Ciena Waveserver 5 OS R2.3.12 Security Target

Document Version:1.8

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History:

Version	Date	Changes
Version 0.1	April 8, 2021	Initial Release.
Version 0.2	April 9, 2021	Updates to Section 1.3.2
Version 0.3	April 12, 2021	Updates to Section 2.3 and 5.
Version 0.4	April 13, 2021	Updates to Section 2.3 and 5 and completion of TSS.
Version 0.5	May 11, 2021	Updates based on QA feedback.
Version 0.6	February 18, 2022	Updated and provided additional comments.
Version 0.7	April 25,2022	Added SSHC requirements
Version 0.8	June 2, 2022	Updated ST with SSHC requirements
Version 0.9	September 10, 2022	Removed SSHC requirements
Version 1.0	April 18, 2023	Address ECR comments for Check-in
Version 1.1	April 26, 2023	Address Second Round of ECR Comments for Check-in
Version 1.2	May 17, 2023	Updates to TSS and address ECR Comment
Version 1.3	May 24, 2023	Addressed QA Comments
Version 1.4	June 13, 2023	Updated version of TOE
Version 1.5	September 6, 2023	Addressed ECR comments for checkout
Version 1.6	October 10, 2023	Address ECR comments for checkout
Version 1.7	November 9, 2023	Address ECR comments for checkout
Version 1.8	December 5, 2023	Address ECR comments for checkout

Contents

1 Introduction

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

1.1 Security Target and TOE Reference

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

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Ciena Waveserver 5 OS R2.3.12 Security Target
ST Version	1.8
ST Date	December 5, 2023
ST Author	Acumen Security, LLC.
TOE Identifier	Ciena Waveserver 5
TOE Version	Waveserver OS R2.3.12
TOE Developer	Ciena Corporation
Key Words	Network Device, Ciena, Optical Transport

1.2 TOE Description and Overview

The Ciena Waveserver 5 is a purpose-built network device, data center interconnect (DCI) platform designed to facilitate high-speed, high-capacity connections between data centers. This platform has been designed to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP 2.2e]. The Waveserver 5 incorporates a range of advanced security features to ensure the integrity and confidentiality of network communications. The TOE uses a Marvell CN9130 processor.

While not an exhaustive list, some the main security mechanisms being leveraged include the following. For information on all the supported security mechanisms, please refer to Section 1.2.2:

1. Encrypted SSH Administration: The device supports encrypted SSH connections for secure remote administration, protecting the communication channel between administrators and the device from unauthorized access and eavesdropping.

2. RADIUS via TLS: The Waveserver 5 is capable of using RADIUS authentication with TLS encryption, ensuring the secure transmission of login credentials and providing an added layer of protection for user authentication.

3. Encrypted Syslog Traffic: The platform can encrypt syslog traffic via TLS to a syslog server, safeguarding the privacy and confidentiality of logs and preventing unauthorized access to sensitive log data.

4. NTP with SHA Authentication: The Waveserver 5 supports the use of NTP with SHA authentication, providing a secure method for time synchronization across network devices and reducing the risk of time-based attacks.

These highlighted security mechanisms, along with other measures, contribute to the Ciena Waveserver 5's ability to not only meet the collaborative Protection Profile for Network Devices, Version 2.2e, but also deliver a comprehensive and secure networking solution for end users.

Waveserver 5 front panel:

Waveserver 5 rear panel:

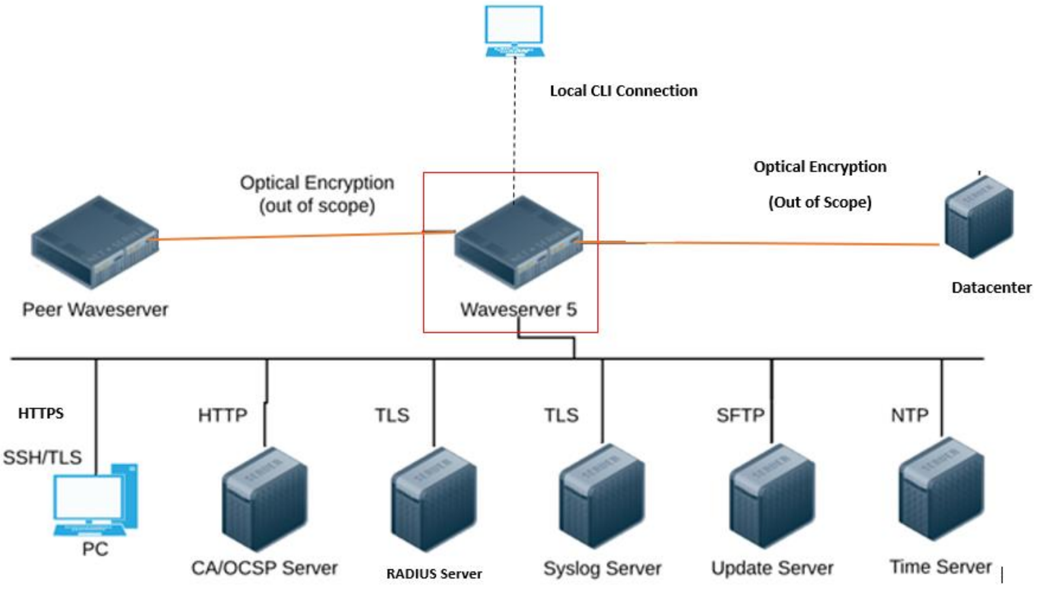

Figure 1 – Representative TOE Deployment

Table 2 – Device Information

Waveserver 5 Appliance	Hardware Specifics
Processor	Marvell CN9130
Enclosure	Dual rack unit
Power Supply	AC or DC power AC input voltage range: 100 Vac to 277 Vac DC input voltage range: 180 Vdc to 300 Vdc Power consumption: 0.4 W/Gb
Environment Characteristics	Normal operating temperature: -5 °C to +45 °C (23 °F to 113 °F)

1.2.1 Physical Boundaries

The TOE boundary is the hardware appliance, which is comprised of hardware and software components. It is deployed in an environment that contains the various IT components as depicted in Figure 1 above highlighted in red. The TOE guidance documentation can be found on the Ciena website: https://www.ciena.com. An account is required to access the guidance documents and any software updates.

The TOE is shipped with the software pre-installed on it. Software updates are available for download from the Ciena website.

1.2.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP.

1.2.2.1 Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in Table 11. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE is capable of storing audit events locally and exporting them to an external syslog server using TLS v1.1 or TLS v1.2 protocol. Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event. The syslog server supports the following severity levels: emergency, alert, error, warning, notice, info and debug. In order to enable the logging to syslog server, a user must be logged in with an administrative access privilege and provision the settings to use a syslog server.

1.2.2.2 Cryptographic Support

The TOE leverages Waveserver 5 Cryptographic Library for all cryptographic services. The related CAVP validation details are provided in Table 13. All algorithms claimed have CAVP certificates. The operating system is Linux Kernel v4.14. The TOE leverages the Waveserver 5 Cryptographic Library for its cryptographic functionality.

1.2.2.3 Identification and Authentication

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password-based authentication and public key based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.

1.2.2.4 Security Management

The TOE supports local and remote management of its security functions including:

- Local console CLI administration.
- Remote CLI administration via SSHv2 and HTTPS/TLS.
- Timed user lockout after multiple failed authentication attempts.
- Password configurations.
- Role Based Access Control – Superuser (Security Administrator), Admin and limited user (User).
- Configurable banners to be displayed at login.
- Timeouts to terminate administrative sessions after a set period of inactivity.
- Protection of secret keys and passwords.

1.2.2.5 TOE Access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 10 minutes of session inactivity. An administrator can terminate their GUI session by clicking on the logout button. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

1.2.2.6 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys and private keys from unauthorized disclosure. Passwords are stored in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE maintains the date and time by the setting of the time manually by a security administrator or by synchronizing with an NTP server configured by a security administrator.

1.2.2.7 Trusted Path/Channels

The TOE supports TLS v1.1 or TLS v1.2 for secure communication to the following IT entities: Syslog server and Radius server. The TOE supports HTTPS/TLS (WebUI) and SSH v2 (remote CLI) for secure remote administration.

1.2.3 TOE Documentation

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

- Ciena Waveserver 5 Security Target, Version 1.8, December 5, 2023 [ST]
- Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document, Version 1.3, November 9, 2023 [AGD]

1.3 TOE Environment

The following environmental components are required or not required to operate the TOE in the evaluated configuration:

Table 3 – Environmental Components

Component	Required	Purpose/Description
Terminal	Yes	Local workstation directly connected to the console interface of the Waveserver. Configuration over the Waveserver CLI is possible here.
PC	Yes	Remote workstation used to administer the Waveserver. Primary administration is via a remote CLI protected with SSH. A webUI is also available and protected with HTTPS. This is primarily available for monitoring.
Syslog Server	Yes	Remote audit server used to offload logs from the Waveserver. Communication is protected over TLS.
Certificate Authority	Yes	Remote CA used for various certificate related operations, such as, signing CSRs and issuing external server certificates.
OCSP Server	Yes	Revocation server supporting certification authentication. The product supports OCSP certificate revocation. Communication is over HTTP.
RADIUS Server	Yes	External RADIUS server. It is used by the Waveserver in support of administrative authentication. The communications are via RADSEC which is RADIUS protected with TLS.
Time Server	No	Optional Component: External time server used to synchronize time with other entities. Communication is protected using NTP authentication.
Update Server	No	Optional Component: Update server is used to push updates to the TOE

1.4 Product Functionality not Included in the Scope of the Evaluation

The following product functionalities are not included in the CC evaluation:

- Peer Waveserver and the datacenter connection is used for communication over the optical network and protected via encryption. This connection is not part of the evaluated configuration.
- The following interfaces are not in scope of the evaluation:
    - NETCONF

- gRPC
- RESTCONF
- Swagger
- FTP
- SFTP with Update server

2 Conformance Claims

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

2.1 CC Conformance Claims

The TOE is conformant to the following:

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

2.2 Protection Profile Conformance

This ST claims exact conformance to the following:

- Collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [CPP_ND_V2.2E]

2.3 Conformance Rationale

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

2.3.1 Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v2.2e have been considered. Table identifies all applicable TDs.

Table 4 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0792: NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	Yes	
TD0790: NIT Technical Decision: Clarification Required for testing IPv6	Yes	
0670 – NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
0639 – NIT Technical Decision for Clarification for NTP MAC Keys	Yes	
0638 – NIT Technical Decision for Key Pair Generation for Authentication	Yes	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
0636 – NIT Technical Decision for Clarification of Public Key User Authentication for SSH	No	SSH Client is not claimed in this evaluation
0635 – NIT Technical Decision for TLS Server and Key Agreement Parameters	Yes	
0633 – NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	No	The TOE does not support IPsec and is not claimed.
0632 – NIT Technical Decision for Consistency with Time Data for vNDs	No	TOE is not virtual
0631 – NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
TD0592: NIT Technical Decision for Local Storage of Audit Records	Yes	
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	No	TOE is not virtual
TD0581 – NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
TD0580 – NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
TD0572: Restricting FTP_ITC.1 to only IP address identifiers	Yes	
TD0571: Guidance on how to handle FIA_AFL.1.	Yes	
TD0570: clarification about FIA_AFL.1.	Yes	
TD0569: Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	No	DTLSS is not claimed.
TD0564: Vulnerability Analysis Search Criteria.	Yes	
TD0563: Clarification of audit date information	Yes	
TD0556: NIT Technical Decision for RFC 5077 question	No	TOE doesn't support session resumption or session tickets
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	No	TOE doesn't support session resumption or session tickets
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
TD0546: DTLS - clarification of Application Note 63	No	DTLS is not claimed.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0538: Outdated link to allowed-with list	Yes	
TD0537: Incorrect reference to FCS_TLSC_EXT.2.3	Yes	
TD0536: Update Verification Inconsistency	Yes	
TD0528: Missing EAs for FCS_NTP_EXT.1.4	Yes	
TD0527: Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	

3 Security Problem Definition

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

3.1 Threats

The threats included in Table 4 are drawn directly from the PP specified in Section 2.2.

Table 4 – Threats

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

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

3.2 Assumptions

The assumptions included in Table 5 are drawn directly from PP specified in Section 2.2.

Table 5 – Assumptions

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

ID		Assumption
A.TRUSTED_ADMINISTRATOR		The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES		The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE		The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION		The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3 Organizational Security Policies

The OSPs included in Table 6 are drawn directly from the PP specified in Section 2.2.

Table 6 – OSPs

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

4 Security Objectives

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

4.1 Security Objectives for the Operational Environment

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

Table 7 – Security Objectives for the Operational Environment

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

4.2 Security Objectives Rationale

The Protection Profiles to which this ST claims conformance are as follows:

- NDcPP v2.2e, Section 5

5 Security Requirements

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

Table 8 – SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_SSHS_EXT.1	SSH Server Protocol
FCS_TLSC_EXT.1	TLS Client Protocol without Mutual Authentication
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSS_EXT.1	TLS Server Protocol Without Mutual Authentication
FCS_TLSS_EXT.2	TLS Server Support for Mutual Authentication
FCS_NTP_EXT.1	NTP Protocol
FIA_AFL.1	Authentication Failure Management
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Password-based Authentication Mechanism
FIA_UAU.7	Protected Authentication Feedback
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
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MOF.1/Services	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTF.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_STM_EXT.1	Reliable Time Stamps
FPT_TUD_EXT.1	Trusted Update
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_TAB.1	Default TOE Access Banner

Requirement	Description
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1/Admin	Trusted Path

5.1 Conventions

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

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of "EXT" after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

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

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

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

c) *All administrative actions comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*
- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
- *Resetting passwords (name of related user account shall be logged).*
- *[no other actions]*;

d) *Specifically defined auditable events listed in Table* 9

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 9*.*

Table 9 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start-up of the audit function	None
	Shutdown of the audit function	None

Requirement	Auditable Events	Additional Audit Record Contents
	Administrative Login	Name of user account shall be logged if individual user accounts are required for Administrators
	Administrative Logout	
	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 cryptographic keys	In addition to the action itself, a unique key name or key reference shall be logged
	Changing of cryptographic keys	
	Deleting of cryptographic keys	
	Resetting passwords	Name of related user account shall be logged.
FAU_GEN.2	None	None
FAU_GEN_EXT.1	None	None
FAU_STG_EXT.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_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
FCS_RBG_EXT.1	None	None
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSC_EXT.2	None	None
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSS_EXT.2	Failure to authenticate the client	Reason for failure
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
FIA_X509_EXT.3	None	None

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None
FMT_MTD.1/CoreData	All management activities of TSF data	None
FMT_SMF.1	All Management 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_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	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_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism	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

5.2.1.2 FAU_GEN.2 User Identity Association

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

5.2.1.3 FAU_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 [overwrite previous audit records according to the following rule: *[oldest audit events being replaces with new ones]*] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

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

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

]

5.2.2.2 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 "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526]

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

- For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [
  - logically addresses the storage location of the key and performs a [single, overwrite consisting of [zeroes];

that meets the following: *No Standard*

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

FCS_COP.1.1/DataEncryption
The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [CBC, CTR, GCM] *mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3,* [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].

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

FCS_COP.1.1/SigGen
The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm [

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048, 3072, or 4096 bits]]
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256, 384 or 521 bits]

]
that meet the following: [

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

].

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

FCS_COP.1.1/Hash
The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and **message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

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

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512*]* and cryptographic key sizes *[256, 384, 512 (in bits) used in HMAC]* **and message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”*.

5.2.2.8 FCS_HTTPS_EXT.1 HTTPS Protocol

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

FCS_HTTPS_EXT.1.2
The TSF shall implement the HTTPS protocol using TLS.

FCS_HTTPS_EXT.1.3
If a peer certificate is presented, the TSF shall [not establish the connection] if the peer certificate is deemed invalid.

5.2.2.9 FCS_RBG_EXT.1 Random Bit Generation

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

FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[1]* platform-based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.2.2.10 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [*NTP v4 (RFC 5905)*].

FCS_NTP_EXT.1.2
The TSF shall update its system time using [

- Authentication using [*SHA1*] as the message digest algorithm(s);
  ].

FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.2.2.11 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol in accordance with: RFCs *4251, 4252, 4253, 4254*, *[*4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308 section 3.1, 8332*].*

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

FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than *[256000]* 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: [aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521] as its public key algorithm(s) and rejects all other public key algorithms.

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

FCS_SSHS_EXT.1.7
The TSF shall ensure that [diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] 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.

5.2.2.12 FCS_TLSC_EXT.1 TLS Client Protocol without Mutual Authentication

FCS_TLSC_EXT.1.1
The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

] and no other ciphersuites.

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv6 address in the 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 [

- Not implement any administrator override mechanism

].

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

5.2.2.13 FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

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

5.2.2.14 FCS_TLSS_EXT.1 TLS Sever Protocol Without Mutual Authentication

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

[

- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_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 [TLS 1.1].

FCS_TLSS_EXT.1.3
The TSF shall perform key establishment for TLS using [ECDHE curves [secp256r1, secp384r1, secp521r1] and no other curves]].

FCS_TLSS_EXT.1.4
The TSF shall support [no session resumption or session tickets].

5.2.2.15 FCS_TLSS_EXT.2 TLS Sever Support for Mutual Authentication

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

FCS_TLSS_EXT.2.2
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSS_EXT.2.3
The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[2-10]* 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 [prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

5.2.3.2 FIA_PMG_EXT.1 Password Management

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

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

b) Minimum password length shall be configurable to between [*8*] and [1*28*] characters.

5.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1
The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

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

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

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1
The TSF shall provide a local [password-based, SSH public key-based], [*RADIUS*] authentication mechanism to perform local administrative user authentication.

5.2.3.5 FIA_UAU.7.1 Protected Authentication Feedback

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

5.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates.**
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev
The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.7 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].

Application Note: This SFR has been updated as per TD0537.

5.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1
The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2
The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour

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

5.2.4.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

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

5.2.4.3 FMT_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1.1/Services
The TSF shall restrict the ability to **start and stop services** to *Security Administrators*.

5.2.4.4 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData
The TSF shall restrict the ability to manage the *TSF data to Security Administrators.*

5.2.4.5 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys
The TSF shall restrict the ability to *manage* the *cryptographic keys* to *Security Administrators*.

5.2.4.6 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [*digital signature*] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- [
    - Ability to start and stop services;
    - Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);
    - Ability to modify the behaviour of the transmission of audit data to an external IT entity;
    - Ability to re-enable an Administrator account;
    - Ability to set the time which is used for time-stamps;
    - Ability to configure NTP;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
    - Ability to manage the cryptographic keys;
    - Ability to import X.509v3 certificates to the TOE's trust store;

    ].

5.2.4.7 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1
The TSF shall maintain the roles:

- *Security Administrator.*

FMT_SMR.2.2
The TSF shall be able to associate users with roles.

FMT_SMR.2.3
The TSF shall ensure that the conditions

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

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FTP_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.

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

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

5.2.5.3 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2
The TSF shall [allow the Security Administrator to set the time, synchronise time with an NTP server].

5.2.5.4 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), at the request of the authorised user, at the conditions *[by performing a system or card level restart command]*] to demonstrate the correct operation of the TSF: [*Software integrity test, AES Known Answer Test, HMAC-SHA-256/384/512 Known Answer Test, SHA-256/384/512 Known Answer Test, RSA Signature Known Answer Test, ECDSA Signature Known Answer Test, RNG Known Answer Test*].

5.2.5.5 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1
The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

FPT_TUD_EXT.1.2
The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

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

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1
The TSF Shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.2.6.2 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.*

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 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 use of the TOE.

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

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

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

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

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin
The TSF shall **be capable of using [<u>SSH, TLS, HTTPS</u>] to** provide a communication path between itself and **authorized** <u>remote</u> **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 <u>remote **Administrators**</u> to initiate communication via the trusted path.

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

5.3 TOE SFR Dependencies Rationale for SFRs

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

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and any relevant EPs/Modules/Packages, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 10.

Table 10 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functionality specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.5 Assurance Measures

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

Table 11 – TOE Security Assurance Measures

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

6 TOE Summary Specifications

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

Table 12 – TOE Summary Specification SFR Description

Requirement	TSS Description
FAU_GEN.1	The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in Table 11. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event. All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection. Administrative tasks of generating, deleting cryptographic keys contain the necessary audit information as mandated by FAU_GEN.1.1. Audit events for deleting keys, generating keys are listed below: SSH server key delete: eventlog: ssh [CienaWOS@1271.3 TIME-FORMAT="uTC" EVENT-ID="29-024" EVENT-NAME="SshKeyDelete" EVENT-ORIGIN="ssh"] Ssh server key delete eventlog: ssh [CienaWOS@1271.3 TIME-FORMAT="uTC" EVENT-ID="29-013" EVENT-NAME="GenerateKey" EVENT-ORIGIN="ssh"] Ssh Generate Key eventlog: DeviceCertificateAdd [CienaWOS@1271.3 TIME-FORMAT="uTC" EVENT-ID="24-036" EVENT-NAME="DeviceCertificateAdd" EVENT-ORIGIN="security"] X.509 Device Certificate Name test Installed
FAU_GEN.2	For audit events that result from actions of identified users, the TOE is able to associate each auditable event with the identity of the user that caused the event.
FAU_STG_EXT.1	The TOE can be configured to export audit events securely to a syslog server using TLS v1.2 or TLS v1.1 protocol using X.509 certificates. The TOE stores up to 4 files each holding up to 10,000 audit data locally on compact flash. When a file is full, a new file is created. When the local data is full, the oldest audit events are overwritten to allow new audit events to be created. Security Administrators can access the audit events and have the ability to clear the audit events. This way, audit events are protected against unauthorized access. The TOE transmits audit data to an external syslog server in real time. If there is a TLS connection failure, the TOE will continue to store local audit events on the TOE and will transmit any locally stored contents when connectivity to the syslog server is restored.
FCS_CKM.1	RSA and ECC schemes are used in support of TLS communications. The TOE supports RSA key sizes of 2048 and 3072 bits. RSA keys are used in support of digital signature for both TLS and SSH communications. The TOE supports Elliptical NIST curve sizes of P-256, P-384 and P-521 conforming to Cryptographic key generation conforming to FIPS PUB 186-4

Requirement	TSS Description
	Digital Signature Standard (DSS)”, Appendix B.4. The Elliptic keys are used in support of ECDH key exchange. The TOE supports FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and RFC 3526 and it used for key generation. The TOE supports DH group 14 as a key exchange method for SSH. Please refer to Table 13 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.
FCS_CKM.2	The TOE supports Cryptographic Key Establishment using the following schemes: Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”; FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526] ECC schemes are used in support of TLS communications. FFC “safe prime” groups are used as an SSH key exchange method in support of FCS_SSHS_EXT.1.7. The TOE acts as both a sender and receiver for Elliptic curve-based key establishment scheme. Please refer to Table 13 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.
FCS_CKM.4	The TOE satisfies all requirements as specified in FCS_CKM.4 of NDcPP v2.2e for destruction of keys. Please refer to Table 14 Cryptographic Key Destruction. The TOE does not support non-volatile memory storage device-level swap and cache files therefore there is nothing to examine or test. The TOE performs a secure erase of non-volatile memory storage using an interface that is supported by the NVRAM device.
FCS_COP.1/DataEncryption	The TOE supports AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772. The AES key sizes supported are 128 bits and 256 bits and the AES modes supported are: CBC, CTR and GCM. All AES 128- and 256-bit key lengths are supported by CAVP certificate #A3284. Only 256 bits is supported by CAVP certificate #A3283. Please refer to Table 13 Cryptographic Algorithm Certificates for NIST CAVPs for AES.
FCS_COP.1/Hash	 The TOE supports Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used in TLS and SSH connections. The following hashing algorithms supported: SHA-1, SHA-256, SHA-384 and SHA-512. The message digest sizes supported are: 160, 256, 384 and 512 bits.

<table>
<tr><th>Requirement</th><th>TSS Description</th></tr>
<tr><td></td><td>Please refer to Table 13 Cryptographic Algorithm Certificates for NIST CAVPs for SHS.</td></tr>
<tr><td>FCS_COP.1/KeyedHash</td><td>The TOE supports Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2. HMAC algorithms is used in support of TLS and SSH sessions.
<table>
<tr><td>HMAC Algorithms</td><td>Hash Functions</td><td>Block Sizes</td><td>Key Lengths</td><td>MAC Lengths</td></tr>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
<tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>1024 bits</td><td>512 bits</td><td>512 bits</td></tr>
</table>

Please refer to Table 13 Cryptographic Algorithm Certificates for NIST CAVPs for HMAC.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides Cryptographic signature generation and verification in accordance with the following cryptographic algorithms:
• RSA digital signature conforming to 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.
• The RSA key sizes supported are: 2048, 3072 and 4096 bits.
• The TOE uses Elliptical curve digital signature algorithm conforming to 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.
• The Elliptical curve key size supported is 256, 384 and 521 bits.

Please refer to Table 13 Cryptographic Algorithm Certificates for NIST CAVPs for RSA and ECDSA.</td></tr>
<tr><td>FCS_HTTPS_EXT.1</td><td>The TOE supports remote management of the TOE over an HTTPS connection using TLS v1.2 implementation. In this scenario, the TOE acts as a server. The HTTPS protocol complies with RFC 2818.</td></tr>
<tr><td>FCS_NTP_EXT.1</td><td>The TOE supports the use of NTP server for time updates where the following NTP version: NTPv4 (RFC 5905) is supported. The TOE updates its system time using authentication using SHA1 as the message digest algorithm to verify the authenticity of the timestamp and the TOE does not update the timestamps from broadcast and/or multicast addresses.
The TOE supports configuration of three (3) NTP time sources in the Operational Environment.</td></tr>
<tr><td>FCS_RBG_EXT.1</td><td>The TOE uses Hash_DRBG (SHA-256) conforming to ISO/IEC 18031:2011.
The Hash_DRBG is seeded with HW_TRNG with a minimum of 256 bits of entropy. Since this is third party TRNG, the vendor does not have access to the collection of the raw noise. The 3rd party claims that there is 0.73 bits of entropy per symbol for a symbol size of one bit after digitization. The 3rd party claims an output of at least 7.51729 bits per byte, or 30.069 bits of min entropy per 32-bit block. The 3rd party vendor has received an Entropy Source Validation (ESV) certificate from CMVP with Entropy certificate #E23.</td></tr>
</table>

Requirement	TSS Description
	https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/23
FCS_SSHS_EXT.1	The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308 section 3.1, and 8332. The TOE supports password-based authentication and public key authentication. The following public key algorithms: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521. This list is conforming to FCS_SSHS_EXT.1.5. The TOE accepts packet size up to 256K and meets the requirements of RFC 4253. The TOE supports the following encryption algorithms: aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com for SSH transport. There are no optional characteristics specified for FCS_SSHS_EXT.1.4. This list is identical to those claimed for FCS_SSHS_EXT.1.4. The TOE supports the following data integrity MAC algorithms: hmac-sha2-256, hmac-sha2-512 and implicit. This list corresponds to the list in FCS_SSHS_EXT.1.6. The TOE supports the following key exchange algorithms: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521. This list corresponds to the list in FCS_SSHS_EXT.1.7. The TOE is capable of rekeying. The TOE verifies the following thresholds: • No longer than one hour • No more than 1GB of transmitted data The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey. The TOE can be configured to bind a local user with a public key. When the user logs in via SSH client, the authenticating client proves it holds the corresponding private key by providing a signature (encrypted message) that the server will verify using the public key. As per https://datatracker.ietf.org/doc/html/rfc4252#section-7
FCS_TLSC_EXT.1	The TOE supports TLS v1.2 and TLS v1.1 and rejects all other TLS and SSL versions. The TOE supports the following ciphersuites: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 The TOE shall verify the peer certificate fingerprint against a configured value and verify certificate fields against locally configured peer DNS name or IP address (Subject Name Authorization) as per RFC6125 Section 6, IPv4 address in CN or SAN and IPv6 address in CN or SAN. The TOE does support wildcards. The TOE supports the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. This behavior is performed by default. The TSF shall validate the extendedKeyUsage field according to the following rules:

Requirement	TSS Description
	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 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 TOE processes the incoming connection and then performs the CN validation using the OpenSSL library and performs the translation to canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) using standard Linux inet utilities to convert
FCS_TLSC_EXT.2	The TOE supports TLS v1.2 and TLSv1.1 protocol for use with X.509v3 based authentication and rejects all other TLS and SSL versions. The TOE supports the following ciphersuites: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. For TLS mutual authentication, both server-side and client-side certificates are utilized. Mutual Authentication shall be performed when the TOE acts as a TLS Server or Client. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: RFC 5280 certificate validation and certificate path validation supporting a **minimum path length of three certificates**. The certificate path must terminate with a trusted CA certificate. The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. The TOE only treats a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. The revocation check is performed by submitting a request to the OCSP responder and verifying the responder's signed response. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection.

Requirement	TSS Description
	OCSP revocation status checks take place wherever a TLS Certificate connection is implemented.
FCS_TLSS_EXT.1	The TOE supports the following ciphersuites: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 The TOE will deny connections from clients requesting SSL v2.0, SSL v3.0, TLS v1.0 and TLS v1.1. The TOE performs key establishment for TLS using ECDHE curves: secp256r1, secp384r1, secp521r1. The TOE does not support session resumption or session tickets. The TOE configuration of OpenSSL server has an option to specify the minimum version of TLS that should be accepted. Once the OpenSSL server is running it enforces that version control through restricted handshake options in the negotiations with the TLS client
FCS_TLSS_EXT.2	The TOE supports TLS v1.2 protocol with mutual authentication for use with X.509v3 based authentication. The TOE supports the following ciphersuites: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 The ciphersuites specified are those listed in FCS_TLSS_EXT.2. The TOE denies connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1. The TOE implements EC Diffie-Hellman supporting NIST curves: secp256r1, secp384r1, secp521r1. The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Mutual Authentication shall be performed when TOE acts as TLS Server or Client. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates. • The certificate path must terminate with a trusted CA certificate. The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE • The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. The TSF shall validate the extendedKeyUsage field according to the following rules: 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.

Requirement	TSS Description
	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 The TOE only treats a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. The revocation check is performed by submitting a request to the OCSP responder and verifying the responder's signed response. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection. The TOE supports DNS name and IP addresses as its reference identifiers. When the syslog client receives an X.509 certificate from their respective servers, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails and the channel is terminated. If there are no SANs of the correct type in the certificate, then the TSF will compare the reference identifier to the Common Name (CN) in the certificate Subject. If there is no CN, then the verification fails and the channel is terminated. If the CN exists and does not match, then the verification fails and the channel is terminated. Otherwise, the reference identifier verification passes and additional verification actions can proceed. The TOE does support wildcards. The does not support session resumption or session tickets. The TOE does not support any fallback authentication for new TLS connections.
FIA_AFL.1	The Administrator can configure the maximum number of failed attempts for the CLI interface. The lockout feature can be configured from 2-10 unsuccessful attempts. When the defined number of unsuccessful attempts have been met, the TOE will not allow the user to login until the defined time period has elapsed. If the lockout attempts is set to, for example, 5 attempts, then the user will be locked out after the 5th consecutive failed login attempt. This means that the 6th and subsequent attempts will fail to gain access to the TOE even if the credential being offered is correct. The authentication failures cannot lead to a situation where no administrator access is available as the local CLI access would be accessible to the user as the local CLI cannot be locked out.
FIA_PMG_EXT.1	The TOE provides the following password management capabilities for administrator passwords; • Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [“ ?”, “ ‘ “, “, “ + “, “ / “, “ : ”, “ ; “, “ < “, “ > “, “ = “, “ [“, “] “, “, “ ~ “, “ { “, “ } “, and “ |” • Minimum password lengths shall be configurable to 8 characters to maximum of 128 characters. The default minimum password length is 8 characters.
FIA_UIA_EXT.1	The TOE does not permit any actions prior to Administrators logging into the TOE. They are able to view the banner at the login prompt. Administrative access to the TOE is facilitated through one of several interfaces:

Requirement	TSS Description
	• Connecting to the console port using RJ45-DB9 cable or USB-C-to-USB-C, USB-C-to-USB-A cables for the USB-C port. • Remotely connecting to each appliance via SSHv2 or RADsec via TLS • Remotely connecting to appliance WebUI via HTTPS/TLS Regardless of the interface at which the administrator interacts, the TOE prompts the user for a username and password. When the user provides the correct username and password, this is compared to the known user database and if they match then the user is granted access. Otherwise, the user will not be granted access to the TOE. The TOE does not provide a reason for failure in the cases of a login failure. For remote administration, the TOE supports RSA public key authentication and password based authentication. If the user uses public key based authentication and it is successful then the user is granted access to the TOE. If the user uses password based authentication and they provide valid username and password then the user is granted access to the TOE. If the user enters invalid user credentials, they will not be granted access and will be presented the login page.
FIA_UAU_EXT.2	The TOE provides a local password based authentication mechanism to perform local administration user authentication.
FIA_UAU.7	For all authentication at the local CLI the TOE displays only "*" characters when the administrative password is entered so that the password is obscured.
FIA_X509_EXT.1/Rev	The TOE supports mutual authentication using X.509 certificates conforming to RFC 5280. Mutual Authentication is performed when Waveserver acts as TLS Server. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates. • The certificate path must terminate with a trusted CA certificate. The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE • The TSF shall validate the revocation status of the certificate using the Online Certificate Status Protocol (OCSP) as specified in RFC 6960. The TSF shall validate the extendedKeyUsage field according to the following rules: 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 If it is a customer enrolled certificate, the validity period of the certificate is verified at the time of installation as well as a periodic checks is used to ensure validity. When the TOE receives a remote certificate during the secure channel establishment (syslog or RADIUS), the validity of the remote entity certificate is verified. The TOE also verifies the chain of trust by validating each certificate contained in the chain and verifying that a certificate path consists of trusted

Requirement	TSS Description
	CA certificates and verify the validity of the certificates. These checks are done prior to loading the certificates onto the TOE. The revocation check is performed by submitting a request to the OCSP responder and verifying the responder's signed response. If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection. Revocation checking is performed when the TOE receives a server certificate from a TLS server or client (in mutually authenticated connections). The check is performed on all certificates in the chain except for the Root. Revocation checking is handled the same way on authentication for TLS servers and RADIUS connections.
FIA_X509_EXT.2	X.509 certificate can be used to authenticate and establish secure communication channel for RADIUS, and Syslog servers. The X.509 certificates are also used for establishing secure communication using HTTPS/TLS for the Web GUI. The TOE supports RSA based certificates and ECC based certificate in PKCS#12. The TOE supports X509 certificates to authenticate. RSA Based Certificates. The supported RSA key size shall be 2048 bits and 3072 bits. The TOE supports the following signing algorithms for RSA based certificates: RSA with SHA256 RSA with SHA384 RSA with SHA512 ECC Based Certificate The supported Elliptic Curves are: secp256 secp384 secp521 The TOE supports the following signing algorithms for ECC based certificates: • ECDSA with SHA256 • ECDSA with SHA384 • ECDSA with SHA512 The TOE allows each TLS service (RADIUS, Syslog and HTTPS/TLS) to be configured with its own certificate. Once a certificate is configured for RADIUS server, that certificate will be used for all RADIUS server connection authentication. Likewise, once a certificate is configured for TLS Syslog, that certificate will be used for all TLS Syslog collector server connection authentication. Finally, once a certificate is configured for HTTP Server, that certificate will be used for all HTTPS connection authentication. The TOE allows user to specify one X.509 Certificate/Private Key to be used for authentication with remote TLS Syslog server and RADIUS server. The TOE when operating as a TLS Client will check the validity of the TLS Server certificate prior to making a TLS connection with the TLS server. The TOE when operating as a TLS Server will check the validity of the TLS Client certificate prior to making a TLS connection with the TLS client. The X.509 certificate validation is determined based on reference ID verification, certificate path, extendedKeyUsage field, certificate expiry date and the certificate revocation status.

Requirement	TSS Description
	If the TOE is unable to establish a connection to OCSP responder to determine the validity of a certificate, the TOE will not accept the certificate thus not establishing the connection. The TOE chooses which certificate to use by the admin configuring them and then importing the trusted CA onto the TOE truststore. Any certificate signed by the trusted CA is valid unless other factors are accounted for (OCSP revocation, certificate modification, invalid EKU in server certificates, etc.)
FIA_X509_EXT.3	The CSR includes a mandatory auto generated public key and a mandatory user provisioned Common Name. The TOE allows the user to optionally enter the following information in the CSR: • Company Name or Organization (O); • Department or Organization Unit (OU); • Country (C); The TOE can import and validate the certificate chain of the CA that signs the CSR response. The CSR response shall also be validated against the current outstanding CSR signing request. It shall be removed once the corresponding CSR response is imported and validated. The TOE is capable of generating a Certificate Request as specified by RFC 2986. The TOE does not support the “device-specific information” within Certificate Request message.
FMT_MOF.1/ManualUpdate	Only Security Administrators can perform manual software updates.
FMT_MOF.1/Functions	The TSF ensures that only Security Administrators possess the authority to determine and modify the behavior of this function. This means only Security Administrators can configure, enable, or disable the transmission of audit data to external entities. The TSF restricts the ability to determine and modify the behavior of audit data handling solely to Security Administrators. This ensures that the management and handling of audit records, such as its collection, storage, or analysis, are under the control of qualified administrative roles. The TSF will overwrite the oldest audit records with new ones. This ensures that the most recent audit events are always retained in the storage while older events are cyclically replaced. This overwriting behavior is in line with ensuring continuous auditing even when storage constraints are reached, and only Security Administrators have the authority to determine or modify this behavior.
FMT_MOF.1/Services	The following details are the services the Security Administrator has the authority to start and stop: 1. Syslog TLS 2. RADsec via TLS 3. SSH Administrator Access 4. NTP Synchronization
FMT_MTD.1/CoreData	The TOE implements Role Based Access Control (RBAC). Administrative users are required to login before being provided with access to any administrative functions. The TOE restricts the ability to manage the TOE to Security Administrators.

Requirement	TSS Description
	The TOE maintains the following roles: Security administrator (super user), Admin user, and User (Limited user). Each role defined has a set of permissions that will grant them access to the TOE data. The TOE supports handling of X.509v3 certificates and implements a trust store. The Security administrator is the only one authorized to perform actions like import, export and delete certificates and also manage trusted CAs.
FMT_MTD.1/CryptoKeys	The Security Administrator is authorized to manage: • X509 certificates and Certificate Authorities (CAs) 1. Import 2. Export 3. Delete • SSH public keys 1. Import 2. Delete • Passwords 1. Create 2. Reset These keys are managed via a command line interface, which provides granular control over key management (ability to import SSH keys, export cryptographic keys, and delete keys). Importantly, only the trusted Security Administrator is allowed to manage these keys. They can also set up Network Time Protocol (NTP) connections utilizing a SHA1 message digest algorithm, ensuring synchronized timekeeping across devices.
FMT_SMF.1	The Security Administrator (Super user) has the following privileges: Can configure user accounts and manage users and their associated privileges. Ability to administer the TOE locally and remotely. Ability to configure the access banner. Ability to configure the session inactivity time before session termination or locking. Ability to update the TOE, and to verify the updates using digital signatures capability prior to installing those updates. Ability to configure the authentication failure parameters. Ability to set the time which is used for time-stamps. Ability to configure the cryptographic functionality; Ability to re-enable an Administrator account; Ability to set the time which is used for time-stamps; Ability to configure NTP; 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 import X.509v3 certificates to the TOE's trust store; The User (Limited user) has the following privileges: • Able to carry out system monitoring and gather information about the configuration and performance of the system. • Can change their own password, but not other user's passwords.
FMT_SMR.2	The TOE maintains the following user roles: Super user (Security Administrator), Admin and Limited user (User). The Security Administrator is able to manage the TOE both locally and remotely.
FPT_APW_EXT.1	All passwords are stored in a secure directory that is not readily accessible to administrators. The passwords are stored as SHA-512 salted hash.

Requirement	TSS Description
FPT_SKP_EXT.1	The TOE stores all private keys in a secure storage and is not accessible through an interface to administrators. Refer to section 7 Cryptographic Key Destruction, Table 18 Zeroization Table for all detail on key storage**.**
FPT_STM_EXT.1	The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware. The following security functions make use of the time: Audit events Session inactivity X.509 certificate expiration validation
FPT_TST_EXT.1	All crypto algorithms used by the management interface must go through power up self-tests (KAT) before they can be used to provide service. The TOE executes the following power-on self-tests: • Software integrity test – the digital signature of software is validated to ensure its authenticity and integrity before the software is loaded into memory for execution. • AES Known Answer Test – the AES encryption and AES decryption algorithms are tested using test vectors. The results are compared against pre-computed results to ensure the algorithms are operating properly. • HMAC-SHA-256/384/512 Known Answer Test – the HMAC algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • SHA-256/384/512 Known Answer Test – the SHA algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • RSA Signature Known Answer Test – the RSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • ECDSA Signature Known Answer Test – the ECDSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • RNG Known Answer Test – the RNG is seeded with a pre-determined entropy and the RNG output is compared with output values expected for the pre-determined seed. When Waveserver 5 detects a failure during one or more of the self-tests, it raises an alarm. The administrator can attempt to reboot the TOE to clear the error. If rebooting the Waveserver 5 does not resolve the issue, then the administrator should contact their next level of support or their Ciena support group for further assistance. All power up self-tests execution are logged for both successful and unsuccessful completion. The Software Integrity Test is run automatically on start-up, and whenever the system images are loaded. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.
FPT_TUD_EXT.1	Security Administrators have the ability to query the current version of the TOE and they are able to perform manual software updates. The currently active version of the TOE can be queried by issuing the “software show” command. When software updates are available via the http://www.ciena.com website, they can obtain, verify the integrity and install the updates.

Requirement	TSS Description
	The software images are digitally signed using RSA digital signature mechanism. The TOE will use a public key in order to verify the digital signature, upon successful verification the image will be loaded onto the TOE. If the images cannot be verified, the image will not be loaded onto the TOE.
FTA_SSL.3	A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local CLI and remote SSH interfaces. The inactivity time period can range from 1 to 1500 minutes for the CLI interface. The default value is 10 minutes for both the CLI and SSH interface. The configuration of inactivity periods are applied on a per interface basis. A configured inactivity period will be applied to both local and remote sessions in the same manner. When the interface has been idle for more than the configured period of time, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	The Security Administrator is able to terminate their CLI. The way this is performed is by entering the “exit” command after authentication to the TOE.
FTA_SSL_EXT.1	The TOE will terminate the session after a Security Administrator defined period of inactivity.
FTA_TAB.1	Security Administrators can create a customized login banner that will be displayed at the following interfaces: • Local CLI • Remote CLI This banner will be displayed prior to allowing Security Administrator access through those interfaces.
FTP_ITC.1	The TOE supports secure communication to the following IT entities: Syslog server and RADIUS server. The TOE uses TLS v1.2 or TLS v1.1 protocol with X.509 certificate-based authentication. The protocols listed are consistent with those included in the requirements in the ST. The TOE acts as a TLS client in both syslog and RADIUS server connection.
FTP_TRP.1/Admin	The TOE supports HTTPS/TLS and SSH v2.0 for secure remote administration of the TOE. SSH v2.0 session is encrypted using AES encryption to protect confidentiality and uses HMACs to protect integrity of traffic. Remote GUI connections take place over a TLS connection. The TLS session is encrypted using AES encryption and uses HMACs to protect integrity. The protocols listed are consistent with those specified in the requirement.

6.1 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified in the table below.

Table 13 – CAVP Algorithm Certificate References

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard	Ciena Waveserver Crypto Library 1	RSA	#A3284

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	(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	Ciena Waveserver Crypto Library 1	ECDSA	#A3284
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526].	Ciena Waveserver Crypto Library 1	Safe-Primes key generation Safe-Primes Key Verification	#A3284
FCS_CKM.2	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	Ciena Waveserver Crypto Library 1	KAS-ECC-SSC	#A3284

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800- 56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526]	Ciena Waveserver Crypto Library 1	KAS-FFC-SSC	#A3284
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR] and [GCM] mode and cryptographic key sizes [128 bits, 256 bits]	Ciena Waveserver Crypto Library 1	AES	#A3284
		Ciena Waveserver Crypto Library 2		#A3283
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Ciena Waveserver Crypto Library 1	RSA	#A3284
	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	Ciena Waveserver Crypto Library 1	ECDSA	#A3284

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits	Ciena Waveserver Crypto Library 1	SHS	#A3284
FCS_COP.1/ KeyedHash	[HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [256, 384, and 512 bits] and message digest sizes [160, 256, 384, 512] bits	Ciena Waveserver Crypto Library 1	HMAC	#A3284
FCS_RBG_EXT.1	Hash_DRBG (SHA-256)	Ciena Waveserver Crypto Library 1	DRBG	#A3284

6.2 Cryptographic Key Destruction

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

Table 14 – Cryptographic Key Destruction

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Diffie-Hellman Shared Secret	Provide Perfect Forward secrecy	RAM	Overwritten with zeros.
Passwords	User authentication	Only salted hash is stored in file system.	The configuration file is updated when the administrator issues a “configuration save” CLI command. Waveserver 5 also supports a Secure Erase feature that will reset the chassis back to factory default. All content, including the user credentials, will be removed as part of this operation.
Diffie-Hellman Key Pair	Establish SSH Sessions	RAM	Overwritten with zeros.
SSH Private Keys	SSH Server	SSD/File system	Overwritten with zeros.
AES Key	Encrypt/decrypt, X509 certificate passphrase	SSD/File system	Overwritten with zeros.

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
SSH Session Key	SSH Server	SSH Session Key is stored only in RAM.	Overwritten with zeros.
RNG Seed	Output from TRNG is used to seed the DRBG	RAM	Overwritten with zeros.
TLS Session Key	TLS syslog, RADsec, HTTPS	RAM	Overwritten with zeros.

7 Acronym Table

Table 15 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
DTLS	Datagram Transport Layer Security
EP	Extended Package
GUI	Graphical User Interface
IP	Internet Protocol
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RSA	Rivest, Shamir, & Adleman
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionalities
TSS	TOE Summary Specification