Trend Micro
TippingPoint Security Management System
Security Target

Version 1.0
7 October 2019

Prepared for:

11305 Alterra Parkway
Austin, TX 78758

Prepared By:

Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

This section introduces the Target of Evaluation (TOE) and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary, and list of abbreviations.

The TOE is TippingPoint Security Management System (SMS) from TrendMicro. SMS provides an appliance-based solution that acts as the control center for managing large-scale deployments of TippingPoint devices, including TippingPoint Threat Protection System (TPS) and TippingPoint Intrusion Prevention System (IPS). A single SMS can manage multiple TippingPoint devices—the maximum number depends on usage, network, and other environmental conditions.

The ST contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the SFRs
- Rationale (Section 7)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Trend Micro TippingPoint Security Management System Security Target

ST Version – Version 1.0

ST Date – 7 October 2019

TOE Identification – TippingPoint Security Management System H3 Appliance (TPNN0302), TippingPoint Security Management System H3 XL Appliance (TPNN0303), and TippingPoint vSMS Enterprise Virtual Appliance (TPNN0304), all running SMS v5.2.0.

TOE Developer – Trend Micro Incorporated

Evaluation Sponsor – Trend Micro Incorporated

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017.
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

- Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2.

1.3 Conventions

The following conventions are used in this document:

- Security Functional Requirements—Part 1 of the CC defines the approved set of operations that may be applied to functional requirements: iteration; assignment; selection; and refinement.
    - Iteration—allows a component to be used more than once with varying operations. In this ST, iteration is identified with a number in parentheses following the base component identifier. For example, iterations of FCS_COP.1 are identified in a manner similar to FCS_COP.1(1) (for the component) and FCS_COP.1.1(1) (for the elements).
    - Assignment—allows the specification of an identified parameter. Assignments are indicated using bold text and are enclosed by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection—allows the specification of one or more elements from a list. Selections are indicated using bold italics and are enclosed by brackets (e.g., [***selection***]).
    - Refinement—allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST—other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

This ST uses a number of terms that have a specific meaning within the context of the ST and the TOE. This glossary provides a list of those terms and how they are to be understood within this ST.

Capability	An ability to affect an object in the TOE, e.g., the ability to add a device.
Device	A TippingPoint product being managed by SMS.
Event	Data logged in the SMS database in response to traffic triggered by the filters and rules defined in profiles. Events include the date and time the event was triggered, the severity of the event, the source and destination information (including IP address and port) of the traffic that triggered the event, the name and type of the filter or rule triggering the event, the profile associated with the filter or rule, and the device where the event was triggered.
Filter	A set of rules and conditions used by TippingPoint devices to detect and handle malicious network traffic. One of the TOE's main capabilities is to distribute filter profiles to TippingPoint devices in the network.
Profile	A collection of rules or filters that provides a method for setting up security configuration options for devices.
Responder	A policy-based service that reacts to triggers and performs a set of actions that provide security mitigation to block malicious traffic, inform the administrator of possible threats, and place the host into remediation.
Response action	An action performed by SMS when host traffic triggers a response policy. Response actions include: notification actions; reputation entry (blacklist) actions; IPS quarantine actions; and switch actions.
Response policy	Defines the detection of a security event and the SMS response.

Report As the TOE detects malicious attacks and manages network usage, event data is logged in the database. The TOE provides a set of options to generate reports about the compiled and stored log information.

Role A collection of capabilities. The TOE has three predefined or built-in roles: **superuser**; **admin**; and **operator**.

User Group A user group provides a way to align capabilities with functional areas of the TOE. A user group pairs a role with resources that group members can access. The TOE has one predefined user group called **superuser**. The **superuser** user group includes the **superuser** role and provides access to all TOE features and functionality. Additional groups can be created by authorized administrators.

1.5 Abbreviations and Acronyms

The following abbreviations and acronyms are used throughout this ST:

API	Application Programming Interface
CAC	Common Access Card—a user authentication mechanism supported by the TOE
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DV	Digital Vaccine—a downloadable security package of filters for TippingPoint devices
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention System
IT	Information Technology
NTP	Network Time Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service—a networking protocol supporting remote user authentication
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
SMS	Security Management System
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus—a networking protocol supporting remote user authentication
TLS	Transport Layer Security
TMC	Threat Management Center—a TippingPoint service center that monitors sensors around the world for the latest attack information and builds and distributes attack filters. The TMC website also serves as a central repository for product documentation, FAQs, the TippingPoint Knowledge Base, and related information.
TOE	Target of Evaluation

TOS	TippingPoint Operating System
TPS	Threat Protection System—a TippingPoint network security platform product offering protection against network vulnerabilities, exploits and known and zero-day attacks.
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

2. TOE Description

The TOE is TippingPoint Security Management System (SMS), v5.2.0. It is a server-based solution that can act as the control center for managing large-scale deployments of TippingPoint Threat Protection System (TPS) and Intrusion Prevention System (IPS) products. It is also able to communicate threat data with TippingPoint Deep Discovery products. A single SMS can manage multiple TippingPoint devices—the maximum number depends on usage, network, and other environmental conditions.

2.1 Overview

The TOE is available as a rack-mountable hardware appliance or as a software-based product (vSMS) that operates in a virtual environment.

The core functionality provided by the TOE is the ability to create multiple filter profiles that are distributed to specific devices. Devices can be organized into groups or security zones to facilitate distribution and updating of security profiles, rather than doing this individually for each device. Administrators can also use the TOE to keep managed devices updated with the latest TippingPoint Operating System (TOS) software and Digital Vaccine (DV) packages.

The main components of the TOE are:

- SMS Server—provisioned as a rack-mountable appliance or as a virtual server (vSMS)
- SMS Client—a Java-based application for Windows, Linux or Mac workstations.

Note that SMS also provides a web-based interface (the web management console) that enables administrators to install or upgrade SMS client software, monitor the TippingPoint devices installed on the network, and access Threat Insights. However, except for its role in the installation of the SMS Client on a management workstation, the web management console is excluded from the scope of evaluation, as are its associated HTTP and REST APIs.

The SMS Server in its evaluated configuration provides the following administrative interfaces:

- SMS Client—a Java-based application for Windows, Linux or Mac workstations. The SMS Client provides a Graphical User Interface (GUI) enabling administrators to configure and manage the SMS and TippingPoint TPS and IPS devices installed on the network.
- SMS Command Line Interface (CLI)—a text-based interface that enables users with **superuser** rights to log on to and configure the SMS Server.

The SMS Server is built on top of CentOS and includes a MariaDB database and JBoss 5.1 GA application server. It also incorporates Network Security Services and OpenSSL cryptographic modules to provide support respectively for Transport Layer Security (TLS) and Secure Shell (SSH) cryptographic protocols.

The SMS Client consists of a GUI and a dashboard to enable users to manage TippingPoint TPS and IPS devices and interact with the following services and components:

- Threat Management Center (TMC)—centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.
- ThreatLinQ—TippingPoint service that works with the TMC to collect and analyze information about the security posture of the Internet.
- Digital Vaccine (DV)—update service that includes up-to-date filter packages for protecting the network.

Communication between the SMS Server and SMS Client is secured using HTTPS. HTTPS is also used to protect communication between the SMS Server and managed TippingPoint devices.

The SMS Server additionally supports secure communication with external authentication servers (RADIUS, Active Directory) and external syslog servers.

2.2 Product Description

The TOE provides centralized control for managing large-scale deployments of the following TippingPoint products:

- TippingPoint NX Series Next-Generation Intrusion Prevention System (IPS)—uses a combination of technologies, including deep packet inspection, threat reputation, and advanced malware analysis, on a flow-by-flow basis to detect and prevent attacks on the network.
- TippingPoint Threat Protection System (TPS)—a network security platform that offers comprehensive threat protection, shielding network vulnerabilities, blocking exploits, and defending against known and zero-day attacks.

The TOE also provides capabilities for communicating threat data with TippingPoint Deep Discovery (DD) devices. TippingPoint DD is a threat protection platform providing capabilities to detect, analyze and respond to network-based attacks. The platform includes the following products:

- DD Inspector—a network appliance that monitors all ports and over 100 different network protocols to discover advanced threats and targeted attacks
- DD Email Inspector—stops targeted ransomware attacks by blocking targeted spear phishing emails before they are delivered
- DD Analyzer—provides customized sandboxing for existing security solutions, including endpoint protection, web gateways, firewalls, and IPS products.

The SMS Client GUI provides the following work spaces that support the management of TippingPoint TPS and IPS deployments:

- Devices—the Devices workspace provides a dynamic view of the entire system, graphically depicting TippingPoint TPS and IPS devices currently under SMS management, their segments, and the hosts and services on those segments. Through this workspace, an administrator can monitor and manage all the TippingPoint TPS and IPS devices in the deployment. Device management includes such activities as adding devices to the SMS system, combining devices into related groups, changing device or network configurations, installing TOS updates, temporarily unmanaging a device, replacing a device, or deleting a device from the deployment. When an administrator assumes management of a device, the administrator can control networking configuration, virtual segments and segment groups, filters and customizations, and distribution of filters and software. The administrator can also monitor traffic processing, health, and hardware status on each device and its segments.
- Profiles—a profile is a collection of filters or rules that provides a method for setting up security configuration options for TippingPoint solutions. The TOE ships with a default profile, along with a standard Digital Vaccine with filters that address known security issues. TippingPoint provides regular updates to the Digital Vaccine along with other tools and services to monitor and respond to security threats to the network. The Profiles workspace provides capabilities to create, view, modify, distribute and delete profiles.
- Responder—responder features provide security mitigation to block infected or malicious traffic, inform the administrator of possible threats, and place the host into remediation. Responder policies monitor all traffic according to devices, and use filters to enact another layer of protection. Filters include action sets with options to automatically redirect users and halt trigger traffic flows. The Responder workspace provides a centralized environment for managing security response actions, policies, switches, and response history.
- Events—as the TOE responds to traffic triggered by the filters defined in profiles, data is logged in the SMS database. The Events workspace provides capabilities to filter, view, and save events for all or specific devices, segment groups, and event filter elements. The administrator can save, run, and manage queries through the Events workspace. Saved queries display in the Saved Queries sections in the navigation screen.
- Reports—as the TOE detects malicious attacks and manages network usage, event data is logged in the database. This information details the system's behavior as it responds to network traffic. The TOE provides a set of options to generate reports about the compiled and stored log information. The administrator can use reports in the TOE to generate up-to-the-moment data analysis to help in measuring network data. The Reports workspace enables the administrator to customize existing reports or build them from scratch.

- Admin—the Admin workspace enables the administrator to manage user access, system and audit logs, and system settings. Options available through the Admin workspace are limited to users with the appropriate role and access level.

TOE users (administrators) are assigned to one or more user groups. A user group pairs a role with resources that its members can access. A role is a set of capabilities that allows a user in that role to perform actions on resources (e.g., add a device). The TOE includes three pre-defined roles: **superuser**; **admin**; and **operator**. The **superuser** role grants full capabilities to all resources in the TOE. Note that, although the TOE provides the capability to define new user roles, only the pre-defined roles are supported in the evaluated configuration. However, since user groups are used to define the scope of activities that users can perform (i.e., two user groups of users with the **admin** role may be defined on the TOE, each of which is assigned access to different sets of devices), the creation of new user groups is permitted in the evaluated configuration.

All TOE users must be successfully identified and authenticated by the TOE before gaining access to any other TOE services. The TOE supports local password, remote (RADIUS, TACACS+, Active Directory) and CAC (certificate-based) authentication mechanisms. The TOE provides capabilities to configure minimum strength requirements (e.g., minimum length, required character sets) for passwords. The TOE can be configured to track the number of consecutive failed authentication attempts and lock the offending user account when the configured threshold has been met. The TOE will terminate interactive sessions that have been idle for a configurable period of time.

The TOE is able to generate audit records of security-relevant events occurring on the TOE, including startup and shutdown of the TOE, successful and unsuccessful administrator login attempts, and administrator activities. It provides administrators with the ability to review audit records stored in the audit trail. The audit records are stored on the SMS Server, where they are protected from unauthorized modification and deletion. In addition, the TOE can be configured to export audit records to an external syslog server using a communication channel protected by TLS.

2.3 Physical Boundaries

2.3.1 TOE Components

As discussed in Section 2.1 above, the TOE comprises the SMS Server and the SMS Client. The SMS Server is provisioned as an appliance-based solution and also as a virtual appliance, while the SMS Client is a Java-based application that is downloaded from the SMS Server (regardless whether the deployed SMS Server is a hardware or virtual appliance). Physically, the SMS Server is available in two hardware form-factors: SMS H3 appliance; and SMS H3 XL appliance. The following table summarizes both appliances.

Table 1: TOE Hardware Specifications

Model	SMS H3 Appliance	SMS H3 XL Appliance
Capacity	Up to 200 million historical events	Up to 600 million historical events Provides additional processing and storage recommended for deployments larger than 150 devices.
Form factor	1U Rack-mount (19 in)	2U Rack-mount (19 in)
Management ports	1 x 10/100/1000 BASE-T RJ45	1 x 10/100/1000 BASE-T RJ45
Data ports	4 x 10/100/1000 BASE-T RJ45	4 x 10/100/1000 BASE-T RJ45 2 x 10 GbE SFP+
Hard drives	2 x 600GB 6G SAS 10krpm 2.5 in	6 x 600GB 6G SAS 10krpm 2.5 in
RAID configuration	RAID 1	RAID 10

The Virtual Security Management System (vSMS) virtual appliance is a software-based SMS appliance that operates within a virtual environment. The vSMS platform supports management of an unlimited number (of any model) of TippingPoint devices. With few exceptions, the vSMS platform provides the same functionality, the same user interfaces, and operates the same as a physical SMS appliance. A supported virtual environment must already be installed and configured before vSMS is deployed.

The vSMS can be deployed in VMware or KVM virtual environments. The following are the minimum recommended system requirements for the vSMS platform:

- 300 GB virtual disk size
- 2 virtual CPUs
- 2.27 GHz CPU speed
- 12 GB memory
- 2 virtual network adapters.

Note, two virtual network adapters are required to match a physical SMS. One of the virtual network adapters is for management. The second one is required for High Availability out of band replication, even if replication is not in use.

For a VMware deployment, a supported VMware vSphere environment must already be set up before the vSMS can be installed and used. The vSMS platform uses a VMware Open Virtualization Format (OVF) file to operate, and runs on:

- VMware vSphere Client version 5.5, 6.0, or 6.5
- VMware ESX/ESXi version 5.5, 6.0, or 6.5.

For a KVM deployment, a supported KVM environment must already be set up before the vSMS can be installed and used. KVM deployment of vSMS is supported in the following environments:

- RHEL version 6 (for three cores); libvirt version 0.10.2; QEMU version 0.12.0
- RHEL version 7 with the KVM hypervisor (for four cores); libvirt version 1.1.0; Quick Emulator (QEMU) version 1.5.3.

The KVM environment must have the following tar packages installed:

- `qemu-kvm`
- `virt-install`
- `virt-viewer`.

After the SMS Server (hardware or virtual appliance) has been installed, the SMS Client can be downloaded from the SMS Server and installed onto a physical or virtual workstation running Windows, Linux or Mac OS X.

Note that the SMS Server includes a FIPS-compliant mode of operation. Application of this setting is recommended as a best practice but the security functionality claimed by the TOE does not explicitly require this setting to be enabled or disabled. Therefore, it is neither required by nor excluded from the TOE's evaluated configuration and can be enabled or disabled based on individual site requirements.

2.3.2 Operational Environment Components

In addition to the platform requirements identified above, the TOE may require the following in its operational environment, depending on configuration:

- SSH client application—to access the SMS Server CLI
- NTP server—provides time source for SMS Server
- syslog server—repository for exported audit records
- Active Directory, RADIUS or TACACS+ server—supports external user identification and authentication.

2.4 Logical Boundaries

This section describes the TOE's logical boundaries in terms of the security functions provided by the TOE.

2.4.1 Security Audit

The TOE is able to generate audit records of security-relevant events that occur on the TOE. Each generated audit record includes the following information: date and time of the event; identity of the subject that caused the event (username if the event resulted from the action of an identified user); description of the event; and its outcome. Audit records are stored within the MariaDB database on the SMS Server and are protected from unauthorized modification and deletion. The TOE restricts access to the audit trail to users in the superuser role, who are able to view all the records in the audit trail and to select audit records for display at the SMS Client GUI and sort the displayed records based on date/time, user name, host name, description, or result.

2.4.2 Identification & Authentication

Users must be identified and authenticated to the TOE prior to gaining access to the functions provided by the TOE, regardless of the access method being used (i.e., SMS client or CLI). The TOE supports five types of user authentication: local; RADIUS; Active Directory; TACACS+; and CAC. The TOE can be configured to lock a user account after a number (configurable by the administrator) of consecutive failed authentication attempts.

The TOE can be configured to enforce a password policy that specifies a minimum length for passwords and requirements for the composition of passwords and to re-authenticate the user after a configurable period of time. During the authentication process, the TOE provides only obfuscated feedback to the user.

2.4.3 Security Management

The TOE provides the capabilities necessary for administrators to manage the TOE security functionality. The TOE provides three predefined security management roles: **superuser**; **admin**; and **operator**. The **superuser** role has full capabilities to manage the TOE's security functionality, and specific capabilities are restricted to the **superuser** role.

2.4.4 Protection of the TSF

The SMS Server can be configured to obtain its date and time from a network-based Network Time Protocol (NTP) server, or the administrator can set the date and time manually. The SMS Server can also be configured as an NTP server and the TippingPoint devices it manages can be configured to obtain their date and time from the SMS Server. The administrator can then configure the SMS Server to obtain its time from another NTP Server.

The TOE uses TLS to protect communication between the SMS Client and SMS Server.

2.4.5 TOE Access

The TOE allows the administrator to configure a banner message to be displayed when a user attempts to log in at any of the TOE user interfaces. The administrator can also configure the TOE to display the access history of a user account, including unsuccessful and successful login attempts, when the user successfully logs in to the TOE.

The TOE can limit the number of concurrent sessions belonging to a single user to a value configured by the administrator. The default value when this function is enabled is 4 but can subsequently be set to other values. In the evaluated configuration, an authorized administrator must enable this function.

The TOE will terminate interactive sessions after a period of inactivity configurable by an administrator. By default, interactive sessions are terminated after 30 minutes of inactivity. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

2.4.6 Trusted Path/Channels

The TOE provides a trusted path for administrators of the TOE to communicate with the SMS Server. The trusted path is implemented using SSH for access to the CLI. Administrators initiate the trusted path to the CLI by establishing an SSH connection using an SSH client (e.g., `putty`).

The TOE uses TLS to provide a trusted channel between the SMS Server and the following trusted IT products: external TippingPoint devices it manages; external RADIUS and Active Directory authentication servers; external syslog server; Threat Management Center (TMC).

2.5 TOE Documentation

This section identifies the guidance documentation included in the TOE. The documentation comprises:

- Release Notes, Version 5.2
- URL Reputation Filtering Deployment Guide, June 2018
- Identity Agent Deployment Guide, October 2017
- SMS Command Line Interface (CLI) Reference, April 2019
- SMS H3 – Install Your Security Appliance, May 2017
- SMS H3 XL – Install Your Security Appliance, May 2017
- SMS User Guide, February 2019
- SMS Web API Guide, April 2019
- vSMS Getting Started Guide, July 2019
- SMS Responder User Guide, June 2018

3. Security Problem Definition

This section defines the security problem to be addressed by the TOE, in terms of threats to be countered by the TOE or its operational environment, and assumptions about the intended operational environment of the TOE.

3.1 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE.

A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PROTECT	The TOE software critical to security policy enforcement will be protected from unauthorized physical modification.

3.2 Threats

This section identifies and describes the threats to be countered by the TOE and its operational environment.

T.BRUTE_FORCE	An unauthorized user may gain access to the TOE through repeated password-guessing attempts.
T.INAPPRORIATE_USE	Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures.
T.INTEGRITY_COMPROMISE	An unauthorized user may attempt to modify or destroy audit data, thus removing evidence of unauthorized activity.
T.NETWORK_COMPROMISE	An unauthorized user with access to the network infrastructure attempts to read or modify TSF data communicated between components of the TOE, or between the TOE and external entities.
T.NO_ACCOUNTABILITY	Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.
T.UNAUTHORIZED_ACCESS	An unauthorized user may gain access to the TOE security functions and data.
T.UNAUTHORIZED_ACTIVITY	Authorized users perform unauthorized actions on the TOE.

4. Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 3.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.AUDIT	The TOE shall be able to generate audit records of security-relevant events.
O.AUDIT_REVIEW	The TOE shall provide a means for authorized users to review the audit records generated by the TOE.
O.I_AND_A	The TOE shall provide a means for users to be identified and authenticated before gaining access to TOE services.
O.LOGIN_BANNER	The TOE shall be able to display a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.
O.LOGIN_HISTORY	The TOE shall be able to display to the user, upon successful session establishment, information related to the last successful and unsuccessful attempts at session establishment made by the user.
O.PASSWORD_CONTROLS	The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.
O.PROTECTED _COMMS	The TOE shall protect communications between distributed parts of the TOE, and between the TOE and external entities, from disclosure and modification.
O.SECURITY_MANAGEMENT	The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.
O.SESSION_LIMITS	The TOE shall provide capabilities to restrict the number of concurrent interactive sessions belonging to the same user.
O.SESSION_TERMINATION	The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.
O.STORAGE	The TOE shall protect stored audit records from unauthorized modification or deletion.
O.THROTTLE	The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

4.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE.

OE.PERSONNEL	Those responsible for the TOE must ensure that personnel working as authorized administrators have been carefully selected and trained for proper operation of the TOE.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

5. IT Security Requirements

5.1 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn only from Part 2 of the Common Criteria v3.1 Revision 5.

Table 2: TOE Security Functional Components

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1 – Audit data generation
	FAU_GEN.2 – User identity association
	FAU_SAR.1 – Audit review
	FAU_SAR.2 – Restricted audit review
	FAU_SAR.3 – Selectable audit review
	FAU_STG.1 – Protected audit trail storage
FIA: Identification and Authentication	FIA_AFL.1 – Authentication failure handling
	FIA_ATD.1 – User attribute definition
	FIA_SOS.1 – Verification of secrets
	FIA_UAU.2 – User authentication before any action
	FIA_UAU.5 – Multiple authentication mechanisms
	FIA_UAU.6 – Re-authenticating
	FIA_UAU.7 – Protected authentication feedback
	FIA_UID.2 – User identification before any action
FMT: Security Management	FMT_MOF.1 – Management of security function behaviour
	FMT_MTD.1 – Management of TSF data
	FMT_SMF.1 – Specification of Management Functions
	FMT_SMR.1 – Security roles
FPT: Protection of the TSF	FPT_ITT.1 – Basic internal TSF data transfer protection
	FPT_STM.1 – Reliable time stamps
FTA: TOE Access	FTA_MCS.1 – Basic limitation on multiple concurrent sessions
	FTA_SSL.3 – TSF-initiated termination
	FTA_SSL.4 – User-initiated termination
	FTA_TAB.1 – Default TOE access banners
	FTA_TAH.1 – TOE access history
FTP: Trusted Path/Channels	FTP_ITC.1 – Inter-TSF trusted channel
	FTP_TRP.1 – Trusted path

5.1.1 Security Audit (FAU)

FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [***not specified***] level of audit; and
c) [**the following auditable events:**
- **Reading of information from the audit records**
- **All use of the authentication mechanism**
- **All use of the user identification mechanism**
- **Use of the management functions, including:**
  - **Modifications in the behavior of the functions of the TSF**
  - **Modifications to the values of TSF data**
- **Modifications to the group of users that are part of a role**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

FAU_GEN.2 – User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 – Audit review

FAU_SAR.1.1 The TSF shall provide [**superuser**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 – Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 – Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [**selection and ordering**] of audit data based on [**the following criteria:**
- **Audit records can be selected for display based on date/time ranges**
- **Displayed audit records can be ordered based on date/time, user name, host name, description, or result**].

FAU_STG.1 – Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

5.1.2 Identification and Authentication (FIA)

FIA_AFL.1 – Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [2..10]***] unsuccessful authentication attempts occur related to [**user login**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**lock the user account**].

FIA_ATD.1 – User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **User Identity**
- **Password**
- **Password Expiration**
- **Local Authentication Only**
- **User Groups**
- **Enabled**].

FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**the following constraints for all user accounts:**

- **Minimum length of fifteen characters**
- **At least one uppercase alphabetic character**
- **At least one lowercase alphabetic character**
- **At least one numeric character**
- **At least one non-alphanumeric character**
- **Must differ from previous password in at least half of corresponding character positions**
- **Must differ from User Identity**
- **Must differ from last *n* passwords, where *n* is configurable by an administrator in the range 1..10**].

FIA_UAU.2 – User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.5 – Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [**local passwords; support for remote authentication using RADIUS, Active Directory, or TACACS+; CAC**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**authentication method configured for the TOE, which can be one of the following:**

- **local password-based authentication**
- **remote authentication using RADIUS**
- **remote authentication using Active Directory**
- **remote authentication using TACACS+**
- **Common Access Card (CAC)**

Only one of these authentication methods can be configured at any one time, but the administrator can designate specific user accounts to always require local password-based authentication, regardless of the configured authentication method].

FIA_UAU.6 – Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**administrator has configured re-authentication of active sessions after a set amount of time in the range 8..48 hours**].

FIA_UAU.7 – Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [**obfuscated feedback**] to the user while the authentication is in progress.

FIA_UID.2 – User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security Management (FMT)

FMT_MOF.1 – Management of security function behaviour

FMT_MOF.1.1(1) The TSF shall restrict the ability to [***modify the behaviour of***] the functions [**authentication, system time**] to [**superuser**].

FMT_MOF.1.1(2) The TSF shall restrict the ability to [***enable, disable, modify the behaviour of***] the functions [**TOE access banner display**] to [**superuser**].

FMT_MOF.1.1(3) The TSF shall restrict the ability to [***enable, disable***] the functions [

- **authentication failure handling**
- **concurrent active session limit**
- **client session inactivity timeout**
- **user re-authentication**
- **previous login details display**]

to [**superuser**].

FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [***modify, delete, [add, manage, unmanage]***] the [**devices**] to [**superuser, admin**].

Application Note: Of the operations listed above, admin users can only perform the 'manage' operation.

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***modify, delete, [add]***] the [**responder devices**] to [**superuser**].

FMT_MTD.1.1(3) The TSF shall restrict the ability to [***modify, query, delete, [create, distribute]***] the [**profiles**] to [**superuser, admin**].

FMT_MTD.1.1(4) The TSF shall restrict the ability to [***modify, delete, [create]***] the [

- **device groups**
- **response policies**
- **response actions**
- **user accounts**
- **user groups**]

to [**superuser**].

FMT_MTD.1.1(5) The TSF shall restrict the ability to [***modify, delete, [create]***] the [**saved event queries, saved reports**] to [**superuser, admin**].

FMT_MTD.1.1(6) The TSF shall restrict the ability to [***modify***] the [

- **local password of another user**
- **password policy settings**
- **unsuccessful authentication attempts threshold**
- **re-authentication threshold**
- **maximum number of active user sessions**
- **client session inactivity timeout**
- **banner message**
- **system time**]

to [**superuser**].

FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- **Add, modify, delete, manage and unmanage devices**
- **Create, modify and delete device groups**
- **Create, query, modify, distribute and delete profiles**
- **Create, modify and delete response policies and response actions**
- **Add, modify, and delete responder devices**

- **Query and save events**
- **Create, modify and delete saved event queries**
- **Create, modify and delete saved reports**
- **Enable and disable authentication failure handling function**
- **Modify unsuccessful authentication attempts threshold**
- **Determine and modify behavior of the authentication function**
- **Enable and disable concurrent active session limit function**
- **Modify maximum number of active user sessions**
- **Enable and disable client session inactivity timeout function**
- **Modify client session inactivity timeout**
- **Enable and disable previous login details display function**
- **Enable and disable user re-authentication function**
- **Modify re-authentication threshold**
- **Create, modify and delete user accounts**
- **Create, modify and delete user groups**
- **Modify password policy settings**
- **Determine and modify behavior of the system time function**
- **Modify the system time**
- **Enable, disable and modify behavior of the TOE access banner display function**
- **Modify user passwords**].

FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [

- **superuser**
- **admin**
- **operator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.1.4 Protection of the TSF (FPT)

FPT_ITT.1 – Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure***, ***modification***] when it is transmitted between separate parts of the TOE.

FPT_STM.1 – Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.1.5 TOE Access (FTA)

FTA_MCS.1 – Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**4**] sessions per user.

Application Note: The "by default" clause assumes the TOE has been placed into its evaluated configuration, which requires the administrator to enable the "Limit number of total and user sessions" setting. This setting is not enabled by default, but it enforces the default limit of 4 sessions once enabled.

FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [**period of inactivity configurable in the range of 5..600 minutes for the SMS client and 1..32,000 minutes for the CLI**].

FTA_SSL.4 – User-initiated termination

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 – Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

FTA_TAH.1 – TOE access history

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [***date*, *time*, *location***] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [***date*, *time*, *location***] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

5.1.6 Trusted Path/Channels (FTP)

FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [***the TSF***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**communication with managed devices, remote RADIUS or Active Directory authentication requests, export of syslog records, communication with TMC**].

FTP_TRP.1 – Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***disclosure*, *[undetected modification]***].

FTP_TRP.1.2 The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***[all access to the CLI]***].

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 3: TOE Security Assurance Components

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1 – Security architecture description
	ADV_FSP.2 – Security-enforcing functional specification
	ADV_TDS.1 – Basic design
AGD: Guidance documents	AGD_OPE.1 – Operational user guidance
	AGD_PRE.1 – Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 – Use of a CM system
	ALC_CMS.2 – Parts of the TOE CM coverage
	ALC_DEL.1 – Delivery procedures

Requirement Class	Requirement Component
ASE: Security Target evaluation	ASE_CCL.1 – Conformance claims
	ASE_ECD.1 – Extended components definition
	ASE_INT.1 – ST introduction
	ASE_OBJ.2 – Security objectives
	ASE_REQ.2 – Derived security requirements
	ASE_SPD.1 – Security problem definition
	ASE_TSS.1 – TOE summary specification
ATE: Tests	ATE_COV.1 – Evidence of coverage
	ATE_FUN.1 – Functional testing
	ATE_IND.2 – Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2 – Vulnerability analysis

5.2.1 Development (ADV)

ADV_ARC.1 – Security architecture description

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 – Security-enforcing functional specification

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 – Basic design

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall provide the behaviour summary of each SFR-supporting or SFR-non-interfering TSF subsystem.

ADV_TDS.1.4C The design shall summarise the SFR-enforcing behavior of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.2.2 Guidance Documents (AGD)

AGD_OPE.1 – Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 – Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.
AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle Support (ALC)

ALC_CMC.2 – Use of a CM system

ALC_CMC.2.1D	The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2D	The developer shall provide the CM documentation.
ALC_CMC.2.3D	The developer shall use a CM system.
ALC_CMC.2.1C	The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C	The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 – Parts of the TOE CM coverage

ALC_CMS.2.1D	The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1C	The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C	For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 – Delivery procedures

ALC_DEL.1.1D	The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D	The developer shall use the delivery procedures.
ALC_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Security Target Evaluation (ASE)

ASE_CCL.1 – Conformance claims

ASE_CCL.1.1D	The developer shall provide a conformance claim.
ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.
ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 – Extended components definition

ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
ASE_ECD.1.2D	The developer shall provide an extended components definition.
ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
ASE_ECD.1.5C	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_INT.1 – ST introduction

ASE_INT.1.1D	The developer shall provide an ST introduction.
ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
ASE_INT.1.2C	The ST reference shall uniquely identify the ST.
ASE_INT.1.3C	The TOE reference shall uniquely identify the TOE.
ASE_INT.1.4C	The TOE overview shall summarise the usage and major security features of the TOE.
ASE_INT.1.5C	The TOE overview shall identify the TOE type.
ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.
ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_OBJ.2 – Security objectives

ASE_OBJ.2.1D	The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D	The developer shall provide a security objectives rationale.
ASE_OBJ.2.1C	The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C	The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C	The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
ASE_OBJ.2.4C	The security objectives rationale shall demonstrate that the security objectives counter all threats.
ASE_OBJ.2.5C	The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
ASE_OBJ.2.6C	The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_REQ.2 – Derived security requirements

ASE_REQ.2.1D	The developer shall provide a statement of security requirements.
ASE_REQ.2.2D	The developer shall provide a security requirements rationale.
ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the security requirements.
ASE_REQ.2.4C	All operations shall be performed correctly.
ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.
ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 – Security problem definition

ASE_SPD.1.1D	The developer shall provide a security problem definition.
ASE_SPD.1.1C	The security problem definition shall describe the threats.
ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 – TOE summary specification

ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

5.2.5 Tests (ATE)

ATE_COV.1 – Evidence of coverage

ATE_COV.1.1D	The developer shall provide evidence of the test coverage.
ATE_COV.1.1C	The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 – Functional testing

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.
ATE_FUN.1.1C	The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4C	The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 – Independent testing – sample

ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E	The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.6 Vulnerability Assessment (AVA)

AVA_VAN.2 – Vulnerability analysis

AVA_VAN.2.1D	The developer shall provide the TOE for testing.

AVA_VAN.2.1C	The TOE shall be suitable for testing.
AVA_VAN.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.2.3E	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.
AVA_VAN.2.4E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This section describes the following security functions implemented by the TOE to satisfy the SFRs claimed in Section 5.1:

- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path.

6.1 Security Audit

The SMS Audit Log contains detailed information about user activity. The TOE can generate audit records for the following auditable events:

- The start-up and shutdown of audit functions (the audit function automatically starts at system start-up and can only be shutdown at system shutdown. In both instances, a record of the event is recorded.)
- Reading of information from the audit records
- All use of the authentication mechanism
- All use of the user identification mechanism
- Use of the management functions, including:
  - Modifications in the behavior of the functions of the TSF
  - Modifications to the values of TSF data
- Modifications to the group of users that are part of a role.

All audit events include the date and time of the event, the type of event, the subject identity, and the outcome of the event, such as whether it was a success or failure.

An administrator in the **superuser** role can use the SMS Client GUI to view audit records in the audit trail. The SMS Audit Log screen displays the following information fields for each audit record:

- Date and time the audited event occurred
- User name associated with the account that performed the auditable action
- Name of the host from which the auditable action originated
- Description of the auditable action performed by the user
- Result of the auditable action—either success or failure.

All data is presented in such a manner that it can be read and the contents of the data can be interpreted; thus the reader can understand the content of the information presented.

The administrator can select the audit records to display from the audit trail based on duration (i.e., all audit records generated in the last x minutes, hours or days), or date/time range by specifying a start time and end time. The administrator can sort the displayed audit records, in ascending or descending order, based on any of the displayed information fields, as listed above (i.e., date/time, user name, host name, description, or result).

The SMS Server provides local storage of generated audit records in a MariaDB database that is not accessible from outside the TOE boundary and that protects the stored audit records from unauthorized modification and deletion. The SMS Server can also be configured to transmit audit records to an external syslog server.

The Security Audit security function satisfies the following security functional requirements:

- FAU_GEN.1—audit records are generated for security relevant events and include the date and time of the event, type of event, subject identity, and outcome of the event.
- FAU_GEN.2—audit events generated as the result of actions of identified users include the user identification.
- FAU_SAR.1—the TOE provides users in the **superuser** role with the ability to read all audit information from the audit records. The audit records are displayed in a manner suitable for the authorized user to interpret the information.
- FAU_SAR.2—the TOE prohibits all users read access to the audit records, except those users that have been granted explicit read-access (i.e., users in the **superuser** role).
- FAU_SAR.3— the TOE provides capabilities to select audit records for display based on date/time range and to order displayed audit records based on contents of individual fields in the audit record.
- FAU_STG.1—the TOE protects stored audit records from unauthorized modification and deletion.

6.2 Identification and Authentication

In order to access the TOE, a user must have a user account defined on the TOE. The user account includes the following attributes associated with the user:

- User Identity—also referred to as username. This is the identifier the user provides to log in to the TOE
- Password—used to authenticate the user identity when the TOE or user account are configured for local authentication
- Password Expiration—if enabled, specifies the maximum time in days the password remains valid. Can be set to an integer value in the range 1..365
- Local Authentication Only—specifies the user must authenticate locally to the TOE using their password, regardless of the authentication mechanism that has otherwise been configured for the TOE
- Groups—the user groups of which the user account is a member
- Enabled—indicates whether the user account is enabled or disabled.

Users must be identified and authenticated to the TOE prior to gaining access to the functions provided by the TOE, regardless of the access method being used (i.e., SMS client or CLI). The TOE supports five types of user authentication: local; RADIUS; Active Directory; TACACS+; and CAC:

- Local—authentication is performed locally on the TOE
- RADIUS—authentication is performed on a RADIUS server, while the user role and access rights are maintained on the TOE. If the RADIUS server is unavailable, the TOE can authenticate local users. There is no ability to manage the TOE user account on the RADIUS server, but the user password can be modified only from the RADIUS server
- Active Directory—authentication is performed on the Active Directory (AD) server, while user role and access rights are maintained on the TOE. If the AD server is unavailable, the TOE can authenticate local users if the Authentication Mode for the active group mapping is set to “Allow only users defined in the SMS to login.” If another mode has been configured, only users whose access privileges are maintained locally on the TOE are able to login. There is no ability to manage the TOE user account on the AD server, but the user password can be modified only from the AD server
- TACACS+—authentication is performed on the TACACS+ server, while user role and access rights are maintained on the TOE. If the TACACS+ server is unavailable, the TOE can authenticate local users. There is no ability to manage the TOE user account on the TACACS+ server, but the user password can be modified only from the TACACS+ server

- CAC—authentication is performed on the SMS server using Certificate Authority (CA) certificates and an ActivClient smart card reader. Users are validated against their Active Directory accounts. The SMS matches a user's group in Active Directory with a user group on the SMS. If the SMS is in CAC Authentication mode, all SMS users must log in using CAC. No local users are allowed to log into the SMS client.

Only one authentication method per SMS server is permitted at any one time, but the TSF does allow an administrator to designate user accounts that must always be authenticated locally regardless of the designated authentication source. In this way, you can configure the SMS to use either RADIUS, Active Directory, or TACACS+ as an authentication source, but to specify user accounts that must be authenticated on the TOE.

An administrator is able to configure the TOE to disable the accounts of TOE users after a specified number of consecutive failed login attempts. When the administrator enables this mechanism, the administrator specifies the number of consecutive failed authentication attempts allowed before the account is disabled. The value can be in the range from 2 to 10 attempts.

When the configured number of consecutive failed authentication attempts is met, the user account is disabled and the TOE will not accept any attempts to login to the account. An administrator must enable the account in order for the user to be able to login to the TOE.

The TOE controls the minimum requirements for user names and passwords through the **Security** system preference, which has the following possible values and associated effects.

Level	Description
0 – None	• User names cannot contain spaces • Password length and complexity are not restricted
1 – Low	• User names must be at least six characters • Passwords must be at least eight characters • New password must be different from the previous password

2 – Medium (default)	• User names must be at least six characters
	• Passwords must meet Level 1 (Low) restrictions and the following:
	  o Must contain at least two alphabetic characters
	  o Must contain at least one numeric characters
	  o Must contain at least one non-alphanumeric character

3 – High	• User names must be at least six characters
	• Passwords must meet Level 2 (Medium) restrictions and the following:
	  o Must contain at least 15 characters
	  o Must contain at least one uppercase character
	  o Must contain at least one lowercase character
	  o Must be different from the previous password in at least half of the corresponding character positions

In addition to the restrictions enforced by the configured **Security** level, as described above, the following options related to password policy can also be configured:

- **Require password to be different from user ID**—if configured, prevents a user from having a password that is the same as their user identity
- **Require new password to be different from previous passwords**—if configured, requires the new password to be different from the previous *n* passwords, where *n* can be in the range 1..10
- **Enforce a minimum password lifetime**—if configured, enforces a minimum password lifetime of 24 hours, i.e., after a password change, the user is unable to change the password again until the minimum time has passed.

During the authentication process, the TOE provides only obfuscated feedback to the user. The administrator can configure the TOE to require a user to re-authenticate their current interactive session after a configurable period of time, in the range 8 to 48 hours.

The Identification and Authentication function satisfies the following security functional requirements:

- FIA_AFL.1—the TOE provides the administrator the ability to specify if the TOE will lock a user out after a specified number of unsuccessful login attempts.
- FIA_ATD.1—the TOE maintains the following security attributes associated with each user: User Identity; Password; Password Expiration; Local Authentication Only; User Groups; and Enabled status.
- FIA_SOS.1—the TOE can be configured to enforce a password policy that ensures all secrets (i.e., passwords) associated with user accounts meet policy requirements. The constraints specified in FIA_SOS.1 are met by setting **Security** level to High (3) and configuring the **Require password to be different from user ID** and **Require new password to be different from previous passwords** options.
- FIA_UAU.2—the TOE requires each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
- FIA_UAU.5—the TOE supports the following authentication mechanisms: local password-based authentication; remote authentication using RADIUS, Active Directory or TACACS+; and user identification and authentication using Common Access Card (CAC).
- FIA_UAU.6—the TOE can be configured to re-authenticate a user after a set amount of time from 8-48 hours.
- FIA_UAU.7—the TOE provides only obfuscated feedback to the user during authentication.
- FIA_UID.2—the TOE requires each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.3 Security Management

The TOE uses *capabilities* and *roles* to give users permissions to perform specific actions within the system. A *capability* is an ability to affect an object in the system—for example, the ability to add a device. A *role* is a collection of capabilities.

The TOE includes three predefined roles: **superuser**; **admin**; and **operator**. These predefined roles cannot be modified. The TOE provides the ability to define new roles, but this ability is not supported in the evaluated configuration—users are to be assigned only to predefined roles. Specific management functions available to members of these roles are listed below. At a high level, the roles are given the following capabilities:

- **operator** – read-only capabilities, can perform functions such as running reports/queries, viewing configuration settings, and viewing traffic and audit data.
- **admin** – management of basic configuration settings such as report management, profile management and general device management.
- **superuser** – all other TOE functionality, including management of advanced configuration settings, responder configuration, device configuration, and internal TSF management such as management and users and groups.

The predefined roles have hierarchical permissions so both **admin** and **superuser** roles also have **operator** privileges, and the **superuser** role also has **admin** privileges. The **superuser** role has full access to all management functionality of the TOE. It is also the only role that has access to the SMS CLI.

Access rights and capabilities of users are further controlled through *user groups*. User groups provide a way to align user capabilities with functional areas on the TOE. A user group pairs a role with resources that its members can access. Every TOE user account must be assigned to at least one user group.

The TOE has one predefined user group called **superuser**. The **superuser** user group includes the **superuser** role and provides access to all TOE features and functionality. New user groups must be created to specify access rights for users who do not have **superuser** privileges (i.e., are not assigned to the **superuser** user group). The new user groups assign role capabilities (such as **admin** and **operator** capabilities) to resources. The role assigned to a user group specifies the rights to execute the capabilities to manage the user group resources. When a user group is created, the following resources can be allocated to the user group to specify what resources members of the user group can manage: devices; segment groups; profiles; DV toolkit packages; action sets; and reports.

The TOE provides the following security management functions:

- Manage devices and device groups—the following actions related to this function can be performed by the following roles:
  - General device management (DDoS settings, VLAN management, configuration management, TOS management)—**superuser** or **admin** only
  - Advanced device management (ports, segments, inspection bypass rules, core controller, security configuration)—**superuser** only
  - Create, modify and delete device groups—**superuser** only
  - Assume and relinquish management of a device—**superuser** only

- Manage profiles—the following actions related to this function can be performed by the following roles:
  - Create, edit, or delete query—all roles
  - Create, query, modify, distribute, and delete profiles and profile elements (except for reputation management)—**superuser** or **admin** only
  - Create, update, delete reputation data—**superuser** only

- Manage responder—the following actions related to this function can be performed by the following roles:
  - View responder settings configuration—all roles
  - Create, modify and delete response policies—**superuser** only
  - Create, modify and delete response actions—**superuser** only
  - Add, modify, and delete Responder network devices—**superuser** only

- Manage events—only a user in the **superuser** or **admin** role can perform the following actions:
  - Query and save events
  - Create, modify and delete saved event queries

- Manage reports—only a user in the **superuser** or **admin** role can perform the following actions:
  - Create, modify and delete saved reports.

- Manage authentication function—configure how the SMS Server authenticates user login requests (local password, RADIUS, Active Directory, TACACS+, or CAC). Only a user in the **superuser** role can determine and modify the behavior of the authentication function.

- Manage authentication failure handling function—determine whether the TOE locks a user out after a specified number of unsuccessful login attempts and specify the number of unsuccessful consecutive attempts a user can make before their account is locked out. Only a user in the **superuser** role can enable and disable the authentication failure handling function and modify the unsuccessful authentication attempts threshold.

- Manage user re-authentication function—determine whether the TOE requires the user to re-authenticate after a set interval of time, from 8-48 hours. Only a user in the **superuser** role can enable and disable the user re-authentication function and modify the re-authentication threshold.

- Manage concurrent active session limit function—set the SMS Server to limit the number of concurrent active sessions it allows per user, and specify the maximum number. Only a user in the **superuser** role can enable and disable the concurrent active session limit function and modify the maximum number of active user sessions.

- Manage client session inactivity timeout function—configure the SMS Client to end interactive sessions after a specified period of inactivity. The time period can be set in the range 5-600 minutes. Only a user in the **superuser** role can enable and disable the client session inactivity timeout function and modify the client session inactivity timeout.

- Manage password policy settings—only a user in the **superuser** role can modify the **Security** level and the following password policy options:
    - **Require password to be different from user ID**—if configured, prevents a user from having a password that is the same as their user identity
    - **Require new password to be different from previous passwords**—if configured, requires the new password to be different from the previous *n* passwords, where *n* can be in the range 1..10
    - **Enforce a minimum password lifetime**—if configured, enforces a minimum password lifetime of 24 hours, i.e., after a password change, the user is unable to change the password again until the minimum time has passed.
- Manage the system time function—configure how the SMS Server obtains its date and time. The SMS Server can be configured to obtain its date and time from a network-based NTP server, or the administrator can set the date and time manually. Only a user in the **superuser** role can determine and modify the behavior of the system time function and modify the system time.
- Manage TOE access banner display function—configure the SMS Server to display a banner message when a user attempts to log in to the SMS Client and CLI. The message can be up to 4,000 characters. Only a user in the **superuser** role can enable, disable and modify the behavior of the TOE access banner display function.
- Manage user accounts—create, modify and delete user accounts. Only a user in the **superuser** role can perform these actions.
- Manage user groups—create, modify and delete user groups. Only a user in the **superuser** role can perform these actions.
- Modify user passwords—users can modify their own locally-defined passwords, and a user in the **superuser** role can modify the locally-defined passwords of other users – the TSF cannot be used to modify passwords defined outside the TOE (e.g. RADIUS, Active Directory).

The Security Management function satisfies the following security functional requirements:

- FMT_MOF.1(*)—the TOE is able to restrict the management of aspects of the TSF to users assigned specific administrative roles.
- FMT_MTD.1(*)—the TOE is able to restrict the management of TSF data to users assigned specific administrative roles.
- FMT_SMF.1—the TOE provides the capabilities necessary to manage the security of the TOE.
- FMT_SMR.1—the TOE maintains the following built-in roles: **superuser**; **admin**; and **operator**. The TOE is able to associate users with these roles.

6.4 Protection of the TSF

The administrator is able to configure how the SMS Server component of the TOE obtains its date and time. The SMS Server can be configured to obtain its date and time from a network-based network time protocol (NTP) server, or the administrator can set the date and time manually.

The SMS Server can also be configured as an NTP server and the TippingPoint devices it manages can be configured to obtain their date and time from the SMS Server. The administrator can then configure the SMS Server to obtain its time from another NTP Server.

The TOE uses TLS to protect communication between the SMS Client and SMS Server. The TOE supports TLS v1.0, TLS v1.1, and TLS v1.2. If the TOE has been configured with FIPS mode enabled, TLS 1.2 is not available. The TOE supports the following TLS ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256 (TLS v1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384.

The Protection of the TSF function satisfies the following security functional requirement:

- FPT_ITT.1—the TOE uses TLS to protect TSF data communicated between distributed parts of the TOE.
- FPT_STM.1—the TOE is able to provide reliable time stamps.

6.5 TOE Access

The administrator can enable limits on the number of concurrent sessions that belong to the same user, as well as limits on the total number of concurrent sessions active on the TOE. When enabled, the TOE enforces a default limit of 4 concurrent sessions per user (configurable between 1 and 10).

The TOE can be configured to terminate interactive SMS client sessions after a period of inactivity configurable by an administrator in the range 5-600 minutes. A separate session timeout value can be configured for the CLI in the range 1-32,000 minutes. The TOE also allows user-initiated termination of the user's own interactive session by explicitly logging off.

The TOE can be configured by an administrator to display an advisory banner message prior to allowing an administrator to establish an administrative user session. The banner message will be displayed on the SMS client toolbar or when a user attempts to log in to the following interfaces: SMS client; web management console; command line interface (CLI); and remote SSH client.

The TOE can be configured by an administrator to display previous login details for a user, including the following information:

- Last successful login, including date, timestamp, and IP address
- Last failed login attempt, including date, timestamp, and IP address
- Number of failed login attempts since the last successful login
- Number of successful logins in last N days, where N is configurable between 1 and 30 days
- Any user group or role changes to the user account since the last login.

The display for the TOE access history includes a red 'X' button and the information remains on the screen until the user dismisses it by clicking on the 'X'.

The TOE access function satisfies the following security functional requirements:

- FTA_MCS.1—the TOE can limit the number of concurrent sessions belonging to a single user to a value configured by the administrator. The default value when this function is enabled is 4
- FTA_SSL.3—the TOE will terminate an interactive user session after 30 minutes of inactivity
- FTA_SSL.4—the TOE allows user-initiated termination of the user's own interactive session
- FTA_TAB.1—the TOE allows the administrator to configure a banner message to be displayed when a user attempts to log in at any of the TOE user interfaces
- FTA_TAH.1—the TOE allows the administrator to configure the TOE to display the access history of a user account, including unsuccessful and successful login attempts, when the user successfully logs in to the TOE.

6.6 Trusted Path/Channels

The TOE provides a trusted path for administrators of the TOE to communicate with the SMS Server. The trusted path is implemented using SSH for access to the CLI. Administrators initiate the trusted path to the CLI by establishing an SSH connection using an SSH client (e.g., `putty`).

The TOE uses TLS to protect communication between the SMS Server and the following trusted IT products:

- external TippingPoint devices it manages
- external RADIUS authentication server (using TLS to protect EAP traffic)

- external Active Directory authentication server (using TLS to protect LDAP traffic)
- external syslog server
- external TMC

The TOE supports TLS v1.0, TLS v1.1, and TLS v1.2. As stated in section 6.4, the TOE only supports TLS v1.2 when the optional FIPS mode is not enabled. The TOE supports the following TLS ciphersuites when it is acting as a server:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256 (TLS 1.2 only)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

The Trusted Path/Channels function satisfies the following security functional requirements:

- FTP_ITC.1—the TOE supports a trusted channel with trusted IT products that protects transmitted data from disclosure and undetected modification.
- FTP_TRP.1—the TOE provides a trusted path for administrators to communicate with the TOE, using SSH to access the CLI.

7. Rationale

This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions and threats are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

Table 4: Security Problem Definition to Security Objective Correspondence

	T.BRUTE_FORCE	T.INAPPROPRIATE_USE	T.INTEGRITY_COMPROMISE	T.NETWORK_COMPROMISE	T.NO_ACCOUNTABILITY	T. UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_ACTIVITY	A.MANAGE	A.PROTECT
O.AUDIT					X				
O.AUDIT_REVIEW					X				
O.I_AND_A						X			
O.LOGIN_BANNER		X							
O.LOGIN_HISTORY						X			
O.PASSWORD_CONTROLS	X								
O.PROTECTED_COMMS				X					
O.SECURITY_MANAGEMENT							X		
O.SESSION_LIMITS						X			
O.SESSION_TERMINATION						X			
O.STORAGE			X						
O.THROTTLE	X								
OE.PERSONNEL								X	
OE.PHYSICAL									X

T.BRUTE_FORCE

An unauthorized user may gain access to the TOE through repeated password-guessing attempts.

This threat is countered by the following security objectives:

- O.PASSWORD_CONTROLS—addresses this threat by providing a mechanism that encourages users to choose difficult-to-guess passwords.

- O.THROTTLE—addresses this threat by providing a mechanism, configurable by an administrator, to lock a user account after a specified number of consecutive failed authentication attempts has been met.

T.INAPPRORIATE_USE

Authorized users perform inappropriate actions on the TOE due to ignorance of their responsibilities or operational policies and procedures.

This threat is countered by the following security objective:

- O.LOGIN_BANNER—addresses this threat by displaying a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.

T.INTEGRITY_COMPROMISE

An unauthorized person may attempt to modify or destroy audit data, thus removing evidence of unauthorized activity.

This threat is countered by the following security objective:

- O.STORAGE—addresses this threat by ensuring the TOE is able to protect stored audit records from unauthorized modification and deletion.

T.NETWORK_COMPROMISE

An unauthorized user with access to the network infrastructure attempts to read or modify TSF data communicated between components of the TOE, or between the TOE and external entities.

This threat is countered by the following security objective:

- O.PROTECTED_COMMS—addresses this threat by ensuring communications between components of the TOE and between the TOE and external entities are protected from disclosure and undetected modification.

T.NO_ACCOUNTABILITY

Authorized users of the TOE perform adverse actions on the TOE, or attempt to perform unauthorized actions, which go undetected.

This threat is countered by the following security objectives:

- O.AUDIT—addresses this threat by ensuring the TOE is able to generate audit records of security relevant events.
- O.AUDIT_REVIEW—supports O.AUDIT in addressing the threat by ensuring the TOE provides capabilities for effective review of stored audit records.

T.UNAUTHORIZED_ACCESS

An unauthorized user may gain access to the TOE security functions and data.

This threat is countered by the following security objectives:

- O.I_AND_A—addresses this threat by ensuring all users of the TOE are identified and authenticated prior to gaining further access to the TOE and its services.
- O.SESSION_TERMINATION—supports O.I_AND_A in addressing this threat by providing users with a mechanism to terminate their interactive sessions with the TOE, and by ensuring sessions that have been inactive for a configurable period of time will be terminated by the TOE.
- O.SESSION_LIMITS—supports O.I_AND_A in addressing this threat by ensuring the TOE provides capabilities to restrict the number of concurrent interactive sessions belonging to the same user, reducing the likelihood of a user having multiple unattended active sessions.
- O.LOGIN_HISTORY—supports O.I_AND_A by ensuring users are made aware of the login history of their user accounts each time they login to the TOE.

T.UNAUTHORIZED_ACTIVITY

Authorized users perform unauthorized actions on the TOE.

This threat is countered by the following security objective:

- O.SECURITY_MANAGEMENT—addresses this threat by providing a mechanism that requires authorized users to have appropriate privileges in order to perform actions on the TOE.

A.MANAGE

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

This assumption is satisfied by the following security objective:

- OE.PERSONNEL—this objective satisfies the assumption by ensuring those assigned as authorized administrators are properly trained in operating the TOE.

A.PROTECT

The TOE hardware and software critical to the security policy enforcement will be located within controlled access facilities which will prevent unauthorized physical access.

This assumption is satisfied by the following security objective:

- OE.PHYSICAL—this objective satisfies the assumption by ensuring the TOE is protected from physical attack.

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this ST are fully addressed in this section and each is mapped to the objective it is intended to satisfy. Table 5 summarizes the correspondence of functional requirements to TOE security objectives.

Table 5: Objectives to Requirement Correspondence

	O.AUDIT	O.AUDIT_REVIEW	O.I_AND_A	O.LOGIN_BANNER	O.LOGIN_HISTORY	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_LIMITS	O.SESSION_TERMINATION	O.STORAGE	O.THROTTLE
FAU_GEN.1	X											
FAU_GEN.2	X											
FAU_SAR.1		X										
FAU_SAR.2		X										
FAU_SAR.3		X										
FAU_STG.1											X	
FIA_AFL.1												X
FIA_ATD.1			X									
FIA_SOS.1						X						
FIA_UAU.2			X									
FIA_UAU.5			X									

	O.AUDIT	O.AUDIT_REVIEW	O.I_AND_A	O.LOGIN_BANNER	O.LOGIN_HISTORY	O.PASSWORD_CONTROLS	O.PROTECTED_COMMS	O.SECURITY_MANAGEMENT	O.SESSION_LIMITS	O.SESSION_TERMINATION	O.STORAGE	O.THROTTLE
FIA_UAU.6			X									
FIA_UAU.7			X									
FIA_UID.2			X									
FMT_MOF.1(*)								X				
FMT_MTD.1(*)								X				
FMT_SMF.1								X				
FMT_SMR.1								X				
FPT_ITT.1							X					
FPT_STM.1	X									X		
FTA_MCS.1									X			
FTA_SSL.3										X		
FTA_SSL.4										X		
FTA_TAB.1				X								
FTA_TAH.1					X							
FTP_ITC.1							X					
FTP_TRP.1							X					

O.AUDIT

The TOE shall be able to generate audit records of security-relevant events.

The following security functional requirements contribute to satisfying this security objective:

- FAU_GEN.1—the ST includes FAU_GEN.1 to specify the ability to generate audit records of security-relevant events, and to specify the specific events to be audited and the content of generated audit records of those events.
- FAU_GEN.2—the ST includes FAU_GEN.2 to support FAU_GEN.1 by specifying that generated audit records include the identity of the user that caused the auditable event.
- FPT_STM.1—the ST includes FPT_STM.1 to support FAU_GEN.1 by specifying that the TOE shall be able to provide reliable time stamps, which enables the TOE to include an accurate date and time in each audit record it generates.

O.AUDIT_REVIEW

The TOE shall provide a means for authorized users to review the audit records generated by the TOE.

The following security functional requirements contribute to satisfying this security objective:

- FAU_SAR.1—the ST includes FAU_SAR.1 to specify which roles are to be able to read data from stored audit records.
- FAU_SAR.2—the ST supports FAU_SAR.1 by including FAU_SAR.2 to specify that the ability to read data from stored audit records is restricted to only the roles specified in FAU_SAR.1.

- FAU_SAR.3—the ST supports FAU_SAR.1 by including FAU_SAR.3 to specify capabilities for selecting audit records for display based on time span and for sorting displayed audit records based on audit record attributes, which assists the authorized roles in effectively reviewing the audit trail.

O.I_AND_A

The TOE shall provide a means for users to be identified and authenticated before gaining access to TOE services.

The following security functional requirements contribute to satisfying this security objective:

- FIA_UID.2, FIA_UAU.2—the ST includes FIA_UID.2 and FIA_UAU.2 to specify that users must be successfully identified and authenticated by the TOE before being able to perform any other TSF-mediated actions.
- FIA_ATD.1—the ST supports FIA_UID.2 and FIA_UAU.2 by including FIA_ATD.1 to ensure user identity and authentication data security attributes are associated with individual users.
- FIA_UAU.5—the ST supports FIA_UAU.2 by including FIA_UAU.5 to specify the authentication mechanisms supported by the TOE and the rules by which the TOE authenticates a user's claimed identity.
- FIA_UAU.6—the ST supports FIA_UAU.2 by including FIA_UAU.6 to specify that administrators can configure the TOE to require users must to re-authenticate their current active session after a set amount of time.
- FIA_UAU.7—the ST supports FIA_UAU.2 by including FIA_UAU.7 to specify that only obfuscated feedback is provided to the user while authenticating to the TOE.

O.LOGIN_BANNER

The TOE shall be able to display a configurable advisory warning message to potential users pertaining to appropriate use of the TOE.

The following security functional requirement contributes to satisfying this security objective:

- FTA_TAB.1—the ST includes FTA_TAB.1 to specify the capability to display an advisory warning message regarding unauthorized use of the TOE.

O.LOGIN_HISTORY

The TOE shall be able to display to the user, upon successful session establishment, information related to the last successful and unsuccessful attempts at session establishment made by the user.

The following security functional requirement contributes to satisfying this security objective:

- FTA_TAH.1—the ST includes FTA_TAH.1 to specify the capability to display to the user, after logging in to the TOE, information related to that user's previous successful and unsuccessful attempts to login to the TOE.

O.PASSWORD_CONTROLS

The TOE shall provide a mechanism to reduce the likelihood that users choose weak passwords.

The following security functional requirement contributes to satisfying this security objective:

- FIA_SOS.1—the ST includes FIA_SOS.1 to specify that passwords must meet minimum construction requirements, in terms of length and character set.

O.PROTECTED_COMMS

The TOE shall protect communications between distributed parts of the TOE, and between the TOE and external entities, from disclosure and modification.

The following security functional requirements contribute to satisfying this security objective:

- FPT_ITT.1—the ST includes FPT_ITT.1 to specify that communications between distributed parts of the TOE will be protected from disclosure and modification.
- FTP_ITC.1, FTP_TRP.1—the ST includes FTP_ITC.1 and FTP_TRP.1 to specify that communications between the TOE and external entities (remote users or external IT entities) will be protected from disclosure and modification.

O.SECURITY_MANAGEMENT

The TOE shall restrict the ability to perform security management functions on the TOE to authorized administrators having appropriate privileges.

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1, FMT_SMR.1, FMT_MOF.1(*), FMT_MTD.1(*)—the ST includes these requirements to specify the security management functions to be provided by the TOE (FMT_SMF.1), to specify security management roles (FMT_SMR.1), and to specify the restrictions on management of security function behavior and TSF data (FMT_MOF.1(*), FMT_MTD.1(*)).

O.SESSION_LIMITS

The TOE shall provide capabilities to restrict the number of concurrent interactive sessions belonging to the same user.

The following security functional requirement contributes to satisfying this security objective:

- FTA_MCS.1—the ST includes FTA_MCS.1 to specify the capability for the TSF to restrict the number of concurrent interactive sessions belonging to the same user.

O.SESSION_TERMINATION

The TOE shall provide mechanisms to terminate a user session after a period of inactivity or at the request of the user.

The following security functional requirements contribute to satisfying this security objective:

- FTA_SSL.3—the ST includes FTA_SSL.3 to specify the ability for the TSF to terminate an interactive user session after a period of inactivity.
- FPT_STM.1—the ST includes FPT_STM.1 to support FTA_SSL.3 by specifying that the TOE shall be able to provide reliable time stamps, which enables the TOE to accurately determine when an interactive user session has been inactive for a period of time in excess of the configured inactivity timeout period.
- FTA_SSL.4—the ST includes FTA_SSL.4 to specify the ability for users to terminate their own interactive sessions.

O.STORAGE

The TOE shall protect stored audit records from unauthorized modification or deletion.

The following security functional requirement contributes to satisfying this security objective:

- FAU_STG.1—the ST includes FAU_STG.1 to specify the ability to protect audit records stored in the audit trail from unauthorized deletion and to prevent unauthorized modification of these records.

O.THROTTLE

The TOE shall limit the rate at which consecutive unsuccessful authentication attempts can be performed.

The following security functional requirement contributes to satisfying this security objective:

- FIA_AFL.1—the ST includes FIA_AFL.1 to specify the capability to limit the rate at which consecutive failed authentication attempts (which may indicate a password-guessing attack) can be made.

7.3 Security Assurance Requirements Rationale

EAL 2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The TOE is intended for use in an environment with good physical access security where it is assumed that attackers will have Basic attack potential. The target assurance level of EAL 2 is appropriate for such an environment.

7.4 Requirement Dependency Rationale

The following table identifies the SFRs claimed in the ST, their dependencies as defined in CC Part 2, and how the dependency is satisfied in the ST. It can be seen that all dependencies have been satisfied, either by inclusion in the ST of the appropriate dependent SFRs, or by functionality provided by the operational environment.

Table 6: Requirement Dependencies

Requirement	Dependencies	How Satisfied
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2 (hierarchical to FIA_UID.1)
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (hierarchical to FIA_UAU.1)
FIA_ATD.1	None	None
FIA_SOS.1	None	None
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FIA_UAU.5	None	None
FIA_UAU.6	None	None
FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 (hierarchical to FIA_UAU.1)
FIA_UID.2	None	None
FMT_MOF.1(*)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1(*)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FPT_ITT.1	None	None
FPT_STM.1	None	None
FTA_MCS.1	FIA_UID.1	FIA_UID.2 (hierarchical to FIA_UID.1)
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAB.1	None	None
FTA_TAH.1	None	None
FTP_ITC.1	None	None
FTP_TRP.1	None	None

7.5 TOE Summary Specification Rationale

Section 6, the TOE Summary Specification, describes how the security functions of the TOE meet the claimed SFRs. The following table provides a mapping of the SFRs to the security function descriptions to support the TOE Summary Specification.

Table 7: Security Functions vs. Requirements Mapping

	Security Audit	Identification and Authentication	Security Management	Protection of the TSF	TOE Access	Trusted Path
FAU_GEN.1	X					
FAU_GEN.2	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FAU_STG.1	X					
FIA_AFL.1		X				
FIA_ATD.1		X				
FIA_SOS.1		X				
FIA_UAU.2		X				
FIA_UAU.5		X				
FIA_UAU.6		X				
FIA_UAU.7		X				
FIA_UID.2		X				
FMT_MOF.1(*)			X			
FMT_MTD.1(*)			X			
FMT_SMF.1			X			
FMT_SMR.1			X			
FPT_ITT.1				X		
FPT_STM.1				X		
FTA_MCS.1					X	
FTA_SSL.3					X	
FTA_SSL.4					X	
FTA_TAB.1					X	
FTA_TAH.1					X	
FTP_ITC.1						X
FTP_TRP.1						X