

Trellix Security Enterprise Security Manager v11.6.12 Security Target

Document Version: 2.0

Date: 18 March 2025



6000 Headquarters Dr
Plano, TX 75024



2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
Version 0.1	October 12, 2020	Initial Release
Version 0.2	January 22, 2021	Updates based on vendor comments
Version 0.3	March 24, 2021	Updates based on clarification questions
Version 0.3.1	April 5, 2021	Updated intra-TOE communication Paths
Version 0.3.5	April 8, 2021	Updates and clarification of open issues
Version 0.4	April 26, 2021	Updates for TSS specificity
Version 1.0	June 9, 2021	Updated for QA comments. First release version.
Version 1.1	November 26, 2021	Updated the Table specifying intra-TOE communication and communication between TOE and administrator.
Version 1.2	March 07, 2022	Updated the ST according to recent changes in claims for SFRs and addressed ECR comments.
Version 1.3	April 27, 2023	Updated the ST according to recent changes in claims for SFRs and TOE name change.
Version 1.4	January 10, 2024	Updated the ST according to recent changes in OS version and name along with the addition of the CAVP certificate name.
Version 1.5	August 20, 2024	Updated the ST after addressing check-in ECR comments
Version 1.6	October 30, 2024	Mods per review.
Version 1.7	December 12, 2024	Mods per review.
Version 1.8	January 13, 2025	Updates based on QA review.
Version 1.9	February 3, 2025	Minor cosmetic updates.
Version 1.10	March 5, 2025	No changes. Wanted dates in sync with check-out docs
Version 2.0	March 18, 2025	Minor updates to address ECR comments.

Table of Contents

List of Figures	iii
1 Introduction	1
1.1 Security Target and TOE Reference	1
1.2 TOE Overview	1
1.3 TOE Description.....	1
1.3.1 Component Descriptions	5
1.3.2 Evaluated Configuration	6
1.3.3 Physical Boundary	6
1.4 TOE Operational Environment (OE)	7
1.4.1 Security Functions Provided by the TOE	8
1.4.2 TOE Documentation.....	10
1.5 Product Functionality not Included in the Scope of the Evaluation	10
2 Conformance Claims	11
2.1 CC Conformance Claims	11
2.2 Protection Profile Conformance	11
2.3 Conformance Rationale	11
2.3.1 Technical Decisions	11
3 Security Problem Definition	14
3.1 Threats	14
3.2 Assumptions.....	16
3.3 Organizational Security Policies	17
4 Security Objectives.....	18
4.1 Security Objectives for the Operational Environment.....	18
5 Security Requirements.....	20
5.1 Conventions	21
5.2 Security Functional Requirements	22
5.2.1 Security Audit (FAU).....	22
5.2.2 Communication Partner Control (FCO).....	26
5.2.3 Cryptographic Support (FCS).....	27
5.2.4 Identification and Authentication (FIA)	33
5.2.5 Security Management (FMT)	36
5.2.6 Protection of the TSF (FPT)	37
5.2.7 TOE Access (FTA).....	39

5.2.8	Trusted Path/Channels (FTP)	39
5.3	TOE SFR Dependencies Rationale for SFRs	40
5.4	Security Assurance Requirements	40
5.5	Assurance Measures	41
6	TOE Summary Specifications	42
6.1	Distributed TOE SFR Allocation	57
6.2	Cryptographic Key Destruction	60
6.3	CAVP Algorithm Testing	60
7	Acronym Table	63
	Appendix A	64

List of Figures

Figure 1: Representative TOE Deployment	2
---	---

List of Tables

Table 1: TOE/ST Identification	1
Table 2: TOE Components Communication	2
Table 3: TOE OE Components Communication	4
Table 4: TOE Component Descriptions	6
Table 5: TOE Software Component Descriptions	7
Table 6: Required Environmental Components	8
Table 7: TOE Provided Cryptography	8
Table 8: Technical Decisions (TDs)	11
Table 9: Threats	14
Table 10: Assumptions	16
Table 11: OSPs	17
Table 12: Security Objectives for the Operational Environment	18
Table 13: SFRs	20
Table 14: Security Functional Requirements and Auditable Events	22
Table 15: FAU_STG_EXT.4.1 Table	26
Table 16: Security Assurance Requirements	40
Table 17: TOE Security Assurance Measures	41
Table 18: TOE Summary Specification SFR Description	42
Table 19: Distributed TOE SFR Allocation	58
Table 20: Key Storage and Zeroization	60
Table 21 - CAVP Algorithm Testing References	60
Table 22: Acronyms	63

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1: TOE/ST Identification

Category	Identifier
ST Title	Trellix Security Enterprise Security Manager v11.6.12 Security Target
ST Version	2.0
ST Date	18 March 2025
ST Author	Intertek Acumen Security
TOE Identifier	Trellix Security Enterprise Security Manager
TOE Version	11.6.12
TOE Developer	Trellix
Key Words	Network Device, Distributed

1.2 TOE Overview

The Trellix Security Enterprise Security Manager v11.6.12 brings event, threat, and risk data together to provide strong security intelligence, rapid incident response, seamless log management, and extensible compliance reporting. The TOE is distributed amongst six devices as follows: Enterprise Security Manager (ESM), Event Receiver (ERC), Application Data Monitor (ADM), Advanced Correlation Engine (ACE), Enterprise Log Manager (ELM), and Enterprise Log Search (ELS). The six TOE components are divided into three categories as follows:

- Management Component: ESM
- Data Components: ERC, ADM
- Auxiliary Components: ACE, ELM, ELS

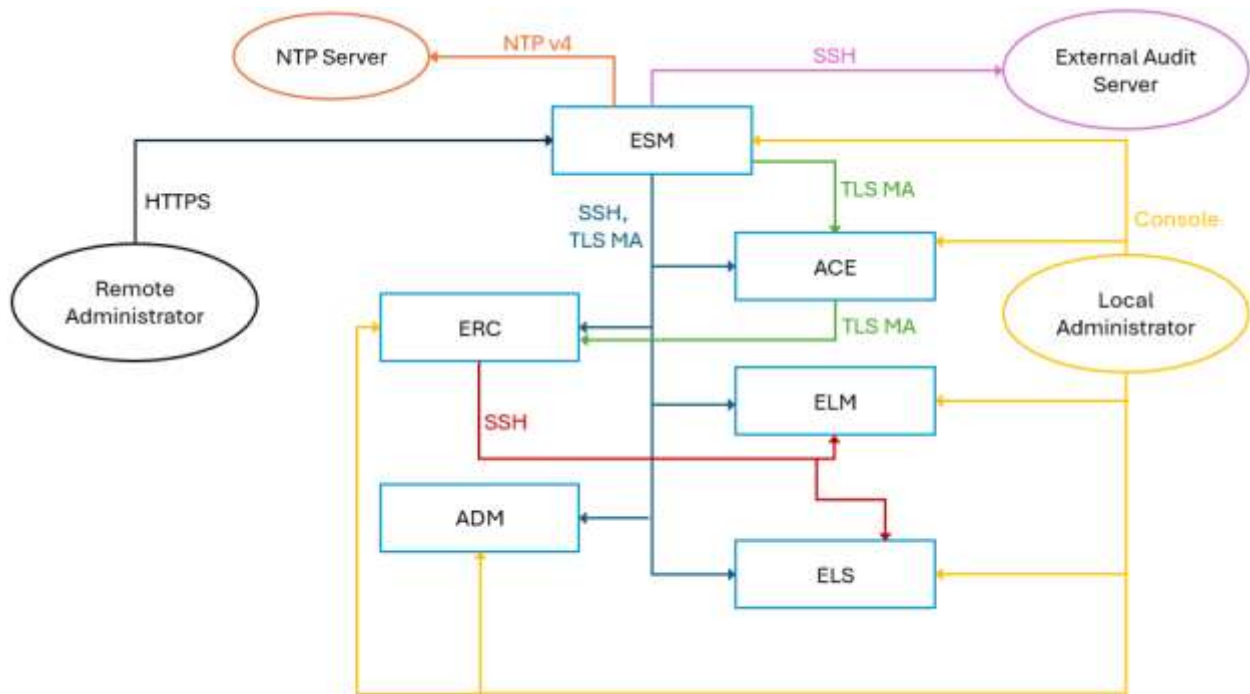
1.3 TOE Description

The TOE includes the hardware and software of the six Trellix Security Enterprise Security Manager components. TOE boundary encompasses all the devices of the Trellix Enterprise solution. The ESM is the central management entity responsible for managing all the other devices (colloquially called child devices) in the solution. All Data (ERC, ADM) and Auxiliary (ACE, ELM, ELS) are considered as child devices. Each of the child devices communicates with the ESM over TLS with mutual-authentication and SSH. The management-plane traffic between the ESM and child devices uses SSH; whereas the data-plane traffic uses X.509v3 mutually authenticated TLS. To manage the ESM (and the child devices via ESM), an

administrator logs into the Web GUI of the ESM using HTTPS over TLS. Alternatively, an administrator may log into the local console of any of the TOE six components for local administration. Additionally, some of the child devices can communicate with each other over SSH and/or TLS trusted channels. The ESM communicates with a remote audit Syslog server over SSH to store the TOE-generated audit records. The Figure 1 below depicts a representative TOE deployment and interaction between the TOE components and external entities.

Note: The different color coding is only used to easily distinguish communication between the endpoints and it has no other significance.












Figure 1: Representative TOE Deployment



The TOE components communicate with each other over TLS or SSH as identified in the following table. The colored lines correspond to the Figure above.

Table 2: TOE Components Communication

TOE Component	Client	Server	Protocol	Purpose / Data Exchanged
ESM	ESM	All other components	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM	All other components	TLS MA	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. All other components act as TLS servers. The TLS channel is Mutually Authenticated.

TOE Component	Client	Server	Protocol	Purpose / Data Exchanged
	ESM 	ACE	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ACE acts as a TLS Server. The TLS channel is Mutually Authenticated.
ACE	ESM 	ACE	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM 	ACE	TLS MA	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. All other components act as TLS servers. The TLS channel is Mutually Authenticated.
	ESM 	ACE	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ACE acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ACE 	ECR	TLS MA	Data Plane. Parsed event log data. ACE acts as a TLS Client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
ERC	ERC 	ELM	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server
	ERC 	ELS	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server
	ESM 	ERC	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	ESM 	ERC	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ACE 	ERC	TLS MA	Data Plane. Parsed event log data. ACE acts as a TLS Client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
ELM	ESM 	ELM	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.

TOE Component	Client	Server	Protocol	Purpose / Data Exchanged
	<u>ESM</u>	ELM	TLS MA	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. All other components act as TLS servers. The TLS channel is Mutually Authenticated.
	<u>ERC</u>	ELM	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server
ADM	<u>ESM</u>	ADM	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	<u>ESM</u>	ADM	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ADM acts as a TLS Server. The TLS channel is Mutually Authenticated.
ELS	<u>ESM</u>	ELS	SSH	Control Plane. All configuration and control data. ESM acts as an SSH client, and other TOE components are SSH servers.
	<u>ESM</u>	ELS	TLS MA	Data Plane. Parsed event log data. ESM acts as a TLS client. ELS acts as a TLS Server. The TLS channel is Mutually Authenticated.
	<u>ERC</u>	ELS	SSH	Data Plane. Raw event log data. ERC acts as an SSH client. ELM and ELS act as an SSH server

The following table describes the Operational Environment communications.

Table 3: TOE OE Components Communication

IT Entity	TOE Component	Protocol	Purpose / Data Exchanged
Remote Administrator	ESM	HTTPS	Control Plane. Administrator's remote GUI session. ESM acts as a non-MA TLS server.
NTP server	ESM	NTP v4	Time synchronization. ESM acts as an NTP client. The communication is unencrypted.
External Audit Server	ESM	SSH	Export audit logs. ESM acts as an SSH client.
Local Administrator	All TOE components	Console	Control Plane. Administrator's local console session. The interface supports the CLI.

1.3.1 Component Descriptions

1.3.1.1 Management Component

Enterprise Security Manager (ESM)

The central point of administration for data, settings, and configuration. Using ESM allows you to keep all configuration settings, user and access group profiles, and event and flow data in a single location. It communicates with devices over an encrypted control channel. Central management for all devices.

1.3.1.2 Data Components

Event Receiver (ERC)

The ERC collects security events and network flow data from multi-vendor sources including firewalls, virtual private networks (VPNs), routers, and other network devices. The Receiver gathers and analyzes data from third-party network and security solutions, allowing for the collection and normalization of this data, which provides a single view across devices from multiple vendors. This allows event and flow data collection from devices that send data feeds to the Receiver.

Application Data Monitor (ADM)

The ADM passively monitors traffic, which it then decodes to detect anomalies in application protocols. The ADM accepts rule expressions and tests them against monitored traffic, inserting records into the event table of the database for each triggered rule. It stores the packet that triggered the rule in the event table's packet field. It also adds application-level metadata to the dB session and query tables of the database for every triggered rule. It stores a text representation of the protocol stack in the query table's packet field.

1.3.1.3 Auxiliary Components:

Advanced Correlation Engine (ACE)

Provides dedicated correlation logic to supplement existing ESM event correlation capabilities. It can be deployed in real-time or historical modes. When operating in real-time mode, events are analyzed as they are collected for immediate threat and risk detection. In historical mode, any available data collected by the ESM can be “replayed” through either or both correlation engines, for historical threat and risk detection. So, when new zero-day attacks are discovered, the ESM can look back to determine whether the organization was exposed to that attack in the past, for “sub-zero day” threat detection. It provides two dedicated correlation engines:

- Risk correlation — A risk detection engine that generates a risk score using rule-less correlation.
- Rule correlation — A threat detection engine that detects threats using a traditional rule-based event correlation.

Enterprise Log Manager (ELM)

Supports the storage and management of, access to, and reporting of log data. You can define data sources as well as store and manage data from these data sources. You can also set up jobs that search, export, and check the data for integrity, allowing you to view the results and save the information. Log data from a given source may be associated with an ELS component or an ELM component, but not both.

Enterprise Log Search (ELS)

The ELS component provides high-speed access to the raw security events in an uncompressed form and is used to perform forensic analysis of events and quickly search through large amounts of log data. This component is optional in Trellix Enterprise installations. Log data from a given source may be associated with an ELS component or an ELM component, but not both.

1.3.2 Evaluated Configuration

The minimum configuration required for a Trellix TOE deployment consists of at least one management component, one data component, and one auxiliary component. In addition to the minimum configuration, additional instances of the data components or auxiliary components can be added to expand upon the minimum configuration in order to address larger enterprise deployments.

All six TOE components are part of the evaluation. However, a minimum configuration of the TOE that was tested is identified below.

- Management Component:
 - Enterprise Security Manager (ESM)
- Data Components:
 - Event Receiver (ERC)
- Auxiliary Components:
 - Advanced Correlation Engine (ACE)

1.3.3 Physical Boundary

The physical boundary of the TOE is illustrated by the solid Blue rectangular boxes in Figure 1 above. The TOE boundary includes the hardware, operating system, and Trellix application software of each of the six TOE components. The following table describes the hardware details and Table 5 describes the software details of the six TOE components.

Table 4: TOE Component Descriptions

Component	Required	Network ports	Processors	Memory
ESM	Yes (1)	One (1) IPMI port	2x Intel Xeon Gold 5218 (Cascade Lake)	16x 16GB DDR4 2933MHz
		Two (2) Ethernet Management ports	2x Intel Xeon Gold 6230 (Cascade Lake)	16x 32GB DDR4 2933MHz
		One (1) VGA to connect Monitor		
		One (1) Ethernet port not used		
ERC	Yes (At least 1)	One (1) IPMI port	1 x Intel Xeon E-2224 (Coffee Lake); or	2 x 16GB DDR4 2666MHz
		Two (2) Ethernet Management ports	2x Intel Xeon Gold 5218 (Cascade Lake)	16x 16GB DDR4 2933MHz

Component	Required	Network ports	Processors	Memory
ADM		One (1) Ethernet Additional Management port One (1) Ethernet port not used Two (2) Ethernet ports for HA	2x Intel Xeon Gold 5218 (Cascade Lake)	16x 32GB DDR4 2933MHz
ACE ELM ELS	Yes (At least 1)	One (1) IPMI port Two (2) Ethernet Management ports One (1) Ethernet Additional Management port One (1) Ethernet port not used Two (2) Ethernet ports for HA	2x Intel Xeon Gold 5218 (Cascade Lake)	16x 16GB DDR4 2933MHz 16x 32GB DDR4 2933MHz

Table 5: TOE Software Component Descriptions

Component	Operating System	Software Build	Cryptographic Library
ESM	Trellix Nitro OS v11.6.12	ESS_update_11.6.12.signed.tgz	BC-FJA (Bouncy Castle FIPS Java API) v 1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
ERC		RECIEVER_Update_11.6.12.signed.tgz	
ADM			
ACE			
ELM			
ELS			

1.4 TOE Operational Environment (OE)

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 6: Required Environmental Components

Components	Description
Management Workstation with Web Browser	This includes any IT Environment Management workstation with a Web Browser that is used by the TOE administrator to support TOE administration through HTTPS protected channel. Any web browser that supports TLS 1.1 or greater may be used.
Management Workstation with Console connection	This includes any Management workstation directly connected to the console port of the TOE. This is used for local management of the TOE.
NTP Server (Optional)	The TOE supports communications with an NTP server to synchronize date and time. The TOE supports communication with NTPv4 servers using SHA2 as the message digest algorithm.
Syslog server	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE. The syslog server must support communications using SSH.

1.4.1 Security Functions Provided by the TOE

The TOE provides the security functions required by NDcPP v2.2e.

1.4.1.1 Security Audit

The TOE keeps local and remote audit records of security relevant events. The TOE internally maintains the date and time which can either be set manually or synchronized with an NTP server.

1.4.1.2 Cryptographic Support

The TOE provides cryptographic support for the services described in Table 7. The related FIPS140-2 validation details are provided in Table 21.

Table 7: TOE Provided Cryptography

Cryptographic Method	Use within the TOE	Library Implementation
TLS Establishment	For inter-TOE-components communication (mutually authenticated TLS). For remote administrative sessions over HTTPS – non mutually authenticated TLS (ESM only).	BC-FJA (Bouncy Castle FIPS Java API) v1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
SSH Establishment	For inter-TOE-components communication	Trellix OpenSSL FIPS Object module v1.0.3
ECDSA Signature Services	Used in SSH session establishment	Trellix OpenSSL FIPS Object module v1.0.3
RSA Signature Services	Used in TLS session establishment Used in SSH session establishment Used in secure software update	BC-FJA (Bouncy Castle FIPS Java API) v1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3

Cryptographic Method	Use within the TOE	Library Implementation
DRBG	Used in TLS session establishment Used in SSH session establishment	BC-FJA (Bouncy Castle FIPS Java API) v1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
SHS	Used in secure software update, as well as in computing hash values for TLS and SSH cryptographic operations	BC-FJA (Bouncy Castle FIPS Java API) v1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
HMAC-SHS	Used to provide TLS traffic integrity verification Used to provide SSH traffic integrity verification	BC-FJA (Bouncy Castle FIPS Java API) v1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3
AES	Used to encrypt TLS traffic Used to encrypt SSH traffic	BC-FJA (Bouncy Castle FIPS Java API) v1.0.2.3 Trellix OpenSSL FIPS Object module v1.0.3

1.4.1.3 Identification and Authentication

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

The TOE components authenticate to one another through X.509 certificates configured during the initial installation and setup process of the TOE (for data planes over TLS) or via public key authentication (for data planes over SSH). Administrators using the Web GUI remotely authenticate to the TOE using usernames and passwords.

1.4.1.4 Security Management

The TOE enables secure local and remote management of its security functions, including:

- Local console CLI administration.
- Remote GUI administration via HTTPS/TLS.
- Intra-TOE communication via SSHv2.
- Timed user lockout after multiple failed authentication attempts.
- Password complexity enforcement.
- Configurable banners to be displayed at login.
- Timeouts to terminate administrative sessions after a set period of inactivity.
- Protection of secret keys and passwords.

1.4.1.5 Protection of the TSF

The TOE ensures the authenticity and integrity of software updates through digital signatures and requires administrative intervention prior to the software updates being installed.

The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions.

1.4.1.6 TOE Access

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

1.4.1.7 Trusted Path/Channels

The TSF provides the following trusted communication channels:

- SSH for an audit server
- TLS/HTTPS for remote administrators
- SSH for communication between TOE components

1.4.2 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- *Trellix Security Enterprise Security Manager Common Criteria Configuration Guide*
- *Trellix Enterprise Security Manager 11.6.x Installation Guide*
- *Trellix Enterprise Security Manager 11.6.x Product Guide*

1.5 Product Functionality not Included in the Scope of the Evaluation

The TOE provides enterprise security and threat monitoring information to network administrators. All TOE features related to information monitoring, analytics, and threat evaluation are out of scope for this evaluation.

The TOE also provides an SSH-based interface which is only used for maintenance or troubleshooting in co-ordination with Trellix Support. This interface is not a management interface and excluded from the evaluation.

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended).
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 (Conformant).

2.2 Protection Profile Conformance

This ST claims exact conformance to the collaborative Protection Profiles for Network Devices, Version 2.2e, March 23, 2020.

2.3 Conformance Rationale

This ST provides exact conformance to NDcPP v2.2e. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date and applicable to NDcPP v2.2e have been considered. The following table identifies all applicable TDs.

Table 8: Technical Decisions (TDs)

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable) and Notes
TD0800: Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	Yes	IPSec is not claimed however, the TD archives TD0663 and therefore applies to this evaluation.
TD0792: NIT Technical Decision: FIA_PMG_EXT.1 – TSS EA not in line with SFR	Yes	Applies to FIA_PMG_EXT.1 TSS.
TD0790: NIT Technical Decision: Clarification Required for testing IPv6	Yes	Applies to FCS_TLSC_EXT.1.2 Test. Archives TD0634.
TD0738: NIT Technical Decision for Link to Allowed-With List	Yes	Admin change. Archives TD0538.
TD0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	Applies to FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2 and Test.

TD0639: NIT Technical Decision for Clarification for NTP MAC Keys	Yes	Clarification.
TD0638: NIT Technical Decision for Key Pair Generation for Authentication	Yes	Clarification.
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	Yes	FCS_SSHC_EXT.1 SFR, App Note, TSS, AGD & Test modified.
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	Yes	FCS_TLSS_EXT.1.3 TSS modified.
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	Yes	FPT_STM_EXT.1.2 SFR and App Note modified. FPT_STM_EXT.1 TSS, AGD, and Test.
TD0631 : NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	FCS_SSHS_EXT.1.2 SFR, App Note, TSS, and Test modified. FCS_SSHS_EXT.1.5 App Note, TSS, and Test modified. FMT_SMF.1 SFR and App Note modified.
TD0592: NIT Technical Decision for Local Storage of Audit Records	Yes	Applies to PP verbiage only.
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	Yes	Applies to Assumptions and Acronyms.
TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	Applies to FCS_CKM.2 SFR.
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	FCS_CKM.2.1 SFR, App Note, TSS, and Test modified. FCS_CKM.1 App Note and Test modified.
TD0572: NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	Clarification, applies to FTP_ITC.1.
TD0571: NIT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	Clarification, applies to FIA_AFL.1.
TD0570: NIT Technical Decision for Clarification about FIA_AFL.1	Yes	Clarification, applies to FIA_AFL.1.
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	Yes	Applies to FCS_TLSS_EXT.1.4 App Note, TSS, AGD, and Test.
TD0564: NIT Technical Decision for Vulnerability Analysis Search Criteria	Yes	Applies to AVA only.
TD0563: NIT Technical Decision for Clarification of audit date information	Yes	Applies to App Note only for FAU_GEN.1.2.
TD0556: NIT Technical Decisions for RFC 5077 question	Yes	Applies to FCS_TLSS_EXT.1.4 Test only.

TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	Yes	Applies to FCS_TLSS_EXT.1.4 Test only.
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	Applies to AVA only.
TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63	No	The ST does not claim DTLS.
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Yes	Applies to FIA_X509_EXT.2.1 App Note only.
TD0536: NIT Technical Decision for Update Verification Inconsistency	Yes	Applies to FPT_TUD_EXT.1.3 AGD.
TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	Yes	Applies to FCS_NTP_EXT.1.4 and FCS_NTP_EXT.1.5 Test.
TD0527: Updated to Certificate Revocation Testing (FIA_X509_EXT.1)	No	The TOE does not support EC certificates.

3 Security Problem Definition

The security problem definition has been taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 9 are drawn directly from the PP and any EPs/Modules/Packages specified in Section 2.2.

Table 9: Threats

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network

ID	Threat
	<p>traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.</p> <p>The use of appropriate secure protocols to provide authentication of endpoints (as in the SFRs addressing T.UNTRUSTED_COMMUNICATION_CHANNELS) are ensured by the requirements in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the authentication requirements for endpoints in inter-component communications are addressed by the requirements in FPT_ITT.1.</p>
T.UPDATE_COMPROMISE	<p>Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.</p>
T.UNDETECTED_ACTIVITY	<p>Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised</p>
T.SECURITY_FUNCTIONALITY_COMPROMISE	<p>Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.</p>
T.PASSWORD_CRACKING	<p>Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.</p>
T.SECURITY_FUNCTIONALITY_FAILURE	<p>An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.</p>

3.2 Assumptions

The assumptions included in Table 10 are drawn directly from the PP and any relevant EPs/Modules/Packages.

Table 10: Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

ID	Assumption
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3 Organizational Security Policies

The OSPs included in Table 11 are drawn directly from the PP and any relevant EPs/Modules/Packages.

Table 11: OSPs

ID	OSP
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 Security Objectives

The security objectives have been taken directly from the claimed PP and any relevant EPs/Modules/Packages and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the Table 12 below, track with the assumptions about the TOE operational environment.

Table 12: Security Objectives for the Operational Environment

ID	Objectives for the Operational Environment
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMN	<p>Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.</p>
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

ID	Objectives for the Operational Environment
OE.COMPONENTS_RUNNING	For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, September 2017, and all international interpretations.

Table 13: SFRs

Requirement Class	Requirement	Description
Security Audit (FAU)	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_GEN_EXT.1	Security Audit Data Generation for Distributed TOE Component
	FAU_STG_EXT.1	Protected Audit Event Storage
	FAU_STG_EXT.4	Protected Local Audit Event Storage for Distributed TOEs
Communication Partner Control (FCO)	FCO_CPC_EXT.1	Component Registration Channel Definition
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_NTP_EXT.1	NTP Protocol
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
	FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
	FCS_TLSS_EXT.1	TLS Server Protocol without Mutual Authentication
	FCS_TLSS_EXT.2	TLS Server Support for Mutual Authentication
	FCS_RBG_EXT.1	Random Bit Generation
Identification and Authentication (FIA)	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UAU_EXT.2	Password-based Authentication Mechanism

Requirement Class	Requirement	Description
	FIA_UAU.7	Protected Authentication Feedback
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_X509_EXT.1/ITT	Certificate Validation
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
Security Management (FMT)	FMT_MOF.1/Functions	Management of Security Functions Behaviour
	FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on security roles
Protection of the TSF (FPT)	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_ITT.1/Join	Basic internal TSF data transfer protection
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
TOE Access (FTA)	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banner
Trusted Path/Channels (FTP)	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1/Admin	Admin Trusted Path

5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text and ~~strikethroughs~~;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.

- Formatting used in the cPP is retained except for text within brackets. If the text within the brackets is an operation completed by the ST author, the formatting follows the first three bullet items of this section is applied. Otherwise, the text within brackets is plaintext.
- Extended SFRs are identified by the addition of “EXT” after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Security Audit (FAU)

5.2.1.1 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 shut-down of the audit functions;
- b) All auditable events for the not specified level of audit; and
- c) *All administrative actions comprising:*
 - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
 - *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
 - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
 - *Resetting passwords (name of related user account shall be logged).*
 - [no other actions];
- d) *Specifically defined auditable events listed in Table 14.*

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, 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 cPP/ST, *information specified in column three of Table 14.*

Table 14: Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_GEN_EXT.1	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG_EXT.4	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoint pairs enabled or disabled.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_NTP_EXT.1	Configuration of a new time server. Removal of configured time server.	Identity if new/removed time server.
FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSC_EXT.2	None	None
FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSS_EXT.2	Failure to authenticate the client.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate. Any addition, replacement, or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FPT_ITT.1/Join	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None.
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

5.2.1.2 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.

5.2.1.3 FAU_GEN_EXT.1 Security Audit Data Generation

FAU_GEN_EXT.1.1

The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

5.2.1.4 FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2

The TSF Shall be able to store generated audit data on the TOE itself. In addition [

- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [the *ESM, ACE, ERC, ELM, ADM, and ELS components*],

].

FAU_STG_EXT.1.3

The TSF shall [overwrite previous audit records according to the following rule: [overwrite oldest record first]] when the local storage space for audit data is full.

5.2.1.5 FAU_STG_EXT.4 Protected Local Audit Event Storage for Distributed TOEs

FAU_STG_EXT.4.1

The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: *[refer to the following table]*.

Table 15: FAU_STG_EXT.4.1 Table

Component	Action Chosen	Rule
ESM	<u>overwrite previous audit records according to the following rule:</u>	<u>overwrite oldest record first</u>
ACE	<u>overwrite previous audit records according to the following rule:</u>	<u>overwrite oldest record first</u>
ERC	<u>overwrite previous audit records according to the following rule:</u>	<u>overwrite oldest record first</u>
ELM	<u>overwrite previous audit records according to the following rule:</u>	<u>overwrite oldest record first</u>
ADM	<u>overwrite previous audit records according to the following rule:</u>	<u>overwrite oldest record first</u>
ELS	<u>overwrite previous audit records according to the following rule:</u>	<u>overwrite oldest record first</u>

Application Note: FAU_STG_EXT.5 have not been included in the ST because all TOE components store audit data locally.

5.2.2 Communication Partner Control (FCO)

5.2.2.1 FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1

The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2

The TSF shall implement a registration process in which components establish and use a communications channel that uses [

- A channel that meets the secure channel requirements in [FPT_ITT.1]

] for at least *TSF data*.

Application Note: The secure channel that is used in the registration process has been iterated as FPT_ITT.1/Join. This channel is then subsequently adopted as a continuing internal communication channel between the different TOE components.

FCO_CPC_EXT.1.3

The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.2.3 Cryptographic Support (FCS)

5.2.3.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

FCS_CKM.1.1

The TSF shall generate **asymmetric** cryptographic key in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526, RFC 7919].

] and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].

5.2.3.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

FCS_CKM.2.1

The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526, groups listed in RFC 7919]

] that meets the following: [assignment: list of standards].

Application Note: Applied TD0581 and TD0580.

5.2.3.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [*
 - instructs a part of the TSF to destroy the abstraction that represents the key;

]

that meets the following: *No Standard.*

5.2.3.4 FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption

The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in [CBC, GCM, CTR] mode* and cryptographic key sizes [128, 256] that meet the following: *AES as specified in ISO 18033-3*, [

- CBC as specified in ISO 10116,
- GCM as specified in ISO 19772,
- CTR as specified in ISO10116

].

5.2.3.5 FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)

FCS_COP.1.1/Hash

The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [~~assignment: cryptographic key sizes~~] and **message digest sizes** [256, 384, 512] **bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.3.6 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash

The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, implicit] and cryptographic key sizes [256-bit, 384-bit, 512-bit] and **message digest sizes** [256, 384, 512] **bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

5.2.3.7 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen

The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits or 3072 bits],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits, 384 bits or 521 bits]

]

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4

].

5.2.3.8 FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2

The TSF shall implement the HTTPS protocol using TLS.

FCS_HTTPS_EXT.1.3

If a peer certificate is presented, the TSF shall [not require client authentication] if the peer certificate is deemed invalid.

5.2.3.9 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1

The TSF shall use only the following NTP version(s) [NTP v4 (RFC 5905)].

FCS_NTP_EXT.1.2

The TSF shall update its system time using [

- Authentication using [SHA256] as the message digest algorithm(s);

].

FCS_NTP_EXT.1.3

The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4

The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.2.3.10 FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1

The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [4344, 5656, 6668, 8308 section 3.1, 8332].

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [no other method].

Application Note: Applied TD0636.

FCS_SSHC_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [256K] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [

- aes256-ctr,
- aes256-gcm@openssh.com

].

FCS_SSHC_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [

- ssh-rsa,
- rsa-sha2-256,
- rsa-sha2-512,
- ecdsa-sha2-nistp256,
- ecdsa-sha2-nistp384,
- ecdsa-sha2-nistp521

] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [

- hmac-sha2-256,
- hmac-sha2-512,
- implicit

] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7

The TSF shall ensure that [

- ecdh-sha2-nistp256

] and [

- diffie-hellman-group16-sha512,
- ecdh-sha2-nistp384

] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_SSHC_EXT.1.9

The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [no other methods] as described in RFC 4251 section 4.1.

5.2.3.11 FCS_SSHS_EXT.1 SSH Server Protocol**FCS_SSHS_EXT.1.1**

The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [4256, 4344, 5656, 6668, 8308 section 3.1, 8332].

FCS_SSHS_EXT.1.2

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [password-based].

FCS_SSHS_EXT.1.3

The TSF shall ensure that, as described in RFC 4253, packets greater than [256K] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4

The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [

- aes256-ctr,
- aes256-gcm@openssh.com

].

FCS_SSHS_EXT.1.5

The TSF shall ensure that the SSH public-key based authentication implementation uses [

- ssh-rsa,
- rsa-sha2-256,
- rsa-sha2-512,
- ecdsa-sha2-nistp256,
- ecdsa-sha2-nistp384,
- ecdsa-sha2-nistp521

] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [

- hmac-sha2-256,
- hmac-sha2-512,
- implicit

] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7

The TSF shall ensure that [

- ecdh-sha2-nistp256

] and [

- diffie-hellman-group16-sha512,
- ecdh-sha2-nistp384

] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

Application Note: Applied TD0631.

5.2.3.12 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1

The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5289

- TLS ECDHE RSA WITH AES 128 CBC SHA256 as defined in RFC5289
- TLS ECDHE RSA WITH AES 256 CBC SHA384 as defined in RFC5289

] and no other ciphersuites.

FCS_TLSC_EXT.1.2

The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, and no other attribute types].

FCS_TLSC_EXT.1.3

When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4

The TSF shall [present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

5.2.3.13 FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1

The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.2.3.14 FCS_TLSS_EXT.1 TLS Sever Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1

The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [

- TLS DHE RSA WITH AES 128 CBC SHA256 as defined in RFC 5246
- TLS DHE RSA WITH AES 256 CBC SHA256 as defined in RFC 5246
- TLS ECDHE RSA WITH AES 128 GCM SHA256 as defined in RFC5289
- TLS ECDHE RSA WITH AES 256 GCM SHA384 as defined in RFC5289
- TLS ECDHE RSA WITH AES 128 CBC SHA256 as defined in RFC5289
- TLS ECDHE RSA WITH AES 256 CBC SHA384 as defined in RFC5289

].

FCS_TLSS_EXT.1.2

The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS v1.1].

FCS_TLSS_EXT.1.3

The TSF shall perform key establishment for TLS using [

- RSA with key size [2048 bits, 3072 bits],
- [Diffie-Hellman parameters with size [2048 bits],
- ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves

]]

FCS_TLSS_EXT.1.4

The TSF shall support [session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)].

5.2.3.15 FCS_TLSS_EXT.2 TLS Sever Support for Mutual Authentication

FCS_TLSS_EXT.2.1

The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.2

When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSS_EXT.2.3

The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

5.2.3.16 FCS_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1

The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2

The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- [4] software-based noise source,
- [1] platform-based noise source

] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.2.4 Identification and Authentication (FIA)

5.2.4.1 FIA_AFL.1 Authentication Failure Management (Refinement)

FIA_AFL.1.1

The TSF shall detect when an Administrator configurable positive integer within *[1-255]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

5.2.4.2 FIA_PMG_EXT.1 Password Management**FIA_PMG_EXT.1.1**

The TSF shall provide the following password management capabilities for administrative passwords:

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!” “@” “#” “\$” “%” “^” “&” “*” “(” “)” “+” “-” “.” “/” “:” “;” “<” “>” “?” “[” “]” “\” “/” “{” “}” “|” “~” “_” “=” “”];
- b) Minimum password length shall be configurable to between [8 characters] and [15] characters.

5.2.4.3 FIA_UAU_EXT.2 Password-based Authentication Mechanism**FIA_UAU_EXT.2.1**

The TSF shall provide a local [password-based] authentication mechanism to perform local administrative user authentication.

5.2.4.4 FIA_UAU.7.1 Protected Authentication Feedback**FIA_UAU.7.1**

The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress **at the local console**.

5.2.4.5 FIA_UIA_EXT.1 User Identification and Authentication**FIA_UIA_EXT.1.1**

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions].

FIA_UIA_EXT.1.2

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

5.2.4.6 FIA_X509_EXT.1/ITT X.509 Certificate Validation**FIA_X509_EXT.1.1/ITT**

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation supporting a minimum path length of two certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.

- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [no revocation method].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
 - *Server certificates presented for TLS shall have the Server Authentication purpose(id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
 - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
 - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose(id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/ITT

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.4.7 FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
 - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
 - *Server certificates presented for TLS shall have the Server Authentication purpose(id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
 - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
 - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose(id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.4.8 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS] and [no additional uses].

FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [accept the certificate].

5.2.4.9 FIA_X509_EXT.3 X.509 Certificate Requests**FIA_X509_EXT.3.1**

The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.5 Security Management (FMT)**5.2.5.1 FMT_MOF.1/Functions Management of Security Functions Behaviour.****FMT_MOF.1.1/Functions**

The TSF shall restrict the ability to [determine the behaviour of, modify the behaviour of] the functions [transmission of audit data to an external IT entity] to *Security Administrators*.

5.2.5.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior**FMT_MOF.1.1/ManualUpdate**

The TSF shall restrict the ability to enable the function to perform manual updates to Security Administrators.

5.2.5.3 FMT_MTD.1/CoreData Management of TSF Data**FMT_MTD.1.1/CoreData**

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.2.5.4 FMT_MTD.1/CryptoKeys Management of TSF Data**FMT_MTD.1.1/CryptoKeys**

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.2.5.5 FMT_SMF.1 Specification of Management Functions**FMT_SMF.1.1**

The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*

- *Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
 - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
 - Ability to manage the cryptographic keys;
 - Ability to configure the cryptographic functionality;
 - Ability to configure the interaction between TOE components;
 - Ability to set the time which is used for time-stamps;
 - Ability to configure NTP;
 - Ability to manage the trusted public keys database;
 - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
 - Ability to import X.509v3 certificates to the TOE's trust store;
-].

Application Note: Applied TD0631.

5.2.5.6 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1

The TSF shall maintain the roles:

- *Security Administrator*

FMT_SMR.2.2

The TSF shall be able to associate users with roles.

FMT_SMR.2.3

The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely;*

are satisfied.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FTP_APW_EXT.1 Protection of Administrator Passwords

FTP_APW_EXT.1.1

The TSF shall store administrative passwords in non-plaintext form.

FTP_APW_EXT.1.2

The TSF shall prevent the reading of plaintext administrative passwords.

5.2.6.2 FPT_ITT.1 Basic Internal TSF Data Transfer Protection (Refinement)

FPT_ITT.1.1

The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE **through the use of [SSH, TLS]**.

5.2.6.3 FPT_ITT.1/Join Basic Internal TSF Data Transfer Protection (Refinement)

FPT_ITT.1.1/Join

The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE **through the use of [SSH]**.

5.2.6.4 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric, and private keys)

FPT_SKP_EXT.1.1

The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.6.5 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1

The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2

The TSF shall [allow the Security Administrator to set the time, synchronise time with an NTP server].

Application Note: Applied TD0632.

5.2.6.6 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1

The TSF shall run a suite of the following self-tests [

- during initial start-up (on power on,
 - periodically during normal operation,
 - at the request of the authorised user
-] to demonstrate the correct operation of the TSF: [
- *cryptographic known-answer tests,*
 - *firmware integrity test,*
 - *pairwise consistency testing of generated keypairs*
 - *DRBG health testing,*

].

5.2.6.7 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1

The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

FPT_TUD_EXT.1.2

The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3

The TSF shall provide means to authenticate firmware/software updates to the TOE using a [digital signature] prior to installing those updates.

5.2.7 TOE Access (FTA)**5.2.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking****FTA_SSL_EXT.1.1**

The TSF Shall, for local interactive sessions, [

- terminate the session

]

after a Security Administrator-specified time period of inactivity

5.2.7.2 FTA_SSL.3 TSF-initiated Termination (Refinement)**FTA_SSL.3.1**

The TSF shall terminate a **remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

5.2.7.3 FTA_SSL.4 User-initiated Termination (Refinement)**FTA_SSL.4.1**

The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

5.2.7.4 FTA_TAB.1 Default TOE Access Banners (Refinement)**FTA_TAB.1.1**

Before establishing an **administrative user** session the TSF shall display a **Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.2.8 Trusted Path/Channels (FTP)**5.2.8.1 FTP_ITC.1 Inter-TSF Trusted Channel (Refinement)****FTP_ITC.1.1**

The TSF shall be **capable of using [SSH]** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [no other entities]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2

The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for *[audit server]*.

5.2.8.2 FTP_TRP.1/Admin Trusted Path (Refinement)**FTP_TRP.1.1/Admin**

The TSF shall **be capable of using [TLS, HTTPS]** to provide a communication path between itself and **authorized remote Administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and provides detection of modification of the channel data**.

FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.3 TOE SFR Dependencies Rationale for SFRs

The PP and any relevant EPs/Modules/Packages contain(s) all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and any relevant EPs/Modules/Packages, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 16: Security Assurance Requirements

Table 16: Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CLL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage

Assurance Class	Assurance Components	Component Description
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.5 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Trellix to satisfy the assurance requirements. The following table lists the details:

Table 17: TOE Security Assurance Measures

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

6 TOE Summary Specifications

This chapter identifies and describes how the Security Functional Requirements identifies above are met by the TOE.

Table 18: TOE Summary Specification SFR Description

Requirement	TSS Description
Security Audit (FAU)	
FAU_GEN.1 FAU_GEN_EXT.1	<p>The TOE generates audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified under the FAU_GEN.1 requirement. Each of the events as specified in the audit record is in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred.</p> <p>The audit trail consists of the individual audit records; one audit record for each event that occurred. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer to view the audit records. The first message displayed is the oldest message in the buffer.</p> <p>The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.</p> <p>SSH hostkeys are generated when a TOE component is registered to the ESM and deleted when the component is deregistered. SSH hostkeys can also be regenerated upon user request. The information stored in the audit log for any of those events is: username, time stamp, Id of the device whose keys are being generated/regenerated, Description of the event. SSH public keys are identified by hostname and TLS public key associated with certificates are identified by the certificate DN.</p> <p>Each TOE component generates and locally caches audit logs. These logs are transmitted to the ESM over kafka, over a TLS inter-TOE trusted channel. Audit logs are consolidated on the ESM and transmitted to an external audit server over SSH. Once audit logs are transmitted from each TOE component to the ESM, the individual component removes the stored logs to avoid duplication. Once the ESM has consumed logs from TOE components, the ESM stores these audit data until local audit data storage capacity is full. The ESM also transmits these audit data to the external audit server as soon as they are received (while the trusted channel is established) or as soon as the trusted channel is available (if it is down). Table 14 identifies which TOE components perform which auditing functions, as auditing related to the SFRs is dependent on whether that SFR is implemented on the TOE component.</p>
FAU_GEN.2	<p>The TOE ensures that each auditable event is associated with the user that triggered the event. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is included in the audit record.</p>
FAU_STG_EXT.1	<p>The TOE is a Distributed TOE. The ESM component is responsible and configured for collecting, aggregating and exporting all audit records to a</p>

Requirement	TSS Description
FAU_STG_EXT.4	<p>specified, external syslog server in real-time. The ESM component stores a limited set of audit records locally and continues to do so if the communication with the syslog server goes down.</p> <p>The TOE protects communications with an external syslog server via SSH. The TOE transmits its audit events to all configured syslog servers at the same time logs are written locally to non-volatile storage.</p> <p>If the SSH connection fails, the TOE continues to store audit records locally on the TOE and will transmit any locally stored contents when connectivity to the syslog server is restored.</p> <p>Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</p> <p>The ESM component of the TOE stores the local audit data from all TOE components. The size of the local audit storage is configurable, based on the maximum storage size of the TOE (i.e., local hard disk size), but is shared with alerts and flows that are collected by TOE Components as part of their operation. Alert/Flow ratios can be configured, which will change the amount of data available to the TOE for storage of local audit data.</p> <p>Audit data is made available only to authorized and authenticated administrators.</p> <p>Each component of the distributed TOE generates and locally stores audit logs. These logs are also transmitted to the ESM component over kafka, a mutually authenticated TLS intra-TOE trusted channel in real-time. Each TOE component continues to store their audit logs locally in case there is an interruption in TLS channel or if ESM is unreachable. Audit logs are consolidated on the ESM and transmitted to an external audit server over SSH.</p> <p>When the local storage on individual TOE components is full, the TOE components will overwrite the oldest audit data first. This situation could only occur if the intra-TOE communication channel is down for an extended period of time, but the TOE components themselves were still operational.</p> <p>When local storage space on the ESM is full, the ESM will overwrite the oldest audit data first. The ESM transmits received and generated audit data to the external audit server as soon as they are received (while the trusted channel is established) or as soon as the trusted channel is available (if it is down).</p>
Communication Partner Control (FCO)	
FCO_CPC_EXT.1	<p>The TOE components registration is performed using FPT_ITT.1/Join. For communication between TOE components, SSH is used in establishment of the secure communication channel. The administrator uses the ESM to link the TOE components to the ESM or remove linked TOE components.</p> <p>The ESM and the other TOE component(s) use SSH to exchange identity information via an SSH trusted channel, where the ESM acts as the SSH client and the TOE component(s) act as the SSH server(s). The administrator configures the connection and specifies the username and password to provide to the TOE component to initiate registration. Each TOE component and ESM have unique SSH hostkey, which are exchanged</p>

Requirement	TSS Description
	<p>during registration to establish their identity. This channel is then subsequently adopted as a continuing internal communication channel between the different TOE components.</p> <p>After registration, intra-TOE communication also takes place over TLS, with the ESM acting as the TLS client(s) and the other TOE components acting as the TLS server.</p>
Cryptographic Support (FCS)	
FCS_CKM.1	<p>In support of secure cryptographic protocols, the TOE supports RSA key generation schemes as specified in NIST SP-800-186-4, with key sizes of 2048 and 3072 bits. The TOE also supports ECC schemes using “NIST curves” P-256, P-384, and P-521 as specified in FIPS PUB 186-4, Appendix B.4. These keys are used in support of digital certificates and keyed authentication for TLS and SSH. The TOE supports FFC schemes using safe prime groups as per NIST SP 800-56A Revision 3, and RFC 3526 and RFC 7919.</p> <p>The relevant NIST CAVP certificate numbers are listed Table 21.</p>
FCS_CKM.2	<p>In support of secure cryptographic protocols, the TOE supports several key establishment schemes, including:</p> <p>ECC based key exchange based on NIST SP 800-56Ar3;</p> <p>FFC schemes using safe-prime based key exchange based on NIST SP 800-56Ar3;</p> <p>ECC and FFC schemes are used for TLS and SSH.</p> <p>The TOE supports Diffie Hellman group 16 for SSH key exchange which is implemented by hardcoding Oakley Group 16 parameters as defined in RFC 3526, Section 3.</p> <p>The TOE supports Diffie Hellman parameters with size 2048 (ffdhe2048) for TLS key exchange which is implemented by P-256 as defined in RFC 7919.</p> <p>The TOE acts as a sender and receiver for all schemes.</p> <p>The relevant NIST CAVP certificate numbers are listed in Table 21.</p>
FCS_CKM.4	<p>The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs). All keys within the TOE are securely destroyed as per the descriptions given in Table 20: Key Storage and Zeroization</p> <p>.</p> <p>The TOE generates SSH private and public keys by default as part of the initial setup and during TOE component registration. The SSH keys can also be regenerated via the Web GUI by an administrator. SSH private and public keys are zeroized when the TOE is factory reset, a TOE component is de-registered (removed), or when commanded to regenerate the SSH keys by the administrator.</p> <p>The TOE generates TLS private and public keys used for inter-TOE communication by default as part of the initial setup. TLS private and public keys are also generated as part of Certificate Signing Request (CSR). TLS private and public keys are destroyed when the associated X509v3 certificate is removed from the trust store of the TOE. The TLS private and</p>

Requirement	TSS Description
	<p>public keys used in inter-TOE communication cannot be changed or modified. They can only be destroyed as part of factory reset.</p> <p>All other keys are ephemeral, and are destroyed by the TOE when their associated session is terminated.</p> <p>The TOE does not make use of a value that does not contain any CSP to overwrite keys. The TOE does not have any circumstances that may not conform to key destruction requirements.</p>
FCS_COP.1/DataEncryption	<p>The TOE provides symmetric encryption and decryption capabilities using 128 and 256-bit AES in CBC mode, CTR mode and GCM mode as described in ISO 10116 and ISO 19772, respectively. AES is implemented in the following protocols: TLS and SSH.</p> <p>The relevant NIST CAVP certificate numbers are listed Table 21.</p>
FCS_COP.1/Hash	<p>The TOE provides cryptographic hashing services using SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004. Hashing is used for the following:</p> <ul style="list-style-type: none"> • TLS • SSH • Digital signature verification as part of trusted update validation • NTP authentication if NTP is configured, <p>The relevant NIST CAVP certificate numbers are listed Table 21.</p>
FCS_COP.1/KeyedHash	<p>The TOE provides keyed-hashing message authentication services using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 as specified in FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code," and FIPS 180-4, "Secure Hash Standard."</p> <p>HMAC is implemented in the following protocols: TLS and SSH.</p> <p>The relevant NIST CAVP certificate numbers are listed Table 21.</p>
FCS_COP.1/SigGen	<p>The TOE provides cryptographic signature generation and verification services using:</p> <ul style="list-style-type: none"> • RSA Signature Algorithm with key size of 2048 and 3072, • ECDSA Signature Algorithm with NIST curves P-256, P-384 and P-521. <p>The RSA and ECDSA signature verification services are used in the SSH protocols. RSA signature verification is used for the TLS protocol and for verification of trusted update packages.</p> <p>The relevant NIST CAVP certificate numbers are listed Table 21.</p>
FCS_HTTPS_EXT.1	<p>The TOE provides management functionality over an HTTPS connection using TLS acting as a TLS Server (Refer to Figure 1 ". TOE does not use HTTPS in a client capacity. The TOE's HTTPS protocol complies with RFC 2818.</p> <p>RFC 2818 is, quite simply, HTTP over TLS. The TOE implements all SHALL, SHOULD, and MUST statements in the RFC, and conforms to all SHALL NOT, SHOULD NOT, or MUST NOT statements. Client identification is performed as per the validation specifications in FIA_X509_EXT.1 which will meet the requirements described in Section 3.2 of RFC 2818.</p>
FCS_NTP_EXT.1	<p>The TOE supports communication with NTPv4 time servers and implements the NTP client protocol(s) in conformance with RFC 1305 and RFC 5905.</p>

Requirement	TSS Description																	
	<p>The TOE synchronizes with an NTP server for its reliable and accurate timestamp. The TOE can be configured to support at least three (3) NTP servers. The TOE supports NTPv4 and validates the integrity of the time-source using SHA256. The TOE’s ntpd client is version 4.2.8p12.</p>																	
<p>FCS_SSHC_EXT.1</p>	<p>The ESM and ERC components support SSH Client.</p> <table border="1" data-bbox="581 464 1386 877"> <thead> <tr> <th data-bbox="581 464 812 541">Component (SSH Client)</th> <th data-bbox="816 464 1060 541">SSH Server</th> <th data-bbox="1065 464 1386 541">Purpose</th> </tr> </thead> <tbody> <tr> <td data-bbox="581 548 812 625">ESM</td> <td data-bbox="816 548 1060 625">To all components.</td> <td data-bbox="1065 548 1386 625">Data Plane. Correlation Data for analysis.</td> </tr> <tr> <td data-bbox="581 632 812 709">ESM</td> <td data-bbox="816 632 1060 709">To External Audit Server</td> <td data-bbox="1065 632 1386 709">Export audit logs.</td> </tr> <tr> <td data-bbox="581 716 812 793">ERC</td> <td data-bbox="816 716 1060 793">To ELM</td> <td data-bbox="1065 716 1386 793">Data Plane. Raw event log data.</td> </tr> <tr> <td data-bbox="581 800 812 877">ERC</td> <td data-bbox="816 800 1060 877">To ELS</td> <td data-bbox="1065 800 1386 877">Data Plane. Raw event log data.</td> </tr> </tbody> </table> <p>As an SSH client, TOE components implement AES256 in CTR mode, and AES256 in GCM mode for their bulk encryption ciphers. TOE components support HMAC-SHA2-256 and HMAC-SHA2-512 as their MAC algorithms. TOE components support ECDH-SHA2-NISTp256, DH-Group16-SHA512, and ECDH-SHA2-NISTp384 as their key exchange algorithms.</p> <p>As an SSH client, TOE components support only public-key and host-key public key authentication using the SSH-RSA, RSA-SHA2-256, RSA-SHA2-512, ECDSA-SHA2-NISTp256, ECDSA-SHA2-NISTp384, and ECDSA-SHA2-NISTp521 public key authentication algorithms and rejects all others. The TOE components store a SSH server’s host-key public key as “Known Hosts” and associates the server identity with server’s IP address, Device Name, and Fingerprint. TOE components conform to RFCs 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8303 section 3.1 and 8332.</p> <p>Large SSH packets are defined as those greater than 256 kB. This is calculated by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet if this limit is exceeded. Dropped packets are silently discarded, with no response sent back to the originator.</p> <p>The TOE does not implement any “optional characteristics” for any cryptographic algorithm.</p> <p>The TOE implements rekeying. Two thresholds are checked and are not configurable by the administrator. First, the TOE rekeys after 1 hour has elapsed using the same session key. Second, the TOE rekeys the SSH session after 1 GB of data has been exchanged using the same session key. The TOE will perform a rekey whenever either threshold is hit.</p> <p>Applied TD0636,</p>			Component (SSH Client)	SSH Server	Purpose	ESM	To all components.	Data Plane. Correlation Data for analysis.	ESM	To External Audit Server	Export audit logs.	ERC	To ELM	Data Plane. Raw event log data.	ERC	To ELS	Data Plane. Raw event log data.
Component (SSH Client)	SSH Server	Purpose																
ESM	To all components.	Data Plane. Correlation Data for analysis.																
ESM	To External Audit Server	Export audit logs.																
ERC	To ELM	Data Plane. Raw event log data.																
ERC	To ELS	Data Plane. Raw event log data.																
<p>FCS_SSHS_EXT.1</p>	<p>All of the TOE components, except ESM, support SSH Server.</p> <table border="1" data-bbox="581 1824 1386 1890"> <thead> <tr> <th data-bbox="581 1824 774 1890">Component (SSH Server)</th> <th data-bbox="779 1824 954 1890">SSH Client</th> <th data-bbox="959 1824 1386 1890">Purpose</th> </tr> </thead> <tbody> </tbody> </table>			Component (SSH Server)	SSH Client	Purpose												
Component (SSH Server)	SSH Client	Purpose																

Requirement	TSS Description														
	ACE	From ESM	Control Plane. All configuration and control data.												
	ERC	From ESM	Control Plane. All configuration and control data.												
	ELM	From ESM	Control Plane. All configuration and control data.												
		From ERC	Data Plane. Raw event log data.												
	ADM	From ESM	Control Plane. All configuration and control data.												
	ELS	From ESM	Control Plane. All configuration and control data.												
		From ERC	Data Plane. Raw event log data.												
	<p>As an SSH server, TOE components implement AES-256 in CTR mode, and AEAD AES-256 in GCM mode for their bulk encryption ciphers. TOE components support HMAC-SHA2-256 HMAC-SHA2-512, and the AEAD AES GCM implicit MAC as their MAC algorithms. TOE components support DH-Group16-SHA512, ECDH-SHA2-NISTp256, ECDH-SHA2-NISTp384 as their key exchange algorithms.</p> <p>As an SSH server, TOE components support password-based authentication, public-key authentication as well as host public key authentication algorithms. When using public-key authentication, the SSH server verifies the user's/client's identity by matching the presented public key against a stored copy of the public key in server's authorized_keys file.</p> <p>The public-key authentication and host-key public key authentication algorithms supported for SSH connections by the TOE are ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 and ecdsa-sha2-nistp521. algorithms and rejects all others. TOE components exactly conform to RFCs 4251, 4252, 4253, 4254, 4256, 4344, 5656, 6668, 8303 section 3.1 and 8332.</p> <p>Large SSH packets are defined as those greater than 256 kB. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet if this limit is exceeded.</p> <p>The TOE implements rekeying. Two thresholds are checked and are not configurable by the administrator. First, the TOE rekeys after 1 hour has elapsed using the same session key. Second, the TOE rekeys the SSH session after 1 GB of data has been exchanged using the same session key. The TOE will perform a rekey whenever either threshold is hit.</p>														
	FCS_TLSC_EXT.1	<p>ESM and ACE components act as TLS client as follows:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #fff9c4;">Component (TLS client)</th> <th style="background-color: #fff9c4;">TLS server (MA)</th> <th style="background-color: #fff9c4;">Purpose</th> </tr> </thead> <tbody> <tr> <td rowspan="2">ESM</td> <td>To all components.</td> <td>Data Plane. Correlation Data for analysis</td> </tr> <tr> <td>To ACE</td> <td>Data Plane. Parsed event log data.</td> </tr> <tr> <td>ACE</td> <td>To ERC</td> <td>Data Plane. Parsed event log data.</td> </tr> </tbody> </table>			Component (TLS client)	TLS server (MA)	Purpose	ESM	To all components.	Data Plane. Correlation Data for analysis	To ACE	Data Plane. Parsed event log data.	ACE	To ERC	Data Plane. Parsed event log data.
	Component (TLS client)	TLS server (MA)	Purpose												
ESM	To all components.	Data Plane. Correlation Data for analysis													
	To ACE	Data Plane. Parsed event log data.													
ACE	To ERC	Data Plane. Parsed event log data.													

Requirement	TSS Description									
	<p>The TOE implements the TLS protocol version 1.2 and is restricted to the following ciphersuites (which are not configurable):</p> <p>When used for intra-TOE communication, TOE components support:</p> <ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 <p>If the TOE component receives a handshake message proposing an outdated version of TLS, the TOE will reject the connection. The TOE component will always propose only TLSv1.2.</p> <p>The reference identifiers for all TOE components are generated by default and cannot be configured or modified. The reference identifier is a DNS Name as per RFC 6125 Section 6.</p> <p>When the TOE client (ESM or ACE) receives an X.509 certificate from their respective servers, the client will compare the reference identifier with the established Subject Alternative Names (SANs) and Common Name (CN) in the certificate. If there is no SAN, then the verification fails, and the channel is terminated. If the SAN exists and does not match the reference identifier, then the verification fails, and the channel is terminated. Otherwise, the reference identifier verification passes, and additional verification actions can proceed.</p> <p>The TOE doesn't support IP addresses and wildcard as reference identifiers for TLS-based communications.</p> <p>The TOE does not implement certificate pinning. Each TOE component only supports the trusted CA certificate(s) needed for verification of the trust chain and its own entity certificate.</p> <p>The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. The remote endpoint server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve ciphersuites.</p>									
FCS_TLSC_EXT.2	<p>When used for intra-TOE trusted channels, the TOE components implement TLS with mutual authentication based on X.509v3 certificates.</p>									
FCS_TLSS_EXT.1 FCS_TLSS_EXT.2	<p>Various TOE components act as TLS server as follows:</p> <table border="1" data-bbox="581 1675 1336 1900"> <thead> <tr> <th data-bbox="581 1675 781 1738">Component (TLS Server)</th> <th data-bbox="784 1675 954 1738">TLS Client</th> <th data-bbox="958 1675 1336 1738">Purpose</th> </tr> </thead> <tbody> <tr> <td data-bbox="581 1743 781 1837">ESM</td> <td data-bbox="784 1743 954 1837">From Remote Workstation</td> <td data-bbox="958 1743 1336 1837">Control Plane. Administrator's remote GUI session. ESM acts as a non-MA TLS server.</td> </tr> <tr> <td data-bbox="581 1841 781 1900">ACE</td> <td data-bbox="784 1841 954 1900">From ESM</td> <td data-bbox="958 1841 1336 1900">Data Plane. Correlation Data for analysis. ESM acts as a TLS</td> </tr> </tbody> </table>	Component (TLS Server)	TLS Client	Purpose	ESM	From Remote Workstation	Control Plane. Administrator's remote GUI session. ESM acts as a non-MA TLS server.	ACE	From ESM	Data Plane. Correlation Data for analysis. ESM acts as a TLS
Component (TLS Server)	TLS Client	Purpose								
ESM	From Remote Workstation	Control Plane. Administrator's remote GUI session. ESM acts as a non-MA TLS server.								
ACE	From ESM	Data Plane. Correlation Data for analysis. ESM acts as a TLS								

Requirement	TSS Description		
			client. ACE act as TLS servers. The TLS channel is Mutually Authenticated.
		From ESM	Data Plane. Parsed event log data. ESM acts as a TLS client. ACE acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ERC	From ESM	Data Plane. Parsed event log data. ESM acts as a TLS client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
		From ACE	Data Plane. Parsed event log data. ACE acts as a TLS Client. ERC acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ELM	From ESM	Data Plane. Correlation Data for analysis. ESM acts as a TLS client. ELM acts as TLS servers. The TLS channel is Mutually Authenticated.
	ADM	From ESM	Data Plane. Parsed event log data. ESM acts as a TLS client. ADM acts as a TLS Server. The TLS channel is Mutually Authenticated.
	ELS	From ESM	Data Plane. Parsed event log data. ESM acts as a TLS client. ELS acts as a TLS Server. The TLS channel is Mutually Authenticated.
<p>The TOE implements the TLS protocol version 1.2 and is restricted to the following ciphersuites (which are not configurable):</p> <p>When used as a TLS server the TOE support:</p> <ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 			

Requirement	TSS Description
	<p>If the TOE component receives a handshake message proposing an outdated version of TLS, the TOE will reject the connection. A TOE component will always propose only TLSv1.2.</p> <p>The ESM acts as a TLS server without mutual authentication to provide the Web GUI interface for remote administration. All other TOE components (child devices) act as a TLS server with mutual authentication to provide inter-TOE communication.</p> <p>The TOE supports the following key establishment methods as a TLS Server: For ESM:</p> <ul style="list-style-type: none"> • RSA with key size [2048 bits, 3072 bits], • [Diffie-Hellman parameters with size [2048 bits], • ECDHE curves [secp384r1, secp521r1] <p>For All Child Devices:</p> <ul style="list-style-type: none"> • RSA with key size [2048 bits], • [Diffie-Hellman parameters with size [2048 bits], • ECDHE curves [secp256r1, secp384r1, secp521r1] <p>The reference identifiers for TOE components are generated by default and cannot be configured or modified. The reference identifier is a DNS Name as per RFC 6125 Section 6.</p> <p>When the TOE server (child devices) receives an X.509 certificate from their respective client (ESM), the server will compare the reference identifier with the established Subject Alternative Names (SANs) and Common Name (CN) in the certificate. If there is no SAN, then the verification fails, and the channel is terminated. If the SAN exists and does not match the reference identifier, then the verification fails, and the channel is terminated. Otherwise, the reference identifier verification passes, and additional verification actions can proceed.</p> <p>The TOE doesn't support IP addresses and wildcard as reference identifiers for TLS-based communications.</p> <p>The TOE does not implement certificate pinning. Each TOE component only supports the trusted CA certificate(s) needed for verification of the trust chain and its own entity certificate.</p> <p>The TLS server supports session resumption, based on SessionIDs as described in RFC5246. If the session ID belongs to a previously valid/successful session, the TOE reuses the same session ID and hence resumes the session, following a shorter, partial TLS handshake. However, in case a session ID belonging to a previously invalid/failed TLS session is presented, the TOE implicitly rejects it by presenting a new session ID in the 'Server Hello' message, and proceeds with a fresh and complete handshake, thereby not resuming the previous session.</p>

Requirement	TSS Description
FCS_RBG_EXT.1	<p>The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90.</p> <p>The entropy source used to seed the Deterministic Random Bit Generator is a random set of bits regularly supplied to the DRBG from 4 software noise sources and 1 platform-based noise source. The combined 256-bit seed value contains 256 bits of independent and identically distributed (IID) entropy.</p> <p>All RNG entropy source samplings are continuously health tested by the NIST DRBG as per SP 900-90A before using them as a seed.</p> <p>The relevant NIST CAVP certificate numbers are listed in listed Table 21.</p>
Identification and Authentication (FIA)	
FIA_AFL.1	<p>The TOE tracks authentication failures for users. The maximum number of unsuccessful failures before lockout occurs is configurable by the administrator, with a range of 1-255.</p> <p>When the offending account becomes locked after too many failures, the TOE will block all authentication attempts until an administrator-defined period of time has elapsed. Once the period of time has elapsed, the locked account will automatically unlock without administrator intervention.</p> <p>Account lockouts are only enforced at the remote GUI interfaces. Local authentication at the local console is not blocked, so a local administrator may always manage the TOE regardless of the status of remote account lockouts.</p>
FIA_PMG_EXT.1	<p>The TOE supports the definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", "+", "-", ".", "/", ":", ";", "<", ">", "?", "[", "]", "\\", "'", "{", "}", " ", "~", "`", "=", and ",").</p> <p>The minimum password length is configurable by the Administrator and may be set between 8 and 15 characters.</p>
FIA_UAU_EXT.2 FIA_UIA_EXT.1	<p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Administrative access to the TOE is facilitated through the following interfaces:</p> <ul style="list-style-type: none"> • Directly connecting to each of the TOE component’s appliance at the local console and authenticating with a username and password. • Remotely connecting to the ESM component’s GUI via HTTPS/TLS <p>For both interfaces, the TOE prompts the user for credentials. Only after the administrative user presents the correct authentication credentials will they be granted access to the TOE administrative functionality. No TOE administrative access is permitted until an administrator is successfully identified and authenticated.</p> <p>Other than reading the TOE banner, the TOE does not permit any administrative function to be accessible until after an administrator is successfully identified and authenticated. Successful authentication is</p>

Requirement	TSS Description
	<p>indicated by being presented with the command prompt (for CLI administration) or the ESM management application main page (for GUI administration).</p> <p>Each TOE component is capable of independently identifying and authenticating administrative users and sessions.</p>
FIA_UAU.7	<p>There are no TSS activities required for this SFR. Refer to FPT_APW_EXT.1 Protection of Administrator Passwords.</p>
<p>FIA_X509_EXT.1/ITT FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3</p>	<p>The TOE performs X.509 certificate validation at the following three points:</p> <ul style="list-style-type: none"> • TOE TLS client authentication of server X.509 certificates; • TOE TLS server authentication of client X.509 certificates; • When certificates are loaded into the TOE. <p>In all three scenarios, certificates are checked for several validation characteristics:</p> <ul style="list-style-type: none"> • If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid; • The certificate chain must terminate with a trusted CA certificate; • Server certificates consumed by the TOE TLS client must have a 'serverAuthentication' extendedKeyUsage purpose; • Client certificates consumed by the TOE TLS server (for mutual authentication) must have a 'clientAuthentication' extendedKeyUsage purpose; <p>When the server receives an X.509 certificate, the server will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails and the channel is terminated. If there are no SANs of the correct type in the certificate, then the TSF will compare the reference identifier to the Common Name (CN) in the certificate Subject. If there is no CN, then the verification fails and the channel is terminated. If the CN exists and does not match, then the verification fails and the channel is terminated. Otherwise, the reference identifier verification passes and additional verification actions can proceed.</p> <p>A trusted CA certificate is defined as any certificate loaded into the TOE's trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE.</p> <p>Certificate revocation checking is performed using CRL. The CRL signing certificate must have the CRL signing purpose in the KeyUsage extension.</p> <p>The X.509 certificates for each of the given scenarios are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows:</p> <ul style="list-style-type: none"> • The public key algorithm and parameters are checked • The current date/time is checked against the validity period • revocation status is checked • Issuer name of X matches the subject name of X+1 • Name constraints are checked • Policy OIDs are checked • Policy constraints are checked; issuers are ensured to have CA signing bits

Requirement	TSS Description
	<ul style="list-style-type: none"> • Path length is checked • Critical extensions are processed <p>If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted and the TLS connection is terminated.</p> <p>As part of the verification process, the CRL is used to determine whether the certificate is revoked or not. If the CRL server cannot be contacted, then the TOE will choose to automatically accept the certificate in this case. Certificate revocation checking is performed on the leaf and intermediate CA certificates using CRL the list as a part of authentication step.</p> <p>The TSF allows Security Administrators to generate Certificate Signing Requests. The following information will be used to generate a certificate request for sending to a certificate authority for signing.</p> <ul style="list-style-type: none"> • RSA Key size: (2048, 3072) • Country Code (i.e. US): • State or Province Full Name: • City: • Company Name: • Organization Unit Name: • ESM Host Name: • Email Address:
Security Management (FMT)	
FMT_MOF.1/Functions FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys FMT_SMF.1 FMT_SMR.2	<p>The TOE implements the following role for role-based access control: Security Administrator, also called “admin”. All users of the TOE are admin users.</p> <p>The TOE and TOE components may be managed as follows:</p> <p>Locally, at the local console of the ESM (to manage the ESM component) or at the local console of an individual TOE component (for management of the individual child devices).</p> <p>Remotely, via the ESM management application Web GUI to either manage the ESM or any TOE components.</p> <p>The TOE restricts the ability to configure Syslog server connection to the Admin role. The TOE restricts the ability to manage SSH, TLS and any configured X.509 private keys to the Admin role. All management of the TOE and all TOE components is primarily performed through the ESM component, which replicates the configuration changes to all sub-components.</p> <p>The administrator may perform the following management actions via the Web GUI:</p> <ul style="list-style-type: none"> • Administer the TOE remotely • Configure the access banner • Configure the session inactivity timer before session termination • Update the TOE, and verify updates using digital signature verification • Configure the authentication failure parameters for FIA_AFL.1 • Modify the behaviour of transmission of audit data to the external audit server

Requirement	TSS Description																																														
	<ul style="list-style-type: none"> • Manage cryptographic keys • Configure cryptographic functionality • Configure the interaction between TOE components • Set the time, and configure NTP servers • Manage the trusted public keys database • Manage the TOE's trust store and the X.509v3 certificates contained therein <p>The administrator may perform the following management actions via the local Console:</p> <ul style="list-style-type: none"> • Administer the TOE locally • Configure the session inactivity timer before session termination • Set the time • Execute on-demand self-tests <p>Below is the distribution of management actions for all TOE components:</p> <table border="1"> <thead> <tr> <th>Management Functions</th> <th>ESM</th> <th>Child devices</th> </tr> </thead> <tbody> <tr> <td>Ability to administer the TOE locally and remotely.</td> <td>X</td> <td>X</td> </tr> <tr> <td>Ability to configure the access banner.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to configure the session inactivity time before session termination or locking.</td> <td>X</td> <td>X</td> </tr> <tr> <td>Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates.</td> <td>X</td> <td>X</td> </tr> <tr> <td>Ability to configure the authentication failure parameters for FIA_AFL.1.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to modify the behaviour of the transmission of audit data to an external IT entity.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to manage the cryptographic keys.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to configure the cryptographic functionality.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to configure the interaction between TOE components.</td> <td>X</td> <td>X</td> </tr> <tr> <td>Ability to set the time which is used for time-stamps.</td> <td>X</td> <td>X</td> </tr> <tr> <td>Ability to configure NTP.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to manage the trusted public keys database;</td> <td></td> <td>X</td> </tr> <tr> <td>Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.</td> <td>X</td> <td></td> </tr> <tr> <td>Ability to import X.509v3 certificates to the TOE's trust store.</td> <td>X</td> <td></td> </tr> </tbody> </table>		Management Functions	ESM	Child devices	Ability to administer the TOE locally and remotely.	X	X	Ability to configure the access banner.	X		Ability to configure the session inactivity time before session termination or locking.	X	X	Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates.	X	X	Ability to configure the authentication failure parameters for FIA_AFL.1.	X		Ability to modify the behaviour of the transmission of audit data to an external IT entity.	X		Ability to manage the cryptographic keys.	X		Ability to configure the cryptographic functionality.	X		Ability to configure the interaction between TOE components.	X	X	Ability to set the time which is used for time-stamps.	X	X	Ability to configure NTP.	X		Ability to manage the trusted public keys database;		X	Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.	X		Ability to import X.509v3 certificates to the TOE's trust store.	X	
Management Functions	ESM	Child devices																																													
Ability to administer the TOE locally and remotely.	X	X																																													
Ability to configure the access banner.	X																																														
Ability to configure the session inactivity time before session termination or locking.	X	X																																													
Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates.	X	X																																													
Ability to configure the authentication failure parameters for FIA_AFL.1.	X																																														
Ability to modify the behaviour of the transmission of audit data to an external IT entity.	X																																														
Ability to manage the cryptographic keys.	X																																														
Ability to configure the cryptographic functionality.	X																																														
Ability to configure the interaction between TOE components.	X	X																																													
Ability to set the time which is used for time-stamps.	X	X																																													
Ability to configure NTP.	X																																														
Ability to manage the trusted public keys database;		X																																													
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors.	X																																														
Ability to import X.509v3 certificates to the TOE's trust store.	X																																														

Requirement	TSS Description
Protection of the TSF (FPT)	
FPT_APW_EXT.1	<p>The TOE stores Security Administrator passwords. All passwords are stored in a secure directory that is not readily accessible to administrators. The passwords are stored in a hashed form in the underlying filesystem of the TOE.</p> <p>The TOE's GUI logon page obscures entered passwords by displaying an asterisk ("*") for each password character entered. The TOE CLI interface obscures the passwords by not echoing entered characters.</p>
FPT_ITT.1 FPT_ITT.1/Join	<p>For communication between TOE components, SSH is used in establishment of the secure communication channel. The administrator uses the ESM component to link the TOE components to the ESM or remove linked TOE components.</p> <p>This channel is then subsequently adopted as a continuing internal communication channel between the different TOE components.</p> <p>After registration, intra-TOE communication also takes place over TLS, with the ESM acting as the TLS client(s) and the other TOE components acting as the TLS server.</p> <p>All communications between TOE components occurs in either an SSH or TLS protected channel.</p>
FPT_SKP_EXT.1	<p>The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Refer to Table 20: Key Storage and Zeroization for key storage details.</p>
FPT_STM_EXT.1	<p>The TOE provides a source of date and time information used in audit event timestamps, admin inactivity, and admin lockout timer. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from as many as three NTP servers. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.</p> <p>Applied TD0632.</p>
FPT_TST_EXT.1	<p>Each TOE component runs a suite of self-tests during initial start-up to verify its correct operation. If any of the tests fail, either the TOE component will not complete its power-up boot sequence or the TOE component will enter an error state until an Administrator intervenes. The TOE component does not provide any cryptographic services while in an error state.</p> <p>During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST. This includes KATs for all cryptographic algorithms implemented by the TSF:</p> <ul style="list-style-type: none"> • cryptographic known-answer tests <ul style="list-style-type: none"> ○ HMAC KAT ○ AES KAT ○ AES GCM KAT

Requirement	TSS Description
	<ul style="list-style-type: none"> ○ XTS-AES KAT ○ RSA KAT ○ ECDSA PCT ● firmware integrity test ○ RSA PCT ● pairwise consistency testing of generated keypairs ○ ECC CDH KAT ● DRBG health testing ○ DRBG KAT <p>The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded.</p> <p>Periodically, during normal operation, the TOE performs focused DRBG health testing every time a new random number is generated:</p> <ul style="list-style-type: none"> ● DRBG Tested as required by [SP800-90] Section 11 ● DRBG FIPS 140-2 continuous test for stuck fault ● NDRNG FIPS 140-2 continuous test for NDRNG <p>Whenever the TSF generates key-pairs, pairwise consistency (ECDSA, or RSA) are performed.</p> <p>A KAT (Known Answer Test) test is a test where a cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer to determine the correctness of the implementation.</p> <p>A PCT (Pairwise Consistency Test) test is run when an asymmetrical key pair is generated. It uses the public key to encrypt a plaintext, and uses the private key to decrypt the encrypted text. If the decryption is successful, the test succeeds. Otherwise, the test fails.</p> <p>Additionally, an administrator can execute these self-tests anytime on demand via the console CLI of each TOE component.</p> <p>Because the TOE executes a complete battery of self-testing prior to and during normal operation, and because failures of the self-tests will cause the TOE to stop execution, normal operation of the TOE is guaranteed. Any time the TOE is running, all self-testing has completed successfully. All TOE components execute all of these self-tests.</p>
FPT_TUD_EXT.1	<p>The Security Administrator can query the current software version running on each of the TOE components via the Web GUI. The management application permits the administrator to initiate updates on each TOE component individually.</p> <p>Software images will not be installed without explicit administrative intervention. Update candidates are obtained through the TOE vendor distribution network, as downloadable image files from the internet or on physical media. All of the TOE component image files are digitally signed (using a 2048-bit RSA key) so their integrity can be verified during the upgrade process.</p> <p>An image that fails an integrity or signature verification check will not be loaded and the update process fails. If the update process fails, the TOE does not update the software. An error is logged into the audit log, and the TOE deletes the update candidate.</p>

Requirement	TSS Description
	<p>When an update image file successfully passes the integrity and signature verification check, it will be loaded and installed. The device will perform an automated reboot and execute the updated firmware.</p> <p>The TOE does not support delayed activation. When the update process succeeds, the TOE logs the success to the audit trail and reboots, during which device functionality is not available.</p>
TOE Access (FTA)	
FTA_SSL_EXT.1 FTA_SSL.3	A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE GUI (remote) and CLI interfaces (local). The configuration of inactivity periods are applied on a per interface basis. A configured inactivity period will be applied to both local and remote sessions in the same manner. When the interface has been idle for more than the configured period of time, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	A Security Administrator is able to exit out of both local and remote administrative sessions using the “Log Out” choice value “2” at the Console CLI or the Sign Out button in the ESM management application.
FTA_TAB.1	<p>Security Administrators can define a custom login banner that will be displayed at both the local CLI and the remote GUI interfaces.</p> <p>This banner will be displayed prior to allowing Security Administrator access through those interfaces. The advisory notice and the consent warning message can be configured differently for remote and local access interface.</p>
Trusted Path/Channels (FTP)	
FTP_ITC.1	<p>The TOE supports communications with Audit Servers.</p> <p>Each of these connections are protected via an SSH connection. This protects the data from disclosure by encryption using AES and by HMACs that verify that data has not been modified.</p> <p>SSH provides assured identification of the non-TSF endpoint by validating the public key received from the endpoint. The TOE retains a hostkey file which is used to verify that the audit server is known and trusted.</p> <p>The TOE is responsible for initiating the trusted channel with the external trusted IT entities.</p>
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted session. Remote GUI connections take place over a HTTPS over TLS connection. The TLS session is encrypted using AES encryption and uses HMACs to protect integrity, and secure identification of the endpoints is provided by X.509v3 certificates for TLS connections.

6.1 Distributed TOE SFR Allocation

For a distributed TOE, the SFRs in the cPP must be met by the TOE as a whole. However, each TOE component will not necessarily meet each SFR. The following table specifies when each SFR must be implemented by a component. The following applies:

- blue columns are used for the ESM Management Component,

- the orange columns are for ERC and ADM, Data components and
- the light green columns are for ACE, ELM, and ELS, the Auxiliary components.

The following categories are used to define the SFR allocations and defined in the cPP:

- All Components (All): All components that comprise of the distributed TOE must independently satisfy the requirement.
- At least one Component (One): This requirement must be fulfilled by at least one component within the distributed TOE.
- Feature Dependent (Feature Dependent): These requirements will only be fulfilled where the feature is implemented by the distributed TOE component.

The Audit column indicates whether the SFR produces an audit record. Refer to Table 14 for detail audit record information.

Table 19: Distributed TOE SFR Allocation

Requirement	Audit	SFR Allocation	ESM	ERC	ADM	ACE	ELM	ELS
FAU_GEN.1	No	All	X	X	X	X	X	X
FAU_GEN.2	No	All	X	X	X	X	X	X
FAU_GEN_EXT.1	No	All	X	X	X	X	X	X
FAU_STG_EXT.1	No	All	X	X	X	X	X	X
FAU_STG_EXT.4	No	Feature Dependent	X	X	X	X	X	X
FCO_CPC_EXT.1	Yes	All	X	X	X	X	X	X
FCS_CKM.1	No	One	X	X	X	X	X	X
FCS_CKM.2	No	All	X	X	X	X	X	X
FCS_CKM.4	No	All	X	X	X	X	X	X
FCS_COP.1/DataEncryption	No	All	X	X	X	X	X	X
FCS_COP.1/Hash	No	All	X	X	X	X	X	X
FCS_COP.1/KeyedHash	No	All	X	X	X	X	X	X
FCS_COP.1/SigGen	No	All	X	X	X	X	X	X
FCS_HTTPS_EXT.1	Yes	Feature Dependent	X					
FCS_NTP_EXT.1	Yes	Feature Dependent	X					
FCS_SSHC_EXT.1	Yes	Feature Dependent	X	X				
FCS_SSHS_EXT.1	Yes	Feature Dependent		X	X	X	X	X
FCS_TLSC_EXT.1	Yes	Feature Dependent	X			X		
FCS_TLSC_EXT.2	No	Feature Dependent	X			X		
FCS_TLSS_EXT.1	Yes	Feature Dependent	X	X	X	X	X	X
FCS_TLSS_EXT.2	No	Feature Dependent		X	X	X	X	X
FCS_RBG_EXT.1	No	All	X	X	X	X	X	X

Requirement	Audit	SFR Allocation	ESM	ERC	ADM	ACE	ELM	ELS
FIA_AFL.1	Yes	One	X					
FIA_PMG_EXT.1	No	One	X	X	X	X	X	X
FIA_UAU_EXT.2	Yes	One	X	X	X	X	X	X
FIA_UAU.7	No	Feature Dependent	X	X	X	X	X	X
FIA_UIA_EXT.1	Yes	One	X	X	X	X	X	X
FIA_X509_EXT.1/ITT	Yes	Feature Dependent	X	X	X	X	X	X
FIA_X509_EXT.1/Rev	Yes	Feature Dependent	X					
FIA_X509_EXT.2	No	Feature Dependent	X					
FIA_X509_EXT.3	No	Feature Dependent	X					
FMT_MOF.1/Functions	No	Feature Dependent	X					
FMT_MOF.1/ManualUpdate	Yes	All	X	X	X	X	X	X
FMT_MTD.1/CoreData	No	All	X	X	X	X	X	X
FMT_MTD.1/CryptoKeys	No	Feature Dependent	X					
FMT_SMF.1	Yes	Feature Dependent	X	X	X	X	X	X
FMT_SMR.2	No	All	X	X	X	X	X	X
FPT_APW_EXT.1	No	Feature Dependent	X	X	X	X	X	X
FPT_ITT.1	Yes	Feature Dependent	X	X	X	X	X	X
FPT_ITT.1/Join	Yes	Feature Dependent	X	X	X	X	X	X
FPT_SKP_EXT.1	No	All	X	X	X	X	X	X
FPT_STM_EXT.1	Yes	All	X	X	X	X	X	X
FPT_TST_EXT.1	No	All	X	X	X	X	X	X
FPT_TUD_EXT.1	Yes	All	X	X	X	X	X	X
FTA_SSL_EXT.1	Yes	Feature Dependent	X	X	X	X	X	X
FTA_SSL.3	Yes	Feature Dependent	X					
FTA_SSL.4	Yes	Feature Dependent	X	X	X	X	X	X
FTA_TAB.1	No	One	X	X	X	X	X	X
FTP_ITC.1	Yes	One	X					
FTP_TRP.1/Admin	Yes	One	X					

6.2 Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4:

Table 20: Key Storage and Zeroization

Keys/CSPs	Type	Storage Location	Method of Zeroization
Diffie Hellman private key	DH Key	In Memory/RAM	Overwrite with zeros
Diffie Hellman public key	DH Key	In Memory/RAM	Overwrite with zeros
SSH Private Key	RSA Private Key	On Disk	Request TSF to destroy abstraction
SSH Public Key	RSA Public Key	On Disk	Request TSF to destroy abstraction
SSH Session Key	AES Key	In Memory/RAM	Overwrite with zeros
TLS Private Key	RSA Private Key	On Disk	Request TSF to destroy abstraction
TLS Public Key	RSA Public Key	On Disk	Request TSF to destroy abstraction
TLS Session Encryption Key	AES Key	In Memory/RAM	Overwrite with zeros
TLS Session Integrity Key	HMAC Key	In Memory/RAM	Overwrite with zeros

6.3 CAVP Algorithm Testing

The table below describes the CAVP mapping for the SFRs, algorithms, crypto libraries and certificates.

Table 21 - CAVP Algorithm Testing References

SFR	Algorithm	Implementation Name	CAVP Alg	Certificate
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	Trellix OpenSSL FIPS Object Module	RSA KeyGen (FIPS186-4)	#A2624
		BC-FJA (Bouncy Castle FIPS Java API)	(2048 and 3072 bits)	#A4800
	ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	Trellix OpenSSL FIPS Object Module	ECDSA KeyGen (FIPS186-4)	#A2624
		BC-FJA (Bouncy Castle FIPS Java API)	ECDSA KeyVer (FIPS186-4)	#A4800
			(P-256, P-384 and P-521 curves)	
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete	Trellix OpenSSL FIPS Object Module	No NIST CAVP, CCTL has performed all assurance/evaluation activities.	No NIST CAVP, CCTL has performed all

	Logarithm Cryptography” and [RFC 3526, RFC 7919]			assurance /evaluation activities.
		BC-FJA (Bouncy Castle FIPS Java API)	Safe Primes Key Generation (ffdhe2048, MODP-4096)	#A4800
FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3 “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	KAS-ECC-SSC-Sp800-56Ar3 (P-256, P-384 and P-521 curves)	#A2624 #A4800
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526, groups listed in RFC 7919]	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	KAS-FFC-SSC-Sp800-56Ar3 (ffdhe2048, MODP-4096)	#A2624 #A4800
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR, GCM] mode and cryptographic key sizes [128 bits, 256 bits]	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	AES-CBC, AES-CTR, AES-GCM (128 and 256 bits)	#A2624 #A4800
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4) (2048 and 3072 bits)	#A2624 #A4800
	For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4) (P-256, P-384 and P-521 curves)	#A2624 #A4800
FCS_COP.1/ Hash	cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-256, SHA-384, SHA-512] and cryptographic key sizes [assignment: cryptographic key	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	SHA2-256 SHA2-384 SHA2-512	#A2624 #A4800

	sizes] and message digest sizes [<u>256, 384, 512</u>] bits			
FCS_COP.1/ KeyedHash	keyed-hash message authentication in accordance with a specified cryptographic algorithm [<u>HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, implicit</u>] and cryptographic key sizes [160-bit, 256-bit, 384-bit, 512-bit] and message digest sizes [<u>256, 384, 512</u>] bits	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 implicit	#A2624 #A4800
FCS_RBG_EX T.1	random bit generation services in accordance with ISO/IEC 18031:2011 using [<u>CTR_DRBG (AES)</u>]	Trellix OpenSSL FIPS Object Module BC-FJA (Bouncy Castle FIPS Java API)	Counter DRBG (AES 256)	#A2624 #A4800

7 Acronym Table

Table 22: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ACE	Advanced Correlation Engine
ADM	Application Data Monitor
CC	Common Criteria
CRL	Certificate Revocation List
DEM	Database Event Monitor
DSB	Data Streaming Bus
ELM	Enterprise Log Manager
ELS	Enterprise Log Search
EP	Extended Package
ERC	Event Receiver
ESM	Enterprise Security Manager
GUI	Graphical User Interface
IP	Internet Protocol
KAT	Known Answer Test
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PCT	Post-Quantum Cryptography
PP	Protection Profile
RSA	Rivest, Shamir, & Adleman
SIEM	Security Information and Event Management
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality TSF = TOE for pND ¹
TSS	TOE Summary Specification

¹ Applied TD0591.

Appendix A

The following is a list of libraries TBD.