E-Series and EF-Series w SANtricity v11.90R5

Security Target

Version 1.9

July 2026

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	14 July 2025	M Baldock	Initial Release
1.1	25 Aug 2025	M Baldock	Addressing ORs
1.2	19 Sept 2025	M Baldock	Addressing ORs
1.3	05 Nov 2025	M Baldock	TOE version update
1.4	29 Jan 2026	M Baldock	AGD version update
1.5	27 Apr 2026	M Baldock	Addressing ORs
1.6	25 May 2026	M Baldock	Addressing ORs
1.7	09 May 2026	M Baldock	Addressing comments
1.8	22 June 2026	M Baldock	Addressing ORs
1.9	02 July 2026	M Baldock	TOE name fix

Table of Contents

1 Introduction 5

1.1 Overview 5
1.2 Identification 5
1.3 Conformance Claims 5
1.4 Terminology 6

2 TOE Description 7

2.1 Type 7
2.2 Usage 7
2.3 Security Functions / Logical Scope 8
2.4 Physical Scope 10

3 Security Problem Definition 12

3.1 Threats 12
3.2 Assumptions 13
3.3 Organizational Security Policies 14

4 Security Objectives 15

5 Security Requirements 16

5.1 Conventions 16
5.2 Extended Components Definition 16
5.3 Functional Requirements 17
5.4 Assurance Requirements 33

6 TOE Summary Specification 34

6.1 Security Audit 34
6.2 Cryptographic Support 34
6.3 Identification and Authentication 37
6.4 Security Management 40
6.5 Protection of the TSF 41
6.6 TOE Access 43
6.7 Trusted Path/Channels 44

7 Rationale 45

7.1 Conformance Claim Rationale 45
7.2 Security Objectives Rationale 45
7.3 Security Requirements Rationale 45

List of Tables

Table 1: Evaluation identifiers 5
Table 2: NIAP Technical Decisions 5
Table 3: Terminology 6
Table 4: CAVP Certificates 9
Table 5: TOE models 10
Table 6: Threats 12
Table 7: Assumptions 13
Table 8: Organizational Security Policies 14
Table 9: Security Objectives for the Operational Environment 15
Table 10: Extended Components 16
Table 11: Summary of SFRs 17
Table 12: Audit Events 19

Table 13: Assurance Requirements 33
Table 14: Key Agreement Mapping 35
Table 15: HMAC Characteristics 35
Table 16: Keys 41
Table 17: Passwords 42
Table 18: NDcPP SFR Rationale 45

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the E-Series and EF-Series w SANtricity v11.90R5 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	E-Series and EF-Series w SANtricity v11.90R5 Build: 11.90.00.9134
Security Target	E-Series and EF-Series w SANtricity v11.90R5 Security Target, v1.9

1.3 Conformance Claims

2 This ST supports the following conformance claims:

a) CC version 3.1 revision 5

b) CC Part 2 extended

c) CC Part 3 conformant

d) collaborative Protection Profile for Network Devices, v3.0e (referenced within as NDcPP)

e) NIAP Technical Decisions per Table 2

Table 2: NIAP Technical Decisions

TD #	Name	Source	Applicability Rationale
TD0836	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	NDcPP	Applicable.
TD0868	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	NDcPP	Not Applicable. IPSEC not claimed.
TD0879	NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	NDcPP	Applicable.
TD0880	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	NDcPP	Applicable.
TD0886	Clarification to FAU_STG_EXT.1 Test 6	NDcPP	Applicable.
TD0899	NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	NDcPP	Applicable.

TD #	Name	Source	Applicability Rationale
TD0900	NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	NDcPP	Applicable.
TD0921	NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	NDcPP	Applicable.
TD0923	NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	NDcPP	Applicable.
TD0973	NIT Technical Decision: FCS_(D)TLSS_EXT.1.3 Test 2 DHE Ciphersuite Conditionality	NDcPP	Applicable.
TD0990	NIT Technical Decision: CTR_DRBG in FCS_RBG_EXT.1.2	NDcPP	Applicable.
TD1033	Sunset Dates for NDcPP Configurations	NDcPP	Applicable.

1.4 Terminology

Table 3: Terminology

Term	Definition
CC	Common Criteria
EAL	Evaluation Assurance Level
NDcPP	collaborative Protection Profile for Network Devices
PP	Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality

2 TOE Description

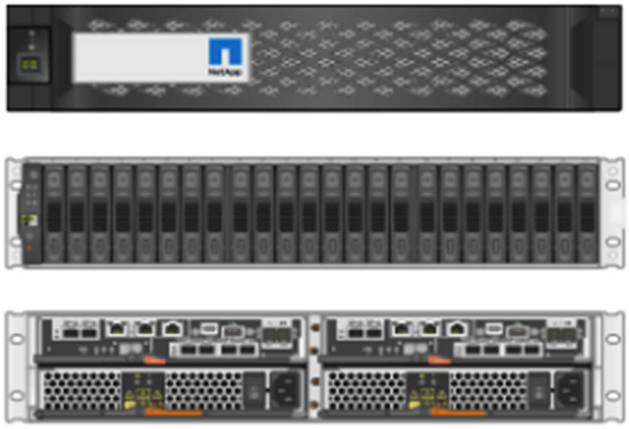
2.1 Type

3 The TOE is a network device that provides networked storage for dedicated, high-bandwidth applications like data analytics, video surveillance, and disk-based backup that need simple, fast, reliable SAN storage.

2.2 Usage

4 **Figure 1** shows an E-Series hardware device (front, open front, rear).

Figure 1: Example TOE



2.2.1 Interfaces

5 The TOE management interfaces are shown in Figure 2.

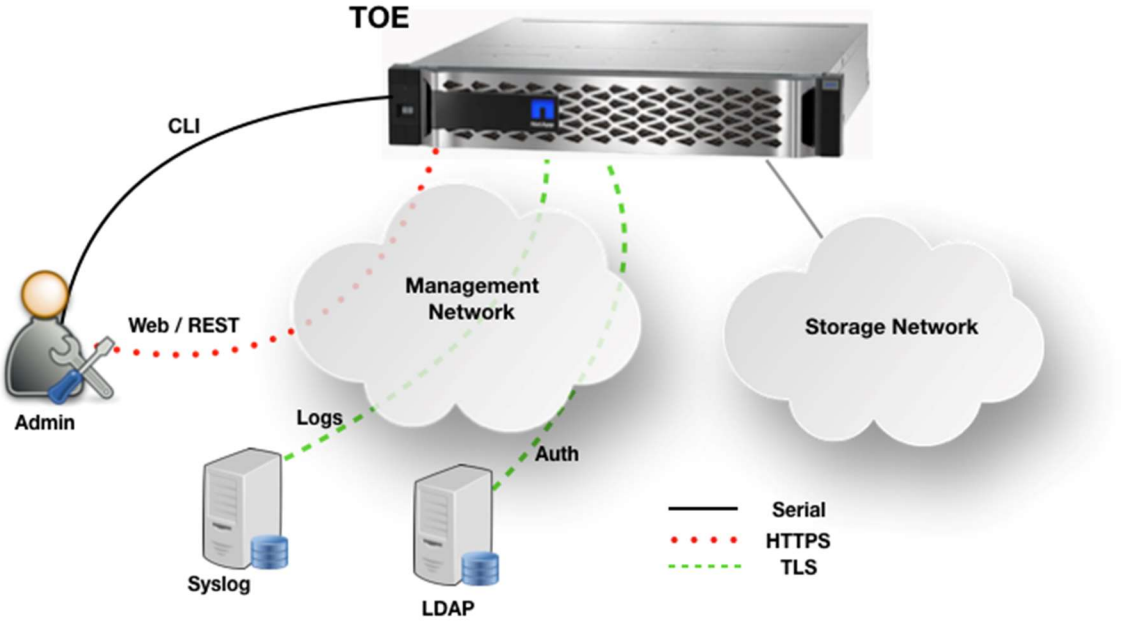


Figure 2: TOE interfaces

6 The TOE interfaces are as follows:

a) **CLI.** Administrative CLI via direct serial connection.

b) **Web / REST.** Administrator access via Web GUI or REST API[1] over HTTPS.

c) **Logs.** Logs are transmitted to a Syslog server via TLS.

d) **Authentication (auth).** The TOE communicates with an LDAP server via TLS.

7 Each hardware device contains two redundant controllers which provide the TOE security functions. The controller management interfaces are separately addressable on the network however configuration data is shared for redundancy.

2.3 Security Functions / Logical Scope

8 The TOE provides the following security functions:

a) **Trusted Path/Channels.** The TOE protects the integrity and confidentiality of communications as noted in section 2.2.1 above, and using cryptographic algorithms as described in Table 4.

b) **Security Management.** The TOE enables secure management of its security functions, including:

i) Administrator authentication with passwords

ii) Configurable password policies

iii) Role Based Access Control

iv) Access banners

v) Management of critical security functions and data

vi) Protection of cryptographic keys and passwords

c) **Protection of the TSF.** The TOE performs a suite of self-tests to ensure the correct operation and enforcement of its security functions. The TOE performs diagnostic self-tests and cryptographic module self-tests during start-up and generates audit records to record a failure. Self-tests comply with the FIPS 140-2 requirements for self-testing.

d) **Identification and Authentication.** The TOE ensures that all users must be authenticated before accessing its functions and data. The TOE uses X.509 certificates to support authentication for TLS. Certificate revocation checking is performed using OCSP.

e) **TOE Access.** TOE can be accessed directly via serial connection or remotely via TLS connection. When a user account has sequentially failed authentication the configured number of times, the account will be locked for a Security Administrator defined time period.

f) **Security Audit.** The TOE generates audit records of user and administrator actions. The TOE includes the user identity in audit events resulting from actions of identified users. The Security Administrator can configure the TOE to send logs in real-time to a syslog server via TLS.

g) **Cryptographic Support** The TOE implements a cryptographic module. The cryptographic module has the ability to generate and destroy cryptographic

[1] RESTful API can be used directly with an API tool such as “curl”. The Web GUI also makes use of the RESTful API.

keys. Relevant Cryptographic Algorithm Validation Program (CAVP) certificates are shown in Table 4.

Table 4: CAVP Certificates

SFR	Operational Environment	Module	Algorithm(s) (keys/curves/digest-size)	Usage	CAVP Cert#
FCS_CKM.1 – Cryptographic Key Generation	SANtricity OS 11.90 Intel(R) Xeon(R) D-1715TER CPU @ 2.40GHz (Ice Lake-D) SANtricity OS 11.90 Intel(R) Xeon(R) D-2164IT CPU @ 2.10GHz (Skylake) SANtricity OS 11.90 Intel(R) Xeon(R) D-2123IT CPU @ 2.20GHz (Skylake)	Bouncy Castle BC-FIPS v 11.90	RSA Key Gen (186-4) with key sizes of 2048 bits	FCS_TLSC_EXT.1 FCS_TLSS_EXT.1	A7093
			ECDSA Key Gen (186-4) with key sizes of 256, 384 and 521 bits		
			DSA Key Gen (186-4) with key sizes of 2048 bits		
FCS_CKM.2 – Cryptographic Key Establishment			KAS-ECC		
			KAS-FFC		
FCS_COP.1/DataEncryption – AES Data Encryption/Decryption			AES-GCM-128 AES-GCM-256		
FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)			RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4) Key sizes of 2048 bits, 3072 bits, 4096 bits		
			ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4) With key sizes of 256, 384 and 521 bits		
FCS_COP.1/Hash			SHA-256		

SFR	Operational Environment	Module	Algorithm(s) (keys/curves/digest-size)	Usage	CAVP Cert#
Cryptographic Operation (Hash Algorithm)			SHA-384		
FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)			HMAC-SHA-256 HMAC-SHA-384		
FCS_RBG_EXT.1 Random Bit Generation			Hash_DRBG(SHA-256)		

2.4 Physical Scope

9 The physical boundary of the TOE includes SANtricity OS 11.90 and hardware shown in Table 5. The TOE is delivered via commercial courier.

Table 5: TOE models

Model	CPU	Max Capacity	Max Drives
E4012 (DE212C)	Intel(R) Xeon(R) D-1715TER CPU @ 2.40GHz (Ice Lake-D)	264TB	96 HDD/SSD
E4060 (DE460C)	Intel(R) Xeon(R) D-1715TER CPU @ 2.40GHz (Ice Lake-D)	1.3PB	300 HDD / 120 SSD
EF300	Intel(R) Xeon(R) D-2164IT CPU @ 2.10GHz (Skylake)	367TB	24 SSD
EF600	Intel(R) Xeon(R) D-2164IT CPU @ 2.10GHz (Skylake)	367TB	24 SSD
EF300C	Intel(R) Xeon(R) D-2123IT CPU @ 2.20GHz (Skylake)	1.5PB	24 SSD
EF600C	Intel(R) Xeon(R) D-2123IT CPU @ 2.20GHz (Skylake)	1.5PB	24 SSD

2.4.1 Guidance Documents

10 The TOE includes the following guidance documents (PDF) which may be downloaded from https://docs.netapp.com/us-en/e-series-santricity/:

a) E-Series and EF-Series w SANtricity v11.90R5 Common Criteria Guide, v1.3 June 22, 2026

b) EF300 and EF600 E-Series storage systems June 12, 2026 https://docs.netapp.com/us-en/e-series/pdfs/sidebar/EF300_and_EF600.pdf

c) NetApp Install hardware E-Series storage systems, June 12, 2026 https://docs.netapp.com/us-en/e-series/pdfs/sidebar/Install_hardware.pdf

d) NetApp E4000 E-Series storage systems, June 12, 2026 https://docs.netapp.com/us-en/e-series/pdfs/sidebar/E4000.pdf

e) NetApp Linux express configuration E-Series storage systems, June 12, 2026 https://docs.netapp.com/us-en/e-series/pdfs/sidebar/Linux_express_configuration.pdf

f) NetApp SANtricity System Manager SANtricity software, April 23, 2026 https://docs.netapp.com/us-en/e-series-santricity-119/pdfs/sidebar/SANtricity_System_Manager.pdf

g) NetApp Get Started SANtricity commands, March 17, 2026 https://docs.netapp.com/us-en/e-series-cli/pdfs/sidebar/Get_started.pdf

2.4.2 Non-TOE Components

11 The TOE operates with the following components in the environment:

a) **Audit Server.** The TOE is capable of sending audit events to a Syslog server.

b) **LDAP Server.** The TOE is capable of utilizing an LDAP server for authentication.

c) **OCSP Responder.** The TOE validates the revocation status of X509 certificates via OCSP.

2.4.3 Functions not included in the TOE Evaluation

12 The SMcli client application is not included in the scope of the TOE evaluation.

3 Security Problem Definition

13 The Security Problem Definition is reproduced from section 4 of the NDcPP.

3.1 Threats

Table 6: Threats

Identifier	Description
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 traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	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.
T.UNDETECTED_ACTIVITY	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

Identifier	Description
	the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
T.SECURITY_FUNCTIONALITY_FAILURE	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.

3.2 Assumptions

Table 7: Assumptions

Identifier	Description
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). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.

Identifier	Description
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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.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

Table 8: Organizational Security Policies

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

4 Security Objectives

14 The security objectives are reproduced from section 5 of the NDcPP.

Table 9: Security Objectives for the Operational Environment

Identifier	Description
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_ADMIN	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. 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.
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.
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. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

5 Security Requirements

5.1 Conventions

15 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

16 **Note:** Operations performed within the Security Target are denoted within brackets []. Operations shown without brackets are reproduced from the NDcPP.

5.2 Extended Components Definition

17 The Extended Components are defined in Appendix C of the NDcPP.

Table 10: Extended Components

Requirement	Title	Source	Applicable TDs
FAU_STG_EXT.1	Protected Audit Event Storage	NDcPP	TD0886, TD0923
FCS_RBG_EXT.1	Random Bit Generation	NDcPP	TD0990
FCS_HTTPS_EXT.1	HTTPS Protocol	NDcPP	
FCS_TLSC_EXT.1	TLS Client Protocol	NDcPP	TD0899
FCS_TLSS_EXT.1	TLS Server Protocol	NDcPP	TD0899, TD0973
FIA_PMG_EXT.1	Password Management	NDcPP	
FIA_UIA_EXT.1	User Identification and Authentication	NDcPP	TD0900
FIA_X509_EXT.1/Rev	X.509 Certificate Validation	NDcPP	
FIA_X509_EXT.2	X.509 Certificate Authentication	NDcPP	
FIA_X509_EXT.3	X.509 Certificate Requests	NDcPP	
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)	NDcPP	
FPT_APW_EXT.1	Protection of Administrator Passwords	NDcPP	
FPT_TST_EXT.1	TSF Testing	NDcPP	TD0836

Requirement	Title	Source	Applicable TDs
FPT_TUD_EXT.1	Trusted Update	NDcPP	
FPT_STM_EXT.1	Reliable Time Stamps	NDcPP	
FTA_SSL_EXT.1	TSF-initiated Session Locking	NDcPP	TD0879

5.3 Functional Requirements

Table 11: Summary of SFRs

Requirement	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
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/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSS_EXT.1	TLS Server Protocol
FIA_AFL.1	Authentication Failure Handling
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication

Requirement	Title
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MOF.1/Functions	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
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
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 Banners
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1/Admin	Trusted Path

5.3.1 Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

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

a. Start-up and 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 Administrator account shall be logged if individual 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 Administrator account shall be logged)]];*

d. *Specifically defined auditable events listed in ~~**Table 2**~~ **Table 12**.*

Table 12: Audit Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS session	Reason for failure
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.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	Origin of the attempt (e.g., IP address)
FIA_UAU.7	None.	None.
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/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Functions	None.	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_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	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).

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session lock	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.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions	• None • None • Reason for failure
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	• None • None • Reason for failure

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

a. Date and time of the event, type of event, subject identity ~~(if applicable)~~, and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of* ***~~Table 2~~ Table 12***.

FAU_GEN.2 User Identity Association

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

FAU_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 consist of a single standalone component that stores audit data locally,

].

FAU_STG_EXT.1.3 The TSF shall maintain a [log file] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [persistent] audit records locally with a minimum storage size of [*500 – 50000 records*].

FAU_STG_EXT.1.5 The TSF shall [overwrite previous audit records according to the following rule: [*overwrite oldest record first*], [*no other action*]] when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [ability to view locally].

5.3.2 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of [*2048 bits, 3072 bits, 4096 bits*] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1;
- 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, or FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Appendix A.2, or ISO/IEC 14888-3, “IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms”, Section 6.6.;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1

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

Application Note: FCS_CKM.1.1 modified by TD0921

FCS_CKM.2 Cryptographic Key Establishment

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 “FIPS 186-Type” parameter-size sets that meet the following: NIST Special Publication 800-56A Revision 3,

"Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

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

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 [destruction of reference to the key directly followed by a request for garbage collection];*
- *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*.

FCS_COP.1/DataEncryption Cryptographic Operation (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* [GCM] mode and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3,* [GCM as specified in ISO 19772].

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,
- Elliptic Curve Digital Signature Algorithm

]

and cryptographic key sizes [

- For RSA: [*2048 bits, 3072 bits, 4096 bits*],
- For ECDSA: [*256, 384 and 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 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 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 implementing [P-256, P-384, P-521] curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST Recommended" curves; or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.

].

Application Note: FCS_COP.1.1/SigGen modified by TD0921

FCS_COP.1/Hash Cryptographic Operation (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] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ and **message digest sizes [256, 384] bits** that meet the following: *ISO/IEC 10118-3:2004*.

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] and cryptographic key sizes *[160,256,384]* **and message digest sizes [256, 384] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

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_RBG_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 [Hash_DRBG [SHA-256]].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*one*] 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.

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

[

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- 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_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

] 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, IPv4 address in the CN].

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [

- without any administrator override mechanism.

].

FCS_TLSC_EXT.1.4 The TSF shall [present the Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [

- present the signature_algorithms extension with support for the following algorithms:

  [

  - rsa_pkcs1 with sha256(0x0401),
  - rsa_pkcs1with sha384(0x0501),
  - rsa_pkcs1 with sha512(0x0601),
  - ecdsa_secp256r1 with sha256(0x0403),
  - ecdsa_secp384r1 with sha384(0x0503),
  - ecdsa_secp521r1 with sha512(0x0603),
  - rsa_pss_rsae with sha256(0x0804),
  - rsa_pss_rsae with sha384(0x0805),
  - rsa_pss_rsae with sha512(0x0806),

  ] and no other algorithms;

- present the signature_algorithms_cert extension with the following Signature Schemes:

[

- rsa_pkcs1 with sha256(0x0401),
- rsa_pkcs1with sha384(0x0501),
- rsa_pkcs1 with sha512(0x0601),
- ecdsa_secp256r1 with sha256(0x0403),
- ecdsa_secp384r1 with sha384(0x0503),
- ecdsa_secp521r1 with sha512(0x0603),
- rsa_pss_rsae with sha256(0x0804),
- rsa_pss_rsae with sha384(0x0805),
- rsa_pss_rsae with sha512(0x0806)

] and no other SignatureSchemes

].

FCS_TLSC_EXT.1.6 The TSF [does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7 The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8 The TSF shall [not use PSKs].

FCS_TLSC_EXT.1.9 The TSF shall [support TLS 1.2 secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746, reject [TLS1.2, TLS 1.3] renegotiation attempts].

Note: LDAP Supports TLS 1.2 renegotiation, Syslog Rejects TLS 1.2 renegotiation.

FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The TSF shall implement [TLS 1.3 (RFC 8446), 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_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- 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_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [RSA with key size [2048, 3072, 4096] bits;].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [

- EC Diffie-Hellman key agreement over NIST curves [secp256r1,secp384, secp521r1] and no other curves;
- Diffie-Hellman parameters [of size 2048 bits]

].

FCS_TLSS_EXT.1.4 The TSF shall support [session resumption based on session IDs according to RFC 5246 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)].

FCS_TLSS_EXT.1.5 The TSF [does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6 The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_TLSS_EXT.1.7 The TSF shall [not use PSKs].

FCS_TLSS_EXT.1.8 The TSF shall [support secure renegotiation in accordance with RFC 5746 by always including the “renegotiation_info” TLS extension in TLS 1.2 ServerHello messages, reject [TLS 1.3] renegotiation attempts].

5.3.3 Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within *[1 - 2,147,483,647]* 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].

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 [1] and [30] characters.*

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;
- [[*storage device services*]]

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.

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [Web GUI password] and [no other mechanism]. The TSF shall provide the following local authentication mechanisms [password-based].

FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

Application Note: FIA_UIA_EXT.1.3 modified by TD0900

FIA_UAU.7 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**.

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 [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- 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 DTLS/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. o Client certificates presented for DTLS/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.

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 [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 [not accept the certificate].

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 [device-specific information, 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.

5.3.4 Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates to Security Administrators*.

FMT_MOF.1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [modify the behaviour of] the functions [transmission of audit data to an external IT entity] to *Security Administrators*.

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*.

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*.

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 remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using* digital signature *capability prior to installing those updates;*
- [
    - Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size);
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to manage the cryptographic keys;
    - Ability to set the time which is used for time-stamps;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - Ability to generate Certificate Signing Request (CSR) and process CA certificate response;
    - Ability to administer the TOE locally;
    - Ability to configure the local session inactivity time before session termination or locking;
    - Ability to configure the authentication failure parameters for FIA_AFL.1;

    ]

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 remotely*

are satisfied.

5.3.5 Protection of the TSF (FPT)

FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

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) to verify the integrity of the TOE firmware and software;
- Prior to providing any cryptographic service and [at no other time, on-demand] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [start-up] self-tests [*Central Processing Unit (CPU) and Memory Basic Input/Output System (BIOS) self-tests*].

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [all failures] by [entering a maintenance mode].

Application Note: This SFR modified by TD0836.

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.

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].

5.3.6 TOE Access (FTA)

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.

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

FTA_SSL.4 User-initiated Termination

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

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing ~~a~~ **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding ~~unauthorised~~ use of the TOE.

5.3.7 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall **be capable of using [TLS] to** provide a **trusted** communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [authentication server]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure **and detection of modification of the channel data.**

FTP_ITC.1.2 The TSF shall permit [**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 [*Syslog and LDAP authentication*].

FTP_TRP.1 /Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using [HTTPS] to** provide a communication path between itself and **authorized** remote **Administrators** ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure **and provides detection of modification of the channel data**.

FTP_TRP.1.2 /Admin The TSF shall permit remote **Administrators** ~~users~~ 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*.

5.4 Assurance Requirements

18 The TOE security assurance requirements are summarized in Table 13.

Table 13: Assurance Requirements

Assurance Class	Components	Description
Security Target Evaluation	ASE_CCL.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 User Guidance
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing - conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

19 In accordance with section 7.1 of the NDcPP, the following refinement is made to ASE:

a) **ASE_TSS.1.1C Refinement:** The TOE summary specification shall describe how the TOE meets each SFR. **In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.**

6 TOE Summary Specification

20 The following describes how the TOE fulfils each SFR included in section 5.3.

6.1 Security Audit

6.1.1 FAU_GEN.1

21 The TOE generates the audit records specified at FAU_GEN.1 containing fields that include the timestamp, IP address (if applicable), action, user (if applicable) and a contextual message indicating success or failure of the action.

22 The following information is logged as a result of the Security Administrator generating/importing or deleting cryptographic keys:

a) **Generate CSR.** Action and key reference.

b) **Add/Remove Certificates.** Action and key reference.

c) **Add/Remove Cryptographic Keys.** Action and key reference.

6.1.2 FAU_GEN.2

23 The TOE includes the user identity in audit events resulting from actions of identified users.

6.1.3 FAU_STG_EXT.1

24 The Security Administrator can configure the TOE to send logs to a Syslog server. Log events are sent in real-time. Logs are sent via TLS as described by FCS_TLSC_EXT.1.

25 The TOE is a standalone TOE that stores audit data locally. The number of audit events that may be stored locally is configurable by the administrator. Audit events can be configured between 500 – 50000 events. When the number of events is exceeded, the TOE will overwrite audit records starting with the oldest audit record. The TOE will allow the number of events to exceed the configured amount by 99 audit records.

26 Local audit data is stored in persistent log files that maintain records after reboot.

27 Only authorized administrators may view audit records and no capability to modify the audit records is provided. An administrator may delete audit logs.

6.2 Cryptographic Support

6.2.1 FCS_CKM.1

28 The TOE supports key generation for the following asymmetric schemes:

a) **RSA 2048/3072/4096-bit.** Used in TLS RSA authentication.

b) **ECC P-256/P-384/P-521.** Used in TLS ECDSA authentication.

c) **FFC Schemes.** Used in TLS DHE authentication.

6.2.2 FCS_CKM.2

29 The TOE supports the following key establishment schemes:

a) **ECC schemes.** Used in TLS ciphersuites with ECDHE key exchange. TOE is both sender and receiver.

b) **FFC schemes.** Used in TLS ciphersuites with DHE key exchange. TOE is both sender and receiver.

30 Table 14 below identifies the scheme being used by each service.

Table 14: Key Agreement Mapping

Scheme	SFR	Service
ECC	FCS_TLSS_EXT.1	Web/REST Trusted Path
	FCS_TLSC_EXT.1	Syslog and LDAP
FFC	FCS_TLSS_EXT.1	Web/REST Trusted Path
	FCS_TLSC_EXT.1	Syslog and LDAP

6.2.3 FCS_CKM.4

31 Cryptographic keys and their related destruction method are identified in Table 16.

6.2.4 FCS_COP.1/DataEncryption

32 The TOE provides symmetric encryption and decryption capabilities using 128 and 256 bit AES in GCM mode for TLS.

33 The relevant NIST CAVP certificate numbers are listed Table 4.

6.2.5 FCS_COP.1/SigGen

34 The TOE provides cryptographic signature generation and verification services using:

a) RSA Signature Algorithm with key sizes of 2048 bits, 3072 bits and 4096 bits

b) ECDSA Signature Algorithm with NIST curves P-256, P-384 and P-521.

35 These RSA and ECDSA signature verification services are used in the TLS protocols.

36 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.6 FCS_COP.1/Hash

37 The TOE provides cryptographic hashing services using SHA-256 and SHA-384.

38 SHA is implemented in the following parts of the TSF:

a) TLS; and

b) Hashing of passwords in non-volatile storage.

39 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.7 FCS_COP.1/KeyedHash

40 The TOE provides keyed-hashing message authentication services using HMAC-SHA-256, and HMAC-SHA-384.

41 HMAC is implemented in the following protocols: TLS.

42 The characteristics of the HMACs used in the TOE are given in Table 15.

Table 15: HMAC Characteristics

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA-384	1024 bits	384 bits	384 bits

43 The relevant NIST CAVP certificate numbers are listed in Table 4.

6.2.8 FCS_HTTPS_EXT.1

44 The TOE Web / REST interface is accessed via an HTTPS connection using the TLS implementation described by FCS_TLSS_EXT.1. The TOE does not use HTTPS in a client capacity. The TOE's HTTPS protocol complies with RFC 2818.

45 RFC 2818 specifies HTTP over TLS. The majority of RFC 2818 is spent on discussing practices for validating endpoint identities and how connections must be setup and torn down. The TOE web GUI operates on an explicit port designed to natively speak TLS: it does not attempt STARTTLS or similar multi-protocol negotiation which is described in section 2.3 of RFC 2818. The web services API attempts to send closure Alerts prior to closing a connection in accordance with section 2.2.2 of RFC 2818.

6.2.9 FCS_RBG_EXT.1

46 The TOE contains a Hash(SHA-256)_DRBG that is seeded from the hardware entropy source (Intel RDRAND). Entropy from the noise source is extracted, conditioned and used to seed the DRBG with 256 bits of full entropy.

47 Additional detail is provided in the proprietary Entropy Description.

6.2.10 FCS_TLSC_EXT.1

48 The TOE operates as a TLS client for the trusted channel with Syslog and LDAP servers.

49 TLS 1.2 and TLS 1.3 are allowed and ciphersuites are restricted to those listed at FCS_TLSC_EXT.1.1. Ciphersuites are not user-configurable.

50 The reference identifier for Syslog and LDAP is configured by the administrator using the Web GUI or REST API. The reference identifiers must be an IPv4 address or DNS name.

51 When the TLS client receives an X.509 certificate from the server, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate.

52 If an IPv4 address is used in the X.509 certificate, then a CN is required. If a CN 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 (IPv4 address or DNS name) in the certificate, then the TOE will compare the reference identifier to the Common Name (CN) in the certificate Subject.

53 If the reference identifier found in the SAN is an IPv4 address then verification fails and the channel is terminated. If there is no CN, then the verification fails and the channel is terminated. If a DNS 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.

54 The TLS client does not support certificate pinning however it does support wildcards.

55 The TLS client will transmit the Supported Elliptic Groups extension in the Client Hello message by default with support for the following NIST curves: P256, P384 and P512. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve ciphersuites. The TOE will accept the connection if any valid Server generated DHE parameter is returned.

56 The TOE presents the signature_algorithms and signature_algorithms_cert extensions and supports the algorithms listed in FCS_TLSC_EXT.1.5. The algorithms present in the Client Hello are supported by default and are not configurable.

57 The TOE prohibits the use of the Early data extension and Post-handshake client authentication according to RFC 8446 Section 4.2.6

58 The TOE does not use PSKs.

59 The TOE supports TLS 1.2 secure renegotiation through the use of the renegotiation_info extension in accordance with RFC 5746 and rejects TLS 1.3 renegotiation attempts for LDAP TLS.

60 The TOE rejects TLS1.2 and TLS 1.3 renegotiation attempts for Syslog TLS.

6.2.11 FCS_TLSS_EXT.1

61 The TOE operates as a TLS server for the Web / REST trusted path.

62 The server allows TLS protocol version 1.2 and 1.3 and is restricted to the ciphersuites identified at FCS_TLSS_EXT.1.1. Ciphersuites are not user-configurable. The TOE rejects the connection when presented with all other TLS and SSL versions from a Client Hello.

63 The TOE supports X.509 certificates using RSA with key sizes of 2048, 3072 and 4096 bits for authenticating itself to clients.

64 The TLS server is capable of negotiating ciphersuites that include ECDHE key agreement scheme sizes P256, P384 and P521 and DHE parameters of size 2048 bits.

65 The TOE supports TLS 1.2 session resumption through the use of session ID’s according to RFC 5246, and TLS 1.3 session resumption according to RFC 8446.

66 Session resumption via Session ID exist within their own contexts.

67 Session resumption with Session IDs occurs when the TOE is presented with the Session ID of the session to be resumed. The TOE checks its cache for a matching ID and resumes if found. If a session ID cannot be found, a new session is established instead.

68 The TOE prohibits the use of the Early Data extension and PSKs

69 The TOE supports TLS 1.2 secure renegotiation through the use of the renegotiation_info extension in accordance with RFC 5746 and rejects TLS 1.3 renegotiation attempts.

6.3 Identification and Authentication

6.3.1 FIA_AFL.1

70 The TOE tracks authentication failures of remote administrators. This tracking occurs separately for each of the two controllers in the TOE appliance.

71 When a user account has sequentially failed the configured number of authentication attempts, the account will be locked for a Security Administrator defined time period.

72 The administrator can configure the maximum number of failed attempts using the REST API or CLI.

73 The local console does not implement the lockout mechanism.

6.3.2 FIA_PMG_EXT.1

74 The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”.

75 The password length is configurable to between 1 and 30 characters by the Administrator.

6.3.3 FIA_UIA_EXT.1

76 Administrative access to the TOE is facilitated through one of several interfaces:

a) Directly connecting to the TOE appliance via console for CLI (local user accounts only)

b) Remotely connecting to the TOE Web GUI via HTTPS (local and LDAP user accounts)

c) Remotely submitting requests to the TOE REST API via HTTPS (local and LDAP user accounts)

77 No administrative access is permitted until an administrator is successfully identified and authenticated.

78 The TOE warning banner is displayed prior to authentication (only applicable to the CLI and Web GUI) and TOE storage services are available.

79 The TOE prompts the user to enter a username and password when accessing the CLI or Web GUI.

80 Each request submitted to the REST API must include a valid username and password.

81 For local user accounts, the TOE compares submitted passwords to the stored representation for the provided username. If there is a match and the user account is not locked (per FIA_AFL.1) a successful logon occurs.

82 For LDAP user accounts, the TOE offloads authentication to the external authentication server. If the user account is not locked and the authentication server authenticates the user, a successful logon occurs.

6.3.4 FIA_UAU.7

83 For all authentication at the local CLI the TOE provides no feedback when the administrative password is entered so that the password is obscured.

6.3.5 FIA_X509_EXT.1/Rev

84 The TOE performs X.509 certificate validation at the following points:

a) TOE TLS client validation of server X.509 certificates;

b) When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates (such as the web server certificate presented by the TOE TLS web GUI).

85 In all scenarios, certificates are checked for several validation characteristics:

a) If the certificate ‘notAfter’ date is in the past, then this is an expired certificate which is considered invalid;

b) The certificate chain must terminate with a trusted CA certificate;

c) Server certificates consumed by the TOE TLS client must have a ‘serverAuthentication’ extendedKeyUsage purpose;

d) A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE.

86 Certificate revocation checking for the above scenarios is performed using OCSP.

87 As X.509 certificates are not used for trusted updates, firmware integrity self-tests or client authentication, the code-signing and clientAuthentication purpose is not checked in the extendedKeyUsage for related certificates.

88 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:

a) The public key algorithm and parameters are checked

b) The current date/time is checked against the validity period revocation status is checked

c) Issuer name of X matches the subject name of X+1

d) Name constraints are checked

e) Policy OIDs are checked

f) Policy constraints are checked; issuers are ensured to have CA signing bits

g) Path length is checked

h) Critical extensions are processed

89 If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted.

6.3.6 FIA_X509_EXT.2

90 The TOE has a trust store where root CA and intermediate CA certificates can be stored. The TOE restricts the ability to access trust store to Security Administrators. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope.

91 Instructions for configuring the trusted IT entities (LDAP and Syslog servers) to supply appropriate X.509 certificates are captured in the guidance documents.

92 As part of the verification process, OCSP is used to determine whether the certificate is revoked or not. If the OCSP responder cannot be contacted, then the TOE will choose to not accept the certificate in this case.

93 There are two ways in which an OCSP responder can be invoked:

a) By default, the TOE will extract the OCSP responder URI from the Authority Information Access field.

b) If configured, the TOE will use a single centralized OCSP responder for all revocation checks.

6.3.7 FIA_X509_EXT.3

94 The TOE can generate Certificate Signing Requests (CSR) with 2048-bit, 3072-bit and 4096-bit RSA keys for the web server certificates. The CSR may contain:

a) Device-specific information:

i) Subject Alternative Name – IP or DNS

ii) Locality

iii) State

b) Common Name – IP, DNS or other user defined name

c) Organization

d) Organizational Unit

e) Country

95 The TOE only accepts Certificate Responses when a valid certification path is found.

6.4 Security Management

6.4.1 FMT_MOF.1/ManualUpdate

96 The TOE restricts the ability to perform software updates to Security Administrators.

6.4.2 FMT_MOF.1/Functions

97 The TOE restricts the ability to modify (enable/disable) transmission of the following audit records to an external audit server to Security Administrators:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit;

c) Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators);

d) 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);

e) 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);

f) Resetting passwords (name of related user account shall be logged); and

g) Specifically defined auditable events listed in Table 12.

98 The Security Administrator modifies transmission of audit records to an external audit server by adding or removing the reference identifier of the remote audit server.

6.4.3 FMT_MTD.1/CoreData

99 The TOE restricts the ability to manage TSF data to Security Administrators.

6.4.4 FMT_MTD.1/CryptoKeys

100 The TOE restricts the ability to delete, generate, import or otherwise manage TLS and any configured X.509 certificates or private keys to Security Administrators via the Web GUI.

6.4.5 FMT_SMF.1

101 The TOE may be managed via Web GUI, REST API or CLI. The specific management capabilities include:

a) Ability to administer the TOE locally (CLI) and remotely (Web GUI & REST API)

b) Ability to configure the access banner (via Web GUI & REST API)

c) Ability to configure the session inactivity time before session termination or locking (via Web GUI & REST API)

d) Ability to update the TOE and to verify the updates (via Web GUI & REST API)

e) Ability to configure local audit behavior (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size) (via Web GUI & REST API)

f) Ability to modify the behavior of the transmission of audit data to an external IT entity using syslog (via Web GUI & REST API)

g) Ability to manage the cryptographic keys (via Web GUI & REST API)

h) Ability to set the time which is used for time-stamps (via Web GUI & REST API)

i) Ability to manage the TOE's trust store and designate X509v3 certificates as trust anchors (via Web GUI & REST API)

j) Ability to generate Certificate Signing Request and process CA certificate response (via Web GUI)

k) Ability to configure the authentication failure parameters via REST API

6.4.6 FMT_SMR.2

102 The TOE implements role based access control based on pre-defined roles that are assigned when creating a user.

103 All TOE users are administrative users who may be assigned the following user roles (which may collectively be considered the 'Security Administrator'):

a) **Storage Monitor.** Has read-only access to storage related configuration data.

b) **Storage Administrator.** Has read-write access to storage related configuration data.

c) **Support Administrator.** Has read-write access to support related management data.

d) **Security Administrator.** Has read-write access to all TOE management data.

6.5 Protection of the TSF

6.5.1 FPT_SKP_EXT.1

104 Keys are protected as described in Table 16. In all cases, plaintext keys cannot be viewed through an interface designed specifically for that purpose.

Table 16: Keys

Key	Algorithm	Storage	Zeroization
TLS Private Key	RSA (2048 bits)	Persistent – Java Keystore	The TLS private key is deleted when a new certificate is generated or when certificates are removed. The TOE will destroy the abstraction that represents the key via the JVM garbage collector.
DH Parameters used for TLS	ECDH (secp256r1, secp512r1)	RAM - plaintext	JVM garbage collector when no longer required.
AES key used for TLS	AES-128 AES-256	RAM - plaintext	JVM garbage collector when no longer required.

6.5.2 FPT_APW_EXT.1

105 Passwords are protected as describe in Table 17. In all cases plaintext passwords cannot be viewed through an interface designed specifically for that purpose.

Table 17: Passwords

Key/Password	Generation/ Algorithm	Storage
Locally stored administrator passwords	User generated	Persistent – Salted SHA-256 hash

6.5.3 FPT_TST_EXT.1

106 At startup, the TOE undergoes the following tests:

a) Software Integrity using HMAC-SHA256

b) AES known answer tests

c) DRBG known answer tests

d) ECDSA known answer tests

e) HMAC known answer tests

f) RSA known answer tests

g) SHS known answer tests

h) Central Processing Unit (CPU) and Memory Basic Input/Output System (BIOS) self-tests – CPU and memory are initialized by exercising a set of known answer tests and the BIOS is compared against a known checksum of the image. The memory is zeroized and then a random pattern is written to and read from the memory.

107 These tests ensure the correct operation of the cryptographic functionality of the TOE, the CPU and BIOS and verify that the correct TOE image is being used. The cryptographic functionality will not be available if the tests fail, and any operation of the TOE supported by this functionality will not be available. If the CPU, or BIOS tests fail, the device will not complete the boot up operation. If the boot loader image verification fails, the boot up operation will fail. When the device completes the boot

up operation, this is evidence that the self-tests have passed, and that the TOE, and the cryptographic functions are operating correctly.

108 The cryptographic module executes the following conditional tests when the related service is invoked:

a) DH Pairwise Consistency Test performed on every DH key pair generation.

b) DRBG Continuous Test performed when a random value is requested from the DRBG.

c) ECDSA Pairwise Consistency Test performed on every EC key pair generation.

d) RSA Pairwise Consistency Test performed on every RSA key pair generation.

e) DRBG Health Checks

109 If a self-test fails, the device enters error mode and halts system operation. All data output and cryptographic services are inhibited when in the error state. Continued operation indicates that the tests have passed, and the TOE is operating correctly.

6.5.4 FPT_TUD_EXT.1

110 The administrator manually downloads and installs firmware updates. The TOE permits only authenticated administrators to use both the Web GUI interactively as well as using the REST API in a non-interactive manner to deploy firmware upgrades. The use of the API to upgrade the TOE will require a specific API call, along with the admin credentials.

111 At the Web UI, the administrator can view firmware version information by navigating to Home > Support > Upgrade Center" and clicking "Inventory".

112 The TOE validates software updates through the use of RSA 3072 digital signatures included in the firmware upgrade bundle as a "sig" file. RSA signatures are defined in FCS_COP.1/SigGen. Digital signatures are verified when an upgrade is initiated. If verification fails, the upgrade is aborted and the failure is logged. If verification succeeds, the upgrade continues and firmware is installed.

6.5.5 FPT_STM_EXT.1

113 The TOE incorporates an internal clock that is used to maintain date and time. The Security Administrator sets the date and time during initial TOE configuration and may change the time during operation.

114 The TOE makes use of time for the following:

a) Audit record timestamps

b) Interactive session timeouts

c) Account lockout timer

d) Certificate validation

6.6 TOE Access

6.6.1 FTA_SSL_EXT.1

115 The TOE terminates an inactive local interactive session (CLI) following a specified period of time. The timeout value is set to fifteen minutes by default but may be configured by the Security Administrator.

6.6.2 FTA_SSL.3

116 The TOE terminates an inactive remote interactive session (Web UI) following a specified period of time. The timeout value is set to thirty minutes by default but may be configured by the Security Administrator.

6.6.3 FTA_SSL.4

117 Administrative users may terminate their own sessions at any time.

6.6.4 FTA_TAB.1

118 The TOE displays an administrator configurable message to users prior to login at the CLI and Web GUI.

6.7 Trusted Path/Channels

6.7.1 FTP_ITC.1

119 The TOE supports secure communication with the following IT entities:

a) Syslog server per FCS_TLSC_EXT.1

b) LDAP server per FCS_TLSC_EXT.1

6.7.2 FTP_TRP.1/Admin

120 The TOE provides the following trusted paths for remote administration:

a) Web GUI over HTTPS per FCS_HTTPS_EXT.1.1

b) REST API over HTTPS per FCS_HTTPS_EXT.1.1

7 Rationale

7.1 Conformance Claim Rationale

121 The following rationale is presented with regard to the PP conformance claims:

a) **TOE type.** As identified in section 2.1, the TOE is network device, consistent with the NDcPP.

b) **Security problem definition.** As shown in section 2.4.3, the threats, OSPs and assumptions are reproduced directly from the NDcPP.

c) **Security objectives.** As shown in section 4, the security objectives are reproduced directly from the NDcPP.

d) **Security requirements.** As shown in section 5, the security requirements are reproduced directly from the NDcPP. No additional requirements have been specified.

7.2 Security Objectives Rationale

122 All security objectives are drawn directly from the NDcPP.

7.3 Security Requirements Rationale

123 All security requirements are drawn directly from the NDcPP. Table 18 presents a mapping between threats and SFRs as presented in the NDcPP.

Table 18: NDcPP SFR Rationale

Identifier	SFR Rationale
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	• The Administrator role is defined in FMT_SMR.2 and the relevant administration capabilities are defined in FMT_SMF.1 and FMT_MTD.1/CoreData, with optional additional capabilities in FMT_MOF.1/Services and FMT_MOF.1/Functions • The actions allowed before authentication of an Administrator are constrained by FIA_UIA_EXT.1, and include the advisory notice and consent warning message displayed according to FTA_TAB.1 • The requirement for the Administrator authentication process is described in FIA_UIA_EXT.1 • Locking of Administrator sessions is ensured by FTA_SSL_EXT.1 (for local sessions), FTA_SSL.3 (for remote sessions), and FTA_SSL.4 (for all interactive sessions) • The secure channel used for remote Administrator connections is specified in FTP_TRP.1/Admin • (Malicious actions carried out from an Administrator session are separately addressed by T.UNDETECTED_ACTIVITY) • If the TOE provides remote administration using a password-based authentication mechanism, FIA_AFL.1

Identifier	SFR Rationale
	provides actions on reaching a threshold number of consecutive password failures.
T.WEAK_CRYPTOGRAPHY	• Requirements for key generation and key distribution are set in FCS_CKM.1 and FCS_CKM.2 respectively • Requirements for use of cryptographic schemes are set in FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, and FCS_COP.1/KeyedHash • Requirements for random bit generation to support key generation and secure protocols (see SFRs resulting from T.UNTRUSTED_COMMUNICATION_CHANNELS) are set in FCS_RBG_EXT.1 • Management of cryptographic functions is specified in FMT_SMF.1
T.UNTRUSTED_COMMUNICATION_CHANNELS	• The general use of secure protocols for identified communication channels is described at the top level in FTP_ITC.1 and FTP_TRP.1/Admin; for distributed TOEs the requirements for inter-component communications are addressed by the requirements in FPT_ITT.1 • Requirements for the use of secure communication protocols are set for allowed protocols in FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_HTTPS_EXT.1, FCS_IPSEC_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2 • Requirements for the use of secure communication protocols implemented by the packages specified in Section 2.2 may be found in the respective package's document. • Optional and selection-based requirements for use of public key certificates to support secure protocols are defined in FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3
T.WEAK_AUTHENTICATION_ENDPOINTS	• 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 • Additional possible special cases of secure authentication during registration of distributed TOE components are addressed by FCO_CPC_EXT.1 and FTP_TRP.1/Join.

Identifier	SFR Rationale
T.UPDATE_COMPROMISE	• Requirements for protection of updates are set in FPT_TUD_EXT.1 • Additional optional use of certificate-based protection of signatures can be specified using FPT_TUD_EXT.2, supported by the X.509 certificate processing requirements in FIA_X509_EXT.1, FIA_X509_EXT.2 and FIA_X509_EXT.3 • Requirements for management of updates are defined in FMT_SMF.1 and (for manual updates) in FMT_MOF.1/ManualUpdate, with optional requirements for automatic updates in FMT_MOF.1/AutoUpdate
T.UNDETECTED_ACTIVITY	• Requirements for basic auditing capabilities are specified in FAU_GEN.1 and FAU_GEN.2, with timestamps provided according to FPT_STM_EXT.1 and if applicable, protection of NTP channels in FCS_NTP_EXT.1. • Requirements for protecting audit records stored on the TOE are specified in FAU_STG.1. • Requirements for secure storage and transmission of local audit records to an external IT entity via a secure channel are specified in FAU_STG_EXT.1 and FAU_STG_EXT.1. • Optional additional requirements for dealing with potential loss of locally stored audit records are specified in FAU_STG_EXT.2, and FAU_STG_EXT.3.
T.SECURITY_FUNCTIONALITY_COMPROMISE	• Protection of secret/private keys against compromise is specified in FPT_SKP_EXT.1 • Secure destruction of keys is specified in FCS_CKM.4 • If (optionally) management of keys is provided by the TOE then this is specified in FMT_SMF.1 and confining this functionality to Security Administrators is required by FMT_MTD.1/CryptoKeys • If optional local administration using a password-based authentication mechanism is provided by the TOE, FIA_UAU.7 provides protection of password entry by providing only obscured feedback at the local console. • If the TOE provides password-based authentication mechanisms, requirements for password lengths and available characters are set in FIA_PMG_EXT.1. Requirements for secure storage of passwords are set in FPT_APW_EXT.1
T.SECURITY_FUNCTIONALITY_FAILURE	• Requirements for running self-test(s) are defined in FPT_TST_EXT.1
P.ACCESS_BANNER	• An advisory notice and consent warning message is required to be displayed by FTA_TAB.1