iMC MagicBox Security Target

Version: 3.4
Date: 2025-07-08
H3C

Document history

Version	Date	Comment	Author
0.1	2022-06-09	Initial version	SGS Brightsight
0.2	2022-06-21	Updated with new evidences	SGS Brightsight
0.3	2022-07-08	Updated SFRs with DAR analysis	SGS Brightsight
0.4	2022-07-14	Update document with new PP claimed	SGS Brightsight
0.5	2022-07-18	Update SFRs with 1.3 version of the PP	SGS Brightsight
0.6	2022-07-19	Added TOE configurations	SGS Brightsight
0.7	2022-08-02	Updated with developer feedback	H3C & SGS Brightsight
0.8	2022-08-03	Updated with SGS Brightsight feedback	H3C
0.9	2022-08-05	Updated with developer feedback	SGS Brightsight
0.10	2022-08-16	Update with SGS Brightsight feedback	H3C
0.11	2022-08-25	Updated with developer feedback	SGS Brightsight
0.12	2023-01-18	Change in scope. Now network device PP as an appliance is used.	SGS Brightsight
0.13	2023-01-22	Update with SGS Brightsight feedback	H3C
0.14	2023-01-31	Update with MagicBox ST	H3C
0.15	2023-02-09	Update with developer feedback	SGS Brightsight
0.16	2023-02-11	Update with SGS Brightsight feedback	H3C
0.17	2023-02-16	Update with developer feedback	SGS Brightsight
0.18	2023-02-17	Update with SGS Brightsight feedback	H3C
0.19	2023-02-17	Final revision and small fixes	SGS Brightsight
1.0	2023-02-17	First release	SGS Brightsight
1.1	2023-02-21	Delete some third-party components	H3C
1.2	2023-03-06	Small fixes and clarifications	SGS Brightsight
1.3	2023-03-15	Update with SGS Brightsight feedback	H3C
1.4	2023-03-17	Update with developer feedback	SGS Brightsight
1.5	2023-04-01	Add TLS as client and FAU_GEN.1.2	H3C
1.6	2023-04-03	Update iMC network infrastructure	H3C
1.7	2023-04-28	Fix small issues	SGS Brightsight
1.8	2023-05-29	Remove info about WSM	H3C
1.9	2023-06-02	Add X.509 SFRs and related information	SGS Brightsight
2.0	2023-06-12	Update some details about TLSC	H3C
2.1	2023-06-12	Small fixes	SGS Brightsight
2.2	2023-06-13	Certificate Authentication just for TLS	H3C
2.3	2023-07-06	Update FIA_X509_EXT.1.1/Rev & FIA_X509_EXT.2.2 & FCS_TLSC_EXT.1.1	H3C
2.4	2023-07-20	Update FCS_TLSC_EXT.1.1 & FCS_TLSC_EXT.1.4	H3C
2.5	2023-09-06	Fix some changes, reformulate conformance claim	SGS Brightsight
2.6	2023-09-21	Fix ORs from evaluation	SGS Brightsight
2.7	2023-11-24	Fix ORs from evaluation	H3C
2.8	2023-11-29	Update with developer feedback	SGS Brightsight

2.9	2023-11-30	Update with SGS Brightsight feedback	H3C
2.10	2024-01-02	Update after developer feedback	SGS Brightsight
2.11	2024-01-02	Update with SGS Brightsight feedback	H3C
2.12	2024-01-05	After developer feedback	SGS Brightsight
2.13	2024-01-08	Update with SGS Brightsight feedback	H3C
3.0	2024-01-09	New release after solving all issues	H3C & SGS Brightsight
3.1	2024-01-09	Fixes FAU_GEN.1 events and FTA_TAB.1 identification	SGS Brightsight
3.2	2024-07-03	Update after OR	SGS Brightsight
3.3	2024-07-14	Update version Information	H3C
3.4	2025-07-08	Update AGD version	SGS Brightsight

Contents

1 Security Target Introduction

The ST describes what is evaluated, including the exact security properties of the TOE in a manner that the potential consumer can rely on.

1.1 Security Target Reference

Title	iMC MagicBox Security Target
Version	See Document History
Date	See Document History
Author	SGS Brightsight

Table 1 Security Target reference

1.2 TOE Reference

TOE Developer	H3C Technologies Co., Ltd.
TOE Name	iMC MagicBox (iMC PLAT, iMC EIA)
TOE Version	iMC 7.3 (PLAT E0708P13, EIA E0629)

Table 2 TOE reference

1.3 TOE Overview

Intelligent Management Center MagicBox with Intelligent Management Center Platform and Intelligent Management Center End-user Intelligent Access component, also referred as **iMC MagicBox (iMC PLAT, iMC EIA)** and from now on during the document referred just as **iMC** or **iMC MagicBox,** is an integrated network management platform for enterprises. It centrally manages switches, routers and provides a diverse range of functions for enterprise network infrastructure, such as automatic configuration and deployment, visualized fault diagnosis, and intelligent capacity analysis. iMC helps enterprises improve O&M efficiency, reduce O&M costs, improve resource utilization, and ensure stable operation for enterprise network systems.

iMC provides role and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure. iMC implements profiling, guest access, and health checks, facilitating centralized management of network access policies.

iMC provides user and device authentication based on 802.1X, non-802.1X and web portal access methods.

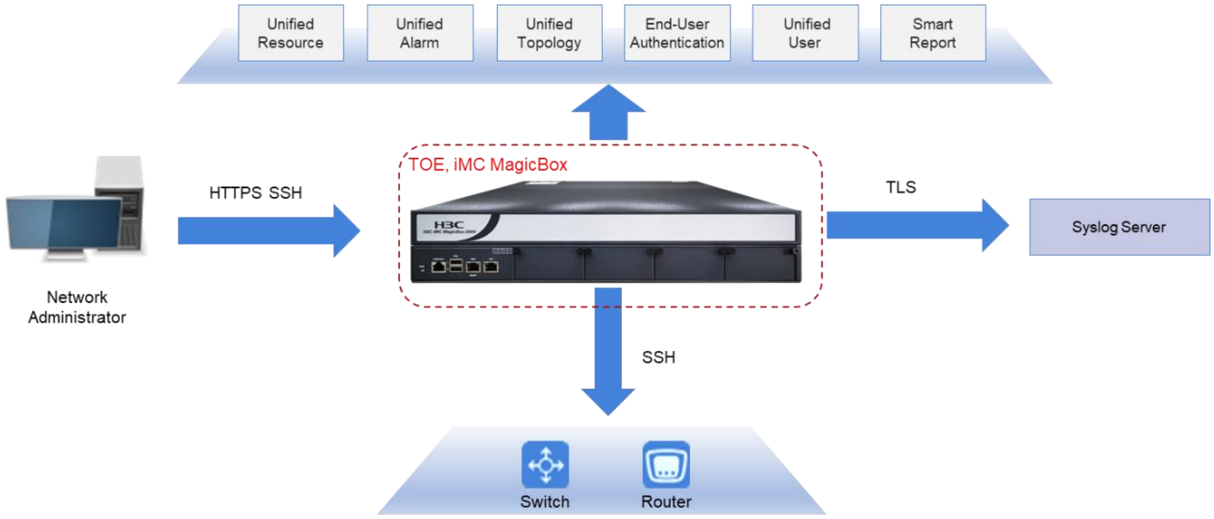

Figure 1: iMC located in the network infrastructure

1.3.1 TOE Type

iMC is available either as a hardware or virtual network appliance and is designed to support a wide range of network, wireless and security protocols to support a wide range of clients. However, the evaluation is limited to the hardware network appliances.

Appliance Model	Component	CPU
H3C iMC MagicBox 2000	iMC PLAT, iMC EIA	Intel Xeonl E5-2620V4, 8 Cores

1.3.2 TOE Usage and Major Security Features

H3C iMC MagicBox consists of one platform (iMC PLAT) and one component (iMC EIA):

iMC PLAT consists of a base platform for delivering network resource management capabilities and optional service modules for extending iMC's functionality. The base platform provides administrators and operators with the basic and advanced functionality needed to manage iMC and the devices, users, and services managed by iMC. The base platform incorporates the essential functional areas of network management – fault, configuration, asset management and auditing, performance, and security.

End-user Intelligent Access (EIA) manages network access of endpoints in enterprise networks that are built with wired, wireless, and VPN network infrastructures. EIA supports defining access scenarios based on the user role, device type, access time, access location, and other criteria and performs strict network access control. It meets the unified operation and maintenance requirements of enterprise networks to manage various access methods, abundant endpoint types, and different user roles and ensures execution of security policies.

The iMC is a network management system, iMC is located at the management and control layer of the network, it can manage and control various network devices, including switches and routers. It provides open interface to quickly integrate with upper-layer application systems such as OSSs, service orchestrators and service application.

For the iMC architecture, in the northbound direction, it provides Web portals and northbound interfaces for O&M personnel, OSS. in the southbound, it provides configuration and management capabilities for H3C network devices and third-party network elements.

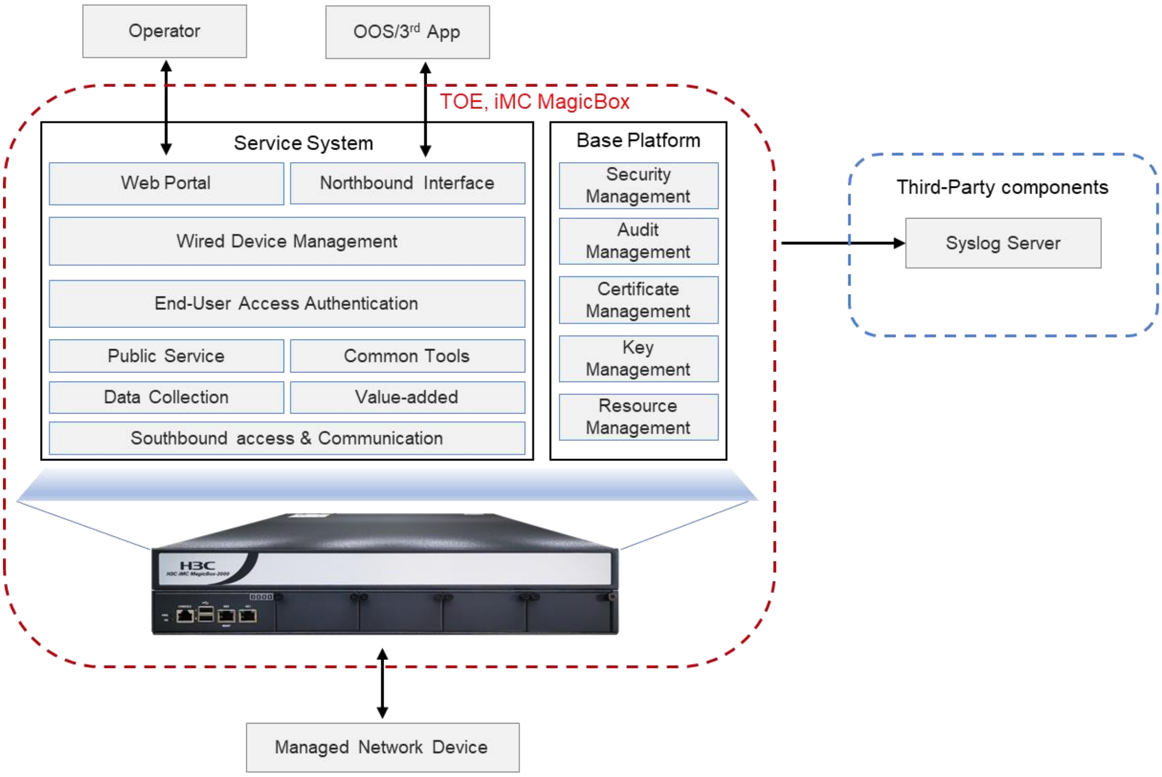

Figure 2: iMC architecture

The TOE provides the following major security features:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

1.3.3 Non-TOE Hardware/Software/Firmware

Required Non-TOE Elements

Element	**Required/Optional**	**Usage/Purpose Description for TOE**
Network Elements	Required	NEs that are managed by the TOE and support different communication protocols with the TOE.
OSS, third-party APP	Optional	The OSS and third-party application connect to the TOE using HTTPS.

Syslog server	Optional	Syslog server used to send syslog messages.

Required non-TOE Client

Operating system	Hardware requirements	Browser

Windows	CPU: Speed ≥ 2.0G;
	Memory: 2GB or higher;
	HD: 50G or higher;
	1*integrated 100MB NIC;
	Sound card.
		Firefox 30 or higher, Chrome 44 or higher
		The recommended resolution width is 1280

1.4 TOE Description

1.4.1 Physical Scope

The physical scope of the TOE consists of iMC device running software version iMC 7.3 (PLAT E0708P13, EIA E0629). The iMC evaluated configuration includes the device shown in below TOE Model.

Appliance Model	Component	CPU
H3C iMC MagicBox 2000	iMC PLAT, iMC EIA	Intel Xeonl E5-2620V4, 8 Cores

TOE Delivery

The delivery of the TOE to the customer is performed by an authorized courier service.
The TOE firmware will be pre-installed at factory.

The TOE deliverables include: the network device, the firmware already installed and the following guidance:

Item	Name	Format	Version
Installation Guides	H3C iMC MagicBox Installation Guide-7.3	PDF	5W102
Configuration Examples	H3C iMC PLAT Configuration Examples	zip	5W108
	H3C iMC UAM Configuration Examples	zip	5PW103
	H3C iMC TAM Configuration Examples	PDF	5PW100
	H3C iMC Enterprise and Standard Platform Administrator Guide-7.3	PDF	5W112
	H3C iMC User Access Manager Administrator Guide-7.3	PDF	5W108
Troubleshooting	H3C IMC PLAT Troubleshooting Guide	PDF	5PW104
	H3C iMC UAM Troubleshooting Guide	PDF	5PW102
TOE Guidance	Preparative and Operative Procedures for CC NDPP iMC Magicbox	PDF	v1.4
	H3C iMC MagicBox - Functional Specification	PDF	v2.2

Item	Name	Format	Version
	H3C iMC MagicBox-DAR	PDF	v0.2

Table 3 TOE deliverables

1.4.2 Logical Scope

This section outlines the logical boundaries of the security functionality of the TOE.

1.4.2.1 Security audit

The TOE generates audit records for security-relevant management and stores the records in the database. Operation logs record operation events of the TOE, logs can record operator name, IP address, component name, operation time, operation and result. The query and filter functions are provided on the iMC GUI, which allows authorized users to search audit logs.

1.4.2.2 Cryptographic support

The TOE provides key management, encryption/decryption, digital signature and so on in support of higher-level cryptographic protocols including SSH, HTTPS and TLS.

1.4.2.3 Identification and authentication

The TOE authenticates all users who access the TOE by user name and password.

1.4.2.4 Security management

The TOE offers security management for all management aspects of the TOE. Security management includes not only authentication and access control management, but also management of security-related data consisting of configuration profiles and runtime parameters.

1.4.2.5 Protection of the TSF

TOE saves all of TSF data in the database, and user cannot read them on the iMC GUI. iMC is deployed on the MagicBox, VM and physical server, only the server administrator can query the version of software and update it.

1.4.2.6 TOE access

TOE is able to configure the operator idle timeout parameter, default 30 mins. User will be automatically offline after exceeding the set operator idle timeout. The administrator can force users to offline.

1.4.2.7 Trusted path/channels

The TOE supports encrypted transmission within the iMC MagicBox server, between devices and the iMC Magic Box server, between browser and the iMC MagicBox server, between syslog server and the iMC MagicBox server and between OSS/third-party application and the iMC MagicBox server.

2 Conformance claims

2.1 CC Conformance Claim

The TOE and ST claim conformance to the CC Version 3.1 revision 5:

- Part 2 extended [CC31R5P2]
- Part 3 conformant [CC31R5P3]

2.2 Protection Profile Conformance

The TOE claims exact conformance to:

- collaborative Protection Profile for Network Devices v2.2e, 23-03-2020.

2.3 Conformance Rationale

The TOE is a device with the role of managing other network devices within the network. It is a standalone physical network device as defined in [PP-ND].

This ST provides exact conformance to the PP stated in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile, performing only operations defined there.

3 Security Problem Definition

The Security Problem Definition is taken from the Security Problem Definition (composed of organizational policies, threat statements, and assumption) described in the Network Devices PP [PP-ND].

4 Security Objectives

4.1 Security Objectives for the TOE

In alignment with the Network Devices PP [PP-ND], no Security Objectives for the TOE are defined.

4.2 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment are taken from the Security Objectives for the Operational Environment described in Section 5.1 of the Network Devices PP [PP-ND].

5 Extended Component Definition

Extended Component Definition has been taken with no modification from the Network Devices PP [PP-ND].

6 Security Functional Requirements

Operations done by the PP [PP-ND] are identified using the following typographical distinctions:

- Unaltered SFRs are stated in the form used in [CC31R5P2] or their extended component definition (ECD);
- Refinement made in the PP or ST: the refinement text is indicated with **bold text** and ~~strikethroughs~~;
- Selection wholly or partially completed in the PP or ST: the selection values are indicated with underlined text

  e.g. '[selection: *disclosure, modification, loss of use*]' in [CC31R5P2] or an ECD might become 'disclosure' (completion) or '[selection: disclosure, modification]' (partial completion) in the ST;
- Assignment wholly or partially completed in the PP or ST: indicated with *italicized text*;
- Assignment completed within a selection in the PP or ST: the completed assignment text is indicated with *italicized and underlined text*

  e.g. '[selection: *change_default, query, modify, delete, [assignment: other operations]*]' in [CC2] or an ECD might become 'change_default, select_tag' (completion of both selection and assignment) or '[selection: change_default, *select_tag*, *select_value*]' (partial completion of selection, and completion of assignment) in the ST;
- Iteration: indicated by adding a string starting with '/' (e.g. 'FCS_COP.1/Hash').

All the application notes defined in the PP [PP-ND] have been considered when writing this document.
Please refer to the PP [PP-ND] for specific details.

6.1 Security Audit (FAU)

6.1.1 Security Audit Data generation (FAU_GEN)

6.1.1.1 FAU_GEN.1 Audit Data Generation

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

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

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

c) All administrative actions comprising:

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*

- [selection: [*assignment*:
  1. User login and logout
  2. User account management
  • Creating, deleting, and modifying user accounts
  • Enabling, disabling user accounts
  3. User group management
  • Creating, deleting, and modifying user groups
  4. Security policy management
  • Modifying password policies
  • Modifying user account policies (Operator Idle Timeout, Concurrent Logins with same Operator Account, Max. Concurrent Logins with same Operator Account)
  5. User session management
  • Kicking out individual user accounts
  6. ACL management
  • Creating, deleting, and modifying ACLs
  7. Authentication server configuration]]

d) Specifically defined auditable events listed in Table 4.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table 4.*

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FAU_STG.1	None.	None.
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_RBG_EXT.1	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_SSHC_EXT.1	Failure to establish an SSH session	Reason for failure

FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_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
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MOF.1/Services	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.

FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	None.

Table 4 Security Functional Requirements and Auditable Events

6.1.1.2 FAU_GEN.2 User identity association

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

6.1.2 Security audit event storage (FAU_STG & Extended – FAU_STG_EXT)

6.1.2.1 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 [selection:

- The TOE shall consist of a single standalone component that stores audit data locally].

FAU_STG_EXT.1.3 The TSF shall [selection: overwrite previous audit records according to the following rule: [assignment: *overwrite starting from oldest records if the usage of the local storage space for audit data arrives 80%(default value)*]] when the local storage space for audit data is full.

6.1.2.2 FAU_STG.1 Protected Audit Trail Storage

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

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

6.2 **Cryptographic Support (FCS)**

6.2.1 Cryptographic Key Management (FCS_CKM)

6.2.1.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

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

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;

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

6.2.1.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [selection:

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”;

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

6.2.1.3 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a* [selection: destruction of reference to the key directly followed by a request for garbage collection];
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [selection:*
  - logically addresses the storage location of the key and performs a [selection: single] overwrite consisting of [selection: zeroes];

that meets the following: *No Standard*.

6.2.2 Cryptographic Operation (FCS_COP.1)

6.2.2.1 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* [selection: CBC] *mode* and cryptographic key sizes [selection: 256 bits] that meet the following: *AES as specified in ISO 18033-3*, [selection: CBC as specified in ISO 10116].

6.2.2.2 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 [selection:

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [assignment: *2048 bits*],

]

that meet the following: [selection:

- 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,

].

6.2.2.3 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 [selection: SHA-256] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes** [selection: **256**] **bits** that meet the following: *ISO/IEC 10118-3:2004*.

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

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [selection: HMAC-SHA-256] and cryptographic key sizes [*assignment: key size (256) used in HMAC]* **and message digest sizes [selection: 256] bits** that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

6.2.3 Random Bit Generation (Extended – FCS_RBG_EXT)

6.2.3.1 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 [selection: 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: 1]* software-based noise source] with a minimum of [selection: 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.

6.2.4 Cryptographic Protocols (Extended – FCS_HTTPS_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSS_EXT)

6.2.4.1 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 HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [selection: not require client authentication] if the peer certificate is deemed invalid.

6.2.4.2 FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs *4251, 4252, 4253, 4254*, [selection: 4344, 6668].

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based].

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than *[assignment:* *256K*] bytes in an SSH transport connection are dropped.

FCS_SSHC_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [selection: aes256-cbc].

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [selection: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512*]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 The TSF shall ensure that [selection: diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [selection: ecdh-sha2-nistp384] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [selection: no other methods] as described in RFC 4251 section 4.1.

6.2.4.3 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254, [selection: 4344, 6668].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than *[assignment: 256K*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [selection: aes128-cbc, aes256-cbc].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [selection: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [selection: diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [selection: no other methods] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

6.2.4.4 FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: IPv4 address in CN or SAN].

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [selection:

• Not implement any administrator override mechanism

]

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

6.2.4.5 FCS_TLSS_EXT.1 TLS Server Protocol Without Mutual Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- 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

and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [selection: TLS 1.1].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [selection: RSA with key size [selection: 2048 bits] and no other curves]].

FCS_TLSS_EXT.1.4 The TSF shall support [selection: session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)].

6.3 Identification and Authentication (FIA)

6.3.1 Authentication Failure Management (FIA_AFL)

6.3.1.1 FIA_AFL.1 Authentication Failure Management (Refinement)

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*assignment: 3 to 10*] 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 [selection: 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].

6.3.2 Password Management (Extended – FIA_PMG_EXT)

6.3.2.1 FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: "~", "`", "=", "+", "|", """, "-", "_", "[", "]", "{", "}", ":", ";", ",", "/", ".", "<", ">", "?"];

b) Minimum password length shall be configurable to between [*assignment: 6*] and [*assignment: 15*] characters.

6.3.3 User Identification and Authentication (Extended – FIA_UIA_EXT)

6.3.3.1 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;
- [selection: no other actions].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.3.4 User authentication (FIA_UAU) (Extended – FIA_UAU_EXT)

6.3.4.1 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [selection: password-based] authentication mechanism to perform local administrative user authentication

6.3.4.2 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress **at the local console**.

6.3.5 Authentication using X.509 certificates (Extended – FIA_X509_EXT)

6.3.5.1 FIA_X509_EXT.1 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 [selection: *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:

o *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.*

o *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*

o *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*

o *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.

6.3.5.2 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 [selection: HTTPS, TLS] and [selection: 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: accept the certificate].

6.4 Security Management (FMT)

6.4.1 Management of functions in TSF (FMT_MOF)

6.4.1.1 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*.

6.4.1.2 FMT_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1/Services The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to *Security Administrators.*

6.4.2 Management of TSF Data (FMT_MTD)

6.4.2.1 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*.

6.4.3 Specification of Management Functions (FMT_SMF)

6.4.3.1 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [selection:* hash comparison*] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- *[selection:*
  - Ability to start and stop services;
  - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
  - Ability to re-enable an Administrator account*;].*

6.4.4 Security management roles (FMT_SMR)

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

are satisfied.

6.5 **Protection of the TSF (FPT)**

6.5.1 Protection of TSF Data (Extended – FPT_SKP_EXT)

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

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

6.5.2 Protection of Administrator Passwords (Extended – FPT_APW_EXT)

6.5.2.1 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.

6.5.3 TSF Testing (Extended – FPT_TST_EXT)

6.5.3.1 FPT_TST_EXT.1 TSF Testing (Extended)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [*assignment:* *disk space check, memory size check, port occupancy check and TCP connection check*].

6.5.4 Trusted Update (FPT_TUD_EXT)

6.5.4.1 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 [selection: 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 [selection: 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: published hash] prior to installing those updates.

6.5.5 Time stamps (Extended – FPT_STM_EXT))

6.5.5.1 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 [selection: allow the Security Administrator to set the time].

6.6 **TOE Access (FTA)**

6.6.1 TSF-initiated Session Locking (Extended – FTA_SSL_EXT)

6.6.1.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- terminate the session*]*

after a Security Administrator-specified time period of inactivity.

6.6.2 Session Locking and Termination (FTA_SSL)

6.6.2.1 FTA_SSL.3 TSF-initiated Termination (Refinement)

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

6.6.2.2 FTA_SSL.4 User-initiated Termination (Refinement)

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

6.6.3 TOE Access Banners (FTA_TAB)

6.6.3.1 FTA_TAB.1 Default TOE Access Banners (Refinement)

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

6.7 **Trusted Path/Channels (FTP)**

6.7.1 Trusted Channel (FTP_ITC)

6.7.1.1 FTP_ITC.1 Inter-TSF Trusted Channel (Refinement)

FTP_ITC.1.1 The TSF shall **be capable of using [selection: SSH, TLS** to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [selection*:* [assignment: *network devices (switches and routers)*]]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data.**

FTP_ITC.1.2 The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*assignment: audit service, network device management*].

6.7.2 Trusted Path (FTP_TRP)

6.7.2.1 FTP_TRP.1/Admin Trusted Path (Refinement)

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

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

7 Security Assurance Requirements

This Security Target claims conformance to the Security Assurance Requirements defined in [PP-ND], section 7, table 3.
The description of the SARs is an exact copy of the Network Devices PP [PP-ND] Section 7.

8 TOE Summary Specification

8.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function as well as all of the events identified in Table 4.

In general, the logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent responsible for the event (e.g., user or network host). The logged audit records also include event-specific content that includes at least all of the content required in Table 4.

The TOE includes an internal log implementation that can be used to store and review audit records locally. The audit log is saved in the local database, and the TOE will overwrite previous audit records if the usage of the local storage space for audit data arrives to 80% (default value).

The TOE can be configured to send generated audit records to an external Audit server in to mitigate the possibility of losing audit records.
The TOE protects the audit records and prevents unauthorized modifications or deletion.

The Security audit function is designed to satisfy the following security functional requirements: FAU_GEN.1, FAU_GEN.2, FAU_STG_EXT.1, FAU_STG.1.

8.2 Cryptographic support

The TOE includes a crypto-module providing supporting cryptographic functions:

- Generate RSA asymmetric key pairs
- AES-CBC for encryption
- Generation and verification of RSA 2048-bit signatures.
- SHA-256 hash algorithm
- HMAC-SHA-256 HMAC algorithm
- AES-256 CTR_DRBG as random number generator

The TOE releases the cryptographic key memory either by overwriting with 0 in C++ if the key is no longer used in non-volatile memory or deleting the key reference, and ensuring garbage collector is immediately called after that for volatile memory.

The TOE implements HTTPS using TLS and compliant with RFC 2818. As a server, the TOE can receive the TLS HTTPS connection initiated by the OSS, third-party application to establish secure channel, and the remote users access TOE though web portal by initiating HTTPS connections. The TOE also can act as a TLS client to initiate secure HTTPS connections with other devices.

As a client, the TOE can initiate SSHv2 connections to establish secure channel with the network devices.

The TOE supports SSHv2 interactive command-line administrator sessions.

The TOE supports TLS sessions in conjunction with HTTPS for web-based administrator access. The TOE TLS server supports the cipher suites listed in FCS_TLSS_EXT.1.1 for web-based administrator access.

For web-based administrator access the TOE performs RSA key establishment with key size 2048 bits. As a server, the TOE can receive the TLS HTTPS connection initiated by the OSS, third-party application to establish secure channel.

The Cryptographic support function is designed to satisfy the following security functional requirements: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RGB_EXT.1, FCS_HTTPS_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1., FCS_TLSS_EXT.1.

8.3 Identification and authentication

The TOE is designed to require users to be identified and authenticated before they can access any of the TOE functions.

The TOE password authentication mechanism enforces password composition rules. A minimum password length can be configured from 6 to 15 characters. Passwords can generally contain alphabetic (upper or lower case) characters, numeric characters, and special characters such as any of “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, "~", "`", "=", "+", "|", """, "-", "_", "[", "]", "{", "}", ":", ";", ",", "/", ".", "<", ">", "?". The TOE supports the configuration of password composition policies such as:

- No password complexity requirement;
- Must Contain Letters and Numbers;
- Must Contain Special Characters;
- Must Contain Letters, Numbers, and Special Characters;
- Must Contain Uppercase Letters, Lowercase Letters, Numbers and Special Characters;
- Password Validity Period (Permanent, 30 days, 60 days, 90 days, 12 Months);

Administrators can connect to the TOE via a local console. Local administrators can access the TOE CLI interface via a serial console (direct) connection by using username and password.

When logging via password, only obscured feedback is provided so the password is not visible when the user is inputting it.

The TOE provides the security administrator the ability to specify the maximum number of unsuccessful authentication attempts before administrator is locked out through the administrative CLI. While the TOE supports a range from 3-10.

When the defined number of unsuccessful authentication attempts has been met, the TOE shall prevent the offending Administrator from accessing TOE using any authentication method until unlock is taken by a Security Administrator or an Administrator defined time period has elapsed.

When acting as a TLS client, the TOE validates and authenticates the certificate presented by the client according to RFC 5280.

The Identification and authentication function is designed to satisfy the following security functional requirements: FIA_AFL.1, FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FIA_X509_EXT.1, FIA_X509_EXT.2.

8.4 Security management

The TOE defines an administrator role that can be assigned more granular privileges via defined privilege levels. Each time a new administrative user is defined a user identifier, username, password, and privilege level must be assigned. There are several pre-defined privilege levels (e.g., Security Administrator, Network Administrator, Network Maintainer, Network Viewer) while additional privilege levels can be defined by the TOE user as may be needed for a specific deployment.

The TOE offers command-line interface providing a range of security management functions for use by Security Administrator. Among the functions available to the Security Administrator are those functions that are necessary to manage all aspects of the cryptographic functions of the TOE, those necessary to enable or disable the network services offered by the TOE, and the functions necessary to review the TOE versions, update the TOE components, and also to verify the validity of those updates.

The TSF restricts the ability to enable the functions to perform manual updates to Security Administrators.

In addition, only security administrators have the right to create or delete users in the TOE. While changing the local user privilege level, the configured new level of the local user cannot be higher than that of the login-in user. In this way no user except administrators can change another user to be at the privilege level of administrator, and only administrators have the ability to perform manual update. Therefore, the manual update is restricted to administrators. The TOE uses groups to organize users.

The TOE enforces that:

- Only Security Administrators have right to configure audit servers where audit records are exported to.
- Only Security Administrators have the privilege to choose the trusted channel for external audit server and decide whether transmit the audit data to an external IT entity or not.
- Only Security Administrators have the privilege to modify the behaviour of TOE Security Functions (e.g. cryptographic algorithm, audit server).

The TOE also offers the following functions, which are limited to the Security Administrator:

- Start-up and shutdown the TOE.
- Manage user account definitions (create, delete, modify, and view user attributes that identify authorized users and their associated role).
- Manage password failure constraints (modify and set the threshold for the number of permitted authentication attempt failures).
- Restoration of disabled users (restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures).
- Manage the internal audit log (archive, create, delete, empty, and review the audit trail).
- Manage the cryptographic functionality.

The Security management function is designed to satisfy the following security functional requirements: FMT_MOF.1/ManualUpdate, FMT_MOF.1/Services, FMT_MTD.1/CoreData, FMT_SMF.1, FMT_SMR.2.

8.5 Protection of the TSF

The TOE stores all pre-shared keys, symmetric keys, and private keys in the file system in Flash that can't be read, copy or extract by administrators; hence no interface access is available.

The administrator passwords are stored to configuration file in cryptographic form hashed with *scrypt* algorithms function, including username passwords, authentication passwords, console and virtual terminal line access passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed to anyone through normal interfaces including Security Administrators.

During start-up of the TOE, the TOE first checks the integrity of the firmware, and then runs a series of self-tests to ensure it is performing its cryptographic functions correctly. If any of these checks fails, the device will halt and require administrator intervention to successfully start-up.

From the Web UI, an administrator can check the version of the installed software. The administrator can install, upgrade, and uninstall the software. Before upgrading the software, administrator need to check the integrity of the software installation package through SHA-256*.*

The administrator is able to set the time on the TOE and therefore providing a reliable timestamp.

The Protection of the TSF function is designed to satisfy the following security functional requirements: FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_TST_EXT.1, FPT_TUD_EXT.1, FPT_STM_EXT.1

8.6 TOE access

The TOE can be configured by an administrator to set an interactive session timeout value (any integer value in minutes and also optionally in seconds, the default timeout is 30 minutes). A session that is inactive (i.e., no commands issuing from the remote client) for the defined timeout value will be terminated, both for local and for remote sessions.

The user will be required to re-enter their user id and their password so they can be re-authenticated in order to establish a new session.

The user also has the ability to terminate his own sessions (log out).

The TOE can be configured to display administrator-configured advisory banners that will be displayed in conjunction with user login prompts. The banner contents are configured by a user in the Security Administrator role.

The TOE access function is designed to satisfy the following security functional requirements: FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4, FTA_TAB.1.

8.7 Trusted path/channels

To support secure remote administration, the TOE includes implementations of HTTPS. In each case, a remote host (presumably acting on behalf of an administrator) can initiate a secure remote connection for the purpose of security management. Note that only the local console is available by default and each of these remote administration services can be independently enabled by an administrator.

In the case of HTTPS, the TOE a web interface. To establish a session with the webserver, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to navigate and thus use the webpage to administrate the TOE.

Remote administrators can access the CLI interface via an SSH protocol connection from an SSH client to remotely manage the TOE

As indicated earlier, the TOE can export audit records to an external audit server. In order to protect exported audit records from disclosure or modification, the TOE can be configured to utilize a HTTPS secure channel for this purpose. This protection is initiated by the TOE whenever Audit connections are established for the purpose of exporting audit records.

The TOE makes use of SSH as a client to manage other network devices, such as switches and routers.

The Trusted path/channels function is designed to satisfy the following security functional requirements: FTP_ITC.1, FTP_TRP.1/Admin.

9 Rationales

9.1 Security Objectives Rationale

This rationale consists of a table mapping all the assumptions against security objectives. It is informative only, as it is a representation of the tracing of assumptions to objectives as defined in [PP-ND] adopted in this ST.

9.1.1 Assumptions to Security Objectives Mapping

Threats and assumptions / **Objectives**	**A.PHYSICAL_PROTECTION**	**A.LIMITED_FUNCTIONALITY**	**A.NO_THRU_TRAFFIC_PROTECTION**	**A.TRUSTED_ADMINISTRATOR**	**A.REGULAR_UPDATES**	**A.ADMIN_CREDENTIALS_SECURE**	**A.RESIDUAL_INFORMATION**
OE.PHYSICAL	X						
OE.NO_GENERAL_PURPOSE		X					
OE.NO_THRU_TRAFFIC_PROTECTION			X				
OE.TRUSTED_ADMIN				X			
OE.UPDATES					X		
OE.ADMIN_CREDENTIALS_SECURE						X	
OE.RESIDUAL_INFORMATION							X

Table 5 Threats and Assumptions to Security Objectives Mapping

9.2 Dependency Rationale

This rationale provided in [PP-ND] annex E.1 shows that all dependencies of all security requirements have been addressed.

10 Abbreviations and glossary

[CC]	Common Criteria
[CEM]	Common Evaluation Methodology
[EAL]	Evaluation Assurance Level
[PP]	Protection Profile
[SAR]	Security Assurance Requirement
[ST]	Security Target
[TOE]	Target of Evaluation
[TSS]	TOE Summary Specification
[TSF]	TOE Security Functionality

11 References

[CC31R5P1]	Common Criteria for Information Technology Security Evaluation. Part 1: Introduction to General Model, Version 3.1, Revision 5, April 2016.
[CC31R5P2]	Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, Version 3.1, Revision 5, April 2016.
[CC31R5P3]	Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, Version 3.1, Revision 5, April 2016.
[PP-ND]	collaborative Protection Profile for Network Devices, v.2.2e, 23-03-2020