name in Imported certificate</li> <li>• The connection to syslog server <i>IP_Address:port_number</i> failed. Error: Syslog TCP connection failed.</li> </ul>                                                                                                                                |
| Failure to establish an HTTPS Session          | Mismatch between configured Server Name and Subject Alt Name in Imported certificate                                                                                                                                                                                                                                                                                                                                                              |
| Failure to establish an SSH session            | <ul style="list-style-type: none"> <li>• Disconnecting: Too many authentication failures [preauth]</li> <li>• Unable to negotiate with <i>IP_Address</i> port <i>port_number</i>: no matching host key type found. Their offer: <i>host_key_type</i> [preauth]</li> <li>• Unable to negotiate with <i>IP_Address</i> port <i>port_number</i>: no matching key exchange method found. Their offer: <i>key_exchange_method</i> [preauth]</li> </ul> |

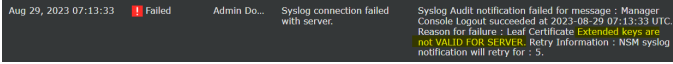
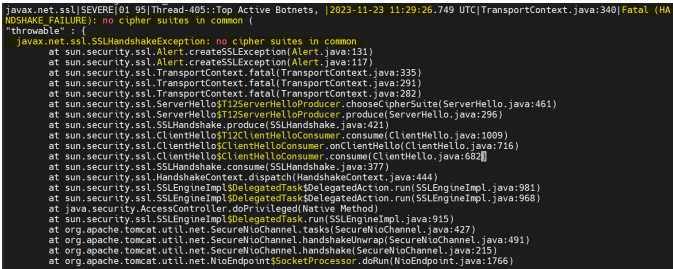
| Action                                                | Log Message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Management activities of system data                  | <ul style="list-style-type: none"> <li>• Read audit log</li> <li>• Successfully set Session Timeout</li> <li>• Logon Banner Configuration updated</li> <li>• Successfully set Password Content, Configuration is ...</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Trusted connections                                   | <ul style="list-style-type: none"> <li>• <b>Initiation:</b> <ul style="list-style-type: none"> <li>• Pktlog Channel back up. Clear the Pktlog Channel Down event of sensor <i>sensor</i></li> <li>• Alert Channel back up. Clear the Alert Channel Down event of sensor <i>sensor</i></li> <li>• Syslog Client - Added to Retry Q</li> <li>• Syslog Client - Flushing and Shutting down</li> <li>• Request for Authentication for User name=<i>Username</i></li> </ul> </li> <li>• <b>Termination:</b> <ul style="list-style-type: none"> <li>• The link on Port: <i>Port_identifier</i> is Down Count: <i>number</i>. The link between this port and the external device to which it is connected is down.</li> <li>• Received disconnect from <i>IP_Address</i> port <i>port_number</i>: disconnected by user</li> <li>• User "<i>User Name</i>" with login id "<i>Username</i>" logged off Trellix IPS Manager from "<i>Hostname (IP_Address)</i>"</li> </ul> </li> <li>• <b>Failure:</b> <ul style="list-style-type: none"> <li>• Certificate having missing Extended keys</li> <li>• Mismatch between configured Server Name and Subject Alt Name in Imported certificate</li> <li>• Received fatal alert: handshake_failure</li> <li>• Connection refused (Connection refused)</li> <li>• Disconnecting: Too many authentication failures [preauth]</li> <li>• Unable to negotiate with <i>IP_Address</i> port <i>port_number</i>: no matching host key type found. Their offer: <i>hostkey_type</i> [preauth]</li> <li>• Unable to negotiate with <i>IP_Address</i> port <i>port_number</i>: no matching key exchange method found. Their offer: <i>key_exchange_method</i> [preauth]</li> </ul> </li> </ul> |
| Unsuccessful attempt to validate an X.509 certificate | <ul style="list-style-type: none"> <li>• Certificate having missing Extended keys</li> <li>• Mismatch between configured Server Name and Subject Alt Name in Imported certificate</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Unsuccessful login attempts limit is met or exceeded  | Login failed: Maximum allowable login attempts <i>number</i> have exceeded                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Action                                                 | Log Message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use of the identification and authentication mechanism | <ul style="list-style-type: none"> <li>• Postponed keyboard-interactive/pam for <i>username</i> from <i>IP_Address</i> port <i>port_number</i> ssh2 [preauth]</li> <li>• Postponed publickey for <i>username</i> from <i>IP_Address</i> port <i>port_number</i> ssh2 [preauth]</li> <li>• Accepted keyboard-interactive/pam for <i>username</i> from <i>IP_Address</i> port <i>port_number</i> ssh2</li> <li>• error: Could not load host key: <i>path_to_hostkey_file</i></li> <li>• Failed keyboard-interactive/pam for <i>username</i> from <i>IP_Address</i> port <i>port_number</i> ssh2</li> <li>• Failed publickey for <i>username</i> from <i>IP_Address</i> port <i>port_number</i> ssh2: RSA SHA256:<i>public_key_value</i></li> <li>• User "<i>username</i>" failed to log in to Trellix IPS Manager from "<i>Hostname (IP_Address)</i>". Login URI: <i>/intruvert/jsp/module/Login.jsp</i>. URI referrer : <a href="https://Hostname//intruvert/jsp/module/Login.jsp">https://Hostname//intruvert/jsp/module/Login.jsp</a> , protocol : HTTP/1.2</li> <li>• Unknown login ID "<i>Username</i>". Login failed from "<i>Hostname (IP_Address)</i>". Login URI: <i>/intruvert/jsp/module/Login.jsp</i>. URI referrer : <a href="https://Hostname//intruvert/jsp/module/Login.jsp">https://Hostname//intruvert/jsp/module/Login.jsp</a> , protocol : HTTP/1.2</li> <li>• Starting Session <i>number</i> of user <i>Username</i></li> <li>• Trellix IPS Manager Login failed at <i>timestamp</i></li> </ul> |
| User session terminated                                | <ul style="list-style-type: none"> <li>• Removed session <i>number</i></li> <li>• User "<i>User Name</i>" with login id "<i>Username</i>" logged out of the Manager from "<i>Hostname (IP_Address)</i>"</li> <li>• Close session: user <i>Username</i> from <i>IP_Address</i> port <i>port_number</i> id <i>number</i></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Table 6. Manager FAU\_GEN.1 Audit Records**

| Re-requirement | Auditable Events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Additional Audit Record Contents | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FAU_GEN.1      | <ul style="list-style-type: none"> <li>Start-up and shut-down of the audit functions</li> <li>Auditable events for the not specified level of audit; and Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).</li> <li>Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).</li> <li>Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).</li> <li>Resetting passwords (name of related user ac-</li> </ul> | None                             | <ul style="list-style-type: none"> <li>Start-up and shut-down of the audit functions                             <pre data-bbox="889 422 1503 491">Apr 4 2024 14:07:35 NSMApp sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/systemctl stop rsyslog Apr 4 2024 14:07:35 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Apr 4 2024 14:07:35 NSMApp sudo:pam_unix(sudo:session): session closed for user root Apr 4 2024 14:07:43 NSMApp sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/systemctl start rsyslog Apr 4 2024 14:07:43 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Apr 4 2024 14:07:43 NSMApp sudo:pam_unix(sudo:session): session closed for user root</pre> </li> <li>Auditable events for the not specified level of audit; and Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).                             <pre data-bbox="889 669 1503 743">Oct 05, 2023 11:56:06 Success User Manager Console Login User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)". Login URL: /admin/web/guest/manager/login.jsp, URI referer: null, protocol: HTTP/1.1. Oct 05, 2023 13:04:17 Success User Manager Console Logout User "Administrator" with login id "admin" logged out of the Manager from "10.1.4.16 (10.1.4.16)".</pre> </li> <li>Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).                             <pre data-bbox="889 890 1503 995">Feb 21 2024 14:20:08 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Feb 21 2024 14:20:08 NSMApp sudo:pam_unix(sudo:session): session closed for user root Feb 21 2024 14:20:15 NSMApp sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/timedatectl set-time 2024-01-01 01:00:00 Feb 21 2024 14:20:15 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Jan 1 2024 01:00:00 NSMApp sudo:pam_unix(sudo:session): session closed for user root Jan 1 2024 01:00:26 NSMApp sshd[1054]:debug3: fd 5 is not 0_WONBLOCK Jan 1 2024 01:00:26 NSMApp sshd[1054]:debug1: Forked child 551. Jan 1 2024 01:00:26 NSMApp sshd[1054]:debug3: send_rexec state: entering fd = 8 config len 1138</pre> </li> <li>Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).                             <pre data-bbox="889 1142 1503 1215">Sep 13, 2023 12:45:37 Success Manager Manager Trust Certificate Import A CA-signed certificate (used by the Manager for trust establishment) was imported into the Manager. Certificate: CN=10.1.4.64, O=Acumen, OU=CC, L=, ST=, C=US Sep 13, 2023 12:36:27 Success Manager Manager CSR File Generation A CSR file (used to generate a CA-signed certificate for trust establishment) was generated by the Manager.</pre> </li> <li>Resetting passwords (name of related user account shall be logged).                             <pre data-bbox="889 1320 1503 1373">Apr 04, 2024 14:15:51 Success Manager User Account Update Updated account for user "test(acumimesec)"; the password of the account has been changed. Apr 04, 2024 14:14:19 Success Manager User Account Creation User account created for user "test(acumimesec)".</pre> </li> </ul> |

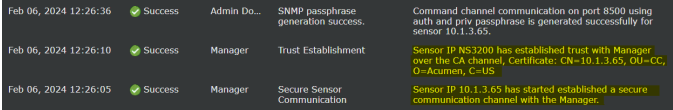
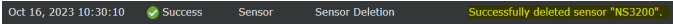
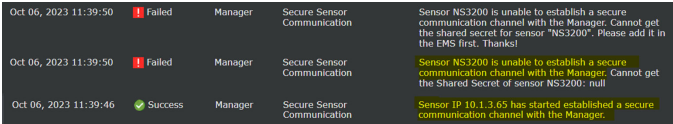
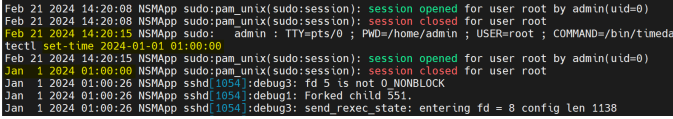


| Re-requirement                    | Auditable Events                   | Additional Audit Record Contents | Audit Logs                                                                           |
|-----------------------------------|------------------------------------|----------------------------------|--------------------------------------------------------------------------------------|
|                                   | count shall be logged).            |                                  |                                                                                      |
| FAU_GE N_EXT.1                    | None                               | None                             | -                                                                                    |
| FAU_GE N.2                        | None                               | None                             | -                                                                                    |
| FAU_ST G_EXT.1                    | None                               | None                             | -                                                                                    |
| FCS_CK M.1                        | None                               | None                             | -                                                                                    |
| FCS_CK M.2                        | None                               | None                             | -                                                                                    |
| FCS_CK M.4                        | None                               | None                             | -                                                                                    |
| FCS_CO P.1/<br>DataEn-<br>ryption | None                               | None                             | -                                                                                    |
| FCS_CO P.1/<br>SigGen             | None                               | None                             | -                                                                                    |
| FCS_CO P.1/<br>Hash               | None                               | None                             | -                                                                                    |
| FCS_CO P.1/<br>Keyed-<br>Hash     | None                               | None                             | -                                                                                    |
| FCS_RB G_EXT.1                    | None                               | None                             | -                                                                                    |
| FCS_TLS C_EXT.1                   | Failure to establish a TLS Session | Reason for failure               |  |
| FCS_TLS S_EXT.1                   | Failure to establish a TLS Session | Reason for failure               |  |

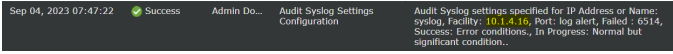
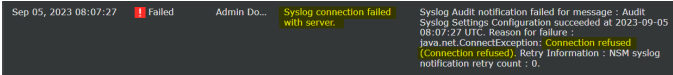
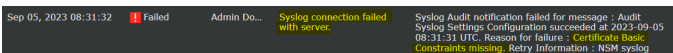
| Re-requirement     | Auditable Events                                                                                                                                                      | Additional Audit Record Contents                      | Audit Logs                                                                                                                                                                                                                                           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FCS_TLS<br>S_EXT.2 | Failure to establish a TLS Session                                                                                                                                    | Reason for failure                                    |                                                                                                                                                                    |
| FCO_CP<br>C_EXT.1  | <ul style="list-style-type: none"> <li>Enabling communications between a pair of components</li> <li>Disabling communications between a pair of components</li> </ul> | Identities of the endpoints pairs enabled or disabled | <p><u>Enabling communications:</u></p>  <p><u>Disabling communications:</u></p>  |
| FIA_AFL.1          | Unsuccessful login attempts limit is met or exceeded.                                                                                                                 | Origin of the attempt (e.g., IP address).             | <p><u>Web GUI:</u></p>  <p><u>SSH:</u></p>                                    |
| FIA_PM<br>G_EXT.1  | None                                                                                                                                                                  | None                                                  | -                                                                                                                                                                                                                                                    |

| Re-requirement | Auditable Events                                           | Additional Audit Record Contents         | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|------------------------------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIA_UIA_EXT.1  | All use of the identification and authentication mechanism | Origin of the attempt (e.g., IP address) | <p><b>Console:</b></p> <pre>Oct 4 2023 10:13:42 NSMApp login:pam_unix(login:session): session opened for user admin by LOGIN(uid=0) Oct 4 2023 10:13:42 NSMApp login:LOGIN ON tty1 BY admin  Oct 4 2023 10:11:50 NSMApp unix_chkpwd(???):password check failed for user (admin) Oct 4 2023 10:11:51 NSMApp login:pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=tty1 ruser=rhost= user=admin Oct 4 2023 10:11:52 NSMApp login:LOGIN SESSION FROM TTY1 FOR admin, terminal=on dot.log</pre> <p><b>SSH:</b></p> <pre>2023-12-15:04 NSMApp sshd [101]:pam_unix(sshd:session): session opened for user admin by (uid=0)Aug 24 2023  Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: ssh_msg_send: type 7 Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: PAM: Authentication failure Oct 4 2023 12:06:06 NSMApp sshd [3090]:error: PAM: Authentication failure for ntp from 10.1.4.16 Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_send entering: type 107 Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_sshpam_query: pam_query returned -1 [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: auth2_challenge_start: device=empty [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_sshpam_free_ctx [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_send entering: type 110 [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_sshpam_free_ctx: waiting for WONTON_ANS PAM FREE_CTX [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_receive expect entering: type 111 [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_receive entering [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_receive entering Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: monitor_read: checking request 110 Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_answer_pam_free_ctx Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: PAM: sshpam_free_ctx entering Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: PAM: sshpam_thread_cleanup entering Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_send entering: type 111 Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: monitor_read: 110 used once, disabling now Oct 4 2023 12:06:06 NSMApp sshd [3090]:debug: mm_request_send entering: type 112 [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:error: maximum authentication attempts exceeded for ntp from 10.1.4.16 port 45556 ssh2 [preauth] Oct 4 2023 12:06:06 NSMApp sshd [3090]:disconnecting: too many authentication failures [preauth]</pre> <p><b>Web GUI:</b></p> <pre>Oct 05, 2023 11:56:06 Success User Manager Console Login User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)": Login URI: /intruvert/jsp/module/Login.jsp , URI referrer : null , protocol : HTTP/1.1.  Oct 05, 2023 11:53:46 Failed User Manager Console Login User "Administrator" failed to log into Manager from "10.1.4.16 (10.1.4.16)": Login URI: /intruvert/jsp/module/Login.jsp , URI referrer : null , protocol : HTTP/1.1.</pre> |

| Re-requirement          | Auditable Events                                           | Additional Audit Record Contents         | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIA_UAU_EXT.2           | All use of the identification and authentication mechanism | Origin of the attempt (e.g., IP address) | <p><b>Console:</b></p> <pre>Oct 4 2023 10:13:42 NSMApp login:pam_unix(login:session): session opened for user admin by LOGIN(uid=0) Oct 4 2023 10:13:42 NSMApp login:LOGIN ON tty1 BY admin</pre> <p><b>SSH:</b></p> <pre>2023 12:15:04 NSMApp sshd [10.1.4.16]: pam_unix(sshd:session): session opened for user admin by (uid=0)Aug 24 2023</pre> <p><b>Web GUI:</b></p> <pre>Oct 05, 2023 11:56:06 Success User Manager Console Login User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)". Login URI: /intruvert/jsp/module/Login.jsp , URI referer : null , protocol : HTTP/1.1.</pre>                                                                                |
| FIA_UAU.7               | None                                                       | None                                     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| FIA_X50_9_EXT.1/Rev     | Unsuccessful attempt to validate a certificate             | Reason for failure                       | <pre>Sep 05, 2023 08:31:32 Failed Admin Do... Syslog connection failed with server. Syslog Audit notification failed for message : Audit Syslog Settings Configuration succeeded at 2023-09-05 08:31:31 UTC. Reason for failure : Certificate Base Constraints missing. Retry Information : NSM syslog notification will retry for : 5.</pre>                                                                                                                                                                                                                                                                                                                                                                                     |
| FIA_X50_9_EXT.1/ITT     | Unsuccessful attempt to validate a certificate             | Reason for failure                       | <pre>Oct 11, 2023 10:44:55 Critical Invalid Device Trust Certificate Detected Device NS3200 tried to establish trust with the Manager using an invalid CA-signed certificate. Validation error: Verification failed Root with leaf certs, signing issue. ??Replace the invalid certificate with a valid one.</pre> <pre>Oct 11, 2023 10:44:55 Critical Device Disconnected The Manager cannot communicate with the device NS3200 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.</pre> |
| FIA_X50_9_EXT.2         | None                                                       | None                                     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| FIA_X50_9_EXT.3         | None                                                       | None                                     | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| FMT_MOF.1/Manual Update | Any attempt to initiate a manual update                    | None                                     | <pre>d [065]:debug3: send packet: type 2Aug 25 2023 08:28:56 NSMApp sshd [082]:debug3: send packet: type 2Aug 25 2023 08:28:56 NSMApp sudo:low-priv : user NOT in sudoers ; TTY=pts/0 ; PWD=/ ; USER=root ; COMMAND=apt updateAug 25 2023 08:29:00 NSMApp sshd [77]:debug3: receive packet: type 88Aug 25 2023 08:29:00 NSMApp sshd [70]:debug3: receive packet: type 88Aug 25 2023</pre>                                                                                                                                                                                                                                                                                                                                         |

| Re-requirement         | Auditable Events                                                                                                                                                                  | Additional Audit Record Contents                                                                                                                        | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FMT_MTD.1/<br>CoreData | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                          |
| FMT_SM F.1             | All management activities of TSF data.                                                                                                                                            | None                                                                                                                                                    | Refer to the below table [Manager Management Functions]                                                                                                                                                                                                                                                                                                                                                    |
| FMT_SMR.2              | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                          |
| FPT_APW_EXT.1          | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                          |
| FPT_ITT.1              | <ul style="list-style-type: none"> <li>Initiation of the trusted channel</li> <li>Termination of the trusted channel</li> <li>Failure of the trusted channel functions</li> </ul> | Identification of the initiator and target of failed trusted channels establishment attempt                                                             | <p><u>Initiation of trusted channel:</u></p>  <p><u>Termination of trusted channel:</u></p>  <p><u>Failure of trusted channel functions:</u></p>  |
| FPT_SKP_EXT.1          | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                          |
| FPT_STM_EXT.1          | Discontinuous changes to time - either Administrator actuated or changed via an automated process                                                                                 | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address) |                                                                                                                                                                                                                                                                                                                        |
| FPT_TSTM_EXT.1         | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                          |

| Re-requirement    | Auditable Events                                                        | Additional Audit Record Contents | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|-------------------------------------------------------------------------|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FPT_TU<br>D_EXT.1 | Initiation of update; result of the update attempt (success or failure) | None                             | <pre> 2023-10-30 12:28:24,278:INFO: main :logCommand:881: [INFO] THE EXECUTED COMMAND IS : upgrade 2023-10-30 12:29:41,022:INFO: main :subprocess_popen:467:The command is ['scp', 'acumsec@10.1.4.16:/home/acumsec/manager_builds/11.1.116.0_corrupted/corrupted_build_setup.bin', '/tmp/'], The Pid is 499, The exit status is 0 2023-10-30 12:29:47,445:INFO: main :subprocess_popen:467:The command is ['/usr/bin/sudo', 'chmod', '+x', '/tmp/corrupted_build_setup.bin'], The Pid is 501, The exit status is 0 2023-10-30 12:30:00,297:INFO: main :subprocess_popen_nine:475:The command is ['/usr/bin/sudo', '/bin/managerinstall', '/tmp/corrupted_build_setup.bin'], The Pid is 505, The exit status is 256 2023-10-30 12:30:00,298:ERROR: main :install update:441: Failed to verify signature of install bundle. Bundle installation failed Traceback (most recent call last): File "/bin/restrictShell.py", line 438, in install update subprocess_popen_nine(['/usr/bin/sudo', '/bin/managerinstall', '/tmp/' + bundle]) File "/bin/restrictShell.py", line 479, in subprocess_popen_nine raise OSError OSError                 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| FTA_SSL<br>_EXT.1 | The termination of a local session by the session locking mechanism     | None                             | <pre> Oct 5 2023 07:54:31 NSMApp sudo: admin : TTY=ttty1 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/bash Oct 5 2023 07:54:31 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Oct 5 2023 07:56:09 NSMApp sshd[3342]:debug3: PAM: sshpam_thread_cleanup entering Oct 5 2023 07:56:24 NSMApp sudo:pam_unix(sudo:session): session closed for user root                 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| FTA_SSL<br>.3     | The termination of a remote session by the session locking mechanism    | None                             | <p><u>SSH:</u></p> <pre> Oct 5 2023 12:47:11 NSMApp sshd[1665]:Starting session: shell on ptty1 for admin from 10.1.4.16 port 50640 id 0 Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug2: fd 3 setting TCP_NODELAY Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: ssh_packet_set_tos: set IP_TOS 0x10 Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug2: channel 0: rfd 12 tsatty Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug2: fd 12 setting 0_NONBLOCK Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: fd 8 is 0 NONBLOCK Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: mm_forward_audit_messages: entering Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug1: Setting controlling tty using TIOCSTTY. Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: send packet: type 98 Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: Copy environment: SELINUX_ROLE_REQUESTED= Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: Copy environment: SELINUX_LEVEL_REQUESTED= Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: Copy environment: SELINUX_USE_CURRENT_RANGE= Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: Copy environment: XDG_SESSION_ID=3002 Oct 5 2023 12:47:11 NSMApp sshd[1665]:debug3: Copy environment: XDG_RUNTIME_DIR=/run/user/500 Oct 5 2023 12:53:11 NSMApp sshd[1665]:Timeout: client not responding. Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug1: do_cleanup Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: PAM: sshpam_thread_cleanup entering Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: mm_request_send entering: type 122 Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: mm_request_receive expect entering: type 123 Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: mm_request_receive entering Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: mm_request_send entering: type 122 Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: monitor_read checking request 122 Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: mm_request_send entering: type 123 Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug3: mm_request_receive entering Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug1: do_cleanup Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug1: PAM: cleanup Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug1: PAM: Closing session Oct 5 2023 12:53:11 NSMApp sshd[1665]:pam_unix(sshd:session): session closed for user admin Oct 5 2023 12:53:11 NSMApp sshd[1665]:debug1: PAM: deleting credentials                 </pre> <p><u>Web GUI:</u></p> <pre> Oct 05, 2023 12:21:43 Success User Manager Console Logout User "Administrator" with login id "admin" logged out of the Manager from "10.1.4.16". Oct 05, 2023 12:43:15 Success User Manager Console Login User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)". Login URI: /intruvert/jsp/module/Login.jsp , URI referer : null , protocol : HTTP/1.1.                 </pre> |
| FTA_SSL<br>.4     | The termination of an interactive session                               | None                             | <p><u>SSH:</u></p> <pre> 2023 12:13:33 NSMApp sshd[3341]:Received disconnect from 10.1.4.16 port 56744:11: disconnected by userAug 25 2023 12:13:33 NSMApp sshd[3341]:Disconnected from 10.1.4.16 port 56744 ... Aug 25 2023 12:13:33 NSMApp sshd[3336]:pam_unix(sshd:session): session closed for user_adminAug 25 2023 12:13:33 NSMApp sshd[3336]:debug1: PAM: deleting credentials                 </pre> <p><u>WebGUI:</u></p> <pre> Oct 05, 2023 13:04:17 Success User Manager Console Logout User "Administrator" with login id "admin" logged out of the Manager from "10.1.4.16 (10.1.4.16)".                 </pre> <p><u>Console:</u></p> <pre> s(xton): session opened for user admin by LOGIN(uid=0)Aug 28 2023 06:36:48 NSMApp Login:LOGIN ON tty1 BY adminAug 28 2023 06:37:51 NSMApp Login:pam_unix(login:session): session closed for user_admin                 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| FTA_TAB<br>.1     | None                                                                    | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

| Re-requirement   | Auditable Events                                                                                                                                                                  | Additional Audit Record Contents                                                                   | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>FTP_ITC.1</p> | <ul style="list-style-type: none"> <li>Initiation of the trusted channel</li> <li>Termination of the trusted channel</li> <li>Failure of the trusted channel functions</li> </ul> | <p>Identification of the initiator and target of failed trusted channels establishment attempt</p> | <p><u>Initiation of the trusted channel:</u></p>  <p><u>Termination of the trusted channel:</u></p>  <p><u>Failure of the trusted channel functions:</u></p>  |

| Re-requirement    | Auditable Events                                                                                                                                                                     | Additional Audit Record Contents             | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTP_TRP .1/ Admin | <ul style="list-style-type: none"> <li>Initiation of the trusted channel.</li> <li>Termination of the trusted channel.</li> <li>Failure of the trusted channel functions.</li> </ul> | Identification of the claimed user identity. | <p><b>Initiation of trusted channel</b></p> <p><b>SSH:</b></p> <pre> Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug1: keyboard-interactive/pam for admin from 10.1.4.16 port 49982 ssh2 Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug1: monitor_child_preauth: admin has been authenticated by privileged process Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_get_keystate: Waiting for new keys Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive_expect entering: type 26 Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive entering Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_get_keystate: GOT new keys Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive_expect entering: type 122 Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive entering Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_send entering: type 123 Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_do_pam_account entering [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_send entering: type 182 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive_expect entering: type 183 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive entering [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_do_pam_account returning 1 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: send_packets: type 52 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_send entering: type 26 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_send_keystate: Finished sending state [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_send entering: type 122 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive_expect entering: type 123 [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: mm_request_receive entering [preauth] Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: ssh_sandbox_parent_finish: finished Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: SELinux support enabled Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug1: pam_unix(sshd:session): session opened for user admin by (uid=0) Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug1: PAM: establishing credentials Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: PAM: opening session Nov 9 2023 12:56:25 NSMApp sshd[1577]: debug3: PAM: sshpam_store_conv called with 1 messages                     </pre> <p><b>Web GUI:</b></p> <pre> Aug 25, 2023 14:25:27 Success User Manager Console Login User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)". Login URI: /mtruver/ssp/module/Login.jsp , URI referer : null , protocol: HTTP/1.1.                     </pre> <p><b>Termination of the trusted channel:</b></p> <p><b>SSH:</b></p> <pre> Oct 5 2023 12:53:11 NSMApp sshd[1660]: debug1: PAM: closing session Oct 5 2023 12:53:11 NSMApp sshd[1660]: pam_unix(sshd:session): session closed for user admin Oct 5 2023 12:53:11 NSMApp sshd[1660]: debug1: PAM: deleting credentials                     </pre> <p><b>Web GUI:</b></p> <pre> Oct 05, 2023 13:04:17 Success User Manager Console Logout User "Administrator" with login id "admin" logged out of the Manager from "10.1.4.16 (10.1.4.16)".                     </pre> <p><b>Failure of trusted channel functions:</b></p> <p><b>SSH:</b></p> <pre> Oct 4 2023 11:55:36 NSMApp login:pam_faillock(login:auth): user unknown Oct 4 2023 11:55:41 NSMApp login:pam_unix(login:auth): check pass; user unknown Oct 4 2023 11:55:44 NSMApp login:pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=ttty1 ruser=rhost= Oct 4 2023 11:55:44 NSMApp login:pam_faillock(login:auth): user unknown Oct 4 2023 11:55:44 NSMApp login:FAILED LOGIN SESSION FROM tty1 FOR configure , permission denied.                     </pre> <p><b>Web GUI:</b></p> <pre> Oct 05, 2023 11:53:46 Failed User Manager Console Login User "Administrator" failed to log into Manager from "10.1.4.16 (10.1.4.16)". Login URI: /mtruver/ssp/module/Login.jsp , URI referer : null , protocol: HTTP/1.1.                     </pre> |
| FAU_ST G_EXT.4    | None                                                                                                                                                                                 | None                                         | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |



| Re-requirement  | Auditable Events                     | Additional Audit Record Contents | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|--------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FCS_HTTPS_EXT.1 | Failure to establish a HTTPS Session | Reason for failure               | <pre> javax.net.ssl.FINE 01 8A https-jsse-nio-0.0.0-443-exec-1 2023-11-23 14:34:25.339 UTC ClientHello.java:678 Consuming ClientHello handshake message (   "clientHello": {     "client version"      : "TLSv1.2",     "random"              : "8C 4F 0C E7 9A 7C D0 8D 7A 28 EC 57 45 FC F2 E2 53 0C 27 04 AE 99 39 8C 7A 10 3F 45 97 C0 ED E6",     "session id"          : "1A 89 F5 41 36 24 2F A6 F4 D0 CF 38 56 AC E8 98 EF DC 6C C5 6C D8 AF 44 46 96 AC 50 70 17 D4 50",     "cipher suites"       : "[TLS_AES_256_GCM_SHA384(0x1302), TLS_CHACHA20_POLY1305_SHA256(0x1303), TLS_AES_128_GCM_SHA256(0x1301), TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(0xC02C), TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xC030), TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(0x009F), UNKNOWN_CIPHER_SUITE(0xC0A9), UNKNOWN_CIPHER_SUITE(0xC0A8), UNKNOWN_CIPHER_SUITE(0xC0A7), UNKNOWN_CIPHER_SUITE(0xC0A6), UNKNOWN_CIPHER_SUITE(0xC0A5), UNKNOWN_CIPHER_SUITE(0xC0A4), UNKNOWN_CIPHER_SUITE(0xC0A3), UNKNOWN_CIPHER_SUITE(0xC0A2), UNKNOWN_CIPHER_SUITE(0xC0A1), UNKNOWN_CIPHER_SUITE(0xC0A0), TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(0x0028), TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0x002F), TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(0x009E), TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(0xC024), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xC028), TLS_DHE_RSA_WITH_AES_256_CBC_SHA384(0x0098), TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(0x0023), TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0x0027), TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(0x0067), TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(0x0093), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0x0097), TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x0039), TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(0xC014), TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0xC010), TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(0x009C), TLS_RSA_WITH_AES_256_GCM_SHA384(0x009D), TLS_RSA_WITH_AES_128_GCM_SHA256(0x009E), TLS_RSA_WITH_AES_256_CBC_SHA384(0x0099), TLS_RSA_WITH_AES_128_GCM_SHA256(0x009F), TLS_RSA_WITH_AES_256_CBC_SHA384(0x0094), TLS_RSA_WITH_AES_128_GCM_SHA256(0x0095), TLS_RSA_WITH_AES_128_CBC_SHA(0x002F), TLS_EMPTY_RENEGOTIATION_INFO_SCSV(0x00FF)"]",     "compression methods": "00",     "extensions"          : {       "ec_point_formats (11)": {         "formats": [uncompressed, ansiX962_compressed_prime, ansiX962_compressed_char2]       },       "supported_groups (10)": {         "versions": [secp192r1]       }     }   } ) javax.net.ssl.FINE 01 8A https-jsse-nio-0.0.0-443-exec-1 2023-11-23 14:34:25.339 UTC ClientHello.java:678 Consuming ClientHello handshake message (   "clientHello": {     "client version"      : "TLSv1.2",     "random"              : "8C 4F 0C E7 9A 7C D0 8D 7A 28 EC 57 45 FC F2 E2 53 0C 27 04 AE 99 39 8C 7A 10 3F 45 97 C0 ED E6",     "session id"          : "1A 89 F5 41 36 24 2F A6 F4 D0 CF 38 56 AC E8 98 EF DC 6C C5 6C D8 AF 44 46 96 AC 50 70 17 D4 50",     "cipher suites"       : "[TLS_AES_256_GCM_SHA384(0x1302), TLS_CHACHA20_POLY1305_SHA256(0x1303), TLS_AES_128_GCM_SHA256(0x1301), TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384(0xC02C), TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384(0xC030), TLS_DHE_RSA_WITH_AES_256_GCM_SHA384(0x009F), UNKNOWN_CIPHER_SUITE(0xC0A9), UNKNOWN_CIPHER_SUITE(0xC0A8), UNKNOWN_CIPHER_SUITE(0xC0A7), UNKNOWN_CIPHER_SUITE(0xC0A6), UNKNOWN_CIPHER_SUITE(0xC0A5), UNKNOWN_CIPHER_SUITE(0xC0A4), UNKNOWN_CIPHER_SUITE(0xC0A3), UNKNOWN_CIPHER_SUITE(0xC0A2), UNKNOWN_CIPHER_SUITE(0xC0A1), UNKNOWN_CIPHER_SUITE(0xC0A0), TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(0x0028), TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0x002F), TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(0x009E), TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384(0xC024), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(0xC028), TLS_DHE_RSA_WITH_AES_256_CBC_SHA384(0x0098), TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256(0x0023), TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256(0x0027), TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(0x0067), TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA(0x0093), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA(0x0097), TLS_DHE_RSA_WITH_AES_256_CBC_SHA(0x0039), TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA(0xC014), TLS_DHE_RSA_WITH_AES_128_CBC_SHA(0xC010), TLS_DHE_RSA_WITH_AES_128_GCM_SHA256(0x009C), TLS_RSA_WITH_AES_256_GCM_SHA384(0x009D), TLS_RSA_WITH_AES_128_GCM_SHA256(0x009E), TLS_RSA_WITH_AES_256_CBC_SHA384(0x0099), TLS_RSA_WITH_AES_128_GCM_SHA256(0x009F), TLS_RSA_WITH_AES_256_CBC_SHA384(0x0094), TLS_RSA_WITH_AES_128_GCM_SHA256(0x0095), TLS_RSA_WITH_AES_128_CBC_SHA(0x002F), TLS_EMPTY_RENEGOTIATION_INFO_SCSV(0x00FF)"]",     "compression methods": "00",     "extensions"          : {       "ec_point_formats (11)": {         "formats": [uncompressed, ansiX962_compressed_prime, ansiX962_compressed_char2]       },       "supported_groups (10)": {         "versions": [secp192r1]       }     }   } ) </pre> |
| FCS_SSH_S_EXT.1 | Failure to establish an SSH session  | Reason for failure               | <pre> Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: no session key loaded: key 0x5f39a06000 is not allowed Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: public key for admin from 10.1.4.16 port 3554 svb2: [COOA SHA256:7f5112bvcyrg+Hmdt7RhoD300j0ahwyBj]20a Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: no request send entering: type 2 Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: userauth:pubkey: authenticating 0 pkalg ecdsa-sha2-nistp256 [preauth] Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: userauth:1:auth: failure:portauth next method:pubkey,keyboard-interactive" [preauth] Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: send packet: type 51 [preauth] Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: receive packet: type 50 [preauth] Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: userauth:request for user admin service ssh-connection method keyboard-interactive [preauth] Sep 27 2023 07:17:13 NSMApp sshd[101]:debug3: attempt 2: failure: 1 [preauth] </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 7. Manager Management Functions

| Management Functions                                                                   | Test cases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                       |            |                              |                                                                                                                                                                                                          |                              |                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ability to administer the TOE locally and remotely                                     | <p><u>Console:</u></p> <pre> Oct 4 2023 10:13:42 NSMApp login:pam_unix(login:session): session opened for user admin by LOGIN(uid=0) Oct 4 2023 10:13:42 NSMApp login:LOGIN ON tty1 BY admin </pre> <p><u>SSH:</u></p> <pre> 3Aug 24 2023 12:15:04 NSMApp sshd[1081]:Accepted keyboard-interactive/pam for admin from 10.1.4.16 port 35496 ssh2Au 2023 12:15:04 NSMApp sshd[1081]:pam_unix(sshd:session): session opened for user admin by (uid=0)Aug 24 2023 </pre> <p><u>WebGUI:</u></p> <table border="1"> <tr> <td>Oct 05, 2023 11:56:06</td> <td></td> <td>Success</td> <td>User</td> <td>Manager Console Login</td> <td>User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)".<br/>Login URI: /intruvert/jsp/module/Login.jsp , URI referrer : null , protocol : HTTP/1.1.</td> </tr> </table> | Oct 05, 2023 11:56:06 |            | Success                      | User                                                                                                                                                                                                     | Manager Console Login        | User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)".<br>Login URI: /intruvert/jsp/module/Login.jsp , URI referrer : null , protocol : HTTP/1.1. |
| Oct 05, 2023 11:56:06                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Success               | User       | Manager Console Login        | User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)".<br>Login URI: /intruvert/jsp/module/Login.jsp , URI referrer : null , protocol : HTTP/1.1. |                              |                                                                                                                                                                                                          |
| Ability to configure the access banner                                                 | <table border="1"> <tr> <td>Apr 03, 2024 13:37:36</td> <td></td> <td>Success</td> <td>IPS Policy</td> <td>Logon Banner Configuration</td> <td>Logon Banner Configuration updated.</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Apr 03, 2024 13:37:36 |            | Success                      | IPS Policy                                                                                                                                                                                               | Logon Banner Configuration   | Logon Banner Configuration updated.                                                                                                                                                                      |
| Apr 03, 2024 13:37:36                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Success               | IPS Policy | Logon Banner Configuration   | Logon Banner Configuration updated.                                                                                                                                                                      |                              |                                                                                                                                                                                                          |
| Ability to configure the session inactivity time before session termination or locking | <table border="1"> <tr> <td>Apr 03, 2024 13:43:09</td> <td></td> <td>Success</td> <td>Manager</td> <td>Save Session Timeout Setting</td> <td>Successfully set Session Timeout.</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Apr 03, 2024 13:43:09 |            | Success                      | Manager                                                                                                                                                                                                  | Save Session Timeout Setting | Successfully set Session Timeout.                                                                                                                                                                        |
| Apr 03, 2024 13:43:09                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Success               | Manager    | Save Session Timeout Setting | Successfully set Session Timeout.                                                                                                                                                                        |                              |                                                                                                                                                                                                          |

| Management Functions                                                                                                                                    | Test cases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                       |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------|--------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------|--------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-----------|--------------|--------------------------------------------|-----------------------------------------|
| <p>Ability to update the TOE, and to verify the updates using <u>digital signature</u> capability prior to installing those updates</p>                 | <p><u>Positive update:</u></p> <pre>Apr 2 2024 06:35:11 NSMApp sshd:3525:debug3: send packet: type 2 Apr 2 2024 06:35:11 NSMApp sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/chmod +x /tmp/setup.bin Apr 2 2024 06:35:11 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Apr 2 2024 06:35:11 NSMApp sudo:pam_unix(sudo:session): session closed for user root Apr 2 2024 06:35:11 NSMApp sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/managerinstall /tmp/setup.bin Apr 2 2024 06:35:11 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) root@NSMApp:/home/admin# cat shell.log   grep "2024-04-02 06:34" 2024-04-02 06:34:49,898:INFO: _main_:subprocess.Popen:467:The command is ['scp', 'acumensec@10.1.3.45:/home/acumensec/final_builds/manager/setup.bin', '/tmp/'], The Pid is 3870, The exit status is 0 root@NSMApp:/home/admin#</pre> <p><u>Negative update:</u></p> <pre>2023-10-30 12:28:24,278:INFO: _main_:LogCommand:881: [INFO] THE EXECUTED COMMAND IS : upgrade 2023-10-30 12:29:41,022:INFO: _main_:subprocess.Popen:467:The command is ['scp', 'acumensec@10.1.4.16:/home/acumensec/manager_builds/11.1.116.8_corrupted/corrupted_build_setup.bin', '/tmp/'], The Pid is 499, The exit status is 0 2023-10-30 12:29:47,445:INFO: _main_:subprocess.Popen:467:The command is ['/usr/bin/sudo', 'chmod', '+x', '/tmp/corrupted_build_setup.bin'], The Pid is 501, The exit status is 0 2023-10-30 12:30:00,297:INFO: _main_:subprocess.Popen:475:The command is ['/usr/bin/sudo', '/bin/managerinstall', '/tmp/corrupted_build_setup.bin'], The Pid is 505, The exit status is 256 2023-10-30 12:30:00,298:ERROR: _main_:install update:441: Failed to verify signature of install bundle. Bundle installation failed Traceback (most recent call last):   File "/bin/restrictShell.py", line 438, in install update     subprocess.Popen(['usr/bin/sudo', '/bin/managerinstall', '/tmp/' + bundle])   File "/bin/restrictShell.py", line 479, in subprocess.Popen     raise OSError OSError</pre> |                       |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| <p>Ability to configure the authentication failure parameters for FIA_AFL.1</p>                                                                         | <table border="1"> <tr> <td data-bbox="544 905 706 1213">Apr 05, 2024 13:38:20</td> <td data-bbox="706 905 803 1213">✔ Success</td> <td data-bbox="803 905 933 1213">Manager</td> <td data-bbox="933 905 1128 1213">Save Password Content Setting</td> <td data-bbox="1128 905 1531 1213">Successfully set Password Content. Current Configuration is Password Cannot be the Same as Login ID : Disabled Track Previous Password Usage : Disabled Number of Characters That Must Be Changed : 0 Number of Previous Passwords to Track : 0 Expire Passwords : Disabled Time to Wait Before New Passwords Can Be Changed : 0 Hours Passwords Expire After : 0 Days Warning Interval : 0 Days Expire Passwords : Disabled Require Strong Passwords : Enabled Minimum Password Length : 8 UPPER Enabled : No Minimum Number of Characters : 1 LOWER Enabled : No Minimum Number of Characters : 1 SPECIAL_CHARS Enabled : No Minimum Number of Characters : 1 NUMERICAL Enabled : Yes Minimum Number of Characters : 1 Login Failure : Enabled Number of Consecutive Login Failures : 5 Prevent Login For : 120000 Minutes UserInactivityPolicyVO{userInactivityCheckEnabled=fal... lockUserDays=1}</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Apr 05, 2024 13:38:20 | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                       | Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Save Password Content Setting                                                                                                                                                                                                                                                                                                                                                                   | Successfully set Password Content. Current Configuration is Password Cannot be the Same as Login ID : Disabled Track Previous Password Usage : Disabled Number of Characters That Must Be Changed : 0 Number of Previous Passwords to Track : 0 Expire Passwords : Disabled Time to Wait Before New Passwords Can Be Changed : 0 Hours Passwords Expire After : 0 Days Warning Interval : 0 Days Expire Passwords : Disabled Require Strong Passwords : Enabled Minimum Password Length : 8 UPPER Enabled : No Minimum Number of Characters : 1 LOWER Enabled : No Minimum Number of Characters : 1 SPECIAL_CHARS Enabled : No Minimum Number of Characters : 1 NUMERICAL Enabled : Yes Minimum Number of Characters : 1 Login Failure : Enabled Number of Consecutive Login Failures : 5 Prevent Login For : 120000 Minutes UserInactivityPolicyVO{userInactivityCheckEnabled=fal... lockUserDays=1} |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| Apr 05, 2024 13:38:20                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Manager               | Save Password Content Setting                                                                                                                                                                                                                                                                                                                                                                   | Successfully set Password Content. Current Configuration is Password Cannot be the Same as Login ID : Disabled Track Previous Password Usage : Disabled Number of Characters That Must Be Changed : 0 Number of Previous Passwords to Track : 0 Expire Passwords : Disabled Time to Wait Before New Passwords Can Be Changed : 0 Hours Passwords Expire After : 0 Days Warning Interval : 0 Days Expire Passwords : Disabled Require Strong Passwords : Enabled Minimum Password Length : 8 UPPER Enabled : No Minimum Number of Characters : 1 LOWER Enabled : No Minimum Number of Characters : 1 SPECIAL_CHARS Enabled : No Minimum Number of Characters : 1 NUMERICAL Enabled : Yes Minimum Number of Characters : 1 Login Failure : Enabled Number of Consecutive Login Failures : 5 Prevent Login For : 120000 Minutes UserInactivityPolicyVO{userInactivityCheckEnabled=fal... lockUserDays=1} |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| <p>Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);</p> | <table border="1"> <tr> <td data-bbox="544 1213 706 1386">Mar 20, 2024 12:42:31</td> <td data-bbox="706 1213 803 1386">★ Informational</td> <td data-bbox="803 1213 933 1386">Audit Logs Rotated</td> <td data-bbox="933 1213 1128 1386">The audit log capacity on the Manager is 50 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 50 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 50 records written.</td> <td data-bbox="1128 1213 1531 1386">N/A 25.02 Manager</td> </tr> <tr> <td data-bbox="544 1386 706 1470">Apr 04, 2024 08:28:36</td> <td data-bbox="706 1386 803 1470">✔ Success</td> <td data-bbox="803 1386 933 1470">Admin Domain</td> <td data-bbox="933 1386 1128 1470">Syslog Server Configuration</td> <td data-bbox="1128 1386 1531 1470">Syslog settings specified for Domain: "/My Company:0" with Profile name: syslog, Host or IP : 10.1.4.16, Port: 6,514, Protocol: TCP, Error message:null.</td> </tr> <tr> <td data-bbox="544 1470 706 1554">Apr 04, 2024 08:28:36</td> <td data-bbox="706 1470 803 1554">✔ Success</td> <td data-bbox="803 1470 933 1554">Admin Domain</td> <td data-bbox="933 1470 1128 1554">Syslog TLS certificate audit.</td> <td data-bbox="1128 1470 1531 1554">Syslog TLS certificate contains Leaf detail as follows: subject:CN=10.1.4.16, issuedBy:CN=AcumenICA, OU=CC, O=Acumen, C=US, validity:Apr 4, 2024 - May 31, 2024, sigAlgo:SHA256WITHRSA, subjectAltName:10.1.4.16, Serial #:4528004407463435150.</td> </tr> <tr> <td data-bbox="544 1554 706 1633">Apr 04, 2024 08:28:34</td> <td data-bbox="706 1554 803 1633">✔ Success</td> <td data-bbox="803 1554 933 1633">Admin Domain</td> <td data-bbox="933 1554 1128 1633">Certificate import in Syslog configuration</td> <td data-bbox="1128 1554 1531 1633">Certificate import has been successful,</td> </tr> </table>                                                               | Mar 20, 2024 12:42:31 | ★ Informational                                                                                                                                                                                                                                                                                                                                                                                 | Audit Logs Rotated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | The audit log capacity on the Manager is 50 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 50 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 50 records written. | N/A 25.02 Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Apr 04, 2024 08:28:36 | ✔ Success | Admin Domain | Syslog Server Configuration   | Syslog settings specified for Domain: "/My Company:0" with Profile name: syslog, Host or IP : 10.1.4.16, Port: 6,514, Protocol: TCP, Error message:null.                                                                                        | Apr 04, 2024 08:28:36 | ✔ Success | Admin Domain | Syslog TLS certificate audit.              | Syslog TLS certificate contains Leaf detail as follows: subject:CN=10.1.4.16, issuedBy:CN=AcumenICA, OU=CC, O=Acumen, C=US, validity:Apr 4, 2024 - May 31, 2024, sigAlgo:SHA256WITHRSA, subjectAltName:10.1.4.16, Serial #:4528004407463435150. | Apr 04, 2024 08:28:34 | ✔ Success | Admin Domain | Certificate import in Syslog configuration | Certificate import has been successful, |
| Mar 20, 2024 12:42:31                                                                                                                                   | ★ Informational                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Audit Logs Rotated    | The audit log capacity on the Manager is 50 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 50 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 50 records written. | N/A 25.02 Manager                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| Apr 04, 2024 08:28:36                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Admin Domain          | Syslog Server Configuration                                                                                                                                                                                                                                                                                                                                                                     | Syslog settings specified for Domain: "/My Company:0" with Profile name: syslog, Host or IP : 10.1.4.16, Port: 6,514, Protocol: TCP, Error message:null.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| Apr 04, 2024 08:28:36                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Admin Domain          | Syslog TLS certificate audit.                                                                                                                                                                                                                                                                                                                                                                   | Syslog TLS certificate contains Leaf detail as follows: subject:CN=10.1.4.16, issuedBy:CN=AcumenICA, OU=CC, O=Acumen, C=US, validity:Apr 4, 2024 - May 31, 2024, sigAlgo:SHA256WITHRSA, subjectAltName:10.1.4.16, Serial #:4528004407463435150.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| Apr 04, 2024 08:28:34                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Admin Domain          | Certificate import in Syslog configuration                                                                                                                                                                                                                                                                                                                                                      | Certificate import has been successful,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| <p>Ability to modify the behaviour of the transmission of audit data to an external IT entity</p>                                                       | <table border="1"> <tr> <td data-bbox="544 1633 706 1701">Apr 04, 2024 08:28:36</td> <td data-bbox="706 1633 803 1701">✔ Success</td> <td data-bbox="803 1633 933 1701">Admin Domain</td> <td data-bbox="933 1633 1128 1701">Syslog Server Configuration</td> <td data-bbox="1128 1633 1531 1701">Syslog settings specified for Domain: "/My Company:0" with Profile name: syslog, Host or IP : 10.1.4.16, Port: 6,514, Protocol: TCP, Error message:null.</td> </tr> <tr> <td data-bbox="544 1701 706 1785">Apr 04, 2024 08:28:36</td> <td data-bbox="706 1701 803 1785">✔ Success</td> <td data-bbox="803 1701 933 1785">Admin Domain</td> <td data-bbox="933 1701 1128 1785">Syslog TLS certificate audit.</td> <td data-bbox="1128 1701 1531 1785">Syslog TLS certificate contains Leaf detail as follows: subject:CN=10.1.4.16, issuedBy:CN=AcumenICA, OU=CC, O=Acumen, C=US, validity:Apr 4, 2024 - May 31, 2024, sigAlgo:SHA256WITHRSA, subjectAltName:10.1.4.16, Serial #:4528004407463435150.</td> </tr> <tr> <td data-bbox="544 1785 706 1850">Apr 04, 2024 08:28:34</td> <td data-bbox="706 1785 803 1850">✔ Success</td> <td data-bbox="803 1785 933 1850">Admin Domain</td> <td data-bbox="933 1785 1128 1850">Certificate import in Syslog configuration</td> <td data-bbox="1128 1785 1531 1850">Certificate import has been successful,</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Apr 04, 2024 08:28:36 | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                       | Admin Domain                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Syslog Server Configuration                                                                                                                                                                                                                                                                                                                                                                     | Syslog settings specified for Domain: "/My Company:0" with Profile name: syslog, Host or IP : 10.1.4.16, Port: 6,514, Protocol: TCP, Error message:null.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Apr 04, 2024 08:28:36 | ✔ Success | Admin Domain | Syslog TLS certificate audit. | Syslog TLS certificate contains Leaf detail as follows: subject:CN=10.1.4.16, issuedBy:CN=AcumenICA, OU=CC, O=Acumen, C=US, validity:Apr 4, 2024 - May 31, 2024, sigAlgo:SHA256WITHRSA, subjectAltName:10.1.4.16, Serial #:4528004407463435150. | Apr 04, 2024 08:28:34 | ✔ Success | Admin Domain | Certificate import in Syslog configuration | Certificate import has been successful,                                                                                                                                                                                                         |                       |           |              |                                            |                                         |
| Apr 04, 2024 08:28:36                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Admin Domain          | Syslog Server Configuration                                                                                                                                                                                                                                                                                                                                                                     | Syslog settings specified for Domain: "/My Company:0" with Profile name: syslog, Host or IP : 10.1.4.16, Port: 6,514, Protocol: TCP, Error message:null.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| Apr 04, 2024 08:28:36                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Admin Domain          | Syslog TLS certificate audit.                                                                                                                                                                                                                                                                                                                                                                   | Syslog TLS certificate contains Leaf detail as follows: subject:CN=10.1.4.16, issuedBy:CN=AcumenICA, OU=CC, O=Acumen, C=US, validity:Apr 4, 2024 - May 31, 2024, sigAlgo:SHA256WITHRSA, subjectAltName:10.1.4.16, Serial #:4528004407463435150.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |
| Apr 04, 2024 08:28:34                                                                                                                                   | ✔ Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Admin Domain          | Certificate import in Syslog configuration                                                                                                                                                                                                                                                                                                                                                      | Certificate import has been successful,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |           |              |                               |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                                                                                                                                                                                                                                 |                       |           |              |                                            |                                         |

| Management Functions                                            | Test cases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ability to configure the cryptographic functionality            | <p>Apr 12, 2024 07:57:43 <span style="color: green;">✔</span> Success Manager <b>Manager CSR File Generation</b> A CSR file (used to generate a CA-signed certificate for trust establishment) was <b>generated by the Manager</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Ability to import X.509v3 certificates to the TOE's trust store | <p>Sep 04, 2023 07:16:06 <span style="color: green;">✔</span> Success Manager <b>Manager Trust Certificate Import</b> A <b>CA-signed certificate</b> (used by the Manager for trust establishment) was imported into the Manager. Certificate : CN=10.1.3.64, O=Acumen, OU=CC, L=, ST=, C=US</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Ability to set the time which is used for timestamps            | <pre>Feb 21 2024 14:20:08 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Feb 21 2024 14:20:08 NSMApp sudo:pam_unix(sudo:session): session closed for user root Feb 21 2024 14:20:15 NSMApp sudo: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/timedatectl set-time 2024-01-01 01:00:00 Feb 21 2024 14:20:15 NSMApp sudo:pam_unix(sudo:session): session opened for user root by admin(uid=0) Jan 1 2024 01:00:00 NSMApp sudo:pam_unix(sudo:session): session closed for user root Jan 1 2024 01:00:26 NSMApp sshd[1054]:debug3: fd 5 is not 0_NONBLOCK Jan 1 2024 01:00:26 NSMApp sshd[1054]:debug1: Forked child 551. Jan 1 2024 01:00:26 NSMApp sshd[1054]:debug3: send_rexec_state: entering fd = 8 config len 1138</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Ability to re-enable an Administrator account                   | <p>Oct 05, 2023 11:56:06 <span style="color: green;">✔</span> Success User <b>Manager Console Login</b> User "Administrator" with login id "admin" successfully logged into the Manager from "10.1.4.16 (10.1.4.16)". Login URI: /intruvert/jsp/module/Login.jsp , URI referer : null , protocol : HTTP/1.1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Ability to manage the trusted public keys database              | <pre>root@NSMApp:/home/admin# tail -f pubKeyAuth.log  [Thu Apr 4 06:59:09 UTC 2024] : Validating Public Key Algorithm  [Thu Apr 4 06:59:09 UTC 2024] : Resetting the permissions of the file .ssh/authorized_keys on local machine  [Thu Apr 4 06:59:09 UTC 2024] : Successfully modified the permissions of .ssh/authorized_keys on remote machine.</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Ability to configure the interaction between TOE components     | <p>Feb 06, 2024 11:38:06 <span style="color: red;">✘</span> Error <b>Trust Establishment Error</b> Device NS3200 is attempting to establish a trust with the Manager, but the device has not been defined in 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 are an exact match) 6.08 Manager</p> <p>Feb 06, 2024 11:38:01 <span style="color: green;">✔</span> Success Manager <b>Secure Sensor Communication</b> <b>Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager.</b></p> <p>Feb 06, 2024 11:38:06 <span style="color: red;">!</span> Failed Manager <b>Secure Sensor Communication</b> <b>Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the shared secret for sensor "NS3200". Please add it in the EMS first. Thanks!</b></p> <p>Feb 06, 2024 11:38:06 <span style="color: red;">!</span> Failed Manager <b>Secure Sensor Communication</b> <b>Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the Shared Secret of sensor NS3200: null</b></p> <p>Feb 06, 2024 12:26:36 <span style="color: green;">✔</span> Success Admin Do... <b>SNMP passphrase generation success.</b> Command channel communication on port 8500 using auth and priv passphrase is generated successfully for sensor 10.1.3.65.</p> <p>Feb 06, 2024 12:26:10 <span style="color: green;">✔</span> Success Manager <b>Trust Establishment</b> <b>Sensor IP NS3200 has established trust with Manager over the CA channel, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US</b></p> <p>Feb 06, 2024 12:26:05 <span style="color: green;">✔</span> Success Manager <b>Secure Sensor Communication</b> <b>Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager.</b></p> |

**Table 8. Sensor FAU\_GEN.1 Audit Records**

| Re-requirement | Auditable Events                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Additional Audit Record Contents | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FAU_GEN.1      | <ul style="list-style-type: none"> <li>Start-up and shut-down of the audit functions</li> <li>Auditable events for the not specified level of audit; and Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).</li> <li>Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed)</li> <li>Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged)</li> <li>Resetting passwords (name of related user ac-</li> </ul> | None                             | <ul style="list-style-type: none"> <li>Start-up and shut-down of the audit functions</li> <li>Auditable events for the not specified level of audit; and Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).</li> <li>Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed)</li> <li>Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged)</li> <li>Resetting passwords (name of related user account shall be logged)</li> </ul> |

```
Apr 08, 2024 08:58:22 Received Sensor Sensor CLI actions Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled"
Apr 08, 2024 08:58:04 Received Sensor Sensor CLI actions Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled"
```

```
Oct 13, 2023 07:00:29 Received Sensor Sensor CLI actions Sensor "NS3200" : "Oct 13 07:00:29 2023: SSHD Password Based Login Success : User = 'admin', Remote Host = 10.1.4.16, Remote Port = 54744"
Oct 13, 2023 12:29:05 Received Sensor Sensor CLI actions Sensor "NS3200" : "Oct 13 12:29:05 2023: SSHD Logout Success : User = 'admin', Remote Host = 10.1.4.16, Remote Port = 38354"
```

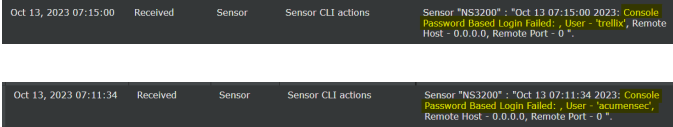
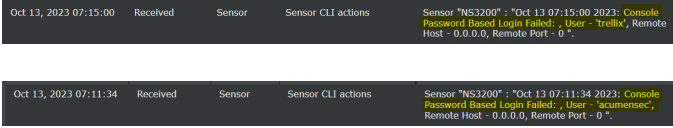
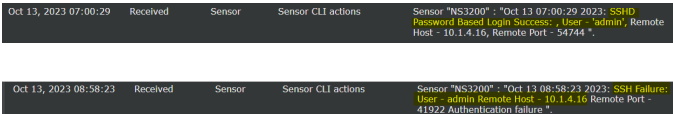
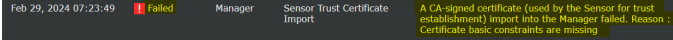
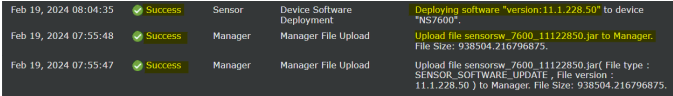
```
Jul 13, 2023 23:33:07 Received Sensor Sensor CLI actions Sensor "NS3200" : "TIME UPDATE - Local: 10.1.3.65 [Display: 37768, RemoteIP: 10.1.3.64, RemotePort: 8593, Old Time = Jul 13 13:33:04 2023, New Time = Jul 13 10:09:07 2023]" /My Company System
```

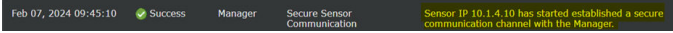
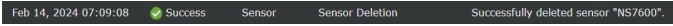
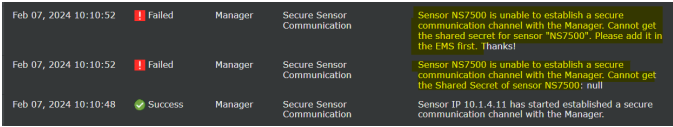
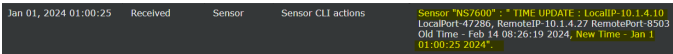
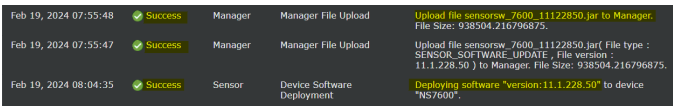
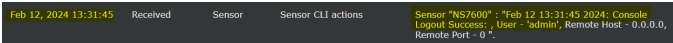
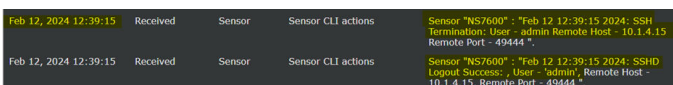
```
Nov 16, 2023 09:17:04 Success Manager Sensor Trust Certificate Import A CA-signed certificate (used by the Sensor for trust establishment) was imported into Sensor: Certificate Alias: NS3200, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US
```

```
Jun 08, 2023 13:53:09 Received Sensor Sensor CLI actions Sensor "NS3200_CCT" : "EXEC CMD : setpassword good2" /My Company admin
Jun 08, 2023 13:53:04 Received Sensor Sensor CLI actions Sensor "NS3200_CCT" : "User 'good2' is created successfully" /My Company System
Jun 08, 2023 13:53:03 Received Sensor Sensor CLI actions Sensor "NS3200_CCT" : "EXEC CMD : adduser good2" /My Company admin
```


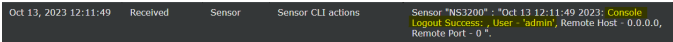
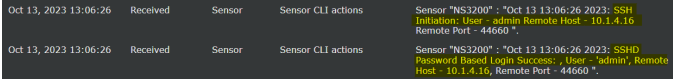
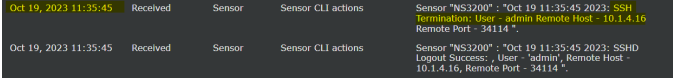
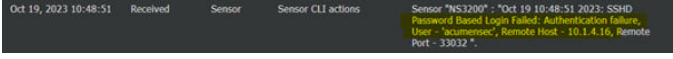
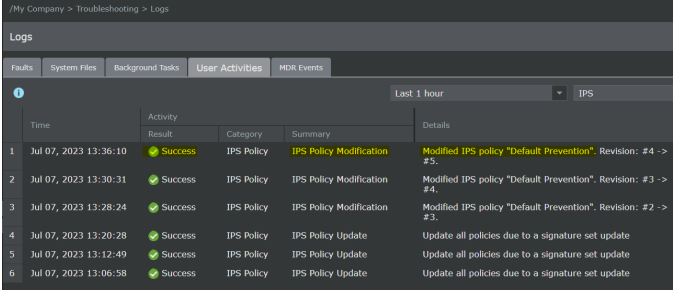
| Re-requirement                | Auditable Events                    | Additional Audit Record Contents | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | count shall be logged)              |                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| FAU_GEN.1/IPS                 | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FAU_GEN_EXT.1                 | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FAU_GEN.2                     | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FAU_STG_EXT.5                 | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CM.M.1                    | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CM.M.2                    | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CM.M.4                    | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CO.P.1/<br>DataEncryption | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CO.P.1/<br>SigGen         | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CO.P.1/<br>Hash           | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_CO.P.1/<br>Keyed-Hash     | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_RBG_EXT.1                 | None                                | None                             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FCS_SSH_C_EXT.1               | Failure to establish an SSH session | Reason for failure               | <pre> NS7600# tail -10f /mnt/config/var/log/messages 2024-02-08T07:30:05.000000+00:00 localhost stunnel - - LOG5[cron]: Updating DH parameters 2024-02-08T07:30:05.000000+00:00 localhost stunnel - - LOG5[main]: Log file reopened 2024-02-08T07:33:53.000000+00:00 localhost stunnel - - LOG5[cron]: DH parameters updated 2024-02-08T07:55:11.000000+00:00 localhost ssh 22326 - - Unable to negotiate with 10.1.4.15 port 22: no matching host key type found. Their offers: ssh-ed25519 2024-02-08T07:55:16.000000+00:00 localhost sshd 22339 - - /home/emb-demo/rfs/fips/R11_1_M_YOSEMITE_BRANCH/rubicon/srcroot/ </pre> |
| FCS_SSH_S_EXT.1               | Failure to establish an SSH session | Reason for failure               | <pre> Feb 08, 2024 14:38:03 Received Sensor Sensor CLI actions Sensor "NS7600" - "Feb 8 14:38:03 2024: SSH Failure: User= admin Remote Host = 10.1.4.15 Remote Port = 40222 Matching publickey not found ." Feb 08, 2024 14:38:03 Received Sensor Sensor CLI actions Sensor "NS7600" - "Feb 8 14:38:03 2024: Public key based Login Failed: Matching publickey not found (User= admin , Remote Host = 10.1.4.15, Remote Port = 40222 ." </pre>                                                                                                                                                                                 |

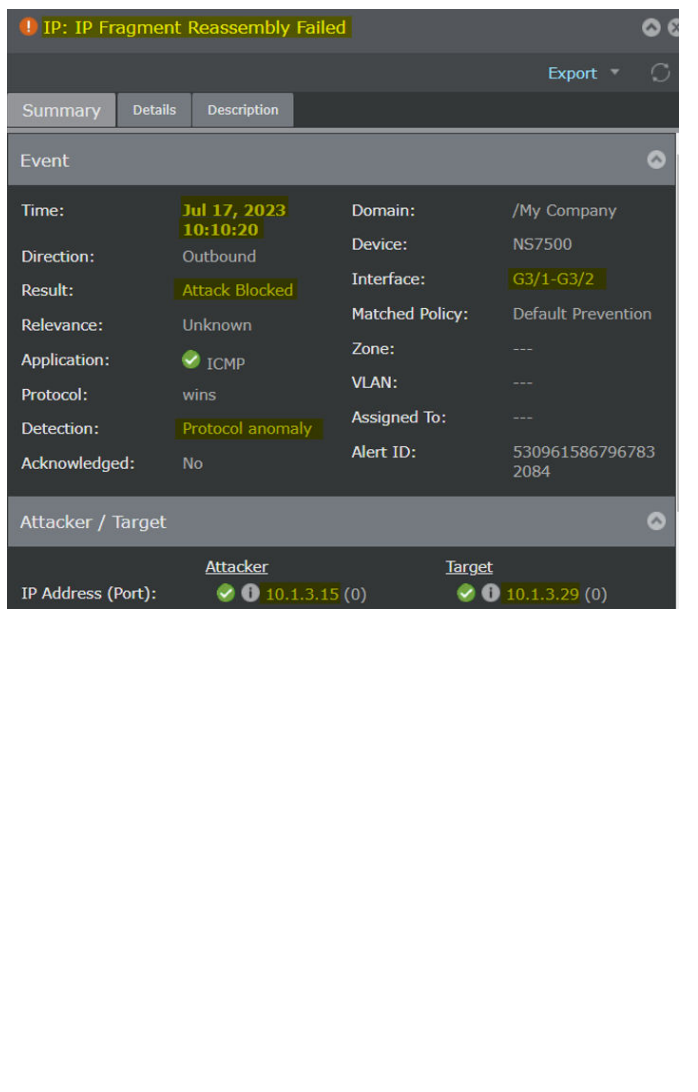
| Re-requirement     | Auditable Events                                                                                                                                                      | Additional Audit Record Contents                      | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FCS_TLS<br>C_EXT.2 | Failure to establish a TLS Session                                                                                                                                    | Reason for failure                                    | <pre> 2024-02-28 13:49:30.979 ERROR [PktLogMIOChannelServerPoolCA- 7] [] iv.core.ControlChannel.NIO:207 - ControlChannelWorkers : run(). /10.1.4.27:8588 =&gt; (/10.1.4.10:49684) IO exception occurred, close the connection.: java.io.IOException: End of socket reached... 2024-02-28 13:49:34.981 INFO [ClassStatusPolling-NS7600] [] iv.core.DiscoveryService:482 - polling for sensor NS7600 failed once, reduce the timeout value and retry: Request fails, problem code is TIMEOUT and explanation is The request has timed out. 2024-02-28 13:49:40.315 WARN [Thread-494] [] iv.core.ControlChannel:197 - fail reading incoming packet --- could be transmit finish java.net.SocketTimeoutException: The finished message cannot be verified. 2024-02-28 13:49:40.315 ERROR [Thread-494] [] iv.core.ControlChannel:80 - *** Connection Impl Error: 10.1.4.10 com.intravert.ext.controlchannel.ControlProtocolException: fail reading at com.intravert.ext.controlchannel.ControlProtocolHandler.getNextMessage(ControlProtocolHandler.java:198) ~[lvctrchannel.jar:7] at com.intravert.ext.controlchannel.SensorIntConnection.protocol[SensorIntConnection.java:68] ~[lvctrchannel.jar:7] at com.intravert.ext.controlchannel.ControlChannelConnection.run(ControlChannelConnection.java:77) ~[lvctrchannel.jar:7] 2024-02-28 13:50:54.985 INFO [ClassStatusPolling-NS7600] [] iv.core.DiscoveryService:510 - Polling for sensor NS7600 failed again the mmi retry: Request fails, problem code is TIMEOUT and explanation is The request has timed out. 2024-02-28 13:52:14.987 INFO [ClassStatusPolling-NS7600] [] iv.core.DiscoveryService:510 - Polling for sensor NS7600 failed again the mm2 retry: Request fails, problem code is TIMEOUT and explanation is The request has timed out. 2024-02-28 13:52:14.987 INFO [ClassStatusPolling-NS7600] [] iv.core.DiscoveryService:228 - (NS7600) A status transition happened ACTIVE --&gt; DISCONNECTED                 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| FCO_CP<br>C_EXT.1  | <ul style="list-style-type: none"> <li>Enabling communications between a pair of components</li> <li>Disabling communications between a pair of components</li> </ul> | Identities of the endpoints pairs enabled or disabled | <p><b>Enabling communications:</b></p> <pre> Feb 07, 2024 09:55:01 Success Admin Domain SNMP passphrase generation success. Command channel communication on port 8500 using auth and prv passphrase is generated successfully for sensor 10.1.4.10. Feb 07, 2024 09:54:48 Success Manager Trust Establishment Sensor IP NS7600 has established trust with Manager over the CA channel. Certificate: CN=10.1.4.10, OU=CC, O=Acumen, L=Rockville, ST=Maryland, C=US Feb 07, 2024 09:54:42 Success Manager Secure Sensor Communication Sensor IP 10.1.4.10 has started established a secure communication channel with the Manager.                 </pre> <p><b>Disabling communications:</b></p> <pre> Feb 14, 2024 07:09:08 Success Sensor Sensor Deletion Successfully deleted sensor "NS7600".                 </pre> <pre> 2024-03-21T13:10:02.000000+00:00 localhost tl -- EMER clllog TYPED CMD: deinstall user - admin 2024-03-21T13:10:02.000000+00:00 localhost tl -- EMER clllog EXEC CMD: deinstall user - admin 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER clllog retain_sensor_ca_cert_to_deinstall: CLI User Input: Retain CA Signed Certificate 2024-03-21T13:10:06.000000+00:00 localhost tl -- EMER clllog ***** 2024-03-21T13:10:06.000000+00:00 localhost tl -- EMER clllog CLI USER CALLS DEINSTALL 2024-03-21T13:10:06.000000+00:00 localhost tl -- EMER clllog ***** 2024-03-21T13:10:06.000000+00:00 localhost tl -- EMER logging get_sensor_private_key [rs2048 case lan:2048 2024-03-21T13:10:06.000000+00:00 localhost tl -- EMER sofa[fn connectSofaUnixSockets] Failed to connect Unix Socket fo r file /usr/local/etc/sofa_nmba_unix_socket.errno 2 (But will retry ,count 1) 2024-03-21T13:10:07.000000+00:00 localhost tl -- EMER sofa[fn connectSofaUnixSockets] Failed to connect Unix Socket fo r file /usr/local/etc/sofa_nmba_unix_socket.errno 2 (But will retry ,count 2) 2024-03-21T13:10:07.000000+00:00 localhost tl -- EMER ctrlch[CCin USER DEINSTALL 2024-03-21T13:10:07.000000+00:00 localhost tl -- EMER ctrlch[CCout] got deinstall, trust 1 inEmHMode 0 2024-03-21T13:10:07.000000+00:00 localhost tl -- EMER ctrlch[CCout] do close (trust:1) IN CHANGE KEYS SNMPv3 Keys(s) successfully changed. 2024-03-21T13:10:08.000000+00:00 localhost tl -- EMER sofa[fn connectSofaUnixSockets] Failed to connect Unix Socket fo r file /usr/local/etc/sofa_nmba_unix_socket.errno 2 (But will retry ,count 3) SNMPv3 Keys(s) successfully changed. 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] close, changeSnpKeys done 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch in closeAndCleanupEMSConn(0) 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch no X509_free_srv_cert done 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch no X509_free_cli_cert done 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch no RSA_free_privkey done 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch out closeAndCleanupEMSConn(0) : Zeroization for the TLS co nnext done. 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] cResetEmHContext for EmIPActive 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] close, cleanup skey 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] close, cleanup scert 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] close, cleanup smscert 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] CC_DOWN, NO TRUST 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch[CCout] CC_DOWN, INSTALL REQUIRED 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER ctrlch postEMSTESTtoBulkFT, sending the Manager Param Chan even t to BulkFT 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER phlog PLin USER DEINSTALL 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER bulkFT bulkFTProcessNSMParamChange: Manager Parameter Changed... lpred. 4 15783747 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER bulkFT bulkFTNSMNotify: Entered... 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER authgw in closeAndCleanupEMSConn(0) 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER bulkFT bulkFTNSMNotify: Trust is not established or Configured from CLI: 0 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER bulkFT bulkFTNSMNotify:3: Raising Disconnect Event 2024-03-21T13:10:09.000000+00:00 localhost tl -- EMER authgwup X509_free_srv_cert done                 </pre> |
| FIA_AFL.<br>1      | Unsuccessful login attempts limit is met or exceeded.                                                                                                                 | Origin of the attempt (e.g., IP address).             | <pre> Feb 09, 2024 14:13:37 Received Sensor Sensor CLI actions Sensor "NS7600": "Feb 9 14:13:37 2024: SSH Failure: User - acumensec Remote Host - 10.1.4.15 Remote Port - 38792 Authentication failure". Feb 09, 2024 14:13:37 Received Sensor Sensor CLI actions Sensor "NS7600": "Feb 9 14:13:37 2024: User 'acumensec' is locked due to too many authentication failures". Feb 09, 2024 14:13:37 Received Sensor Sensor CLI actions Sensor "NS7600": "Feb 9 14:13:37 2024: SSHD Password based Login Failed: Authentication failure, User - 'acumensec', Remote Host - 10.1.4.15, Remote Port - 38792". Feb 09, 2024 14:13:33 Received Sensor Sensor CLI actions Sensor "NS7600": "Feb 9 14:13:33 2024: SSH Failure: User - acumensec Remote Host - 10.1.4.15 Remote Port - 38792 Authentication failure". Feb 09, 2024 14:13:33 Received Sensor Sensor CLI actions Sensor "NS7600": "Feb 9 14:13:33 2024: User 'acumensec' is locked due to too many authentication failures". Feb 09, 2024 14:13:33 Received Sensor Sensor CLI actions Sensor "NS7600": "Feb 9 14:13:33 2024: SSHD Password based Login Failed: Authentication failure, User - 'acumensec', Remote Host - 10.1.4.15, Remote Port - 38792".                 </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| FIA_PM<br>G_EXT.1  | None                                                                                                                                                                  | None                                                  | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

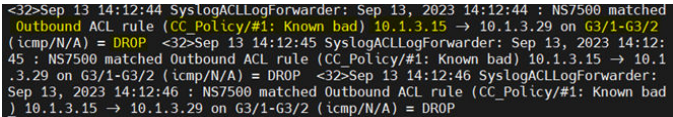
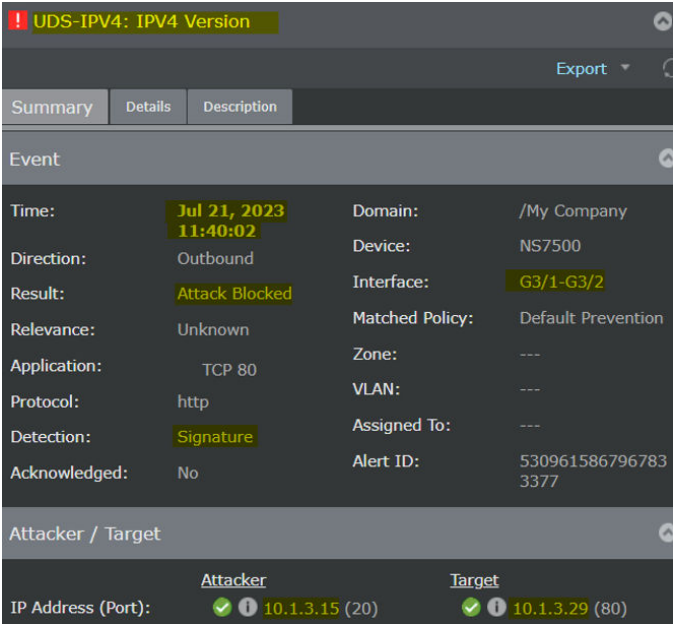
| Re-requirement         | Auditable Events                                           | Additional Audit Record Contents         | Audit Logs                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FIA_UIA_EXT.1          | All use of the identification and authentication mechanism | Origin of the attempt (e.g., IP address) | <p><u>Console:</u></p>  <p><u>SSH:</u></p>    |
| FIA_UAU_EXT.2          | All use of the identification and authentication mechanism | Origin of the attempt (e.g., IP address) | <p><u>Console:</u></p>  <p><u>SSH:</u></p>  |
| FIA_UAU.7              | None                                                       | None                                     | -                                                                                                                                                                                                                 |
| FIA_X509_EXT.1/ITT     | Unsuccessful attempt to validate a certificate             | Reason for failure                       |                                                                                                                               |
| FIA_X509_EXT.3         | None                                                       | None                                     | -                                                                                                                                                                                                                 |
| FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update                    | None                                     |                                                                                                                               |
| FMT_MTD.1/CoreData     | None                                                       | None                                     | -                                                                                                                                                                                                                 |
| FMT_SMF.1              | All management activities of TSF data.                     | None                                     | Refer to the below table [Sensor Management Functions]                                                                                                                                                            |

| Re-quire-ment  | Auditable Events                                                                                                                                                                  | Additional Audit Record Contents                                                                                                                        | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FMT_SM R.2     | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                       |
| FPT_AP W_EXT.1 | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                       |
| FPT_ITT. 1     | <ul style="list-style-type: none"> <li>Initiation of the trusted channel</li> <li>Termination of the trusted channel</li> <li>Failure of the trusted channel functions</li> </ul> | Identification of the initiator and target of failed trusted channels establishment attempt                                                             | <p><u>Initiation of trusted channel:</u></p>  <p><u>Termination of trusted channel:</u></p>  <p><u>Failure of trusted channel functions:</u></p>  |
| FPT_SKP _EXT.1 | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                       |
| FPT_ST M_EXT.1 | Discontinuous changes to time - either Administrator actuated or changed via an automated process                                                                                 | For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address) |                                                                                                                                                                                                                                                                                                                     |
| FPT_TST _EXT.1 | None                                                                                                                                                                              | None                                                                                                                                                    | -                                                                                                                                                                                                                                                                                                                                                                                                       |
| FPT_TU D_EXT.1 | Initiation of update; result of the update attempt (success or failure)                                                                                                           | None                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                     |
| FTA_SSL _EXT.1 | The termination of a local session by the session locking mechanism                                                                                                               | None                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                     |
| FTA_SSL .3     | The termination of a remote session by the session locking mechanism                                                                                                              | None                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                     |



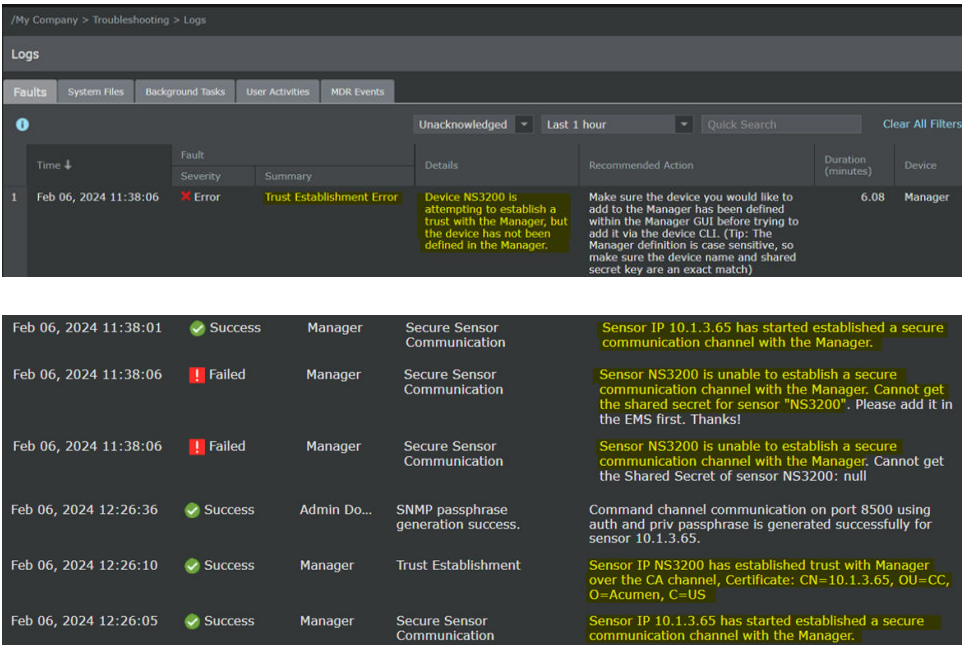
| Re-requirement       | Auditable Events                                                                                                                                                                  | Additional Audit Record Contents                                                                                                  | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| FTA_SSL .4           | The termination of an interactive session                                                                                                                                         | None                                                                                                                              | <p><b>SSH:</b></p>  <p><b>Console:</b></p>                                                                                                                                                                                                         |
| FTA_TAB .1           | None                                                                                                                                                                              | None                                                                                                                              | -                                                                                                                                                                                                                                                                                                                                                                                                                      |
| FTP_TRP .1/<br>Admin | <ul style="list-style-type: none"> <li>Initiation of the trusted channel</li> <li>Termination of the trusted channel</li> <li>Failure of the trusted channel functions</li> </ul> | Identification of the claimed user identity                                                                                       | <p><b>Initiation of the trusted channel:</b></p>  <p><b>Termination of the trusted channel:</b></p>  <p><b>Failure of the trusted channel functions:</b></p>  |
| FMT_SM F.1/IPS       | Modification of an IPS policy element                                                                                                                                             | Identifier or name of the modified IPS policy element (e.g. which signature, baseline, or known-good/known-bad list was modified) |                                                                                                                                                                                                                                                                                                                                    |

| Re-requirement | Auditable Events                                      | Additional Audit Record Contents                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPS_ABD_EXT.1  | Inspected traffic matches an anomaly-based IPS policy | <ul style="list-style-type: none"> <li>• Source and destination IP addresses</li> <li>• The content of the header fields that were determined to match the policy</li> <li>• TOE interface that received the packet</li> <li>• Aspect of the anomaly-based IPS policy rule that triggered the event (e.g. throughput, time of day, frequency, etc.)</li> <li>• Network-based action by the TOE (e.g. allowed, blocked, sent reset to source IP, sent blocking notification to firewall)</li> </ul> |  <p>The screenshot displays an alert window with the following information:</p> <ul style="list-style-type: none"> <li><b>Title:</b> IP: IP Fragment Reassembly Failed</li> <li><b>Summary:</b> Summary, Details, Description</li> <li><b>Event:</b> <ul style="list-style-type: none"> <li>Time: Jul 17, 2023 10:10:20</li> <li>Direction: Outbound</li> <li>Result: Attack Blocked</li> <li>Relevance: Unknown</li> <li>Application: ICMP</li> <li>Protocol: wins</li> <li>Detection: Protocol anomaly</li> <li>Acknowledged: No</li> <li>Domain: /My Company</li> <li>Device: NS7500</li> <li>Interface: G3/1-G3/2</li> <li>Matched Policy: Default Prevention</li> <li>Zone: ---</li> <li>VLAN: ---</li> <li>Assigned To: ---</li> <li>Alert ID: 5309615867967832084</li> </ul> </li> <li><b>Attacker / Target:</b> <ul style="list-style-type: none"> <li>Attacker: 10.1.3.15 (0)</li> <li>Target: 10.1.3.29 (0)</li> </ul> </li> </ul> |

| Re-requirement                  | Auditable Events                                                                                      | Additional Audit Record Contents                                                                                                                                                                                                                                                                                                                                         | Audit Logs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
|---------------------------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--|--|--|--------|--|--|--|---------------------------------|--|--|--|-------|--|--|--|-------|-----------------------|---------|-------------|------------|----------|---------|--------|---------|----------------|------------|-----------|------------|---------|-----------------|--------------------|--------------|--------|-------|-----|-----------|------|-------|-----|------------|-----------|--------------|-----|---------------|----|-----------|---------------------|-------------------|--|--|--|--|----------|--|--------|--------------------|------------------|---|----------------|
| <p>IPS_IPB_EXT.1</p>            | <p>Inspected traffic matches a list of known-good or known-bad addresses applied to an IPS policy</p> | <ul style="list-style-type: none"> <li>• Source and destination IP addresses (and, if applicable, indication of whether the source and/or destination address matched the list)</li> <li>• TOE interface that received the packet.</li> <li>• Network-based action by the TOE (e.g. allowed, blocked, sent reset)</li> </ul>                                             |  <pre> &lt;32&gt;Sep 13 14:12:44 SyslogACLLogForwarder: Sep 13, 2023 14:12:44 : NS7500 matched Outbound ACL rule (CC_Policy/#1: Known bad) 10.1.3.15 -&gt; 10.1.3.29 on G3/1-G3/2 (icmp/N/A) = DROP &lt;32&gt;Sep 13 14:12:45 SyslogACLLogForwarder: Sep 13, 2023 14:12:45 : NS7500 matched Outbound ACL rule (CC_Policy/#1: Known bad) 10.1.3.15 -&gt; 10.1.3.29 on G3/1-G3/2 (icmp/N/A) = DROP &lt;32&gt;Sep 13 14:12:46 SyslogACLLogForwarder: Sep 13, 2023 14:12:46 : NS7500 matched Outbound ACL rule (CC_Policy/#1: Known bad) 10.1.3.15 -&gt; 10.1.3.29 on G3/1-G3/2 (icmp/N/A) = DROP                     </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| <p>IPS_SBD_EXT.1</p>            | <p>Inspected traffic matches a signature-based IPS rule with logging enabled</p>                      | <ul style="list-style-type: none"> <li>• Name or identifier of the matched signature.</li> <li>• Source and destination IP addresses</li> <li>• The content of the header fields that were determined to match the signature</li> <li>• TOE interface that received the packet</li> <li>• Network-based action by the TOE (e.g. allowed, blocked, sent reset)</li> </ul> |  <table border="1"> <thead> <tr> <th colspan="4">! UDS-IPV4: IPV4 Version</th> </tr> <tr> <th colspan="4">Export</th> </tr> <tr> <th colspan="4">Summary   Details   Description</th> </tr> </thead> <tbody> <tr> <td colspan="4">Event</td> </tr> <tr> <td>Time:</td> <td>Jul 21, 2023 11:40:02</td> <td>Domain:</td> <td>/My Company</td> </tr> <tr> <td>Direction:</td> <td>Outbound</td> <td>Device:</td> <td>NS7500</td> </tr> <tr> <td>Result:</td> <td>Attack Blocked</td> <td>Interface:</td> <td>G3/1-G3/2</td> </tr> <tr> <td>Relevance:</td> <td>Unknown</td> <td>Matched Policy:</td> <td>Default Prevention</td> </tr> <tr> <td>Application:</td> <td>TCP 80</td> <td>Zone:</td> <td>---</td> </tr> <tr> <td>Protocol:</td> <td>http</td> <td>VLAN:</td> <td>---</td> </tr> <tr> <td>Detection:</td> <td>Signature</td> <td>Assigned To:</td> <td>---</td> </tr> <tr> <td>Acknowledged:</td> <td>No</td> <td>Alert ID:</td> <td>5309615867967833377</td> </tr> <tr> <td colspan="4">Attacker / Target</td> </tr> <tr> <td></td> <td>Attacker</td> <td></td> <td>Target</td> </tr> <tr> <td>IP Address (Port):</td> <td>✓ 10.1.3.15 (20)</td> <td>✓</td> <td>10.1.3.29 (80)</td> </tr> </tbody> </table> | ! UDS-IPV4: IPV4 Version |  |  |  | Export |  |  |  | Summary   Details   Description |  |  |  | Event |  |  |  | Time: | Jul 21, 2023 11:40:02 | Domain: | /My Company | Direction: | Outbound | Device: | NS7500 | Result: | Attack Blocked | Interface: | G3/1-G3/2 | Relevance: | Unknown | Matched Policy: | Default Prevention | Application: | TCP 80 | Zone: | --- | Protocol: | http | VLAN: | --- | Detection: | Signature | Assigned To: | --- | Acknowledged: | No | Alert ID: | 5309615867967833377 | Attacker / Target |  |  |  |  | Attacker |  | Target | IP Address (Port): | ✓ 10.1.3.15 (20) | ✓ | 10.1.3.29 (80) |
| ! UDS-IPV4: IPV4 Version        |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Export                          |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Summary   Details   Description |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Event                           |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Time:                           | Jul 21, 2023 11:40:02                                                                                 | Domain:                                                                                                                                                                                                                                                                                                                                                                  | /My Company                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Direction:                      | Outbound                                                                                              | Device:                                                                                                                                                                                                                                                                                                                                                                  | NS7500                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Result:                         | Attack Blocked                                                                                        | Interface:                                                                                                                                                                                                                                                                                                                                                               | G3/1-G3/2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Relevance:                      | Unknown                                                                                               | Matched Policy:                                                                                                                                                                                                                                                                                                                                                          | Default Prevention                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Application:                    | TCP 80                                                                                                | Zone:                                                                                                                                                                                                                                                                                                                                                                    | ---                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Protocol:                       | http                                                                                                  | VLAN:                                                                                                                                                                                                                                                                                                                                                                    | ---                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Detection:                      | Signature                                                                                             | Assigned To:                                                                                                                                                                                                                                                                                                                                                             | ---                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Acknowledged:                   | No                                                                                                    | Alert ID:                                                                                                                                                                                                                                                                                                                                                                | 5309615867967833377                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| Attacker / Target               |                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
|                                 | Attacker                                                                                              |                                                                                                                                                                                                                                                                                                                                                                          | Target                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |
| IP Address (Port):              | ✓ 10.1.3.15 (20)                                                                                      | ✓                                                                                                                                                                                                                                                                                                                                                                        | 10.1.3.29 (80)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                          |  |  |  |        |  |  |  |                                 |  |  |  |       |  |  |  |       |                       |         |             |            |          |         |        |         |                |            |           |            |         |                 |                    |              |        |       |     |           |      |       |     |            |           |              |     |               |    |           |                     |                   |  |  |  |  |          |  |        |                    |                  |   |                |

**Table 9. Sensor Management Functions**

| Management Functions                                                                                                      | Test cases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ability to administer the TOE locally and remotely                                                                        | <p>SSH:</p> <pre>Oct 13, 2023 07:00:29 Received Sensor Sensor CLI actions Sensor "NS3200" : "Oct 13 07:00:29 2023: SSHD Password Based Login Success: , User - 'admin', Remote Host - 10.1.4.16, Remote Port - 54744 "</pre> <p>Console:</p> <pre>Oct 13, 2023 10:24:22 Received Sensor Sensor CLI actions Sensor "NS3200" : "Oct 13 10:24:22 2023: Console Password Based Login Success: , User - 'admin', Remote Host - 0.0.0.0, Remote Port - 0 "</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Ability to configure the access banner                                                                                    | <pre>Apr 05, 2024 15:34:40 Success Sensor Sensor Banner Message Template Creation or Update Created or updated the customized Sensor Banner message template of Admin Domain "My Company" for messages "*" * * Authorized users only. Unauthorized users will be prosecuted to the full extent of the law!! * * *</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Ability to configure the session inactivity time before session termination or locking                                    | <pre>2024-04-08T09:19:10.000000+00:00 localhost tl - - - EMER gam checkTrustDNSProxySetting: Proxy config not available 2024-04-08T09:19:17.000000+00:00 localhost tl - - - EMER clllog TYPED CMD: set console timeout 20 2024-04-08T09:19:17.000000+00:00 localhost tl - - - EMER clllog EXEC CMD: set console timeout 20 user - admin 2024-04-08T09:19:17.000000+00:00 localhost tl - - - EMER ivsnor persist vty timeout configuration : 20 2024-04-08T09:19:23.000000+00:00 localhost tl - - - EMER ivsnor var_chassisGrp: tempId:1, temp:22.000000</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates | <p>Positive update:</p> <pre>2024-04-01T13:24:40.000000+00:00 localhost tl - - - EMER clllog TYPED CMD: loadimage scp /home/acumensec/ns_builds/final_builds/sensorImage.3200.jar 2024-04-01T13:24:40.000000+00:00 localhost tl - - - EMER clllog EXEC CMD : loadimage scp /home/acumensec/ns_builds/final_builds/sensorImage.3200.jar user - admin 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER clllog  stat ret: 0 size: 1024 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER clllog encrypted file readsize: 1024 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER logging get_sensor_asymmetric_private_key : Getting sensor's lifetime asymmetric key 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER logging get_sensor_asymmetric_private_key : Calculated Checksum = 0002296b 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER logging get_sensor_asymmetric_private_key : Read checksum = 226b 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER clllog  getAsymmetricPrivateKeyFromProm :: key retrieval success 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER clllog  priv key len : 1025 2024-04-01T13:24:45.000000+00:00 localhost tl - - - EMER clllog  decrypted result: -1 2024-04-01T13:24:48.000000+00:00 localhost tl - - - EMER clllog  stat ret: 0 size: 0 2024-04-01T13:24:48.000000+00:00 localhost tl - - - EMER clllog decryptTheEncryptedSSKeyFile: removed the key file 2024-04-01T13:24:51.000000+00:00 localhost tl - - - EMER clllog systemd_exec: Executed command NO DISPLAY IN FIPSIMAGE, L:127960, status:1 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog  stat ret: 0 size: 1024 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog encrypted file readsize: 1024 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER logging get_sensor_asymmetric_private_key : Getting sensor's lifetime asymmetric key 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER logging get_sensor_asymmetric_private_key : Calculated Checksum = 0002296b 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER logging get_sensor_asymmetric_private_key : Read checksum = 226b 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog  getAsymmetricPrivateKeyFromProm :: key retrieval success 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog  priv key len : 1025 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog  decrypted result: -1 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog  stat ret: 0 size: 0 2024-04-01T13:25:01.000000+00:00 localhost tl - - - EMER clllog decryptTheEncryptedSSKeyFile: removed the key file SSH Key based authentication failed , try with password 2024-04-01T13:25:10.000000+00:00 localhost tl - - - EMER gam gamingIneDeferredUpdateAndConfig : Global GAM Engine Instance is NULL 2024-04-01T13:25:11.000000+00:00 localhost tl - - - EMER clllog systemd_exec: Executed command NO DISPLAY IN FIPSIMAGE, L:127960, status:1 2024-04-01T13:25:11.000000+00:00 localhost tl - - - EMER ivsnor  No prev. OWMGRADE_CONFID file found 2024-04-01T13:25:11.000000+00:00 localhost tl - - - EMER ivsnor Previous version = 11.1.20.41 2024-04-01T13:25:11.000000+00:00 localhost tl - - - EMER ivsnor New Image version is : 11.1.17.2 2024-04-01T13:25:11.000000+00:00 localhost tl - - - EMER ivsnor system_type read is: 118 New Image model is : 118 2024-04-01T13:25:11.000000+00:00 localhost tl - - - EMER ivsnor New Image is : 18461266(Hexbb1102) 2024-04-01T13:25:12.000000+00:00 localhost tl - - - EMER clllog R-SPLIT: Backed up(0) the new image(11.1.17.2). 2024-04-01T13:25:12.000000+00:00 localhost tl - - - EMER ivsnor imgDwnlApplyFile : Deleting ssh keys on sensor version change updating grub for prod going for grub install ... grub install successful. Unpacking newer shell scripts All newer shell scripts copied 2024-04-01T13:28:11.000000+00:00 localhost tl - - - EMER ivsnor Processing HDA1. updatehdai.sh THIS IS A R SERIES(MFE_RFS) SYSTEM Comparing /mnt/part1/boot/bzImage to ./boot/bzImage Comparing /mnt/part1/boot/initrd to ./boot/initrd The kernel/initrd has changed. updating. 2024-04-01T13:28:14.000000+00:00 localhost tl - - - EMER ivsnor Updating rootfs.afio updateafs.sh THIS IS A R SERIES(MFE_RFS) SYSTEM Copying /tftpboot/rootfs.afio to /mnt/ramdisk/afs/ 2024-04-01T13:28:19.000000+00:00 localhost tl - - - EMER ivsnor Updating apps.tgz 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Persisting s1byte L7AE 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Calling onetime for the 2nd time creating cliDowngradeVersion file with CLI VERSION=0x0A010503 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Processing diag apps. 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Updating bcm.tgz Done 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor SW version : 11.1.17 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor QA version 2 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Success creating and persisting imageConfig file 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Calling onetime for the 3rd time creating cliDowngradeVersion file with CLI VERSION=0x0A010503 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER ivsnor Image Update completed 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER logging postSbcSysEvent:wrote 20 bytes out of 20 bytes 2024-04-01T13:28:22.000000+00:00 localhost tl - - - EMER logging THIS IS A FIPS IMAGE return value: 1 New image is FIPS image</pre> <p>Negative update:</p> <pre>Oct 26, 2023 14:18:15 Failed Manager Manager File Upload Failed to upload file corrupted_sensorsw_3200_11122838.jar to Manager. Please check logs for reason. File Size: 380113.1142578125.</pre> |

| Management Functions                                                                                                                             | Test cases                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                             |                                                                                                                        |                                                                                                                                                                                                                                                                      |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|----------|-------------------------|--------------------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------|-----------------------|---------|-----------------------------|--|----------------------------------------------------------------------------------------------|--|--|-----------------------|--------|-----------------------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|-----------------------|--------|-----------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------|--|--|-----------------------|---------|-------------|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------|--|--|-----------------------|---------|---------|---------------------|---------------------------------------------------------------------------------------------------------------------------|--|--|-----------------------|---------|---------|-----------------------------|----------------------------------------------------------------------------------------------|--|--|
| Ability to configure the authentication failure parameters for FIA_AFL.1                                                                         | <table border="1"> <tr> <td>Oct 19, 2023 10:56:16</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "User 'acumensec' is successfully unlocked".</td> </tr> <tr> <td>Oct 19, 2023 10:56:16</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "EXEC CMD : unlockuser acumensec".</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Oct 19, 2023 10:56:16       | Received                                                                                                               | Sensor                                                                                                                                                                                                                                                               | Sensor CLI actions              | Sensor "NS3200" : "User 'acumensec' is successfully unlocked".                                                                                                             | Oct 19, 2023 10:56:16 | Received | Sensor                  | Sensor CLI actions | Sensor "NS3200" : "EXEC CMD : unlockuser acumensec".           |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Oct 19, 2023 10:56:16                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "User 'acumensec' is successfully unlocked".                                                                                                                                                                                                       |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Oct 19, 2023 10:56:16                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "EXEC CMD : unlockuser acumensec".                                                                                                                                                                                                                 |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full); | <table border="1"> <tr> <td>Apr 08, 2024 08:58:22</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled".</td> </tr> <tr> <td>Apr 08, 2024 08:58:04</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled".</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Apr 08, 2024 08:58:22       | Received                                                                                                               | Sensor                                                                                                                                                                                                                                                               | Sensor CLI actions              | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled".                                                                                                              | Apr 08, 2024 08:58:04 | Received | Sensor                  | Sensor CLI actions | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled". |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Apr 08, 2024 08:58:22                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled".                                                                                                                                                                                                        |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Apr 08, 2024 08:58:04                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled".                                                                                                                                                                                                       |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to modify the behaviour of the transmission of audit data to an external IT entity                                                       | <table border="1"> <tr> <td>Apr 08, 2024 08:58:22</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled".</td> </tr> <tr> <td>Apr 08, 2024 08:58:04</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled".</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Apr 08, 2024 08:58:22       | Received                                                                                                               | Sensor                                                                                                                                                                                                                                                               | Sensor CLI actions              | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled".                                                                                                              | Apr 08, 2024 08:58:04 | Received | Sensor                  | Sensor CLI actions | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled". |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Apr 08, 2024 08:58:22                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Enabled".                                                                                                                                                                                                        |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Apr 08, 2024 08:58:04                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "EXEC CMD : Manager Audit Logging Disabled".                                                                                                                                                                                                       |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to configure the cryptographic functionality                                                                                             | <table border="1"> <tr> <td>Apr 12, 2024 08:11:45</td> <td>Success</td> <td>Manager</td> <td>Sensor CSR File Generation</td> <td>A CSR file (used to generate a CA-signed certificate for trust establishment) was generated by Sensor: Certificate Alias: NS3200.</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Apr 12, 2024 08:11:45       | Success                                                                                                                | Manager                                                                                                                                                                                                                                                              | Sensor CSR File Generation      | A CSR file (used to generate a CA-signed certificate for trust establishment) was generated by Sensor: Certificate Alias: NS3200.                                          |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Apr 12, 2024 08:11:45                                                                                                                            | Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Manager                     | Sensor CSR File Generation                                                                                             | A CSR file (used to generate a CA-signed certificate for trust establishment) was generated by Sensor: Certificate Alias: NS3200.                                                                                                                                    |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to import X.509v3 certificates to the TOE's trust store                                                                                  | <table border="1"> <tr> <td>Nov 16, 2023 09:17:04</td> <td>Success</td> <td>Manager</td> <td>Sensor Trust Certificate Import</td> <td>A CA-signed certificate (used by the Sensor for trust establishment) was imported into Sensor: Certificate Alias: NS3200, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Nov 16, 2023 09:17:04       | Success                                                                                                                | Manager                                                                                                                                                                                                                                                              | Sensor Trust Certificate Import | A CA-signed certificate (used by the Sensor for trust establishment) was imported into Sensor: Certificate Alias: NS3200, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Nov 16, 2023 09:17:04                                                                                                                            | Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Manager                     | Sensor Trust Certificate Import                                                                                        | A CA-signed certificate (used by the Sensor for trust establishment) was imported into Sensor: Certificate Alias: NS3200, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US                                                                                           |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to set the time which is used for timestamps                                                                                             | <table border="1"> <tr> <td>Jul 13, 2023 23:33:07</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : " TIME UPDATE : LocalIP-10.1.3.65 LocalPort-37766, RemoteIP-10.1.3.64 RemotePort-8503 Old Time - Jul 13 15:33:04 2023, New Time - Jul 13 18:03:07 2023".</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Jul 13, 2023 23:33:07       | Received                                                                                                               | Sensor                                                                                                                                                                                                                                                               | Sensor CLI actions              | Sensor "NS3200" : " TIME UPDATE : LocalIP-10.1.3.65 LocalPort-37766, RemoteIP-10.1.3.64 RemotePort-8503 Old Time - Jul 13 15:33:04 2023, New Time - Jul 13 18:03:07 2023". |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Jul 13, 2023 23:33:07                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : " TIME UPDATE : LocalIP-10.1.3.65 LocalPort-37766, RemoteIP-10.1.3.64 RemotePort-8503 Old Time - Jul 13 15:33:04 2023, New Time - Jul 13 18:03:07 2023".                                                                                           |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to re-enable an Administrator account                                                                                                    | <table border="1"> <tr> <td>Oct 19, 2023 10:56:16</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "User 'acumensec' is successfully unlocked".</td> </tr> <tr> <td>Oct 19, 2023 10:56:16</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "EXEC CMD : unlockuser acumensec".</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Oct 19, 2023 10:56:16       | Received                                                                                                               | Sensor                                                                                                                                                                                                                                                               | Sensor CLI actions              | Sensor "NS3200" : "User 'acumensec' is successfully unlocked".                                                                                                             | Oct 19, 2023 10:56:16 | Received | Sensor                  | Sensor CLI actions | Sensor "NS3200" : "EXEC CMD : unlockuser acumensec".           |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Oct 19, 2023 10:56:16                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "User 'acumensec' is successfully unlocked".                                                                                                                                                                                                       |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Oct 19, 2023 10:56:16                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "EXEC CMD : unlockuser acumensec".                                                                                                                                                                                                                 |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to manage the trusted public keys database                                                                                               | <table border="1"> <tr> <td>Apr 08, 2024 09:05:03</td> <td>Received</td> <td>Sensor</td> <td>Sensor CLI actions</td> <td>Sensor "NS3200" : "User 'acumensec' Public-Key Imported successfully from remote machine : 10.1.4.16".</td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Apr 08, 2024 09:05:03       | Received                                                                                                               | Sensor                                                                                                                                                                                                                                                               | Sensor CLI actions              | Sensor "NS3200" : "User 'acumensec' Public-Key Imported successfully from remote machine : 10.1.4.16".                                                                     |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Apr 08, 2024 09:05:03                                                                                                                            | Received                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Sensor                      | Sensor CLI actions                                                                                                     | Sensor "NS3200" : "User 'acumensec' Public-Key Imported successfully from remote machine : 10.1.4.16".                                                                                                                                                               |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Ability to configure the interaction between TOE components                                                                                      |  <p>The screenshot shows a log viewer interface with the following content:</p> <p>Logs</p> <p>Unacknowledged Last 1 hour Quick Search Clear All Filters</p> <table border="1"> <thead> <tr> <th>Time ↓</th> <th>Severity</th> <th>Summary</th> <th>Details</th> <th>Recommended Action</th> <th>Duration (minutes)</th> <th>Device</th> </tr> </thead> <tbody> <tr> <td>1 Feb 06, 2024 11:38:06</td> <td>Error</td> <td>Trust Establishment Error</td> <td>Device NS3200 is attempting to establish a trust with the Manager, but the device has not been defined in the Manager.</td> <td>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 are an exact match)</td> <td>6.08</td> <td>Manager</td> </tr> <tr> <td>Feb 06, 2024 11:38:01</td> <td>Success</td> <td>Secure Sensor Communication</td> <td></td> <td>Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager.</td> <td></td> <td></td> </tr> <tr> <td>Feb 06, 2024 11:38:06</td> <td>Failed</td> <td>Secure Sensor Communication</td> <td></td> <td>Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the shared secret for sensor "NS3200". Please add it in the EMS first. Thanks!</td> <td></td> <td></td> </tr> <tr> <td>Feb 06, 2024 11:38:06</td> <td>Failed</td> <td>Secure Sensor Communication</td> <td></td> <td>Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the Shared Secret of sensor NS3200: null</td> <td></td> <td></td> </tr> <tr> <td>Feb 06, 2024 12:26:36</td> <td>Success</td> <td>Admin Do...</td> <td>SNMP passphrase generation success.</td> <td>Command channel communication on port 8500 using auth and priv passphrase is generated successfully for sensor 10.1.3.65.</td> <td></td> <td></td> </tr> <tr> <td>Feb 06, 2024 12:26:10</td> <td>Success</td> <td>Manager</td> <td>Trust Establishment</td> <td>Sensor IP NS3200 has established trust with Manager over the CA channel, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US</td> <td></td> <td></td> </tr> <tr> <td>Feb 06, 2024 12:26:05</td> <td>Success</td> <td>Manager</td> <td>Secure Sensor Communication</td> <td>Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager.</td> <td></td> <td></td> </tr> </tbody> </table> | Time ↓                      | Severity                                                                                                               | Summary                                                                                                                                                                                                                                                              | Details                         | Recommended Action                                                                                                                                                         | Duration (minutes)    | Device   | 1 Feb 06, 2024 11:38:06 | Error              | Trust Establishment Error                                      | Device NS3200 is attempting to establish a trust with the Manager, but the device has not been defined in 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 are an exact match) | 6.08 | Manager | Feb 06, 2024 11:38:01 | Success | Secure Sensor Communication |  | Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager. |  |  | Feb 06, 2024 11:38:06 | Failed | Secure Sensor Communication |  | Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the shared secret for sensor "NS3200". Please add it in the EMS first. Thanks! |  |  | Feb 06, 2024 11:38:06 | Failed | Secure Sensor Communication |  | Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the Shared Secret of sensor NS3200: null |  |  | Feb 06, 2024 12:26:36 | Success | Admin Do... | SNMP passphrase generation success. | Command channel communication on port 8500 using auth and priv passphrase is generated successfully for sensor 10.1.3.65. |  |  | Feb 06, 2024 12:26:10 | Success | Manager | Trust Establishment | Sensor IP NS3200 has established trust with Manager over the CA channel, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US |  |  | Feb 06, 2024 12:26:05 | Success | Manager | Secure Sensor Communication | Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager. |  |  |
| Time ↓                                                                                                                                           | Severity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Summary                     | Details                                                                                                                | Recommended Action                                                                                                                                                                                                                                                   | Duration (minutes)              | Device                                                                                                                                                                     |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| 1 Feb 06, 2024 11:38:06                                                                                                                          | Error                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Trust Establishment Error   | Device NS3200 is attempting to establish a trust with the Manager, but the device has not been defined in 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 are an exact match) | 6.08                            | Manager                                                                                                                                                                    |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Feb 06, 2024 11:38:01                                                                                                                            | Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Secure Sensor Communication |                                                                                                                        | Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager.                                                                                                                                                                         |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Feb 06, 2024 11:38:06                                                                                                                            | Failed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Secure Sensor Communication |                                                                                                                        | Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the shared secret for sensor "NS3200". Please add it in the EMS first. Thanks!                                                                                      |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Feb 06, 2024 11:38:06                                                                                                                            | Failed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Secure Sensor Communication |                                                                                                                        | Sensor NS3200 is unable to establish a secure communication channel with the Manager. Cannot get the Shared Secret of sensor NS3200: null                                                                                                                            |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Feb 06, 2024 12:26:36                                                                                                                            | Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Admin Do...                 | SNMP passphrase generation success.                                                                                    | Command channel communication on port 8500 using auth and priv passphrase is generated successfully for sensor 10.1.3.65.                                                                                                                                            |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Feb 06, 2024 12:26:10                                                                                                                            | Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Manager                     | Trust Establishment                                                                                                    | Sensor IP NS3200 has established trust with Manager over the CA channel, Certificate: CN=10.1.3.65, OU=CC, O=Acumen, C=US                                                                                                                                            |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |
| Feb 06, 2024 12:26:05                                                                                                                            | Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Manager                     | Secure Sensor Communication                                                                                            | Sensor IP 10.1.3.65 has started established a secure communication channel with the Manager.                                                                                                                                                                         |                                 |                                                                                                                                                                            |                       |          |                         |                    |                                                                |                                                                                                                        |                                                                                                                                                                                                                                                                      |      |         |                       |         |                             |  |                                                                                              |  |  |                       |        |                             |  |                                                                                                                                                                                 |  |  |                       |        |                             |  |                                                                                                                                           |  |  |                       |         |             |                                     |                                                                                                                           |  |  |                       |         |         |                     |                                                                                                                           |  |  |                       |         |         |                             |                                                                                              |  |  |

## **COPYRIGHT**

2024 © Musarubra US LLC

Trellix and FireEye are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC, and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Skyhigh Security is the trademark of Skyhigh Security LLC and its affiliates in the US and other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

