Common Criteria Evaluated Configuration Guide (CCECG) for TPS v6.3

Trend Micro TippingPoint Threat Protection System

Document Version 1.0

September 2024

Prepared For:

Trend Micro
11305 Alterra Parkway
Austin, TX 78758
https://www.trendmicro.com

Prepared By:

Leidos AT&E Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046
www.leidos.com

Abstract

This document provides administrative guidance for configuring Trend Micro in accordance with its Common Criteria evaluated configuration.

Table of Contents

1 Introduction

This document provides administrative guidance information for the Trend Micro TippingPoint Threat Protection System. This document describes preparative and operational procedures for the use of the Trend Micro TippingPoint Threat Protection System in its Common Criteria evaluated configuration. This document is a supplement to the Trend Micro TippingPoint Threat Protection Command Line Interface Reference.

1.1 Purpose

This document has been developed to supplement information in the Trend Micro TippingPoint Threat Protection Command Line Interface Reference, so as to satisfy requirements for the content of administrative guidance described in assurance activities specified in the following National Information Assurance Partnership (NIAP) Protection Profile (PP):

collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020, [CPP_ND_V2.2E] including the following optional and selection-based SFRs: FAU_STG.1, FAU_STG_EXT.3/LocSpace, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, and FMT_MOF.1/Functions

- The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:
    - CPP_ND_V2.2E
        - TD0792 – NIT Technical Decision: FIA_PMG_EXT.1 – TSS EA not in line with SFR
        - TD0738 – NIT Technical Decision for Link to Allowed-With List
        - TD0638 – NIT Technical Decision for Key Pair Generation for Authentication
        - TD0636 – NIT Technical Decision for Clarification of Public Key User Authentication for SSH
        - TD0632 – NIT Technical Decision for Consistency with Time Data for vNDs
        - TD0631 – NIT Technical Decision for clarification of public key authentication for SSH Server
        - TD0592 – NIT Technical Decision for Local Storage of Audit Records
        - TD0591 – NIT Technical Decision for Virtual TOEs and hypervisors
        - TD0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3
        - TD0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e
        - TD0572 – NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers
        - TD0571 – NiT Technical Decision for Guidance on how to handle FIA_AFL.1
        - TD0570 – NiT Technical Decision for Clarification about FIA_AFL.1
        - TD0564 – NiT Technical Decision for Vulnerability Analysis Search Criteria
        - TD0563 – NiT Technical Decision for Clarification of audit date information

- TD0547 – NIT Technical Decision for Clarification on developer disclosure of AVA_VAN
- TD0536 – NIT Technical Decision for Update Verification Inconsistency

1.2 References

[ST] Trend Micro TippingPoint Threat Protection System v6.3 Security Target, Version 1.0, September 23, 2024

[CLI] Trend Micro TippingPoint Threat Protection System Command Line Interface Reference, April 2024

[HSIG] Trend Micro TippingPoint Threat Protection System Hardware Specification and Installation Guide, April 2024

[DG] Trend Micro TippingPoint Virtual Threat Protection System (vTPS) User Guide, April 2024

1.3 Abbreviations

The following abbreviations are used in this document:

CA	Certificate Authority
CC	Common Criteria
CLI	Command Line Interface
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
KM	Kernel Virtual Machine
LSM	Local Security Manager
NIAP	National Information Assurance Partnership
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SMS	Security Management System
SSH	Secure Shell
TCP	Transmission Control Protocol
TSF	TOE Security Functions
TOE	Target of Evaluation
VM	Virtual Machine
VS	Virtualization System
vTPS	Trend Micro TippingPoint Threat Protection System virtual appliance model

2 Configuration for Common Criteria

The following Trend Micro TippingPoint Threat Protection System devices running software version 6.3 (collectively, the Target of Evaluation or TOE) have been evaluated as satisfying the requirements specified in the PP listed in Section 1.1 above:

Appliance Model
TPS 1100TX
TPS 5500TX
TPS 8200TX
TPS 8400TX
TPS 8600TXE
TPS 9200TXE
vTPS

The 1100TX includes one I/O module slot, the 5500TX, 8200TX, 8600TXE, and 9200TXE include two I/O module slots, and the 8400TX includes four I/O module slots. The following standard I/O modules are supported for the 1100TX, 5500TX, 8200TX, and 8400TX devices.

Standard I/O module	Trend Micro part number
TippingPoint 6-Segment Gig-T	TPNN0059
TippingPoint 6-Segment GbE SFP	TPNN0068
TippingPoint 4-Segment 10 GbE SFP+	TPNN0060
TippingPoint 1-Segment 40 GbE QSFP+	TPNN0069

The following standard I/O modules are supported solely for the 8600TXE and 9200TXE devices.

Standard I/O module	Trend Micro part number
TippingPoint 6-Segment 25/10/1 GbE SFP28	TPNN0370
TippingPoint 4-Segment 100/40 GbE QSFP28	TPNN0371

The following table identifies the processors used in each of the hardware appliances.

Device	Main Processor	Storage	Network Ports	Operating System / Software
TPS 1100TX	Intel Pentium D-1517 (Broadwell) CPU / 4 Cores, 8 Threads, 1.6GHz, 25W TDP	Storage = 8GB CFAST (Internal) / 8GB (External)	One IOM Slot Hot-Swappable Up to 6 1GE Segments, Up to 4 10GE Segments, 1 40GE Segment	Linux-5.4.58-yocto-standard OpenSSL 3.0.9

Device	Main Processor	Storage	Network Ports	Operating System / Software
TPS 5500TX	Intel Xeon D-1559 (Broadwell) CPU / 12 Cores, 24 Threads, 1.5GHz, 45W TDP	Storage = 32GB CFAST (Internal) / 32GB (External)	Two IOM Slots, Hot-Swappable Up to 12 1GE Segments, Up to 8 10GE Segments, Up to 2 40GE Segments	Linux-5.4.58-yocto-standard OpenSSL 3.0.9
TPS 8200TX	2x Intel Xeon E5-2648Lv3 (Haswell) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W TDP	Storage = 32GB CFAST (Internal) / 32GB (External)	Two IOM Slots, Hot-Swappable Up to 12 1GE Segments, Up to 8 10GE Segments, Up to 2 40GE Segments	Linux-5.4.58-yocto-standard OpenSSL 3.0.9
TPS 8400TX	2x Intel Xeon E5-2648Lv3 (Haswell) CPUs / 12 Cores, 24 Threads, 1.8GHz, 75W TDP	Storage = 128 GB DRAM (Internal) / 32 GB (External)	Four IOM Slots, Hot-Swappable Up to 24 1GE Segments, Up to 16 10GE Segments, Up to 4 40GE Segments	Linux-5.4.58-yocto-standard OpenSSL 3.0.9
TPS 8600TXE	2x Intel Xeon Gold 5318N (Ice Lake) - 80 Cores @ 2.0GHz	Storage = 32GB CFAST (Internal) / 240GB NVMe SSD (External)	Two IOM Slots, Hot-Swappable Up to 12 25GE/10GE/1GE Segments, Up to 8 100GE/40GE Segments	Linux-5.4.58-yocto-standard OpenSSL 3.0.9
TPS 9200TXE	2x Intel Xeon Gold 5318N (Ice Lake) - 80 Cores @ 2.0GHz	Storage = 32GB CFAST (Internal) / 240GB NVMe SSD (External)	Two IOM Slots, Hot-Swappable Up to 12 25GE/10GE/1GE Segments, Up to 8 100GE/40GE Segments	Linux-5.4.58-yocto-standard OpenSSL 3.0.9

The vTPS virtual appliances consist of TPS v6.3.0, running on hosts with Intel Xeon CPUs based on Broadwell or newer that support the RDSEED instruction and one of the following:

- VMware ESXi 7.0 or 8.0
- RHEL version 8 or version 9 KVM

Evaluation testing of vTPS was conducted on the following platforms:

- ESXi 7.0U3 on Intel(R) Xeon(R) Silver 4110 CPU (Skylake microarchitecture)
- KVM on Red Hat Enterprise Linux 8 (8.9) on Intel(R) Xeon(R) Silver 4110 CPU (Skylake microarchitecture)

The vTPS virtual appliances use virtual data ports and do not require I/O modules.

The vTPS appliances are provided as image files:

- vTPS_vmw_6.3.0_ 13244.zip
- vTPS_kvm_6.3.0_ 13244.tar.gz

To fully meet the requirements for evaluated Common Criteria certification, certain features must be configured in a specific way and the devices must be used within certain guidelines. In addition, certain features are not covered by the scope of the evaluation. This document describes Common Criteria configuration guidelines for the Trend Micro devices listed above.

The TPS requires a syslog server for external storage of audit data and an SSH client for remote administrative access to the CLI.

2.1 vTPS Virtual Appliance Installation

The vTPS virtual appliance must be the only guest running in the virtualized environment. The following provides the guidance to install the vTPS Virtual Appliance in the different virtual environments:

Refer to the following sections of [DG] for the guidance to deploy the vTPS appliance.

- ESXi – See Section “Install and deploy a vTPS virtual appliance by using VMware ESXi”
- KVM – See Section “Install and deploy a vTPS virtual appliance by using KVM”

Note that the vTPS must be updated from Trial Mode to Standard Mode in order to be in the evaluated configuration. Instructions for doing this can be found in Chapter 4 of [DG] (“Upgrade from vTPS Trial to vTPS Standard”).

2.2 Scope of Evaluation

The evaluated functionality is scoped exclusively to the security functional requirements specified in [ST]. In particular, the SSH protocol implemented by the Trend Micro TippingPoint devices have been tested, and only to the extent specified by the security functional requirements. The following protocols and features identified in [ST] have not been included in the evaluated configuration:

- The TippingPoint Threat Protection System solution includes Local Security Management (LSM) and Security Management System (SMS) components that provides remote administrative management. In the evaluated configuration, all management must be performed using the CLI.
- The Digital Vaccine service is provided by the TOE developer and assumed to be a trusted service. It may be used in the evaluated configuration, however it is not included in the TOE itself and therefore no claims are made about its ability to provide adequate or timely filter updates.
- The TPS devices can be configured to use sFlow record emission to sample a random flow of traffic and send the data to a collector server for analysis. SFlow and collector services are excluded from the evaluated configuration and must not be configured or used.
- Two TippingPoint Threat Protection appliances can be installed in a redundant network configuration. This system configuration provides High Availability (HA), ensuring that the network traffic always flows at wire speeds in the event of any internal hardware or software failure on the device. HA configurations are not covered in the scope of the evaluation.
- TippingPoint Threat Protection appliances can be installed in a stacking configuration. Stacking enables an organization to increase the overall inspection capacity of the TPS by grouping multiple TX Series devices and pooling their resources. Stacking configurations are not included in the evaluated configuration. The devices are being evaluated in a standalone configuration.
- Optional bypass I/O modules are available for the physical appliance models that provide high

availability for copper and fiber segments. These modules are not included in the TOE and must not be used in the evaluated configuration.

- The TPS intrusion prevention services including collection, inspection, analyzation, and reaction capabilities applied to network traffic have not been evaluated and no claims are made in relation to these functions. They may be used in the evaluated configuration without affecting the claimed security functions.
- Use of RADIUS or TACACS for user authentication is not supported in the evaluated configuration.
- The capability to encrypt the user disk is not covered by the scope of the evaluation.
- Support for IPv6 networks is not covered by the scope of the evaluation.
- Use of NTP is not covered by the scope of the evaluation.

2.3 Operating Environment Assumptions

The following operating environment assumptions must be met for Common Criteria operation:

- The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized this assumption applies to the physical platform on which the VM runs.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
- A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
- The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
- The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

- The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
- The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
- For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

2.4 Configuring the TPS for Common Criteria Compliance

To ensure the TPS device is configured within the requirements of the evaluated configuration for Common Criteria, the following configuration actions must be taken:

- The TPS must be configured to support the Federal Information Processing Standards (FIPS) 140 cryptographic requirements. The *fips-mode-enable* command enables FIPS compliant functionality on a TPS device.

  Before you run this command, always reset the device to factory default settings. When you run this command, it prompts you to confirm that you want to enable FIPS mode. After you enable FIPS mode, it cannot be disabled except by resetting the device to factory defaults. After you run this command, you must reboot the device to enable FIPS mode. Use the *show fipsmode* command to verify FIPS mode is enabled.

  Additionally, to further limit the SSH public key algorithms used, this is changed during initial setup by modifying the ssh config file as root. This is done by using the `service-access enable` command, which outputs information that can be used by Trend Micro support to generate a one-time password for the root user.

  FIPS Mode restricts the cryptographic mechanisms to FIPS-approved algorithms. See section 2.6.2 of this document for more information.

  Note: the cryptographic engine used when the TPS has been placed into FIPS mode is used for all SSH and other cryptographic functionality within the scope of the evaluated configuration of the product. No other cryptographic engine or configuration was evaluated or tested during the Common Criteria evaluation of TPS.

- During initial device configuration an administrative account is created with the default Super User role. The Super User role gives the account full access to the device. This administrative account is used to complete initial configuration. The password must be set prior to first use by the administrator performing the initial setup; there is no ‘default’ password that can be used to access the TOE. Guidance on choosing secure passwords is provided in Section 2.6.4 of this document. The Super User account itself must also be used to create other users and associate roles with roles. Other than super user, the default roles are: admin and operator. See Section 2.8 below for further details.

- The Trend Micro TPS and vTPS appliances must be deployed in a physically secure location to prevent physical tampering. Any person with physical access to the device must have the same level of trustworthiness as an authorized administrator.
- To manage a Trend Micro TPS and vTPS device in a way consistent with the evaluated configuration, device management must be performed via the CLI. Administrators manage the TOE remotely using an SSH connection to the Ethernet Management port on the TOE appliance or locally through the console interface or locally through a direct connection to the Ethernet Management port. Each method provides access to the CLI after an administrator successfully logs in. Prior to administrative login, the Management interface will respond to ICMP requests to confirm connectivity (for remote administrative connections) and displays a warning banner for both local and remote connections. No other TSF-mediated actions are permitted on behalf of an administrative user until the user is successfully authenticated. SSH access is enabled by default to allow CLI access to the device. No configuration is necessary. Non-secure access through Telnet is not permitted.
- In order to log in, the user must provide an identity and authentication data that matches an identity configured on the TOE. Users are defined locally within the TOE with a user identity, password, and user role. Administrators accessing the Ethernet Management port can be defined with an SSH public key for public key-based authentication for SSH connections rather than a password. To upload a public SSH key see [CLI] SSH Configuration Section "To upload a user public key". Users are authenticated directly by the TOE. Any resulting session is dependent upon successful authentication and established sessions are associated with the role(s). SSH access is enabled by default to allow CLI access to the device. While the TOE is configured out-of-the-box to be running an SSH server, it does not supply a client to access it, so users are free to use a third-party SSH client of their choosing to connect to the TOE's IP address over port 22.

  Refer to the [CLI] command: *ips{running-aaa}user* to configure new users. You can create, modify, delete users and add or remove them to/from a user group on the local device database using *ips{running-aaa}user-group*. Access to the CLI is determined by the users' group membership and roles. Role determines a user's access to security functions. Authorization is controlled by granting users access through the authentication context (aaa).
- Telnet, HTTP, and connections over untrusted networks are not supported and must not be enabled. Refer to the [CLI] for more details on using the CLI interface.

2.4.1 Setting the System Time

To set the system time on the Trend Micro TPS, use the command: *date [MMDDhhmm[[CC]YY][.ss]]*. This allows the following values to be set:

- Date
- Time.

Example: *ips{}date 071718202013.59* (sets date to July 17 2013 6:20PM 59 seconds).

Timezone is set using the command: *timezone (GMT|(REGION CITY)).*

The timezone command is found under the general context mode (gen): *ips{running-gen}timezone*.

2.4.2 Configure the syslog server

In the evaluated configuration, TPS forwards generated audit records to an external syslog server as they are written to the local log files. To configure the syslog server, reference CLI Guide Section "To

configure the "Remote System Log" contact to use SSH". It is expected that the syslog server need only be configured once. The SSH client key pair is generated by TPS as part of configuration during initial installation. RSA is the supported algorithm for this.

The following commands provide an example of the commands required to configure the Remote Syslog Export for a syslog server with IP address of 172.16.24 port 514.

```
vtpsESXi{running-notifycontacts-Remote System Log}display
#contact "Remote System Log" # syslog
 server 172.16.1.24 514
 alert-facility 172.16.1.24 514 4
 block-facility 172.16.1.24 514 4
 protocol 172.16.1.24 514 TCP
 ssh-user-name 172.16.1.24 514 <SERVER USER NAME>
 ssh-user-key 172.16.1.24 514 *****
 ssh-host-key 172.16.1.24 514 172.16.1.24 ssh-rsa <SERVER HOST KEY>
 use-ssh 172.16.1.24 514 enable
 period 1
 exit
```

The physical syslog server requires sshd (openssh 8.2p1) and rsyslog (8.2001.0) on an Ubuntu 20.04.3 machine.

2.5 Security Audit

2.5.1 Audit Events

The TPS maintains System and Audit log files. Taken together, these log files provide the security audit trail that satisfies the auditing requirements specified in the PP listed in Section 1.1 of this document.

The Audit logs include events such as administrator configuration of the security functions, and user login and logout. The System logs contain information about the software processes that control the device, including startup routines, run levels, and maintenance routines.

The following tables list the standard fields of each log type that TPS can forward to an external server.

Example System Log

```
2024-05-29 16:46:08.340 [device] [syslog-ng-NOTICE: ] "syslog-ng starting up;
version='3.24.1'"

2024-05-28 13:27:17.016 [1100TX] [syslog-ng-NOTICE: ] "syslog-ng starting up;
version='3.24.1'"
```

System Log Fields

Format: Log Entry Time, Log ID, Device Name, Severity Level, Message.

Table 1 – System Log Fields Audit Record Field Descriptions

System Log Fields	
Field Name	**Description**
Log ID	Displays the system-assigned log ID number (after the Log Entry Time).

System Log Fields	
Field Name	**Description**
Log Entry Time	Displays the time the log was entered in the format YYYY-MM-DD HH:MM:SS.
Device Name	The device name on which the event was logged.
Severity Level	Indicates the designated severity of the event (e.g., NOTICE, ERROR).
Message	Text of the log entry to identify the event that has occurred.

Example Audit Log

```
2024-02-21 13:42:55.251 [1100TX] [8] [CLI] [172. 16. 1.50] [Cfg] [Success]
[cctester] "SSH Public Key deleted for user 'pubkeyuser'"
```

Audit Log Fields

Format: Log Entry Time, Device Name, Access, Interface, IP Address, Process, Result, User, Action.

Table 2 – Audit Log Fields Audit Record Field Descriptions

Audit Log Fields	
Field Name	**Description**
Log Entry Time	Displays the time the log was entered in the format YYYY-MM-DD HH:MM:SS.
Device Name	The device name on which the session was logged.
Access	Displays the access level of the user performing the action (from 0 (no administrative permissions to 8 (super user)). The access levels are defined as: 0 NORMAL_ACCESS (no administrative permissions) 1 OPERATOR_ACCESS 2 CUSTOM_ACCESS[1] 4 ADMINISTRATOR_ACCESS 8 SUPER_USER_ACCESS
Interface	Displays the interface with which the user logged in: CLI for the command line interface. For system-initiated actions, SYS displays in this field.
IP address	Identifies the IP address from which the event originated. Displays a value of 0.0.0.0 for local or internal events.
Process	Identifies the process associated with the event (USER, CFG, UPDATE, POLICY).
Result	Displays the result (SUCCESS or FAILURE) of the action.
User	Displays the user performing the action. For system-initiated actions, SYSTEM displays in this field.
Action	Text of the log entry to identify the event that has occurred.

[1] Custom roles are not included in the evaluated configuration.

The following table lists the auditable events mandated by the requirements in the PP listed in Section 1.1 of this document; identifies to which of the log files each auditable event is written; and provides a sample audit record for each event.

Table 3 – Sample Audit Records

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up and shutdown of the audit functions	Source 'show log-file system'

`2024-05-29 16:46:08.340 [device] [syslog-ng-NOTICE: ] "syslog-ng starting up; version='3.24.1'"`
 	
`2024-05-28 13:27:17.016 [1100TX] [syslog-ng-NOTICE: ] "syslog-ng starting up; version='3.24.1'"`		

FAU_GEN.1	Generating/ import of, changing, or deleting of cryptographic keys	Source 'show log-file audit'

SSH user public key
`2024-02-21 13:34:41.378 [1100TX] [8] [CLI] [172.16.1.50] [Cfg] [Success] [cctester] "SSH Public Key changed for user 'pubkeyuser'"`
 	
`2024-02-21 13:42:55.251 [1100TX] [8] [CLI] [172.16.1.50] [Cfg] [Success] [cctester] "SSH Public Key deleted for user 'pubkeyuser'"`
 	
Remote SSH host key
`2024-07-07 07:55:11.273 [1100TX] [8] [CLI] [172.16.1.50] [Cfg] [Success] [testuser] "Deleted remote syslog address 172.16.1.50 port 22 SSH host key"`
`2024-07-07 07:55:45.950 [1100TX] [8] [CLI] [172.16.1.50] [Cfg] [Success] [testuser] "Updated remote syslog address 172.16.0.22 port 514 SSH host key"`
 	
TOE SSH user private key
`2024-07-07 07:55:11.273 [1100TX] [8] [CLI] [172.16.1.50] [Cfg] [Success] [testuser] "Deleted remote syslog address 172.16.1.50 port 22 SSH user key"`
`2024-07-07 07:55:45.950 [1100TX] [8] [CLI] [172.16.1.50] [Cfg] [Success] [testuser] "Updated remote syslog address 172.16.0.22 port 514 SSH user key"`		

FAU_GEN.2	None.	None.
FAU_STG.1	None	None.
FAU_STG_EXT.1	None.	None.
FAU_STG.3/LocSpace	Low storage space for audit events.	Source 'show log-file system'
`2024-01-10 21:53:30.237 [vtpsKVM] [HEALTHCHECKD-CRIT: ] "Sensor Auditlog - auditlog reading 76 percent is above upper critical threshold of 75 percent"`		
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/ DataEncryption	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/Keyed Hash	None.	None.
FCS_RBG_EXT.1	None.	None
FCS_ SSHC_EXT.1	Failure to establish an SSH Session	Source 'show log-file system' Reason for failure
`2024-05-20 11:58:37.606 [1100TX] [SSHRSL-2002-WARNING: ] "fatal: Host key verification failed."`		
FCS_SSHS_EXT.1	Failure to establish an SSH Session	Source 'show log-file system' Reason for failure
`2024-08-08 17:25:51.961 [vtpsESXi] [SSHD-INFO: ] "Failed publickey for pubkeyuser from 172.16.1.70 port 54186 ssh2: RSA SHA256:jaMpllkRNkql1Vte6pvWRU511aXVdEgK0+rYXlrioBU"`		
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Source 'show log-file audit' Origin of the attempt (e.g., IP address).
`2023-12-20 19:01:26.516 [1100TX] [8] [SYS] [0.0.0.0] [User] [Success] [system] "User 'testuser' locked due to too many (4) failed logins"` `2023-12-20 19:01:26.516 [1100TX] [SYS] [0.0.0.0] [User] [Success] [system] "IP address '172.16.1.50' locked due to too many (4) failed logins"`		
FIA_PMG_EXT.1	None.	None
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Source 'show log-file audit'
`2024-06-27 11:10:57.617 [1100TX] [8] [CLI] [172.16.1.50] [User] [Fail] [testuser] "Login failed for user 'testuser' using 'SSH'"` `2024-06-27 11:11:07.223 [1100TX] [8] [CLI] [172.16.1.50] [User] [Success] [testuser] "User 'testuser' logged in using SSH"`		
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Source 'show log-file audit' Origin of the attempt (e.g., IP address).
`2024-06-27 11:10:57.617 [1100TX] [8] [CLI] [172.16.1.50] [User] [Fail] [testuser] "Login failed for user 'testuser' using 'SSH'"` `2024-06-27 11:11:07.223 [1100TX] [8] [CLI] [172.16.1.50] [User] [Success] [testuser] "User 'testuser' logged in using SSH"`		
FIA_UAU.7	None.	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	Source 'show log-file audit' Any attempt to initiate a manual update.
`2024-07-08 09:24:14.839 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "CLI requested package download from http://revocation1.leidos.ate/transfer/TrendMicro/6.3.0_19999/TPS.`		

Requirement	Auditable Events	Additional Audit Record Contents
IPS.GOLFLE_6.3.0_19999.pkg (172.16.1.70)" 2024-07-08 09:24:21.633 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "Software upgrade request to [6.3.0.19999] package type [TPS IPS.GOLFLE]" 2024-07-08 09:24:56.292 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "OS Update to 6.3.0.19999"		
FMT_MOF.1/Functions	None.	None
FMT_MTD.1/Core Data	None.	None.
FMT_SMF.1	All management activities of TSF data.	None See Table 4 below.
FMT_SMR.2	None.	None
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	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). Source 'show log-file audit'
2024-05-27 12:30:00.007 [1100TX] [8] [CLI] [172.16.0.25] [Cfg] [Success] [testuser] "System time changed from 2024-06-27 12:32:09 to 2024-05-27 12:30:00"		
FPT_TST_EXT.1	None	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	Source 'show log-file audit'
Success 2024-07-08 09:24:14.839 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "CLI requested package download from http://revocation1.leidos.ate/transfer/TrendMicro/6.3.0_19999/TPS.IPS.GOLFLE_6.3.0_19999.pkg (172.16.1.70)" 2024-07-08 09:24:21.633 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "Software upgrade request to [6.3.0.19999] package type [TPS IPS.GOLFLE]"		

Requirement	Auditable Events	Additional Audit Record Contents
2024-07-08 09:24:56.292 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "OS Update to 6.3.0.19999" Failure 2024-07-08 08:57:26.616 [1100TX] [8] [CLI] [172.16.1.50] [Update] [Success] [testuser] "CLI requested package download from http://revocation1.leidos.ate/transfer/TrendMicro/6.3.0_19999/invalid_TPS.IPS.GOLELE 6.3.0_19999.pkg (172.16.1. 70)" 2024-07-08 08:57:32.645 [1100TX] [8] [CLI] [172.16.1.50] [Update] [Success] [testuser] "Software upgrade request to [6.3.0.19999] package type [TPS IPS.GOLFLE]" 2024-07-08 08:57:35.094 [1100TX] [8] [CLI] [172.16.1.50] [Update] [Fail] [testuser] "Software Package Install: Failure: 'Failed package verification'"		
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	Source 'show log-file audit'
2024-06-27 16:45:41.001 [vtpsESXi] [8] [SYS] [0.0.0.0] [User] [Success] [system] "Warn CLI session of inactivity timeout for user 'testuser' connecting from '172.16.0.25'" 2024-06-27 16:48:11.001 [vtpsESXi] [8] [SYS] [0.0.0.0] [User] [Success] [system] "CLI session canceled due to inactivity for user 'testuser' connecting from '172.16.0.25'"		
FTA_SSL.4	The termination of an interactive session.	Source 'show log-file audit'
Console 2024-01-17 18:13:03.001 [1100TX] [8] [CLI] [0.0.0.0] [User] [Success] [cctester] "User 'cctester' logged out using CONSOLE" SSH 2024-06-28 16:03:48.800 [vtpsESXi] [8] [CLI] [172.16.0.25] [User] [Success] [testuser] "User 'testuser' logged out using SSH"		
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	
2024-07-05 13:46:23.639 [1100TX] [8] [CLI] [0.0.0.0] [User] [Success] [testuser] "User ' testuser' logged in using CONSOLE" 2024-07-05 13:51:23.001 [1100TX] [8] [SYS] [0.0.0.0] [User] [Success] [system] "Warn CLI session of inactivity timeout for user ' testuser' connecting from 'CONSOLE'" 2024-07-05 13:56:23.001 [1100TX] [8] [SYS] [0.0.0.0] [User] [Success] [system] "CLI session canceled due to inactivity for user ' testuser' connecting from 'CONSOLE'" 2024-07-05 13:56:23.002 [1100TX] [8] [CLI] [0.0.0.0] [User] [Success] [testuser] "User ' testuser' logged out using CONSOLE"		

Requirement	Auditable Events	Additional Audit Record Contents
FTA_TAB.1	None.	None
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt. Source 'show log-file system'
2024-01-02 20:31:52.375 [1100TX] [syslog-ng-NOTICE:] "Syslog connection established; fd='30', server='AF_INET(172. 16.0.30:514)' , local='AF_INET(0.0.0.0:0)'' 2024-01-02 21:13:33.067 [1100TX] [syslog-ng-NOTICE :] "Syslog connection broken; fd='28', server='AF INET(127.0.0.1:2000)', time_reopen='60'" 2024-01-02 20:31:52.375 [1100TX] [syslog-ng-ERROR:] "Syslog connection failed; fd='27 server='AF_INET(127.0.0.1:2000)' , error='Connection refused (111)', time_reopen='60'"		
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	Source 'show log-file audit'
2024-05-28 15:58:07.054 [vtpsKVM] [8] [CLI] [172. 16.0.25] [User] [Success] [testuser] "User 'testuser' logged in using SSH" 2024-05-28 15:58:41.104 [vtpsKVM] [8] [CLI] [172. 16.0.25] [User] [Success] [testuser] "User 'testuser' logged out using SSH" 2024-06-27 11:10:57.617 [1100TX] [8] [CLI] [172.16.1.50] [User] [Fail] [testuser] "Login failed for user 'testuser' using 'SSH'"		

The following table identifies the auditable administrator actions and the audit record generated when an administrator performs one of these actions. All actions are performed via the administrator CLI.

Table 4 – Sample Audit Records of Administrative Actions

Administrator Action	Audit Record
Configure access banner	2024-06-25 16:17:02.095 [1100TX] [8] [CLI] [172.16.0.25] [Cfg] [Success] [testuser] "Login banner Text is set.
Configure the session inactivity time before session termination or locking	2024-06-25 20:28:30.080 [vtpsESXi] [8] [CLI] [172. 16.0.25] [Cfg] [Success] [testuser] "CLI Inactive timeout set to 5 minutes"
Update the TOE and verify the update	Success 2024-07-08 09:24:14.839 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "CLI requested package download from http://revocation1.leidos.ate/transfer/TrendMicro/6.3.0_19999/TPS.IPS.GOLFLE_6.3.0_19999.pkg (172.16.1. 70)"

Administrator Action	Audit Record
	2024-07-08 09:24:21.633 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "Software upgrade request to [6.3.0.19999] package type [TPS IPS.GOLFLE]" 2024-07-08 09:24:56.292 [1100TX] [8] [CLI] [0.0.0.0] [Update] [Success] [testuser] "OS Update to 6.3.0.19999" Failure 2024-07-08 08:57:26.616 [1100TX] [8] [CLI] [172.16.1.50] [Update] [Success] [testuser] "CLI requested package download from http://revocation1.leidos.ate/transfer/TrendMicro/6.3.0_19999/invalid_TPS.IP S.GOLELE 6.3.0_19999.pkg (172.16.1. 70)" 2024-07-08 08:57:32.645 [1100TX] [8] [CLI] [172.16.1.50] [Update] [Success] [testuser] "Software upgrade request to [6.3.0.19999] package type [TPS IPS.GOLFLE]" 2024-07-08 08:57:35.094 [1100TX] [8] [CLI] [172.16.1.50] [Update] [Fail] [testuser] "Software Package Install: Failure: 'Failed package verification'"
Configure the authentication failure parameters for FIA_AFL.1 Unsuccessful authentication attempts (max login attempts) Lockout time period	2024-06-25 16:42:16.331 [1100TX] [8] [CLI] [172. 16.0.25] [Cfg] [Success] [testuser] "Login maximum-attempts set to '2'" 2024-06-25 16:42:16.331 [1100TX] [8] [CLI] [172.16.0.25] [Cfg] [Success] [testuser] "Login lockout-period set to '2' Minutes"
Configure audit behavior Configure communication with external syslog Configure log size/rotation	Communication with external syslog 2024-05-28 12:45:26.602 [1100TX] [8] [CLI] [172.16.0.25] [Policy] [Success] [testuser] "Modified notification contact 'Remote System Log'" 2024-05-28 12:46:31.174 [1100TX] [8] [CLI] [172. 16.0.25] [Cfg] [Success] [testuser] "Updated remote syslog address 172.16.1.50 port 22" 2024-05-28 12:46:31.174 [1100TX] [8] [CLI] [172.16.0.25] [Cfg] [Success] [testuser] "Updated remote syslog address 172.16.1.50 port 22 SSH host key" Log size/rotation 2024-05-28 13:58:57.736 [1100TX] [8] [CLI] [172. 16.0.25] [Cfg] [Success] [testuser] "logrotate maxFileSize set to 500 MB"
Configure the cryptographic functionality (i.e. enable FIPS mode)	2024-07-19 13:11:22.488 [1100TX] [8] [CLI] [0.0.0.0] [Cfg] [Success] [testuser] "FIPS mode enabled"

Administrator Action	Audit Record
Set time	`2024-05-27 12:30:00.007 [1100TX] [8] [CLI] [172. 16.0.25] [Cfg] [Success] [testuser] "System time changed from 2024-06-27 12:32:09 to 2024-05-27 12:30:00"`
Configure trusted public keys database	`2024-07-08 10:42:06.139 [1100TX] [8] [CLI] [0.0.0.0] [Cfg] [Success] [asanta] "Updated remote syslog address 172.16.0.22 port 514 SSH host key"`

2.5.2 Configuring Log Size/Rotation Settings

The TPS stores the audit records locally and can also be configured to send audit records to an external syslog server using SSH. When configured to send audit records to a syslog server, audit records are also written to the external syslog as they are written locally to the device's audit log (in real-time).

The TPS provides the ability to configure the size of the Audit and System logs. By default the total set of system logs and set of audit logs each take up half the available space. The term 'set' in this context means that if for example system log takes up 60% of the space and it has five backup files in a rotation, each backup and the main file will take up to 10% of the space each. And if audit also has five backup files and takes the other 40% of the space, each of those files will take up to 6.67%. As such these limits are specified as a percentage of internal log disk space using the log-file-size CLI setting. The maximum amount of audit data that are stored locally in each log cannot exceed this percentage and the combined percentage configured for the logs must equal 100%. The log rotation function allows administrators to further control the amount of audit records that are stored. The current log is polled at a configurable interval to see if it has reached the maximum size. The administrator can specify the maximum size of a log file using the 'maxFileSize' parameter to configure how large a file can be (10MB – 500 MB) before rotation is triggered. They can specify the number of files kept in the log rotation (2 – 20) using the 'numfiles' parameter. Within each log file, they can also specify the maximum number of records contained in each file using the 'numrecords' parameter, which sets the number of records between log daemon size checks of 100- 65535). defaultCheckRecords sets the default number of records between log daemon size checks (100-65535), and 'sleepseconds' that determine the frequency with which the logs are checked for and whether rotation is necessary (after a certain period of time of 1 – 65535 seconds has elapsed).

The TPS does not provide an interface where a user can modify the audit records, thus it prevents modification to the audit records. There are no commands to delete individual audit records. Super Users can use the command: **clear log-file** to delete the locally stored Audit log and IPS data files. There are no interfaces to modify stored audit or IPS data.

Note that the command: *'ips{running-log}delete'* is not used to delete audit records but rather to remove a syslog server so that the device no longer sends audit records to it. The command does not affect locally stored audit records and generated audit events will still be logged locally.

The TPS generates an audit record warning that is written to the audit trail when the space allocated for storage of audit records exceeds 75% of capacity. This is not configurable. The audit record can be viewed by issuing the command: *show log-file system*. A sample of the audit record can be seen in Table 3 – Sample Audit Records (FAU_STG.3/LocSpace).

2.6 Cryptographic Support

2.6.1 Cryptographic Self-Tests

The TPS runs software module integrity tests and cryptographic known answer self-tests during initial startup. When successfully run without errors, these tests demonstrate the correct operation of the TSF. If a self-test fails, the TOE enters an error state where a system recovery prompt is displayed. Contact a TippingPoint support representative for assistance. The TOE doesn't perform any cryptographic operations while in the error state. All data output from the TOE is inhibited when an error state exists.

2.6.2 SSH Configuration

The TPS is required to be configured into FIPS mode as described in Section 2.4 of this document. FIPS mode automatically configures the use of FIPS approved algorithms and key sizes as specified in the [ST]. To further limit the SSH symmetric cipher algorithms that are used, the following commands are used:

```
debug ssh ciphers show

debug ssh ciphers <cipher> enable

debug ssh ciphers <cipher> disable
```

TPS is not subject to any situations that could prevent or delay key destruction. TPS strictly conforms to the key destruction requirements as specified in the PP in Section 1.1 of this document and defined in the [ST].

In its evaluated configuration, TPS uses *CTR_DRBG(AES)* for random bit generation and the following algorithms:

- Client:
    - aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com encryption algorithms
    - ssh-rsa, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521 as its server public key algorithms; and
    - hmac-sha1, hmac-sha2-256, hmac-sha2-512 (implicit for aes*-gcm@openssh.com) as its MAC algorithms.
- Server:
    - aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, aes256-gcm@openssh.com encryption algorithms
    - ssh-rsa, rsa-sha2-256, and rsa-sha2-512 as its server public key algoriths; and
    - hmac-sha2-256 and hmac-sha2-512 (implicit for aes*-gcm@openssh.com) as its MAC algorithms.

The following key exchange methods used in SSH are not configurable:

SSH Client

- *diffie-hellman-group14-sha1*
- *ecdh-sha2-nistp256*

- *ecdh-sha2-nistp384*
- *ecdh-sha2-nistp521*

SSH Server

- *ecdh-sha2-nistp256*
- *diffie-hellman-group14-sha256*
- *diffie-hellman-group16-sha512*
- *diffie-hellman-group18-sha512*
- *ecdh-sha2-nistp384*
- *ecdh-sha2-nistp521*

SSH ciphers can be viewed, and enabled or disabled using the following commands:

debug ssh ciphers <cipher-name> enable

debug ssh ciphers <cipher-name> disable

show key

To remain in the evaluated configuration only the ciphers/algorithms specified above may be enabled and less secure ciphers/algorithms must not be enabled.

Note that in the CC evaluated configuration, the "none" MAC algorithm is not allowed. There are no other configuration options.

2.6.2.1 SSH Host Key Configuration

To configure the trusted public keys database for a remote SSH server, a host key must be added for the server. To do this, run 'edit', enter the 'notifycontacts' submenu, and enter 'contact "Remote System Log" to configure the system log. Once in this configuration menu, enter 'ssh-host-key SERVER PORT PUBLICKEY' where SERVER is the IP address of the server, PORT is the port of the server, and PUBLICKEY is the public key of the server.
Reference the "SSH Configuration" section of [CLI] for screenshots and additional information.

2.6.2.2 SSH Client Private Key Configuration

To use public key authentication with a remote SSH server, a private key for the TOE client must be configured. To do this, run 'edit', enter the 'notifycontacts' submenu, and enter 'contact "Remote System Log" to configure the system log. Once in this configuration menu, enter 'ssh-user-key SERVER PORT' where SERVER is the IP address of the server and PORT is the port of the server. Once this is entered, a prompt for the user private key will be provided. Respond to this prompt with the entire private key, including BEGIN PRIVATE KEY and END PRIVATE KEY lines.
Reference the "SSH Configuration" section of [CLI] for screenshots and additional information.

2.6.2.3 SSH User Public Key Configuration

To add or remove a user public key for authentication, run 'edit', enter the 'aaa' submenu, and then enter 'user USER' where USER is the username for which the key is being modified. From here, the key can be managed as follows:

- Adding: enter 'ssh-public-key SSH_PUBLIC_KEY' where SSH_PUBLIC_KEY is the value of the key

- Removing: enter ‘delete ssh-public-key’

Regardless of which action is being performed above, enter ‘commit’ to execute the action.
Reference the “SSH Configuration” section of [CLI] for screenshots and additional information.

2.6.3 Supported Authentication Methods

In the evaluated configuration, the device supports the following methods of administrator authentication:

- Local administrator accounts with local password-based authentication
- Local administrator accounts with public key-based authentication (RSA or ECDSA)

SSH key-based authentication is dependent on administrative action and is specified on a per-user basis. See [CLI] Section *SSH configuration* ‘To upload a user public key’. The following demonstrates an example SSH-PUBLIC-KEY being uploaded:

```
FIPS8400TX1311{running-aaa-user-CCroot}display
user CCroot
  password $password$
  ssh-public-key "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDDyCjeqv0e5giUCzRVcWZPcUGhBHdiavkRcebF4HrtKut
5n7za2rWmZ16qOZZN4p8l54xUH2z2y5dtsdrewPcPkH8s9+kNkQTzjnHwarMLmaC7rYmZ2R7M1E5+WNQnTj+6xx25Ba5c3MoMJYHd
QurEMaPTX+QY4z53AefsrnfOoqIfioG1iSIAD6gZJTPN4uz9Lz40MX2fHCIELDDYtlgI8jiv9olNILVZWBiiK5OHCxtCp1znvfc3u
MBCzcrr35ycq9V2bmoVBtGndIegkhJbAmqaIVek0w01W5UvC81RYz4KVGMCBsbdSHwiCRRMC3YSsLB+qO6DtpDurkgZLKKt"
  exit
```

If the user is using a typical SSH client to log in to the device, they can choose to use a password or key-based authentication at the client side with the SSH options PasswordAuthentication or PreferredAuthentications. See https://man.openbsd.org/ssh_config.5#PasswordAuthentication.

2.6.4 Password Considerations

When password-based authentication is used, administrators need to ensure the passwords they use are suitably secure. Many organizations, as a matter of policy, specify minimum requirements for choosing and constructing user passwords and such policies should be adhered to. Additionally, or where site-specific policies are not defined, administrators should consider the following when choosing passwords:

- Ensure the password is not too short—it is recommended to configure the Password Security Level to its highest setting, which enforces a minimum length of 15 characters.
- Use a mix of upper and lower case alphabetic, numeric, and punctuation characters
- Avoid using dictionary words or words readily associated with you (e.g., name of spouse, pet or favorite sports team)
- Consider using a passphrase—a combination of words that is easy to remember but difficult for an attacker to guess.

The TPS devices support the ability to configure minimum password length and complexity settings. This is accomplished using the command: *ips{running-aaa} password quality (none|low|medium|high).* The password quality levels provide minimum password lengths of 1, 8 or 15 characters. A Password Security Level of None enforces a minimum password length of 1. A Password Security Level of Low or Medium both enforce a minimum password length of 8. A Password Security Level of high requires the passwords to be at least 15 characters. Passwords can be comprised of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “,”, “.”, “/”, “<”, “>”, “?”. Single and double quotes, spaces or back slashes are not allowed. The password quality levels *none|low|medium|high* provide additional restrictions on password composition as follows. A Password Security Level of Medium specifies the following additional password complexity requirements:

- Contains at least two alphabetic characters,

- Contains at least one numeric character, and
- Contains at least one non-alphanumeric character.

A Password Security Level of High requires the passwords to be at least 15 characters and meet the following additional password complexity requirements:

- Contains at least one uppercase character,
- Contains at least one lowercase character, and
- At least half the characters cannot occupy the same positions as the current password.

2.6.5 Authentication Failure Handling

The number of failed authentication attempts allowed before the device locks a privileged account is configurable as is the lock out value. Refer to the [CLI] *ips{running-aaa}login* command. Authentication failures by remote Administrators cannot lead to a situation where no Administrator access is available to the TOE. If remote administrators are locked out, administrator access is still available via the local console. If an Administrator account is temporarily locked out and immediate access is required, an override may be provided by contacting Trend Micro support. The lockout override is a one-time credential provided by Trend Micro support based on the serial number of the device and a random salt.

2.7 TOE Access

2.7.1 Inactivity Timeout

The administrator is automatically logged out, if a login session is idle for more than the specified time. The maximum time (in minutes) without any activity on the CLI before an administrator is automatically logged out can be set to any integer value from one to 32000 using the command: *ips{running-aaa}login* command. See [CLI] for more details.

2.7.2 Access Banner

A login banner is text that is added to the login page so that administrators will see information they must know before they log in. The banner is configured using the command: ips{running-aaa}login-banner as described in "**Contexts and related commands**" section in the CLI Guide.

2.8 Security Management

2.8.1 Administrator Accounts and Roles

The TPS provides a predefined set of user groups that each have an assigned role with set access privileges. The permissions assigned to the default roles/groups cannot be modified. Each user group has an associated role that determines the type of administrative functions that are allowed.

The pre-defined default groups/roles are:

- Administrator – Has Read/Write privileges to all TPS capabilities except administering local users, user groups, and roles; and changing the password for other users. Administrator privileges are for an enhanced administrator user who can view, manage, and configure functions and options in the system.
- Operator – Has Read-only privileges to all TPS capabilities. Operator privileges are for a base-level administrator user who monitors the system and network traffic.

- Super User – Has Read/Write/Execute privileges to all TPS capabilities. Super User privileges include full access to all CLI functions. Only users associated with the Super User role can change the password for another user.

Note: if multiple administrators are needed to fulfill the same role, individual accounts should be created for each user; accounts should not be shared between users.

Device administrators with the Super User role can create other users and assign them to administrator roles. The product also allows administrators with the Super User role to create, edit, and delete any user group except the default groups; however, this functionality was not tested in the evaluation.

The following table identifies the role an administrative user must have to manage the security functions.

Table 5 –Administrator Actions and Role Needed

Administrator Action	**Role**
Startup and shutdown of the audit function	Super User Admin
Configure Access Banner	Super User Admin
configure the session inactivity time before session termination or locking	Super User Admin
update the TOE, and to verify the update	Super User Admin
configure the authentication failure parameters for FIA_AFL.1 • unsuccessful authentication attempts • Lockout time period	Super User Admin
Configure audit behavior • Configure communication with external syslog • Configure log size/rotation	Super User
configure the cryptographic functionality	Super User
Reset another user's password	Super User
Set time	Super User Admin
Create a local user	Super User
Management of password policy	Super User
Ability to manage the trusted public keys database	Super User Admin

2.8.2 Revoking Administrator Privileges

The Security Administrator can revoke administrator privileges in either of the following ways:

- Deleting the user account entirely using the command: *ips{running-aaa}delete user (USER)*, or
- Removing the user from the administrator's group/role using the command: *ips{running-aaa-usergroup-GROUP}delete user USER*.

2.9 TOE Updates

The TPS provides mechanisms to view the current version of the TOE and to install updates of the TOE software. TOE updates are initiated manually by the Super User. The integrity of the update is verified prior to installation using a digital signature. TippingPoint Technical Support releases software updates on the Threat Management Center (TMC): *https://tmc.tippingpoint.com*. Administrators with the Super User role can download and install updates from this site. Installing a new software package forces a reboot of the device. Before performing an upgrade, the following should be considered:

- Refer to the TPS release notes for information specific to your TOS, including DV packages, migration, rollbacks, and traffic interruptions.
- To avoid experiencing traffic interruption whenever the operating system is rebooted, perform a full reboot of the device by running the reboot full command from the device CLI. This issue is not applicable to vTPS devices.
- On vTPS devices, the flow of traffic is interrupted during a TOS upgrade and during a reboot of the device.
- An upgrade resets the authentication settings on your TPS device. If the authentication security level on your device was set to Maximum, the upgrade resets the security level to Medium, which is the default security level. If necessary, update the security level to specify a higher security level. Learn more about authentication settings.
- Verify that a recent license package is installed on the device and if necessary, download and install a new license package from the TMC at https://tmc.tippingpoint.com. Without a recent license package, the device reverts to its unlicensed throughput.
- Maximize the space on your device by removing old TOS versions and packet traces. This ensures a successful installation and allows for a TOS rollback, if necessary. You can remove previous TOS versions by using the SMS, the LSM, or the CLI. For complete information, refer to your product documentation.

The command *show version* displays the current software version.

The administrator uses a Debug command (*debug upgrade URL*) to download a TOE update package directly from the specified URL. The update package is published on Trend Micro support website. The vendor generates a digital signature of the update package by first calculating the SHA-256 hash of the update package, then encrypting the generated hash using its 2048-bit RSA private key. The digital signature is verified by the TOE prior to the package being installed. The process is as follows: the TOE calculates its own SHA-256 hash of the update package, then decrypts the digital signature accompanying the update package using the RSA public key matching the vendor's private key, and comparing the hash it calculated with the decrypted hash value. If they are equal, the package is valid and has not been modified. The digital signature is downloaded as part of the update package, and the TOE is pre-installed with the public key. The TOE starts the update process once it verifies the signature/hash. A package with an invalid signature will not be installed by the TOE.

If a TPS software update fails because of an invalid signature for example, an error report and a system log entry are generated. The device remains at its current version and configuration and the update is not performed. Customers are advised to contact Trend Micro support for assistance with these commands.