Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box Security Target

Issued on: 10 Jun 2026

Version: 1.15

Created by: Hitachi Vantara, Ltd.

This document is a translation of the evaluated and certified security target written in Japanese.

Change History

History	Creation Date	Chapter	Change Details
1.01	2/Feb/2026	All	New
1.02	25/Feb/2026	1	Review of the TOE identification information
1.03	2/Mar/2026	1 7	Review of the TOE identification information Review of the types of characters allowed in passwords
1.04	3/Mar/2026	1 7	Review of the TOE identification information and the non-TOE hardware/software/firmware Review of the information that can be included when creating a CSR
1.05	5/Mar/2026	1	Review of the Table 5
1.06	9/Mar/2026	1	Review of the Table 5
1.07	10/Mar/2026	6,7	Review of the types of characters allowed in passwords
1.08	12/Mar/2026	1	Revision of the guidance document version
1.09	6/Apr/2026	1,7 8	Review of the TLS communication environment Review of the terminology
1.10	9/Apr/2026	1 8	Review of the TOE operational environment Review of the terminology
1.11	17/Apr/2026	1	Addition of definitions for the Remote Management PC and the Local Management PC
1.12	27/Apr/2026	1	Addition of a description of the Private CA Review of the TOE-related User Roles
1.13	19/May/2026	1	Review of a description of the Identification and Authorization function
1.14	4/Jun/2026	1	Revision of the guidance document version
1.15	10/Jun/2026	1	Revision of the guidance document version

Table of Contents

1. ST Overview

This section describes ST reference, TOE reference, TOE overview, and TOE description.

1.1. ST Reference

This section describes the ST identification information.

Title: Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box Security Target
Version: 1.15
Date of Issue: 10 June 2026
Created by: Hitachi Vantara, Ltd.

1.2. TOE Reference

This section describes the TOE identification information.
TOE Reference: Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box HA-DKC-04A-03X

The TOE consists of two physical components: the controller chassis and the drive box.
This TOE is one of the following products.

Table 1 TOE Identification Information

#	TOE Name	Controller Chassis Identification			drive box Identification
		Brand Name	Model Identification Name		
1	Hitachi Virtual Storage Platform One Block 23 with Drive Box HA-DKC-04A-03X	HITACHI	VSP One B 23	Firmware (Version: HA-DKC-04A-03X)	DBN2
2	Hitachi Virtual Storage Platform One Block 24 with Drive Box HA-DKC-04A-03X		VSP One B 24		
3	Hitachi Virtual Storage Platform One Block 26 with Drive Box HA-DKC-04A-03X		VSP One B 26		
4	Hitachi Virtual Storage Platform One Block 28 with		VSP One B 28		

	Drive Box HA-DKC-04A-03X				

Hitachi Virtual Storage Platform One Block 23 with Drive Box HA-DKC-04A-03X is for Japan sales only, and Hitachi Virtual Storage Platform One Block 24 with Drive Box HA-DKC-04A-03X is for out of Japan sales only. Hitachi Virtual Storage Platform One Block 26 with Drive Box HA-DKC-04A-03X and Hitachi Virtual Storage Platform One Block 28 with Drive Box HA-DKC-04A-03X is for Japan/out of Japan sales.

1.3. TOE Overview

1.3.1. TOE Type

TOE is a disk storage device with remote management.

TOE is a network device that functions as a user interface for remote management of TOE and network functions such as sending audit logs to an external audit log server.

1.3.2. Usage of the TOE

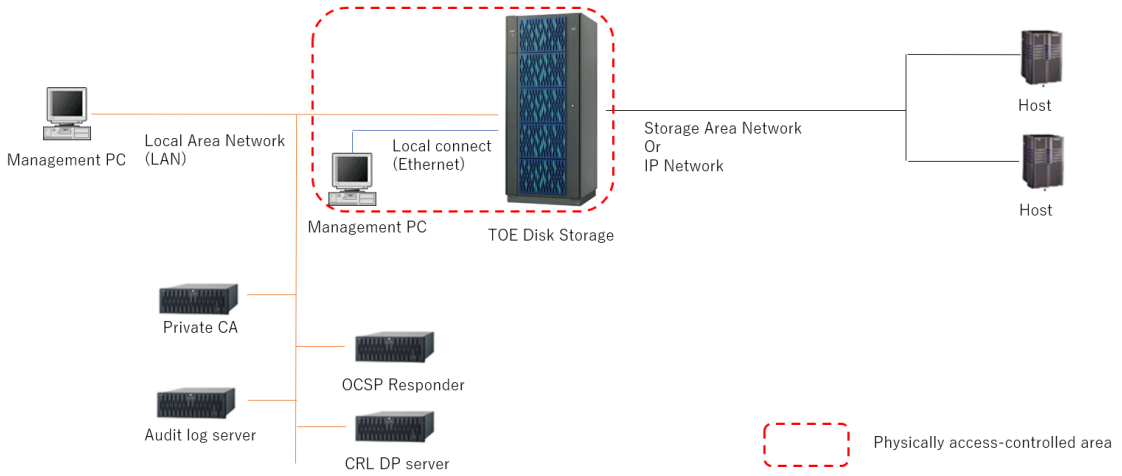


Figure1 TOE Operating Environment

Figure 1 shows the TOE operating environment. For details on the devices appearing in the environment shown in Figure 1, refer to Table2 in the section 1.3.4.

Numerous hosts are connected to the TOE via Storage Area Network or IP network. The TOE provides disk storage functions to the connected hosts.

In addition, the TOE provides network functions such as security management functions for remote management PCs connected via a Local Area Network (LAN) or locally connected(Ethernet) local management PCs, and functions for transferring audit logs to an

audit log server, as well as certificate revocation verification functions using a CRL DP server/OCSP responder.
In addition, a private CA (Certification Authority) within the network is required for certificate issuance.

1.3.3. Major security features of the TOE

The TOE provides security functions that protect assets such as configuration information related to the security functions it handles, by preventing threats to network devices such as unauthorized access to the TOE, bypassing of security functions, abuse of privileges, interception of network communications, and data tampering. The security functions provided by the TOE include a security audit function that records events occurring within the TOE in an audit log; various cryptographic functions, such as the encryption of communication data; functions for identifying and authenticating administrators and devices; functions that provide security management, such as firmware updates; functions that protect security features, such as self-tests performed during TOE startup; session management functions for administrator sessions; and secure communication using HTTPS with LAN connected remote management PCs, and secure communication using TLS with LAN connected audit log servers.
Note that security functions related to storage functions (e.g., encryption of stored data, encryption of user data on Storage Area Networks and IP Networks, and host authentication functions) are excluded from the scope of evaluation based on this ST.

1.3.4. non-TOE hardware/software/firmware required by the TOE

This section lists the non-TOE hardware/software/firmware required by the TOE. Table 2 lists the required hardware and software. Both the OCSP responder and the CRL DP server are required for certificate revocation checking. however, in the operational environment, it is sufficient that either an OCSP responder or a CRL DP server is provided.

Table 2 non-TOE hardware/software/firmware required by the TOE

Hardware	Software/Firmware	Description
Host	● Host computer supporting the following communication protocols ➢ For Storage Area Networks ✧ Fibre Channel	A computer that accesses disk storage devices. It connects to disk storage devices via a Storage Area Network or IP Network.

Hardware	Software/Firmware	Description
	➢ For IP Networks ✧ iSCSI, NVMe/TCP	Hosts, Storage Area Networks, IP Networks are excluded from evaluation under this ST.
Remote Management PC	● OS ➢ Windows 11 ● Browser ➢ TOE supported Google Chrome, Mozilla Firefox ● REST API client ➢ Software or scripts that utilize REST APIs, as well as tools (such as curl) for sending HTTPS requests	A computer that uses the HTTPS to manage the TOE remotely. Used for communication with the TOE management program called ESM (Embedded Storage Manager).
Local Management PC	● OS ➢ Windows 11 ● Browser ➢ TOE supported Google Chrome, Mozilla Firefox	When an administrator is locked out of their account remotely and cannot log in to the TOE, this computer connects directly to the TOE and uses HTTPS to manage the TOE locally. Used for communication with the TOE management program called ESM.
Audit log server	A server using rsyslogd is assumed in this environment.	A server that uses the Syslog over TLS to store the TOE audit logs
OCSP Responder	A server using OpenSSL is assumed in this environment.	A server that uses the OCSP protocol to refer to the certificate revocation list of a certification authority and to return the status of the relevant

Hardware	Software/Firmware	Description
		certificate
CRL DP Server	A server that uses protocols such as HTTP is assumed in this environment.	A server that uses HTTP to hosts a list of certificates revoked by the certification authority
Private CA	A server using OpenSSL is assumed in this environment.	Private CA certificate authority server used for signing certificates.

1.3.5. Evaluator Test Configuration

The configuration used for the TOE evaluation is shown below.

Table 3 Configuration used for the evaluation of the TOE

Category	Software
Remote Management PC	OS: Windows 11 Pro Browser: Google Chrome 141.0.7390.108, Mozilla Firefox 144.0 REST API Client: Script using Python 3.13.5
Local Management PC	OS: Windows 11 Pro Browser: Google Chrome 141.0.7390.108
Audit Log Server	OS: Ubuntu 21.10 Audit Log Server: rsyslogd 8.2302.0
OCSP Responder	OS: Kali Linux 2023.4 OCSP Responder: Server using OpenSSL 3.0.8
CRL DP Server	OS: Kali Linux 2023.4 CRL DP Server: HTTP server using Python 3.13.5
Private CA	OS：Kali Linux 2023.4 CA Certificate Authority: OpenSSL 3.0.8 based Certificate Authority

There are no differences in management functions available between the local management PC and the remote management PC. However, for evaluator testing, the confirmation of each function is, in principle, conducted only on the remote management PC.

1.4. TOE Description

1.4.1. Physical Scope of the TOE

The TOE consists of disk storage devices (Hitachi Virtual Storage Platform One Blocks 23,

24, 26, and 28) comprising hardware and firmware, and guidance documents.
The TOE consists of a controller chassis and drive boxes. Although the TOE consists of two enclosures, the controller chassis and the drive box the functions that provide SFR operate only on the controller chassis, making it a non-distributed TOE.
Customers order TOE hardware by selecting one of the models listed in Table4, and the unit is shipped from the manufacturing site configured with the selected model. The TOE firmware is distributed pre-installed on the controller chassis.
TOE guidance documents are distributed to customers in PDF format via the web page. For sales in Japan, TOE guidance documents are also distributed to customers in PDF format in the media (DVD-R) attached to the product.
You can download the guidance documents from the following web page.
Sales for Japan: https:
https://itpfdoc.hitachi.co.jp/Pages/document_list/manuals/vsp_rh20k_mid2u_1040.html
Sales for out of Japan:
https://docs.hitachivantara.com/p/vsp-one-block
The components included in the physical scope of the TOE are listed below.

The identification information for each model is shown below. The TOE consists of two components: a controller chassis and a drive box; however, it is shipped with the drive box connected to the controller chassis.

Table 4 Hardware constituting the TOE Identified

#	TOE Name	Sales Destination	Controller Chassis			Drive Box
			Brand Name	Model Identification Name		
1	Hitachi Virtual Storage Platform One Block 23 with Drive Box HA-DKC-04A-03X	Japan	HITACHI	VSP One B 23	Firmware (Version: HA-DKC-04A-03X)	DBN2
2	Hitachi Virtual Storage Platform One Block 24 with Drive Box HA-DKC-04A-03X	Outside of Japan		VSP One B 24		
3	Hitachi Virtual Storage Platform One Block 26 with Drive Box HA-DKC-04A-03X	Japan/Outside of Japan		VSP One B 26		
4	Hitachi Virtual Storage Platform One Block 28 with	Japan/Outside of		VSP One B		

	Drive Box HA-DKC-04A-03X	Japan		28		

The TOE guidance for the components of the TOE is shown below.

Table 5 TOE Guidance

#	Sales Destination	Guidance Name	Format	Version
1	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 System Administrator Guide (In Japanese)	PDF	4050-1J-U50-41
2	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 ESM Message Guide (In Japanese)	PDF	4050-1J-U07-41
3	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 Audit Log Reference Guide (In Japanese)	PDF	4050-1J-U00-41
4	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 System Provisioning Guide (In Japanese)	PDF	4050-1J-U09-41
5	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 VSP One Block Administrator REST API	PDF	4050-1J-U41-40

		Reference Guide (In Japanese)		
6	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 VSP One Block Administrator Users Guide (In Japanese)	PDF	4050-1J-U40-40
7	Japan	Hitachi Virtual Storage Platform One Block 23, Block 26, Block 28 Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H, 5600H Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H Hitachi Virtual Storage Platform F350, F370, F700, F900 Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900 REST API Reference Guide (In Japanese)	PDF	4060-1J-U71-60
8	Japan	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 SIM Reference (In Japanese)	PDF	4050-1J-U21-41
9	Japan	Hitachi Virtual Storage Platform One Block 23/26/28 with Drive Box HA-DKC-04A-03X Users guidance (In Japanese)	PDF	1.14
10	Out of Japan	Hitachi Virtual Storage Platform One Block A3-04-0x System Administrator Guide	PDF	MK-23VSP1B009-03
11	Out of Japan	Hitachi Virtual Storage Platform One Block 20 A3-03-2x Installation Guide	PDF	MK-23VSP1B008-03

12	Out of Japan	Hitachi Virtual Storage Platform One Block SVOS 10.4 Maintenance Utility Messages	PDF	MK-23VSP1B005-03
13	Out of Japan	Hitachi Virtual Storage Platform One Block SVOS 10.4 Provisioning Guide	PDF	MK-23VSP1B012-03
14	Out of Japan	Hitachi Virtual Storage Platform One Block SVOS 10.4 VSP One Block Administrator REST API Reference Guide	PDF	MK-23VSP1B002-02
15	Out of Japan	Hitachi Virtual Storage Platform One Block SVOS 10.4 VSP One Block Administrator Users Guide	PDF	MK-23VSP1B001-02
16	Out of Japan	Hitachi Virtual Storage Platform One Block Hitachi Virtual Storage Platform 5000 Series Hitachi Virtual Storage Platform E Series Hitachi Virtual Storage Platform G130, G/F350, G/F370, G/F700, G/F900 SVOS 10, SVOS RF 9 REST API Reference Guide	PDF	MK-23VSP1B003-05
17	Out of Japan	Hitachi Virtual Storage Platform One Block 24/26/28 with Drive Box HA-DKC-04A-03X Users guidance	PDF	1.13

1.4.2. Logical Scope of the TOE

1.4.2.1. TOE-Related User Roles

This ST assumes the following users in relation to disk storage devices. In this TOE, there are four roles: Security Administrator (View & Modify), Storage Administrator (Initial Configuration), Audit Log Administrator (View & Modify), and User Maintenance, who perform settings related to security functional requirements. The roles of each user are described in Table6.

Table 6 Roles in the TOE

#	Role	Description
1	Security Administrator (View & Modify)	An administrator who performs account management tasks such as registering, modifying, and deleting

		administrator accounts, update Web server certificates, management of keys using the Web GUI or REST API.
2	Storage Administrator (Initial Configuration)	An administrator who performs initial configuration tasks, such as configuring the date and time of the disk storage device or setting messages displayed on the access banner, using the Web GUI or REST API.
3	Audit Log Administrator (View & Modify)	An administrator who uses the Web GUI or REST API to download audit logs and configure settings related to the audit log server and other settings concerning audit logs generated by storage devices.
4	User Maintenance	An administrator who performs user maintenance tasks, such as program updates, using the Web GUI.

1.4.2.2. Security Functions Provided by TOE

1.4.2.2.1. Security Audit

Security audit is a function that records operations or events related to the TOE's security functions as audit information and stores them within the TOE. The recorded audit data can be downloaded by an administrator and can also be transferred to an external audit log server using the Syslog protocol.

The TOE audit log includes the user information of the administrator who performed the operation, information on the success or failure of the associated processing, the target operation, processing details, and the date and time the operation was performed. Date and time information is appended to the TOE audit log. If there is no available space in the internal audit log file to record additional audit logs, the oldest audit log is overwritten to record the latest audit log.

1.4.2.2.2. Cryptographic Support

Cryptographic support refers to the functions used by the TOE for cryptographic key generation, key exchange, and key destruction; data encryption and decryption; signature generation and verification; hash and HMAC generation and verification; and random number generation. The TOE uses these cryptographic functions for encrypted communication using HTTPS with remote management PCs, or encrypted communication using TLS with audit log servers as well as for the protection of TSF data.

1.4.2.2.3. Identification and Authentication

Identification and authentication refer to the functions used to identify and authenticate

administrator accounts using a user ID and password during login for remote and local administrator accounts, or to verify X.509v3 certificates supporting TLS authentication when audit logs are transferred to the audit log server.
The TOE supports user ID and password-based identification and authentication for logins by remote and local administrators via the Web GUI or REST API. Regarding the identification and authentication of remote administrators, the TOE provides functions to manage administrator account passwords and to lock out administrator accounts for a period defined by the Security Administrator if they fail authentication consecutively more than the number of failed attempts set by the Security Administrator.
Additionally, when identifying and authenticating an audit log server using an X.509v3 certificate, TOE communicates with an OCSP responder or a CRL DP server to verify the revocation status of the audit log server's certificate. If the certificate is revoked, TOE terminates communication with the target audit log server.

1.4.2.2.4. Security Management

Security management is a function that enables control and configuration of TSF data operations based on the roles of administrator accounts. To enable such control and configuration, the TOE maintains roles for operating security management functions and associates them with authorized TOE users who have been authenticated by the identification and authentication functions. Furthermore, the TOE provides security management functions such as setting password policies for administrator accounts, configuring the number of allowed authentication failures, and setting the time interval before re-authentication is permitted.

1.4.2.2.5. Protection of the TSF

Protection of the TOE refers to the following functions that the TOE employs to protect the TSF and TSF data:

・Firmware integrity tests and known-answer tests of cryptographic algorithms performed during TOE startup
・Verification of firmware authenticity during TOE firmware updates
・Password hashing performed when saving administrator account credentials
・Verification of the validity period of X.509v3 certificates and configuration of the date and time by the administrator for timestamps applied to audit logs

1.4.2.2.6. TOE Access

TOE Access refers to the functionality for managing sessions related to remote/local

administrator access using the Web GUI/REST API, or the functionality for displaying notes regarding TOE usage as configured by the administrator in an access banner when accessing the TOE.
TOE provides the following features to manage administrator access sessions:
・Termination of administrator access sessions that have been inactive for a specified period
・Termination of sessions by the administrator logging out

1.4.2.2.7. Trusted Path/Channels

Trusted Path/Channels is a function that secures communication channels by using HTTPS for communication between the TOE and the remote management PC, and TLS for communication between the TOE and the audit log servers.

2. Conformance Claims

2.1. CC Conformance Claim

This ST conforms to the following standards.
Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
Part 2: Security Functional Requirements, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
Part 3: Security Assurance Requirements, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
Security Functional Requirements: Part 2 Extended
Security Assurance Requirements: Part 3 Conformant

2.2. PP Claims

The PPs to which this ST and TOE conform are as follows
PP Reference: Collaborative Protection Profile for Network Devices
PP Version: 3.0e
PP Date: December 6, 2023

In addition, this ST and TOE apply the following Technical Decisions issued by the Network Device International Community

Table 7 Applicable Technical Decisions

#	ID	Title
1	RFI#202401	Redundant requirements in FPT_TST_EXT.1
2	RFI#202402a	Separation of test definitions for TLSv1.2 v1.3 (renegotiation) Client
3	RFI#202402b	Separation of test definitions for TLSv1.2 v1.3 (renegotiation) Server
4	RFI#202405	Clarification of audit selections in FMT_SMF.1.1
5	RFI#202409	Correction of FCS_TLSS_EXT.1.4
6	RFI#202413	Missing section header in NDcPP Appendix B
7	RFI#202415	FCS_COP.1.1/SigGen Needs assignment added
8	RFI#202418	FAU_STG_EXT.1

2.3. Package Claims

No packages claim compliance in this ST.

2.4. Conformance Claim rationale

Since it satisfies the following requirements specified by the PP and achieves "Exact Conformance" as required by the PP, the TOE type is consistent with NDcPP v3.0e.

a) TOE Type: The TOE possesses network functions for remote management and audit data transmission and is a network device. (Described in section 1.3)
b) Security Problem Definition: The content of the NDcPP is directly incorporated regarding threats, assumptions, and the organizational security policy. (Described in chapter 3)
c) Security Objectives: The security objectives directly incorporates the content of the NDcPP. (Described in chapter 4)
d) Security Requirements: The content of NDcPP is directly incorporated regarding security requirements, and no additional requirements are included. (Described in chapter 6)

3. Security Problem Definition

3.1. Threats

The TOE counters the threats described in this section.

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 tunneling protocols to protect critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully carry out man-in-the-middle attacks, replay attacks, and other exploits. Successful attacks will result in the loss of confidentiality and integrity of critical network traffic and could potentially lead to a compromise of the network device itself.

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may exploit secure protocols that use weak methods to authenticate endpoints, such as a shared password that is easily guessable or transmitted in plaintext. The consequences are the same as those of a poorly designed protocol: an attacker could impersonate the administrator or another device, and could insert themselves into the network traffic to perform a man-in-the-middle attack. The result is that critical network traffic is exposed with , potentially leading to a loss of confidentiality and integrity, and the network device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update to the software or firmware that undermines the device's security functionality. Non-validated updates or updates validated using insecure or weak cryptography leave the 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 the Administrator's knowledge. This could result in the attacker finding a way (e.g., misconfiguration, product flaw) to compromise the device, and the Administrator would be unaware 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's 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 exploit failed or compromised security functionality and might subsequently use or abuse security functions without prior authentication to access, alter, or modify device data, critical network traffic, or the device's security functionality.

3.2. 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 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 regarding 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 un or 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 or services that could be deemed 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 is evaluated as a pND, following Case 2 vNDs, the VS is considered part of

the TOE with only one vND instance for each physical hardware platform. The exception is 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.

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 for the device itself, including administrative data and audit data. Traffic traversing the Network Device and destined for another network entity is not covered by the ND cPP. It is assumed that this protection will be provided by cPPs and PP-Modules for specific types of Network Devices (e.g., firewalls).

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of the organization's security. This includes being appropriately trained, following policies, and adhering to guidance documentation. Administrators are trusted to ensure that passwords and 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 who actively works to bypass or compromise the device's security. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g., through offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (also known as the "root store," "trusted CA Key Store," or similar) as a trust anchor prior to use (e.g., through offline verification).

A.REGULAR_UPDATES

The Network Device firmware and software are assumed to be updated by an Administrator on a regular basis in response to the release of product updates addressing 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 no unauthorized access is possible to 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 Policy

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions on use, legal agreements, or any other appropriate information to which the Administrator consents by accessing the TOE.

4. Security Objectives

4.1. Security 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 its own VM and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION

The TOE does not provide any protection for 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 expected 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 if such certificate can no longer be trusted

OE.UPDATES

The TOE firmware and software are updated by an Administrator on a regular basis in

response to the release of product updates addressing 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 no unauthorized access is possible to 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. Extended Component Definitions

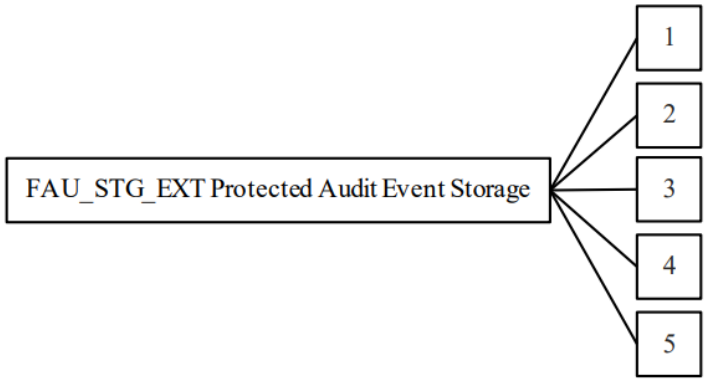
5.1. Security Audit (FAU)

5.1.1. Protected Audit Event Storage(FAU_STG_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to securely transmit audit data between the TOE and an external IT entity.

Component Levelling



FAU_STG_EXT.1 Protected audit event storage requires the TSF to use a trusted channel implementing a secure protocol.

FAU_STG_EXT.2 Counting lost audit data requires the TSF to provide information about auditrecords affected when the audit log becomes full.

FAU_STG_EXT.3 Action in case of possible audit data loss requires the TSF to generate a

warning before the audit trail exceeds the local storage capacity.
FAU_STG_EXT.4 Protected Local audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.
FAU_STG_EXT.5 Protected Remote audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.

Management: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3,FAU_STG_EXT.4, FAU_STG_EXT.5

The following actions could be considered for the management functions in FMT:

a. The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3, FAU_STG_EXT.4. FAU_STG_EXT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FAU_STG_EXT.1 Protected Audit Event Storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF Trusted Channel

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 [selection:

- The TOE shall consist of a single standalone component that stores audit data locally,
- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data].

FAU_STG_EXT.1.3 The TSF shall maintain a [selection: log file, database, buffer, [assignment:other local logging method]] 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 [selection: persistent, nonpersistent] audit records locally with a minimum storage size of [assignment: number of records and/or file/buffer size(s)].

FAU_STG_EXT.1.5 The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: 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 [selection: none, manual export, ability to view locally].

5.2. Cryptographic Support (FCS)

5.2.1. Random Bit Generation (FCS_RBG_EXT)

Family Behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Component Levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FCS_RBG_EXT.1 Random Bit Generation

Hierarchical to: No other components

Dependencies: No other components

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: Hash_DRBG [selection: SHA-256, SHA-384, SHA-512], HMAC_DRBG [selection:

SHA-256, SHA384, SHA-512], CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source] with a minimum of [selection: 128 bits, 192 bits, 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.

5.2.2. Cryptographic Protocols (FCS_HTTPS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

5.2.2.1. FCS_HTTPS_EXT.1 HTTPS Protocol

Family Behaviour

Components in this family define the requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component Levelling

FCS_HTTPS_EXT.1 HTTPS Protocol requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management: FCS_HTTPS_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components

Dependencies: [FCS_TLSC_EXT.1 TLS Client Protocol, or FCS_TLSS_EXT.1 TLS Server Protocol]

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

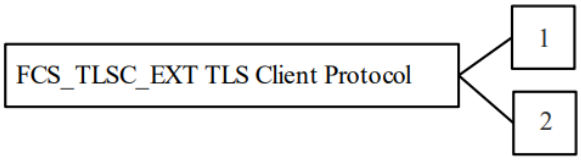
FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

5.2.2.2. FCS_TLSC_EXT TLS Client Protocol

Family Behaviour

The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol. This is a new family defined for the FCS class.

Component Levelling



FCS_TLSC_EXT.1 TLS Client Protocol requires that the client side of TLS be implemented as specified.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication requires that the client side of the TLS implementation include mutual authentication.

Management: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment
b. TLS session establishment
c. TLS session termination

FCS_TLSC_EXT.1 TLS Client Protocol

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_RBG_EXT.1 Random Bit Generation
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSC_EXT.1.1

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

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- 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_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- 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_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- 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_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
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

TLS_AES_128_CCM_8_SHA256] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN, IPv6 address in the CN or in the SAN, IPv4 address in the SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types].

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

- Without any administrator override mechanism
- except with the following administrator override: If the TSF fails to

determine the revocation status the TSF shall allow the administrator to provide override authorization to establish the connection on a per certificate basis.
].

FCS_TLSC_EXT.1.4 The TSF shall [selection: not present the Supported Groups Extension, present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] and no other curves/groups] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [selection:

- present the signature_algorithms extension with support for the following algorithms:
  [selection:
  - 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),
  - rsa_pss_pss with sha256(0x0809),
  - rsa_pss_pss with sha384(0x080a),
  - rsa_pss_pss with sha512(0x080b)
  -] and no other algorithms;
- present the signature_algorithms_cert extension with the following Signature Schemes:
  [selection:
  - 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),
- rsa_pss_pss with sha256(0x0809),
- rsa_pss_pss with sha384(0x080a),
- rsa_pss_pss with sha512(0x080b)
-] and no other SignatureSchemes

].

FCS_TLSC_EXT.1.6 The TSF [selection: provides, 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 [selection: not use PSKs, only use PSKs in TLS 1.3 session resumption with forward secrecy].

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

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_RBG_EXT.1 Random Bit Generation
- FCS_TLSC_EXT.1 TLS Client Protocol
- FIA_X509_EXT.1 X.509 Certificate Validation

- FIA_X509_EXT.2 X.509 Certificate Authentication

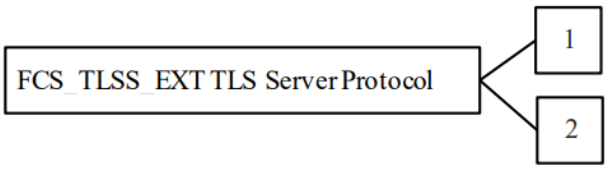
FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.2.2.3. FCS_TLSS_EXT TLS Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol. This is a new family defined for the FCS class.

Component Levelling



FCS_TLSS_EXT.1 TLS Server Protocol requires that the server side of TLS be implemented as specified.

Management: FCS_TLSS_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSS_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment
b. TLS session establishment
c. TLS session termination

FCS_TLSS_EXT.1 TLS Server Protocol
Hierarchical to: No other components
Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- 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_RBG_EXT.1 Random Bit Generation
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: 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:
[selection:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- 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_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- 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_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- 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_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
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [selection: RSA with key size [selection: 2048, 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using:

[selection:

- RSA key exchange with key size [selection: 2048, 3072, 4096] bits;
- EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves;
- Diffie-Hellman parameters [selection: of size 2048 bits, of size 3072 bits, of size 4096 bits, of size 6144 bits, of size 8192 bits, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]

].

FCS_TLSS_EXT.1.4 The TSF shall support [selection: no session resumption, session resumption based on session IDs according to RFC 5246 (TLS 1.2), session resumption based on session tickets according to RFC 5077 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)].

FCS_TLSS_EXT.1.5 The TSF [selection: provides, 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 [selection: not use PSKs, only use PSKs in TLS 1.3 session resumption with forward secrecy].

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

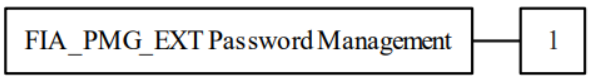
5.3. Identification and Authentication (FIA)

5.3.1. Password Management (FIA_PMG_EXT)

Family Behaviour

The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained. This is a new family defined for the FIA class.

Component Levelling



FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

There are no management functions foreseen.

Audit: FIA_PMG_EXT.1

There are no auditable events foreseen.

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components.

Dependencies: No other components

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

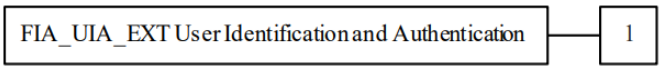
a. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: other characters]];
b. Minimum password length shall be configurable to between [assignment: minimum number of characters supported by the TOE] and [assignment: number of characters greater than or equal to 15] characters.

5.3.2. User Identification and Authentication (FIA_UIA_EXT)

Family Behaviour

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process. This is a new family defined for the FIA class.

Component Levelling



FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions.

Management: FIA_UIA_EXT.1

The following actions could be considered for the management functions in FMT:

a. Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. All use of the identification and authentication mechanism
b. Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1 User Identification and Authentication
Hierarchical to: No other components.
Dependencies: FTA_TAB.1 Default TOE Access Banners
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;
- [selection: no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]].

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 [selection: Web GUI password, SSH password, SSH public key, X.509 certificate, [assignment: other authentication mechanism]] and local authentication mechanisms [selection: none, password-based, [assignment: other authentication mechanism]].

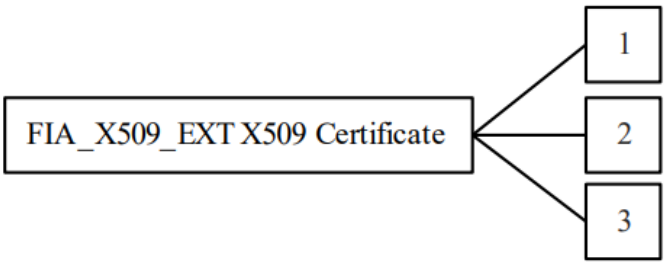
FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

5.3.3. Authentication using X.509 certificates (FIA_X509_EXT)

Family Behaviour

This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules, use of certificates for authentication for protocols and integrity verification, and the generation of certificate requests. This is a new family defined for the FIA class.

Component Levelling



FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification and potentially other functions that require certificates.

FIA_X509_EXT.3 X509 Certificate Requests, requires the TSF to be able to generate Certificate Request Messages and validate responses.

Management: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions could be considered for the management functions in FMT:

a. Remove imported X.509v3 certificates
b. Approve import and removal of X.509v3 certificates
c. Initiate certificate requests

Audit: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable functions foreseen.

FIA_X509_EXT.1 X.509 Certificate Validation

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation.
- 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 [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method].
- The TSF shall validate the extendedKeyUsage field according to the following rules: [assignment: rules that govern contents of the extendedKeyUsage field that need to be verified]

FIA_X509_EXT.1.2 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

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: DTLS, HTTPS, IPsec,SSH,TLS,no protocols], and [selection: code signing for system software updates [assignment: other uses], 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 [selection: allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate]

FIA_X509_EXT.3 X.509 Certificate Requests

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FIA_X509_EXT.1 X.509 Certificate Validation

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 [selection: 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.

5.4. Protection of the TSF (FPT)

5.4.1. Protection of TSF Data (FPT_SKP_EXT)

Family Behaviour

Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys. This is a new family modelled after the FPT_PTD Class.

Component Levelling

FPT_SKP_EXT Protection of TSF Data	1

FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

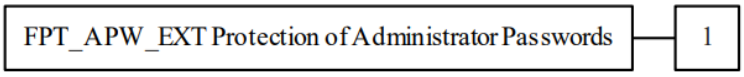
FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)
Hierarchical to: No other components.
Dependencies: No other components.
FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.4.2. Protection of Administrator Passwords (FPT_APW_EXT)

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure. This is a new family defined for the FPT class.

Component Levelling



FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management functions foreseen.

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

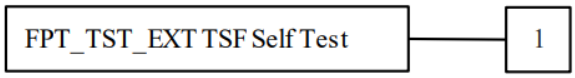
FPT_APW_EXT.1 Protection of Administrator Passwords
Hierarchical to: No other components
Dependencies: No other components.
FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.
FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.4.3. TSF Self-Test (FPT_TST_EXT)

Family Behaviour

Components in this family address the requirements for self-testing the TSF for selected correct operation. This is a new family defined for the FPT class.

Component Levelling



FPT_TST_EXT.1 TSF Self-Test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management functions foreseen.

Audit: FPT_TST_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Indication that TSF self-test was completed
b. Failure of self-test

FPT_TST_EXT.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No other components.

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 [selection: at no other time, on-demand, continuously, [assignment: conditions under which self-tests should occur]] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [selection: no other, start-up, on-demand, continuous, at the conditions [assignment: conditions under which self-tests should occur]] self-tests [assignment: 'list an identifier for each self-test that is additional to those identified in the first two bullet points'].

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [selection: all failures, [assignment: list of failures detected by self-tests]] by [selection: entering a maintenance mode, rebooting, [assignment: other methods to enter a secure state]].

5.4.4. Trusted Update (FPT_TUD_EXT)

Family Behaviour

Components in this family address the requirements for updating the TOE firmware and/or software. This is a new family defined for the FPT class.

Component Levelling

FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.
FPT_TUD_EXT.2 Trusted update based on certificates applies when using certificates as part of trusted update and requires that the update does not install if a certificate is invalid.

Management: FPT_TUD_EXT.1, FPT_TUD_EXT.2

The following actions could be considered for the management functions in FMT:

a. Ability to update the TOE and to verify the updates
b. Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1/SigGen) and [selection: no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]]
c. Ability to update the TOE, and to verify the updates using [selection: digital signature, no other mechanism] capability prior to installing those updates

Audit: FPT_TUD_EXT.1, FPT_TUD_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Initiation of the update process.
b. Any failure to verify the integrity of the update

FPT_TUD_EXT.1 Trusted Update
Hierarchical to: No other components
Dependencies: FCS_COP.1/SigGen Cryptographic operation (for Cryptographic Signature and Verification), or FCS_COP.1/Hash Cryptographic operation (for cryptographic hashing)
FPT_TUD_EXT.1.1 The TSF shall provide [assignment: Administrators] the ability to query the currently executing version of the TOE firmware/software and

[selection: the most recently installed version of the TOE firmware/software; no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: Administrators] the ability to manually initiate updates to TOE firmware/software and [selection: support automatic checking for updates, support automatic updates, no other update mechanism].

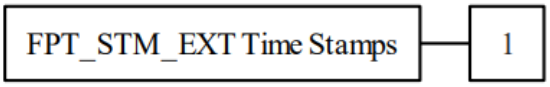
FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: X.509 certificate, digital signature] prior to installing those updates.

5.4.5. Time stamps (FPT_STM_EXT)

Family Behaviour

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps. This is a new family defined for the FPT class.

Component Levelling



FPT_STM_EXT.1 Reliable Time Stamps is hierarchic to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM_EXT.1

The following actions could be considered for the management functions in FMT:

a. Management of the time
b. Administrator setting of the time.

Audit: FPT_STM_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Discontinuous changes to the time.

FPT_STM_EXT.1 Reliable Time Stamps
Hierarchical to: No other components
Dependencies: No other components.

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 [selection: allow the Security Administrator to set the time, synchronise time with an NTP server, obtain time from the underlying virtualization system].

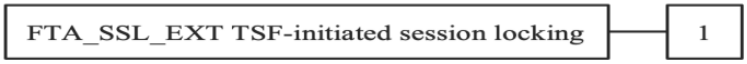
5.5. TOE Access (FTA)

5.5.1. TSF-initiated Session Locking (FTA_SSL_EXT)

Family Behaviour

Components in this family address the requirements for TSF-initiated and userinitiated locking, unlocking, and termination of interactive sessions. The extended FTA_SSL_EXT family is based on the FTA_SSL family.

Component Levelling



FTA_SSL_EXT.1 TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity. It is the only component of this family.

Management: FTA_SSL_EXT.1

The following actions could be considered for the management functions in FMT:

a. Specification of the time of user inactivity after which lock-out occurs for an individual user.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1 TSF-initiated Session Locking

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator reauthenticate to the TSF prior to unlocking the session;
- terminate the session]

after a Security Administrator-specified time period of inactivity.

6. Security Requirements

This section describes the security requirements.

6.1. Conventions

The conventions used to describe security functional requirements are as follows:

- The part assigned, selected or refined in the NDcPP: Indicated in **bold**.
- The part assigned or selected in this ST: Indicated in *italics*.
- Iteration: Indicated by adding a string beginning with "/".

Note that text within [ ] indicates the result of an assignment or selection.

Extended SFRs are identified by appending the label "EXT" to the end of the SFR name.

6.2. Security Functional Requirements

Describes the security functional requirements provided by the TOE.

The following components are included in CC Part 2.

Table 8 Security functional requirements provided by the TOE

Functional Requirements	Title
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG.1	Protected Audit Trail Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/Data Encryption	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)
FIA_AFL.1	Authentication Failure Management
FIA_UAU.7	Protected Authentication Feedback
FMT_MOF.1/ManualUpdate	Management of Security Functions Behavior
FMT_MOF.1/Functions	Management of Security Functions Behavior
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
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

The following components are extensions of CC Part 2.

Table 9 Extended Security Functional Requirements Provided by the TOE

FAU_STG_EXT.1	Protected Audit Event Storage
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSS_EXT.1	TLS Server Protocol
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
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
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric, and private 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

6.2.1. 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 Table 10.**]

Table 10 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG.1	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_TLSC_EXT.2	None	None
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login	Origin of the attempt (e.g.,

	attempts limit is met or exceeded.	IP address).
FIA_PMG_EXT.1	None	None
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 Administrator actuated	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).

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_SSL_EXT.1	The termination of a local session by the session lock	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 Table 10.**]

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.1 Protected Audit Trail Storage

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

unauthorized deletion.

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

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 [*250000 records*].

FAU_STG_EXT.1.5 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.

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

6.2.2. 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-bit, 3072bit, 4096bit*] *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 cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard*

(DSS)", Appendix B.1;

- *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 7919*].

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

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";*
- *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 7919*].

] ~~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** [*single overwrite consisting of zeros*] **;**
- **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**

[

- *logically addresses the storage location of the key and performs a* [*single*] *overwrite consisting of* [*a new value of 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** [*CTR, GCM*] **mode**] and cryptographic key sizes [*128 bits, 256 bits*] that meet the following: [**AES as specified in ISO 18033-3,** [*CTR as specified in ISO 10116, 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, 3072bits, 4096bits],*
- *For ECDSA: [256 bits, 384bits, 521bits]*

]

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*

]

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, 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**].

FCS_COP.1/KeydHash 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 [*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 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 [*CTR_DRBG (AES)*].

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

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*

]

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [*the IPv4 address in the SAN, IPv6 address in the SAN*].

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, ffdhe3072, ffdhe4096*] *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),*
- *rsa_pss_pss with sha256(0x0809),*
- *rsa_pss_pss with sha384(0x080a),*
- *rsa_pss_pss with sha512(0x080b)*
-] and no other algorithms;

]

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 [*reject* [*TLS 1.2, TLS 1.3*] *renegotiation attempts*].

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.

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_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_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [*RSA with key size* [*2048, 3072, 4096*] *bits; ECDSA over NIST curves* [*secp256r1, secp384r1, secp521r1*] *and no other curves*].

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

- *EC Diffie-Hellman key agreement over NIST curves* [*secp256r1, secp384r1, secp521r1*] *and no other curves;*
- *Diffie-Hellman parameters* [*of size 2048 bits, ffdhe3072, ffdhe4096*]

].

FCS_TLSS_EXT.1.4 The TSF shall support [*session resumption based on session tickets according to RFC 5077 (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 [*only use PSKs in TLS 1.3 session resumption with forward secrecy*].

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*].

6.2.3. 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** [*1-999*]] 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:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*"!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("、")"、" "、"'"、"+"、","、"-"、"."、"/"、":"、";"、"<"、"="、">"、"?"、"["、"¥"、"]"、"_"、"`"、"{"、"|"、"}"、"~"*];
- Minimum password length shall be [**configurable to between** [*6*] **and** [*63*] **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;
- [*ICMP echo, REST API(GET /configuration/version, GET /v1/objects/storages)*].

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,*[*REST API password*]] and 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.

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, 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 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.**
  - **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 [*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 [*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 [*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.

6.2.4. 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 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 configure the reference identifier for the peer;*
- *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.

6.2.5. 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*] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [*no other*] self-tests

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [*all failures*] *by* [*rebooting*].

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*].

6.2.6. TOE Access (FTA)

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_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [*terminate the session*] after a Security Administrator-specified time period of inactivity.

FTA_TAB.1 Default TOE Access Banners

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 ~~unauthorised~~ use of the TOE.

6.2.7. 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,** [*no other capabilities*] 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 TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*audit server*].

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**].

6.3. Security Assurance Requirements

The TOE security assurance requirements are shown in Table11.

Table 11 Security Assurance Requirements

Assurance Class	Assurance Component
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparatory procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labelling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability survey (AVA_VAN.1)

6.4. Security Functional Requirements Rationale

The results of the dependency analysis for the TOE security functional requirements in this ST are shown in Table12.

Table 12 Security Functional Requirements Rationale

TOE Security Functional Requirements	Required Dependencies	Dependencies Met by the ST	Dependencies not met by the ST
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1 (This is an extension of the item on the left, and the provision of a trusted timestamp is	None

		included in the requirements)	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UIA_EXT.1 (The timing of user identification is included in the requirements)	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	None
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	FCS_CKM.2, FCS_CKM.4	None
FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	None
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1	None
FCS_COP.1/ DataEncryption	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.4	FCS_CKM.1 (During TLS communication, the key used for data encryption/decryption is not an asymmetric key compliant with FCS_CKM.1 , but rather a symmetric key established via key exchange compliant with FCS_CKM.2; therefore, use

			FCS_CKM.2 instead of FCS_CKM.1 to resolve the dependency.)
FCS_COP.1/SigGen	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	None
FCS_COP.1/Hash	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	None (Since this SFR specifies keyless hash operations, key initialization and destruction are not relevant.)	None
FCS_COP.1/ KeyedHash	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.4	FCS_CKM.1 (Since the key used for HMAC is not an asymmetric key compliant with FCS_CKM.1, but rather a symmetric key established via key establishment compliant with FCS_CKM.2, use FCS_CKM.2 instead of FCS_CKM.1 to resolve the dependency.)
FCS_HTTPS_EXT.1	FCS_TLSC_EXT.1 or FCS_TLSS_EXT.1	FCS_TLSS_EXT.1	None
FCS_RBG_EXT.1	None	None	None

FCS_TLSC_EXT.1	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/ DataEncryption, FCS_COP.1/ SigGen, FCS_COP.1/Hash, FCS_COP.1/ KeyedHash, FCS_RBG_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/ DataEncryption, FCS_COP.1/ SigGen, FCS_COP.1/Hash, FCS_COP.1/ KeyedHash, FCS_RBG_EXT.1, FIA_X509_EXT.1/R ev, FIA_X509_EXT.2	None
FCS_TLSC_EXT.2	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/DataE ncryption, FCS_COP.1/SigGe n, FCS_COP.1/Hash, FCS_COP.1/Keyed Hash, FCS_RBG_EXT.1, FCS_TLSC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/DataE ncryption, FCS_COP.1/SigGe n, FCS_COP.1/Hash, FCS_COP.1/Keyed Hash, FCS_RBG_EXT.1, FCS_TLSC_EXT.1, FIA_X509_EXT.1/R ev, FIA_X509_EXT.2, FIA_X509_EXT.3	None
FCS_TLSS_EXT.1	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/ DataEncryption, FCS_COP.1/	FCS_CKM.1, FCS_CKM.2, FCS_COP.1/ DataEncryption, FCS_COP.1/	None

	SigGen, FCS_COP.1/Hash, FCS_COP.1/ KeyedHash, FCS_RBG_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2	SigGen, FCS_COP.1/Hash, FCS_COP.1/ KeyedHash, FCS_RBG_EXT.1, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2	
FIA_AFL.1	FIA_UAU.1	FIA_UIA_EXT.1 (The timing of user authentication is included in the requirements)	None
FIA_PMG_EXT.1	None	None	None
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1	None
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1 (The user authentication timing required by the requirement is included in the requirement)	None
FIA_X509_EXT.1/Rev	FIA_X509_EXT.2	FIA_X509_EXT.2	None
FIA_X509_EXT.2	FIA_X509_EXT.1	FIA_X509_EXT.1/Rev	None
FIA_X509_EXT.3	FCS_CKM.1, FIA_X509_EXT.1	FCS_CKM.1, FIA_X509_EXT.1/Rev	None
FMT_MOF.1/ ManualUpdate	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (This is a hierarchically higher than the one listed on the left, and maintaining the security roles	None

		specified in the requirements is included in the requirements), FMT_SMF.1	
FMT_MOF.1/ Functions	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (This is a hierarchically higher than the one listed on the left, and maintaining the security roles specified in the requirements is included in the requirements), FMT_SMF.1	None
FMT_MTD.1/ CoreData	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (This is a hierarchically higher than the one listed on the left, and maintaining the security roles specified in the requirements is included in the requirements), FMT_SMF.1	None
FMT_MTD.1/ CryptoKeys	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (This is a hierarchically higher than the one listed on the left, and maintaining the security roles	None

		specified in the requirements is included in the requirements), FMT_SMF.1	
FMT_SMF.1	None	None	None
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1 (The timing of user identification is included in the requirements)	None
FPT_SKP_EXT.1	None	None	None
FPT_APW_EXT.1	None	None	None
FPT_TST_EXT.1	None	None	None
FPT_TUD_EXT.1	FCS_COP.1/ SigGen or FCS_COP.1/Hash	FCS_COP.1/ SigGen, FCS_COP.1/Hash	None
FPT_STM_EXT.1	None	None	None
FTA_SSL.3	None	None	None
FTA_SSL.4	None	None	None
FTA_SSL_EXT.1	FIA_UAU.1	FIA_UIA_EXT.1 (The timing of user authentication, which is a requirement, is included in the requirements)	None
FTA_TAB.1	None	None	None
FTP_ITC.1	None	None	None
FTP_TRP.1/Admin	None	None	None

7. TOE Summary Specifications

7.1. Security Audit (FAU)

7.1.1. FAU_GEN.1

The audit functions of the TOE are shown in Table13 and Table14.

The audit logs acquired by the TOE consist of basic information and detailed information that varies depending on the operation of each audited function. Note that in the TOE implementation for FAU_STG_EXT.1, since there is no configuration function for locally stored audit logs, audit records related to FAU_STG_EXT.1 are not generated by the TOE.

Table 13 Basic Information for Audit Logs

#	Item	Content
1	Version Number	Outputs the model name or the version number of the output format
2	Date	Outputs the date on which the event occurred.
3	Time	Outputs the time on which the event occurred.
4	Time Zone	Outputs the time difference from GMT (Greenwich Mean Time).
5	External Interface Name	Outputs information identifying through which external interface the operation that generated the event was performed.
6	User ID	Outputs the user ID used to identify the TOE user.
7	Function Name	Outputs a string indicating the name of the function that performed the configuration operation.
8	Operation Name or Event Name	Outputs the abbreviated name of the operation for each function.
9	Parameters	Outputs the parameters of the executed configuration operation.
10	Operation Result	Outputs the result of the operation.
11	Source Host Identification Information	Outputs the IP address of the local/remote management PC.
12	Log entry serial number	Outputs the serial number of the stored log information.

Table 14 Specific Audit Items for Each Functional Requirement

#	Functional	Audit Item	Function	Operation	Additional

	Requirement		Name	Name or Event Name	Information to Be Collected
1	FAU_GEN.1	Start-up of the audit functions	Maintenance	Power On Storage	-
		Shut-down of the audit functions	Maintenance	Power Off Storage	-
		Administrator Login	BASE	Login	-Table13 #11 Sender Host Identification Information
		Administrator Logout	BASE	Logout	-Table13 #11 Sender Host Identification Information
		Changes to TSF data related to configuration changes	For changes to TSF data, refer to the following item numbers #7, #9, #11		
		Create or Delete of RSA and ECDSA keys	BASE	Certificate Setting	Identification information for created/deleted private keys
		Audit Log Server Configuration -Enable/Disable transmission to the audit log server -Apply or Remove client certificates for the audit log server (including certificate chains such as root certificates+intermediate	AuditLog	Set Up Syslog Server	-Identification information for applied/removed certificates -Reason for certificate validation failure

		certificates+client certificates) -Apply or Remove the root certificate that signed the audit log server certificate			
		Apply or remove Web Server Certificates (Including certificate chains such as root certificates+intermediate certificates+server certificates)	Maintenance	Update Cert Files	-Identification information for applied/deleted certificates -Reason for certificate validation failure
		Password Reset (change of another user's password by a Security Administrator (View & Modify)	Maintenance	Edit User	Target User ID
2	FCS_HTTPS_EXT.1	Communication failure with the management PC using HTTPS	BASE	TLS Connection Establishment	-Reason for communication failure -Identification information of the communication source
3	FCS_TLSC_EXT.1	Communication failure with the audit log server using the TOE's TLS client function	BASE	TLS Connection Establishment	-Reason for communication failure -Identification information of the audit log server

4	FCS_TLSS_EXT.1	Communication failure with the management PC using the TOE's TLS server function	See #2		
5	FIA_AFL.1	Reached the limit for failed login attempts	BASE	Login	- "Lockout = yes" is recorded for login attempts by locked-out users. - Table13 #11 Source host identification information
6	FIA_UIA_EXT.1	Login attempts via Web GUI or REST API	See the administrator's login in #1		
7	FIA_X509_EXT.1/ Rev	Certificate verification failure during TLS communication	BASE	TLS Connection Establishment	Reason for certificate verification failure
		Audit Log Server Configuration -Apply or remove the audit log server's client certificate (including the certificate chain such as the root certificate+intermediate certificate+client certificate) -Apply or remove the root certificate that signed the audit log	See Audit Log Server Configuration in #1		

		server certificate -Certificate validation failure when applying the client certificate and root certificate for the audit log server			
		Web Server Certificate Configuration -Apply or remove Web server certificates (Including certificate chains such as root certificates+intermediate certificates+server certificates) -Certificate validation failure when applying a web server certificate	See "Apply or Remove Web Server Certificates" in #1		
8	FMT_MOF.1/ ManualUpdate	Start manual update	Maintenance	Update Firmware	-
9	FMT_SMF.1	Configuration of Messages Displayed on the Access Banner	Maintenance	Edit Login Message	-
		Configuring the Inactivity Timeout for Remote/Local Administrator Sessions (Web Interface)	Maintenance	Edit Session Management Information	-
		Account Policy Settings	Maintenance	Set Up PolicyEmail	-Number of authentication

		-Setting the number of failed authentication attempts -Setting the time interval before re-authentication is allowed after a failed login -Setting the minimum password length for the administrator password			failures -Set lockout duration -Minimum character count for administrator passwords
		Create or Delete CSR and RSA/ECDSA Keys	See "Create or Delete of RSA and ECDSA Keys" in #1		
		Audit log server configuration -Application or remove of the root certificate that signed the audit log server's client certificate and server certificate (including the certificate chain) -Certificate validation failure when applying the root certificate that signed the audit log server's client and server certificates	See "Audit Log Server Configuration" in #1		
		Web Server Certificate Configuration	See "Apply or Remove Web Server Certificates" in #1		

		-Apply or remove Web server certificates (Including certificate chains such as root certificates+intermediate certificates+server certificates) -Certificate validation failure when applying a web server certificate			
		Creating a User Group Associated with a Role	Maintenance	Create UserGroup	-User group ID -Role Type
		Creating a User (Setting User ID and Password, Associating with a User Group)	Maintenance	Create User	-
		Password Change (Security administrator (View & Modify) changing other users' passwords)	See Password Reset in #1		
		Administrator Changing Their Own Password	Maintenance	Edit User Password	-
10	FPT_TUD_EXT.1	Start Update Update Attempt Successful	Maintenance	Update Firmware	- Table13 #10 "Normal end" is recorded as the result of the operation.

		Update attempt failed	Maintenance	FcWizard	- Table13 #10 "Error" is recorded as the result of the operation.
11	FPT_STM_EXT.1	Changing the date and time	Maintenance	Set Up Date & Time	Date and Time Before and After Change
12	FTA_SSL.3	Termination of Remote Session by TSF	BASE	Logout	-Table13 #11 Source host identification information is blank -If a user whose session has timed out is connected remotely, "Session Type=Remote Session" is recorded.
13	FTA_SSL.4	Session termination by administrator	See Administrator Logout in #1		
14	FTA_SSL_EXT.1	Termination of local session by TSF	BASE	Logout	-Table13 #11 Source host identification information is blank -If a user whose session has timed out is a local connection, "Session

					Type=Local Session" is recorded.
15	FTP_ITC.1	Initiation of trusted channel	BASE	TLS Connection Establishment	-Identification information of the destination audit log server
		Failure to establish a trusted channel	See #3		
		Termination of trusted channel	BASE	TLS Connection Termination	-Identification information of the destination audit log server
16	FTP_TRP.1/ Admin	Initiation of trusted path	BASE	TLS Connection Establishment	-Identification information of the communicating party
		Failure to establish a trusted path	See #2		
		Termination of trusted path	BASE	TLS Connection Termination	-Identification information of the communicating party

7.1.2. FAU_GEN.2

As shown in Table13, the TOE assigns the user ID of the administrator account that caused each audited event to the audit record it generates.

7.1.3. FAU_STG.1

The TOE does not provide an interface for modifying or deleting audit records.

In addition, the amount of audit records stored internally by the TOE is described in 7.1.4 FAU_STG_EXT.1.

Locally stored audit logs are stored permanently.

7.1.4. FAU_STG_EXT.1

The TOE has the following audit functions.

- The TOE transmits audit records to an external audit log server in real time using a secure channel encrypted via TLS communication, as described in FTP_ITC.1. The Syslog protocol is used for transmission to the external audit log server. Each time the TOE generates an audit record, it stores it internally and simultaneously sends it to the registered audit log server. Note that up to two audit log servers can be registered with the TOE. If two audit log servers are registered, the TOE sends audit records to both servers.
- Audit records are stored internally for a maximum of 250,000 lines. When the maximum number of lines is reached, the system returns to the first line of the log and overwrites it with new information, thereby deleting the oldest entries (wrap-around method).
- The TOE consists of a single standalone component that stores audit records locally.
- The TOE provides a function to download audit records to the management PC in case the transmission of audit records to the audit log server fails due to network problems or other issues. The TOE allows only the Audit Log Administrator (View & Modify) to use this audit log download function.
- The TOE does not provide users with an interface to edit or delete audit records.
- The TOE local log is in log file format and is stored in non-volatile memory.

7.2. Cryptographic Support (FCS)

7.2.1. FCS_CKM.1

The TOE supports the asymmetric key generation schemes shown in Table15.

Table 15 TOE Key Generation Specifications

Key Generati	Key Size	SFR	Service	Remarks

on Scheme				
RSA	2048 bits, 3072 bits, 4096 bits	FCS_COP.1 /SingGen	Used for RSA signature generation/verification during TLS communication	Compliant with FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3
FFC	2048 bits	FCS_CKM.2	For DH key exchange during TLS communication	Compliant with FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1
FFC (safe-prime)	3072 bits, 4096 bits	FCS_CKM.2	For DH key exchange during TLS communication	Compliant with NIST Special Publication 800-56A Revision 3 and RFC 7919
ECC	256 bits, 384 bits, 521 bits (P-256/P-384/P-521)	FCS_CKM.2	For ECDH key exchange during TLS communication	Compliant with FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
	256 bits, 384 bits, 521 bits (P-256/P-384/P-521)	FCS_COP.1 /SingGen	For ECDSA signature generation/verification during TLS communication	

7.2.2. FCS_CKM.2

The TOE supports the key establishment schemes shown below.

Table 16 TOE Key Establishment Specifications

Key Establishment Scheme	SFR	Service

DH (FIPS 186-Type)	Compliant with NIST Special Publication 800-56A Revision 3	FCS_TLSS_EXT.1	Management PC Communication
DH (safe-prime)	Compliant with NIST Special Publication 800-56A Revision 3 and RFC 7919	FCS_TLSC_EXT.1	Audit Log Server Communication
		FCS_TLSS_EXT.1	Management PC communication
ECDH	Compliant with NIST Special Publication 800-56A Revision 3	FCS_TLSC_EXT.1	Audit Log Server Communication
		FCS_TLSS_EXT.1	Management PC communication

7.2.3. FCS_CKM.4

The TOE supports the following key destruction methods.

Table 17 Key Destruction Specifications for the TOE

Key Type	Key Generator	Storage Location	Reason for Destruction	Destruction Method
TLS session key	DRBG of FCS_RBG_EXT.1	RAM	End of TLS session	Single overwrite of 0 data
TLS ECDH private key	DRBG of FCS_RBG_EXT.1	RAM	End of TLS session	Single overwrite of 0 data
TLS DH private key	DRBG of FCS_RBG_EXT.1	RAM	End of TLS session	Single overwrite of 0 data
Client's private key	DRBG of FCS_RBG_EXT.1	RAM	End of TLS session	Single overwrite of 0 data
		SSD	Administrator updates the private key	single overwrite of new key
Web server private	DRBG of FCS_RBG_EXT.1	RAM	Termination of TLS session	Single overwrite of 0 data

key		SSD	Administrator updates the private key	single overwrite of new key

The TOE client private key or web server private key is a private key generated by a Security Administrator (View & Modify) using the TOE's private key generation function. The generated private key is stored on the SSD. The target private key becomes available for communication with the audit log server or the management PC by uploading a client certificate or web server certificate—which contains a corresponding public key to the TOE.
Keys stored in the volatile area are deleted by overwriting them once with zero data using OpenSSL's OPENSSL_cleanse(). Keys in the volatile area are always discarded upon termination of the TLS session; there are no configurations or conditions that cause key disposal to fail or be delayed.
When a Security Administrator (View & Modify) creates a new key using the Web GUI, the TOE deletes the old key by overwriting the old key file's path (logical address) with the new key information once using the fwrite function. The deletion operation will fail if attempted while other operations are in progress, but it can be successfully executed if retried after those operations have completed. Furthermore, if the address changes due to wear leveling when overwriting the key file with the new key value, the deletion of the key is delayed until garbage collection occurs.

7.2.4. FCS_COP.1/DataEncryption

The TOE provides symmetric encryption and decryption functions using 128-bit and 256-bit AES (compliant with ISO 18033-3) in each mode shown in the table.
The key lengths and uses for each CTR and GCM mode are shown in Table18.

Table 18 Key Length and Intended Use for Each Mode

Mode		Key Length	Usage
CTR	Compliant with ISO 10116	256 bits	Random bit generation
GCM	Compliant with ISO 19772	128 bits 256 bits	Encrypted communication using HTTPS/TLS

7.2.5. FCS_COP.1/SigGen

The TOE provides signature generation/verification services using cryptographic algorithms with the following key lengths.

a) RSA algorithm (compliant with FIPS PUB 186-4 Section 5.5 and ISO/IEC 9796-2)
   - Key sizes: 2048 bits, 3072 bits, 4096 bits

b) ECDSA algorithm (compliant with FIPS PUB 186-4 Section 6, Appendix D NIST Curves [P-256, P-384, P-521] and ISO/IEC 14888-3 Section 6.4)
   - Key sizes: 256 bits, 384 bits, 521 bits

The TOE provides RSA and ECDSA signature generation/verification services for the following purposes.
- Communication using the TLS protocol with external entities (when the TOE acts as a client or as a server)
- Self-test
- Verification of TOE update files

The cryptographic algorithms used for signature generation/verification services for each use case are shown below.

Table 19 Supported Cryptographic Algorithms for Signature Generation/Verification Services

Service	TOE (Server)'s TLS Protocol	TOE (Client)'s TLS Protocol	Self-Test	TOE Update File Verification
Signature Generation Service	RSA: 2048, 3072, 4096 bits ECDSA: 256, 384, 521 bits	RSA: 2048, 3072, 4096 bits ECDSA: 256, 384, 521 bits	-	-
Signature Verification Service	-	RSA: 2048, 3072, 4096 bits ECDSA: 256, 384, 521 bits	RSA: 4096 bits	RSA: 4096 bits

7.2.6. FCS_COP.1/Hash

The TOE provides cryptographic hashing services using SHA-256, SHA-384, and SHA-512, which comply with ISO/IEC 10118-3:2004.

The TOE's hash functions are used in the following cryptographic functions.

Table 20 Relationship between Hash Functions and Other Cryptographic functions

Hash Function	Message Digest Size	Cryptographic function	Usage
SHA-256	256 bits	HMAC function	Hashing messages using HMAC in TLS communication

		RSA Signature generation/Signature Verification	Hashing during digital signature verification for TLS communication, self-tests, and update file verification of TOE.
			Hashing performed during signing and verification of public keys used in DH/ECDH key exchange in TLS communication
		ECDSA Signature generation/Signature Verification	Hashing during digital signature verification in TLS communication
			Hashing during signature generation and verification of public keys used in DH/ECDH key exchange in TLS communication
SHA-384	384 bits	HMAC function	Hashing messages using HMAC in TLS communication
		RSA Signature generation/Signature Verification	Hashing during digital signature verification in TLS communication
			Hashing performed during signing and verification of public keys used in DH/ECDH key exchange in TLS communication
		ECDSA Signature generation/Signature	Hashing during digital signature verification in

		Verification	TLS communication
			Hashing performed during signing and verification of public keys used in DH/ECDH key exchange in TLS communication
SHA-512	512 bits	RSA Signature generation/Signature Verification	Hashing during digital signature verification in TLS communication
			Hashing performed during signing and verification of public keys used in DH/ECDH key exchange in TLS communication
		ECDSA Signature generation/Signature Verification	Hashing during digital signature verification in TLS communication
			Hashing performed during signing and verification of public keys used in DH/ECDH key exchange in TLS communication
		Password Hash	Hashing administrator password

7.2.7. FCS_COP.1/KeyedHash

TOE provides a keyed hash message authentication service using HMAC-SHA-256 and HMAC-SHA-384, which comply with ISO/IEC 10118-3:2004. HMAC is implemented in the TLS protocol. Table 21 shows the HMACs used by the TOE.

Table 21 HMAC specification of TOE

Algorithm	Hash function	Key length	Block size	MAC length used

HMAC-SHA-256	SHA-256	256 bits	512 bits	256 bits
HMAC-SHA-384	SHA-384	384 bits	1024 bits	384 bits

7.2.8. FCS_HTTPS_EXT.1

The TOE's web interface is accessed via an HTTPS connection using the TLS implementation described in FCS_TLSS_EXT.1. The TOE provides HTTPS services only in server mode and does not use HTTPS in client mode.

The TOE's web server provides HTTPS protocol communication in accordance with RFC 2818. The details of compliance with RFC 2818 are shown below.

Table 22 TOE HTTPS Implementation

Requirements	TOE Implementation Details
Connection Initiation	All HTTPS data is transmitted as "application data."
Connection Closure	Exchange an "alert close notify" with the client before closing the TLS connection. Note that TOE supports session resumption.
Server Behavior	The TOE sends an "alert close notify" when closing the TLS connection.
Port Number	TOE accepts HTTPS connections on port 443.
URI Format	You can connect to the TOE web server using URIs in the "https" format.
Endpoint Identification	The TOE provides a web server as an HTTPS server. The TOE's web server does not support TLS mutual authentication.

7.2.9. FCS_RBG_EXT.1

To generate 256-bits random numbers using a CTR_DRBG (AES 256) compliant with ISO/IEC 18031:2011, the TOE requires 256 bits of entropy plus 128 bits for the nonce (half the security strength), for a total of 384 bits of entropy. The TOE's DRBG uses the LS1046A, a CPU from NXP Semiconductors, as an entropy source and obtains a 384-bits seed from the entropy source . The output of the LS1046A is full entropy[1], and the 384-bits seed contains at least 384 bits of entropy.

[1] Full entropy refers to data that contains the maximum possible amount of information, where each bit cannot be predicted from any other bit.

7.2.10. FCS_TLSC_EXT.1

TOE uses the TLS client function to communicate with the audit log server.
The TLS client supports only TLS protocol versions 1.2 (RFC 5246) and 1.3 (RFC 8446).
However, it does not support renegotiation.
The TOE supports only the cipher suites listed below and does not have the capability to change the cipher suite used for communication. Furthermore, it does not use a PSK for key exchange.

Table 23 Cipher Suites Supported by Client Functions

#	Cipher Suite
1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
5	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
6	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
7	TLS_AES_128_GCM_SHA256
8	TLS_AES_256_GCM_SHA384

The TOE supports the signature algorithms listed below.
TOE does not have a configuration function to change the signature algorithm.

Table 24 Supported Signature Algorithms

#	Signature Algorithm	Key Length
1	RSA	2048-bits
2		3072-bits
3		4096-bits
4	ECDSA	256-bits
5		384-bits
6		521-bits

The TOE's signature_algorithms extension supports the algorithms listed below and does not use any algorithms other than those listed.
Note that the TOE does not have the capability to change the signature algorithm settings.

Table 25 Algorithms supported by the signature_algorithms extension

#	TLS Protocol Version	Algorithm
1	1.2	*rsa_pkcs1 with sha256(0x0401)*
2		*rsa_pkcs1 with sha384(0x0501)*
3		*rsa_pkcs1 with sha512(0x0601)*
4	1.2/1.3	*ecdsa_secp256r1 with sha256(0x0403)*
5		*ecdsa_secp384r1 with sha384(0x0503)*
6		*ecdsa_secp521r1 with sha512(0x0603)*
7		*rsa_pss_rsae with sha256(0x0804)*
8		*rsa_pss_rsae with sha384(0x0805)*
9		*rsa_pss_rsae with sha512(0x0806)*
10	1.3	*rsa_pss_pss with sha256(0x0809)*
11		*rsa_pss_pss with sha384(0x080a)*
12		*rsa_pss_pss with sha512(0x080b)*

TOE supports the TLS extensions listed below and does not use other TLS extensions such as the Early data extension and Post-handshake client authentication defined in Section 4.2.6 of RFC 8446.

Table 26 Supported TLS Extensions

#	TLS Protocol Version	TLS Extensions
1	1.2	signature_algorithms
2		supported_groups
3	1.3	signature_algorithms
4		supported_versions
5		supported_groups
6		key_share

The TOE performs certificate validation when communicating with the audit log server. For details on certificate validation, refer to Table30Validation Details and Target Certificates During the TLS Handshake. If the TOE fails to validate a certificate, there is no room for administrator intervention regarding whether to establish a secure connection, and the TOE will not establish a secure connection.

The TOE supports SAN (Subject Alternative Name) as a reference identifier. Reference

identifiers can be configured via the Web GUI when the Audit Log Administrator (View & Modify) sets up the audit log server, or they can be configured using IP addresses when setting up individual servers. However, when configuring IP addresses, it is not possible to specify IP address ranges or IP addresses that include subnet masks. Note that when the Audit Log Administrator (View & Modify) or Security Administrator (View & Modify) configures a server or creates a certificate, the TOE does not enforce compliance with RFC 5952 or RFC 3986 for the input.
When the TOE receives a server certificate from a server, it first checks whether a SAN value exists within the certificate. If a SAN value is present, it verifies whether that value matches the reference identifier configured by the Security Administrator (View & Modify). If the SAN value in the certificate does not match the reference identifier configured by the Security Administrator (View & Modify), the verification fails. Verification also fails if no SAN value exists in the certificate, and communication with the server will not occur.
When an IP address is specified as the reference identifier, the TOE converts the IP address configured by the Security Administrator (View & Modify) from text format to network byte-order binary format and compares it with the SAN value. Both IPv4 and IPv6 addresses are supported.
Additionally, TOE supports the elliptic curves secp256r1, secp384r1, and secp521r1, as well as the FFDH group extensions ffdhe3072 and ffdhe4096, and presents the supported elliptic curves and group extension algorithms in the Client Hello message without requiring configuration by an administrator. If the server on the other end does not support the Supported Groups Extension supported by TOE, TOE will fail to communicate with that server. Note that in the case of TLS 1.2, TOE will establish a session using DHE2048 or ffdhe3072 in the Server Key Exchange sent by the server, but if any other DHE parameters are specified, TOE will terminate the connection.
The identifier configured by the Audit Log Administrator (View & Modify) is set in the following section of the audit log server configuration screen.

- Audit Log Server Settings Screen
  - Host Name / IP Address field

7.2.11. FCS_TLSC_EXT.2

The TOE performs mutual authentication when communicating with the audit log server. During the TLS handshake with the audit log server, the TOE sends an X.509v3 client certificate to the audit log server. The audit log server verifies the TOE's client certificate and performs authentication.
To configure the TLS communication environment with the audit log server, TOE users must

create a client certificate that meets the following requirements and upload it to TOE after performing the following steps.

1. The Security Administrator (View & Modify) creates a private key+CSR on the TOE and downloads the CSR
2. The downloaded CSR is handed over to the Audit Log Administrator (View & Modify), who has it signed by a trusted CA
3. The Audit Log Administrator (View & Modify) uploads the signed certificate

To do this, the TOE user generates a key pair and CSR on the TOE, has them signed by a separate CA, and uploads the issued client certificate to the TOE.

- If an intermediate certificate exists, prepare a signed public key certificate consisting of a certificate chain that includes the intermediate certificate.
- The certificate chain hierarchy of the client certificate to be uploaded must be 20 levels or less, including the root CA certificate.
- The public key cryptosystem of the client certificate to be uploaded must be RSA or ECDSA.
- Ensure that the Common Name and Subject Alternative Name fields in the client certificate are set to the ESM's IP address.

7.2.12. FCS_TLSS_EXT.1

The TOE uses the TLS server function for communication with the management PC.
The TLS server permits only TLS protocol versions 1.2 (RFC 5246) and 1.3 (RFC 8446). It also supports renegotiation.
The TOE supports only the cipher suites listed below.

Table 27 Cipher suites supported by the server function

#	Cipher Suite
1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
5	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
6	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
7	TLS_AES_128_GCM_SHA256
8	TLS_AES_256_GCM_SHA384

During the TLS handshake, TOE checks the protocol version and cipher suite specified by the client and refuses communication if an older SSL version (SSL 1.0, SSL 2.0, SSL 3.0) or

an older TLS version (TLS 1.0, TLS 1.1) is specified. TOE does not support session resumption using session IDs (RFC 5246) in TLS 1.2. However, TOE supports session resumption using session tickets (RFC 5077) in TLS 1.2 and session resumption using session tickets (RFC 8446) in TLS 1.3. Session tickets are encrypted using AES-256-GCM.TOE uses a PSK and DHE key exchange to maintain forward secrecy during session resumption in TLS 1.3 communications. For example, communications using a different channel or a manually configured PSK are not permitted. The TOE supports the structure specified in Section 4 of RFC 5077. When a client specifies an established session, the TOE checks the expiration time of the target session and requests a full handshake if it has expired. Note that the TOE maintains an independent session cache for each context, and a session established in one context cannot be resumed in another context.

TOE includes the "renegotiation_info" extension in the TLS 1.2 Server Hello, in accordance with RFC 5746.

The TOE supports cipher suites that include DHE and ECDHE. However, the cipher suite cannot be reconfigured. Upon receiving a supported group extension from the peer, the TOE prioritizes and uses the key exchange algorithm with the highest security strength based on the following priority order; it does not have the capability to change the key exchange algorithm used. If the TOE does not receive a supported DHE group extension from the peer, it will terminate the communication. Among algorithms of equivalent security strength, the one with the shorter key length is prioritized. The key exchange priorities for each TLS version in the TOE are shown below.

Table 28 Priority of Key Exchange Algorithms

#	Key Exchange Algorithm	Key Length	Priority_TLS1.3	Priority_TLS1.2	ffdhe Group	Elliptic Curve
1	DHE	2048-bits*	-	4	-	-
2		3072-bits	5	-	ffdhe3072	-
3		4096-bits	3	-	ffdhe4096	-
4	ECDHE	256-bits	4	3	-	secp256r1
5		384-bits	2	2	-	secp384r1
6		521 bits	1	1	-	secp521r1

*Key exchange using DHE with a 2048-bits key length is available only for TLS 1.2 communications.

When the TOE selects key parameters such as key length based on the priorities shown in Table28 it notifies the client of the selected key agreement parameters via the Server Key Exchange for TLS 1.2 and via the Key Share Extension for TLS 1.3, in accordance with the rules.

The signature algorithms supported by TOE are listed below.

Table 29 Supported Signature Algorithms

#	Signature Algorithm	Key Length
1	RSA	2048 bits
2		3072-bits
3		4096-bits
4	ECDSA	256-bits
5		384-bits
6		521-bits

The TOE prohibits extensions to the Early Data Extension.

TOE can use RSA key pairs and ECDSA key pair certificates for its own authentication. The supported RSA key lengths and ECDSA elliptic curves are as follows:

・RSA: 2048-bits/3072-bits/4096-bits

・ECDSA: secp256r1/secp384r1/secp521r1

7.3. Identification and Authentication (FIA)

7.3.1. FIA_AFL.1

The TOE tracks authentication failures by remote administrators via the Web GUI or REST API.

An administrator account that fails authentication consecutively more than the number of times defined by the Security Administrator (View & Modify) (1 to ,999 times) will be locked for the duration defined by the Security Administrator (View & Modify) (60 to 345,600 seconds). Note that the count of consecutive authentication failures is tied to the administrator account.

TOE allows authentication attempts for locked administrator accounts but always returns an authentication failure response. Locked users can access TOE again once the lock period has elapsed.

Note that only the specific administrator account that failed authentication will be locked; other administrator accounts will still be able to log in.

The account lock mechanism does not apply when using a local connection. Therefore, even if all user accounts are locked, TOE management functions are still provided through local administration.

7.3.2. FIA_PMG_EXT.1

TOE has a password management function for administrator accounts.
Administrator passwords may consist of any combination of uppercase and lowercase letters, numbers, and the special characters "!", "@", "#", "$", "%", "^", "&", "*", "(), ")", "", "'", "+", ",", "-", and "."/", ":", ";", "<", "=", ">", "?", "[", "¥", "]", "_", "`", "{", "|", "}", and "~".
The minimum password length can be set by the Security Administrator (View & Modify) to between 6 and 63 characters; passwords shorter than the length set by the Security Administrator (View & Modify) cannot be created. Note that the maximum length is fixed at 63 characters.

7.3.3. FIA_UIA_EXT.1

TOE provides a Web GUI and a REST API interface for remote administrative access to TOE; however, to access either interface, administrators must be identified and authenticated using a user ID and password. In the Web GUI, the user enters their user ID and password into the text boxes and clicks the login button. For the REST API, the user issues a POST request containing the user ID and password to obtain a session. Both the Web interface and the REST API interface are used for remote connections from an administrative PC.
Additionally, the TOE provides a Web GUI for local administrators' access to the TOE; administrators must enter their user ID and password into the text boxes and click the login button to be identified and authenticated.

When the TOE receives an ICMP echo request, it responds to the request regardless of whether the source is an identified/authenticated administrator or IT entity. Furthermore, when an unauthenticated administrator attempts to access the Web GUI, a message preconfigured by the Storage Administrator (Initial Configuration) is displayed on the login screen's access banner. Upon successful login, the management screen is displayed.
When using the REST API, only the following commands are provided to administrators prior to identification and authentication; TOE security features are not provided.

・Retrieve REST API version information
・Retrieving a list of disk storage devices

Authenticated administrators are provided with various configuration and reference functions, including TOE security features.

7.3.4. FIA_UAU.7

When performing local administration, the password displayed on the login screen is shown as masked characters.

7.3.5. FIA_X509_EXT.1/Rev

The TOE verifies X.509 certificates at the following times:

(a) When importing various certificates

(b) During the TLS handshake

Whether the certificate being verified is a chain certificate or a leaf certificate, the TOE verifies all certificates in the certificate chain; if even a single certificate fails to meet the verification criteria, the certificate verification is deemed to have failed. Therefore, the verification process and results remain unchanged regardless of whether the certificate being verified is a chain certificate or a leaf certificate. Additionally, signature verification is performed during import and during the handshake to verify that the certificate is correctly linked to the trust anchor. The TOE supports verification of certificate chains with three or more certificates.

(a) The verification items performed during certificate import are listed below.

The TOE allows you to import one web server certificate (including the chain structure from the root certificate), one client certificate for the audit log server (primary and secondary), and one root certificate for the audit log server (primary and secondary). The imported certificates are managed within the TOE according to their intended use. When uploading a server certificate via a certificate chain, verify that the chain terminates with a CA certificate. When configuring audit log server certificates and uploading client certificates via a certificate chain, verify that the chain terminates with a CA certificate. When importing each certificate, the TOE will not import any certificate that fails to meet even one of the following verification criteria.

i. Signature verification for all certificates included in the certificate chain

ii. Verification of the CA flag in basicConstraints (verification that the CA flag is set to TRUE for the CA certificate)

(b) The verification items performed during the TLS handshake are listed below.

The TOE will not establish a secure connection if the following verification criteria are not met. Upon receiving the server certificate from the audit log server, the TOE verifies that the certificate chain extends back to the root certificate registered in advance on the audit log

server configuration screen. Note that the revocation verification described in section iv below complies with RFC 6960 for OCSP and RFC 5280 for CRL.

I. When the TOE acts as the server

When the TOE acts as the server, since the server certificate verification is performed on the client side, the TOE does not perform any certificate verification during the handshake.

II. When the TOE acts as a client

i. Certificate Validity Check
ii. Certificate signature verification (chain verification)
iii. Verification of basicConstraints
    1. The basicConstraints extension field exists and the CA flag is "TRUE"
    2. The basicConstraints extension field exists and the CA flag is "FALSE"
iv. Revocation verification using OCSP/CRL
v. Verification of extendedKeyUsage
    1. Verification of Server Authentication Purpose
    2. Verification of OCSP Signing Purpose (OCSP)

The table below shows which certificates are subject to the above validations.

Table 30 Verification Details and Target Certificates During the TLS Handshake

Certificate / (b) Verification Item	I. When the TOE acts as the client				
	Audit log server's server certificate	Client certificate for the audit log server	Root CA certificate included in the audit log server's certificate chain	Intermediate CA certificate included in the audit log server's certificate chain	OCSP Responder Certificate
i	✓	×	×	✓	✓
ii	✓	×	×	✓	✓
iii.1	×	×	×	✓	×
iii.2	✓	×	×	×	×

iv	✓	×	×	✓	×
v.1	✓	×	×	×	×
v.2	×	×	×	×	✓

Legend: ✓: Subject to verification
×: Not subject to verification

The TOE supports the function of verifying the revocation status of the audit log server's server certificate and the intermediate CA certificates included in the audit log server's certificate chain using OCSP or CRL.
To perform revocation verification using OCSP, an OCSP responder must be installed in the TOE's operating environment and connected to the network, as shown in Figure1. Additionally, the OCSP URL must be configured in the AuthorityInfoAccess extension field of the certificate to be verified.
To perform revocation verification using a CRL, a CRL DP (Distribution Point) server must be installed in the TOE's operating environment and connected to the network, as shown in Figure1. Additionally, the URL of the CRL DP server must be specified in the CRL DP extension field of the certificate for which revocation verification is to be performed.
If a certificate contains both the AuthorityInfoAccess extension and the CRL DP extension, the TOE prioritizes OCSP revocation verification. If a revocation check response is received from the OCSP responder, the TOE uses that information to determine revocation. If a connection to the OCSP responder cannot be established, the TOE then accesses the CRL DP to retrieve the CRL and perform the revocation check. If a CRL is obtained from the CRL DP, the TOE determines revocation based on that information. If a connection to the CRL DP cannot be established, the revocation verification fails.
If revocation verification fails, the TOE does not accept the certificate subject to revocation verification and does not establish communication with the IT entity that presented the certificate.

Signature verification of the OCSP responder certificate or CRL uses the certificate of the CA that issued the OCSP response or CRL, namely the certificate in (c) or (d).

The TOE does not support the following extendedKeyUsage:
・Code Signing purpose
・Client Authentication purpose

7.3.6. FIA_X509_EXT.2

During HTTPS/TLS communication, the TOE authenticates the counterpart device using the SAN (Subject Alternative Name) extension field of an x509v3 certificate compliant with RFC 5280. For details on device authentication using the SAN extension field, refer to7.2.10. Additionally, as described at7.3.5, the TOE can import one Web server certificate, one client certificate for the audit log server (primary and secondary), and one root certificate for the audit log server (primary and secondary), and the TOE manages only one generation of each. Therefore, the certificate used is unique depending on the communication partner, and the TOE does not select a certificate during communication.

To set up an operational environment where the TOE can use certificates, a private CA (Certificate Authority) is required to sign certificate requests. TOE users must submit certificate requests to the established private CA to obtain signed certificates, which are then imported into the TOE. When performing revocation verification using OCSP/CRL, as shown in Figure1, an OCSP responder and a CRL DP server must be connected to the TOE as part of the TOE's operational environment.

When using only either an OCSP responder or a CRL DP server for revocation verification, the verification will fail if the TOE cannot establish communication with the peer entity. When using both an OCSP responder and a CRL DP server, the revocation verification will fail if communication cannot be established with either the OCSP responder or the CRL DP server.

7.3.7. FIA_X509_EXT.3

The TOE provides an interface via the Web GUI to generate a CSR as specified in RFC 2986. When creating a CSR on the TOE, the CSR may include the following information. Note that the CSR also includes the public key.

・Country Name
・Organization Name
・Organization Unit Name
・Common Name

As described in "7.3.5," when a certificate is imported, the TOE performs signature verification on all certificates included in the target certificate chain.

7.4. Security Management (FMT)

The TOE maintains an internal mapping table of operations and roles. When an administrator

requests an operation, the TOE determines whether the operation can be executed based on the administrator's role as defined.

7.4.1. FMT_MOF.1/ManualUpdate

The TOE restricts the ability to perform firmware updates to only User Maintenance who have the authority to perform firmware updates; firmware updates cannot be performed from interfaces used by other administrators.
For details, refer to Table31 in 7.4.5 FMT_SMF.1.

7.4.2. FMT_MOF.1/Functions

TOE restricts the ability to change (enable/disable) the transmission of audit records to an external audit server to the Audit Log Administrator (View & Modify), and this cannot be changed from the interfaces used by other administrators.
For details, see the Table 31 in 7.4.5 FMT_SMF.1.

7.4.3. FMT_MTD.1/CoreData

TOE restricts the ability to manage the following to Security Administrator (View & Modify), and it cannot be managed from the interfaces used by other administrators.

- Creating user groups associated with roles
- Creating users (setting user IDs and passwords, associating user groups)
- Setting the minimum password length for the administrator password
- Administrators changing their own passwords
- Password reset (changing another user's password)
- Setting the remote session inactivity time before session termination
- Setting the number of failed login attempts for administrators and the time before re-authentication is allowed after a failed login
- Importing the Web server's server certificate
- Importing the web server certificate's root certificate into the TOE's trust store / Deleting the web server certificate's root certificate from the trust store (by overwriting)

The TOE restricts the ability to manage the following to the Audit Log Administrator (View & Modify), and these settings cannot be managed via the interfaces used by other administrators.

- Administrators changing their own passwords
- Configuring the audit log server
- Importing the audit log server's client certificate

・Importing the audit log server certificate's root certificate into the TOE trust store / Deleting the audit log server certificate's root certificate from the trust store (by overwriting)

TOE restricts the ability to manage the following to the Storage Administrator (Initial Configuration), and these cannot be managed from the interfaces used by other administrators:

・Administrators changing their own passwords
・Configuring the message displayed in the access banner
・Set the date and time

The TOE restricts the ability to manage the following to User Maintenance; these cannot be managed via the interfaces used by other administrators.

・Administrators changing their own passwords

For details, refer to Table31 in 7.4.5 FMT_SMF.1.

Note that, as indicated in 7.3.3 FIA_UIA_EXT.1, the following functions are provided prior to administrator authentication; however, these functions are limited to GET requests for information and responses to ICMP, and cannot modify TSF data. Furthermore, since the addresses accessed via GET requests do not contain TSF data, TSF data cannot be read using these functions.

- Accessing the login screen via the Web GUI and viewing the message displayed on the login screen banner
- ICMP echo
- GET requests using the following REST API
    - /configuration/version
    - /configuration/storages

7.4.4. FMT_MTD.1/CryptoKeys

TOE restricts the ability to generate X.509 certificate signing requests (CSRs) and RSA/ECDSA keys to Security Administrator (View & Modify) via the web GUI; these cannot be generated from the interfaces used by other administrators.

When importing a certificate into the TOE, you must upload the certificate chain for verification.

The roles required to import certificates into the TOE vary depending on the type of certificate. The roles required for each certificate import operation are listed below. These

operations cannot be performed from interfaces used by administrators other than those listed below.

・Audit log server root certificate/client certificate (including the certificate chain from the root certificate): Audit Log Administrator (View & Modify)

・TOE Web Server Certificate (including the certificate chain from the root certificate): Security Administrator (View & Modify

For details, refer to Table31 in Section 7.4.5 FMT_SMF.1.

7.4.5. FMT_SMF.1

The TOE provides the administrator with the management functions listed below via the WebGUI or REST API remote management interface. Additionally, the TOE provides the administrator with the management functions listed below via the WebGUI local management interface. (All WebGUI management screens are provided identically via both the remote management interface and the local management interface.)

Note that to use the local management interface, the TOE and the management PC must be directly connected via a LAN cable.

Table 31 Correspondence Table of Management Operations, Interfaces, and Roles

#	Management Function	Interface		Role Required for Operation
		Web GUI Screen	REST API Commands	
Ability to administer the TOE remotely				
1	Creating user groups associated with roles	-	/v1/objects/user-groups	Security Administrator (View & Modify)
2	Creating a user (setting user ID and password, associating with a user group)	[Maintenance Utility] - [Administration] - [User Management Screen]	/v1/objects/users	Security Administrator (View & Modify)
3	Setting the minimum password length for the administrator password	[Maintenance Utility] - [Administratio	—	Security Administrator (View

		n] – [User Account Policy]		& Modify)
4	Administrator Password Change	[Maintenance Utility] - [Menu] - [System Administration] - [Change Password]	—	Security Administrator (View & Modify), Storage Administrator (Initial Configuration), Audit Log Administrator (View & Modify), User Maintenance
5	Password Reset (Changing Another User's Password)	[Maintenance Utility] - [Administration] - [User Management Screen]	-	Security Administrator (View & Modify)
Ability to configure the access banner				
6	Configure the message displayed in the access banner	[Maintenance Utility] - [Menu] - [System Administration] - [Login Message Edit Screen]	-	Storage Administrator (Initial Configuration)
Ability to configure the remote session inactivity time before session termination/Ability to configure the local session inactivity time before session termination or locking				
7	Setting the inactivity time before	[Maintenance	-	Security

	remote/local administrator sessions end (Web interface)	Utility] - [Menu] – [System Administration] – [Session Timeout]		Administrator (View & Modify)
Ability to update the TOE and verify the updates using digital signature capability prior to installing them				
8	TOE firmware updates and verification of the firmware to be updated	[Maintenance Utility] - [Management] - [Firmware Screen]	-	User Maintenance
Ability to configure the authentication failure parameters for FIA_AFL.1				
9	Setting the number of authentication failures allowed for the administrator, and setting the time until re-authentication is permitted after a failure	[Maintenance Utility] - [Administration] – [User Account Policy]	-	Security Administrator (View & Modify)
Ability to modify the behavior of audit data transmission to an external IT entity				
10	Enable/Disable Sending to Audit Log Server	[Maintenance Utility] - [Administration] - [Audit Log Settings Screen]	-	Audit Log Administrator (View & Modify)
Ability to manage cryptographic keys Ability to generate a Certificate Signing Request (CSR) and process the CA certificate response;				
11	Creation/deletion of CSR and RSA/ECDSA keys	[Maintenance Utility] - [Menu] - [System Management] – [Create CSR and Self-Signed	-	Security Administrator (View & Modify)

		Certificate]		
12	Audit Log Server Settings ・Importing Client Certificates (When importing client certificates, import them as a chain configuration that includes the root certificate and intermediate CA certificates) *1	[Maintenance Utility] - [Administration] - [Audit Log Settings Screen]	-	Audit Log Administrator (View & Modify)
13	Renewal of TOE Web Server Certificate ・Importing Web Server Certificates (When importing the Web server certificate, import it as a chain configuration that includes the root certificate and intermediate CA certificates) *1	[Maintenance Utility] - [Menu] – [System Management] – [Certificate File Update]	-	Security Administrator (View & Modify)
Ability to set the time used for timestamps				
14	Settings for the date and time used below ・Recording timestamps ・Verification of certificate expiration dates	[Maintenance Utility] - [Administration] - [Date and Time Settings Screen]	-	Storage Administrator (Initial Configration)
Ability to configure the peer's reference identifier				
15	Audit Log Server Settings ・IP address (Up to two primary/secondary servers can be configured)	[Maintenance Utility] - [Administration] - [Audit Log Settings Screen]	-	Audit Log Administrator (View & Modify)
Ability to manage the TOE's trust store and designate X.509 v3 certificates as trust anchors				
16	Import the audit log server's root CA certificate (which signs the intermediate CA certificate or server certificate) (Up to two servers —	[Maintenance Utility] - [Administration] - [Audit Log	-	Audit Log Administrator (View & Modify)

	primary and secondary—can be imported) *1	Settings Screen]		
17	Import the root certificate for the TOE web server certificate (When importing the web server certificate, import it as a chain configuration that includes the root certificate and intermediate CA certificate) *1	[Maintenance Utility] - [Menu] – [System Administration] - [Certificate File Update]	-	Security Administrator (View & Modify)

*1 If you import a new certificate while an existing certificate is already imported, the old certificate will be deleted and replaced with the new one.

7.4.6. FMT_SMR.2

In TOE, users are created by associating them with user groups that have been configured with the following roles: Security Administrator (View & Modify), Storage Administrator (Initial Configuration), Audit Log Administrator (View & Modify), and User Maintenance. Furthermore, when a user logs in, a role is associated with them, and this association persists until they log out. TOE maintains the association between users and roles through this mechanism.

Each Security Administrator can remotely manage the TOE.

For the roles required for TOE management operations, refer to Table31 in 7.4.5 FMT_SMF.1.

7.5. Protection of the TSF (FPT)

7.5.1. FPT_SKP_EXT.1

As described in 7.2.3 FCS_CKM.4, each key is stored in RAM or on the SSD according to Table 17. The TOE does not provide users with an interface to access keys stored in RAM or on the SSD.

7.5.2. FPT_APW_EXT.1

Since each administrator's password information is stored in hashed form within the TOE, plaintext passwords cannot be accessed. Furthermore, the TOE does not provide any local or remote management interfaces for reading passwords. Note that PBKDF2 (Password-Based Key Derivation Function 2) is used to hash administrator passwords, and SHA512 is specified as the hash function used within PBKDF2.

7.5.3. FPT_TST_EXT.1

The TOE performs the self-tests described below when the device boots up.

a) Firmware Integrity Test

b) known answer test for the following cryptographic algorithms

i. AES
ii. DRBG
iii. RSA
iv. ECDSA
v. HMAC
vi. DH
vii. ECDH

In the test described in a), the integrity of the firmware is verified by using a public key to validate the digital signature associated with the firmware. The public key is a key pre-installed in the TOE for the purpose of verifying the firmware signature. If the firmware is incomplete, such as having been tampered with, the digital signature verification test will fail. In the event of a failure, the verification test is rerun by rebooting the system. The firmware subject to verification includes the entire firmware that constitutes the TSF, including the OS and kernel. By performing integrity tests on the entire firmware including the OS and kernel that serve as the operational foundation of TSF we can ensure that all TSF functions are provided in a complete and intact state.

In the test described in b), a known answer test is performed for each cryptographic algorithm provided by the TOE. If the output of the cryptographic algorithm differs from the known answer, the test fails because the cryptographic function is not operating correctly. In the event of a failure, the known answer test is re-executed by rebooting the system. Since the TSF performs known answer tests on all cryptographic algorithms that constitute the TOE's cryptographic functions, conducting this test ensures that the TOE's cryptographic functions are operating correctly.

The above tests demonstrate the correct operation of the device by verifying that no changes have been made to the operating system or any firmware, that only tested code is being executed by the TSF, and that the underlying hardware can load the OS and correctly process each known answer test.

If a test fails, the TOE suppresses its own startup, records a Service Information Message (SIM) indicating that the firmware is incomplete, and reboots the system. Tests a) and b) are also performed during the reboot. If the TOE starts up normally, this guarantees that there are no abnormalities in the TOE firmware, that the cryptographic functions provided by the

TOE operate correctly, and that a correctly functioning TSF can be provided.

7.5.4. FPT_TUD_EXT.1

When any role (Security Administrator (View & Modify), Storage Administrator (Initial Configuration), Audit Log Administrator (View & Modify), or User Maintenance) checks the version via the Web GUI, the TOE responds with the currently active TOE version.
A User Maintenance with permission to execute firmware updates performs a manual firmware update from the management PC using the firmware media for the update. The firmware verification content is equivalent to the integrity verification performed at device startup, and the verification method is described in 7.5.3 FPT_TST_EXT.1.
When a User Maintenance instructs a manual firmware update via the Web GUI, the TOE performs an integrity check before the firmware update process; if the integrity check succeeds, the firmware update process proceeds. If the firmware integrity check fails, the TOE does not perform the firmware update. The updated firmware becomes active immediately after installation is complete.

7.5.5. FPT_STM_EXT.1

The following TOE functions utilize date and time.

a) Timestamp function for recording in audit logs
b) Certificate validity verification function

The TOE incorporates an internal clock to manage the date and time used by the two functions described above. Only the Storage Administrator (Initial Configuration) can change the date and time settings via the remote management interface or the local management interface, and the TOE records such changes in the audit log.
Functions a) and b) use the internal clock; since the TOE's built-in RTC (Real-Time Clock) provides accurate time, audit logs are recorded with reliable dates and times, and certificate validity is verified using reliable dates and times.

7.6. TOE Access (FTA)

7.6.1. FTA_SSL.3

For the web interface, the TOE terminates inactive remote web interface sessions after a specified period has elapsed. The Security Administrator (View & Modify) can set the timeout value to 60, 90, or 120 minutes.
For the REST API, the TOE terminates inactive remote REST API interface sessions after a specified period has elapsed. The REST API session timeout can be set by each administrator

between 1 and 300 seconds when the session is created.

7.6.2. FTA_SSL.4

For the Web interface, administrators can terminate their own session at any time by performing a logout operation via the Web GUI.
For the REST API, administrators can log out at any time by presenting the session information (token) issued by the TOE upon login and performing the session termination operation. Both the Web interface and the REST API interface are used for remote connections from the management PC.

7.6.3. FTA_SSL_EXT.1

The local connection session terminates inactive local web interface sessions after a specified period. Security Administrator (View & Modify) can set the timeout value to 60 minutes, 90 minutes, or 120 minutes.

7.6.4. FTA_TAB.1

The implementation of pre-login messages for each remote interface and local interface used to manage TOE is described below.
a) For the Web Interface
The TOE displays notes and warning messages regarding TOE usage, which are preconfigured by the Storage Administrator (Initial Configuration), on a banner on the login screen before logging in via the Web GUI. This behavior is the same for both remote and local interfaces.
b) For the REST API interface
The TOE does not display pre-login messages when accessed via the REST API through the remote management interface.

7.7. Trusted Path/Channels (FTP)

7.7.1. FTP_ITC.1

The TOE supports secure communication using TLS for sending audit logs to the audit log servers. Additionally, the TOE verifies the server certificate sent by the audit log server as described in 7.3.5 FIA_X509_EXT.1/Rev to authenticate the audit log server as the communication partner. The method for identifying the server certificate is described in 7.2.10 FCS_TLSC_EXT.1.
Additionally, the TOE performs mutual authentication during TLS communication with the audit log server. A summary specification regarding mutual authentication with the audit log

server is described in 7.2.11 FCS_TLSC_EXT.2.

7.7.2. FTP_TRP.1/Admin

The TOE supports secure communication using HTTPS to enable remote management of the TOE-by-TOE administrators via the Web GUI and REST API. Specifically, HTTPS communication is provided for all operational actions, including administrator login authentication.

8. Terminology

8.1. ST Technical Terms

Administrator	See Security Administrator.
TOE security functionality	Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs [Terminology from CC Part 1]
TSF Data	Data for the operation of the TOE upon which the enforcement of the SFR relies. [CC Part 1 terminology]
SAN	Abbreviation for Subject Alternative Name. One of the extension fields in an X.509 v3 certificate. By using SAN, a single certificate can certify multiple domain names or IP addresses.
Security Administrator	The terms “Administrator” and “Security Administrator” are used interchangeably in this document at present and are used to represent a person that has authorized access to the TOE to perform configuration and management tasks.
SIM	Abbreviation for Service Information Message. A message displayed in the Maintenance Utility when maintenance of a disk storage device is required.
Operational Environment	Environment in which the TOE is operated. [Term from CC Part 1]
External Entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. [CC Part 1 terminology]
Threat Agent	Entity that can adversely act on assets. [CC Part 1

	Terminology]
Iteration	Use of the same component to express two or more distinct requirements. [CC Part 1 terminology]
Trusted Channel	A means by which a TSF and another trusted IT product can communicate with necessary confidence. [CC Part 1 terminology]
Trusted Path	Means by which a user and a TSF can communicate with the necessary confidence. [CC Part 1 terminology]
Controller Chassis	A chassis that houses the TOE's controller board, drives, and power supply.
Describe	Provide specific details of an entity. [CC Part 1 terminology]
Selection	The act of identifying one or more items from a list within a component. [CC Part 1 Terminology]
Organisational Security Policy	Set of security rules, procedures, or guidelines for an organisation. [CC Part 1 Terminology]
Security Problem	Statement which in a formal manner defines the nature and scope of the security that the TOE is intended to address. [CC Part 1 Terminology]
Security Objective	Statement of an intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions. [CC Part 1 terminology]
Security Requirement	Requirement, stated in a standardised language, which is meant to contribute to achieving the security objectives for a TOE. [CC Part 1 terminology]
Drive Box	A housing that houses a drive. While a TOE may also house a drive within the controller chassis, this housing is designed to be connected to the controller chassis to expand the system's drive capacity. Note that this enclosure only writes data to the drive and does not have the capability to provide the SFRs described in this ST.
Target of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance. [Terminology from CC Part 1]
Fibre Channel/iSCSI	High-speed network technologies used to build Storage

	Area Networks.
Protection Profile	Implementation-independent statement of security needs for a TOE type. [CC Part 1 Terminology]
Extension	Addition to an ST or PP of functional requirements not contained in CC Part 2 and/or assurance requirements not contained in CC Part 3. [CC Part 1 terminology]
Assignment	The specification of an identified parameter in a component (of the CC) or requirement. [CC Part 1 terminology]
Maintenance Utility	A web GUI that allows you to manage storage system and network settings, user information, and license keys.
VSP One Block Administrator	A web GUI that allows you to manage storage system configurations and resources.

8.2. Abbreviations

The following abbreviations are used in this document.

API	Application Programming Interface
CC	Common Criteria
cPP	Collaborative PP
CRL	Certificate Revocation List
CRL DP	CRL Distribution Point
CSR	Certificate Signing Request
DKC	Disk Controller
ESM	Embedded Storage Manager
FIPS	Federal Information Processing Standards
FW	Firmware
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
LAN	Local Area Network
NDcPP	Collaborative Protection Profile for Network Devices
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
OCSP	Online Certificate Status Protocol
PC	Personal Computer

PP	Protection Profile
REST	Representational State Transfer
REST API	RESTful API
RFC	Request for Comments
SAN	Subject Alternative Name
SIM	Service Information Message
SSD	Solid State Drive
SSL	Secure Sockets Layer
ST	Security Target
SFR	Security Functional Requirement
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE security functionality
VSP	Virtual Storage Platform