Assurance Activity Report

Version 1.8

for

Ciena Waveserver 5 OS R2.3.12

Security Target Name
Ciena Waveserver 5 OS R2.3.12 Security Target Version 1.5

Collaborative Protection Profile for Network Devices (NDcPP)
Version 2.2e

Revision History:

Version	Date	Changes
Version 1.0	03/12/2019	Initial Release
Version 1.1	05/18/2023	Updated AAR with findings for TSS, Testing and Guidance. Added applicable TDs
Version 1.2	05/23/2023	Addressed QA Comments
Version 1.3	06/14/2023	Updated version of TOE
Version 1.4	09/06/2023	Addressed ECR Comments for checkout
Version 1.5	10/10/2023	Addressed ECR Comments for checkout
Version 1.6	11/09/2023	Addressed ECR Comments for checkout
Version 1.7	11/27/2023	Addressed ECR Comments for checkout
Version 1.8	12/4/2023	Addressed ECR Comments for checkout

Table of Contents

Evaluated by:

2400 Research Blvd Suite 395,
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:

Ciena Corporation
7035 Ridge Road
Hanover, Maryland 21076
United States of America

The Author of the Security Target:

Intertek Acumen Security, LLC
2400 Research Blvd Suite 395
Rockville, MD, 20850

The TOE Evaluation was Sponsored by:

Ciena Corporation
7035 Ridge Road
Hanover, Maryland 21076
United States of America

Evaluation Personnel:

Toan Truong
Furukh Siddique

Common Criteria Version

Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version

CEM Version 3.1 Revision 5

1 Target of Evaluation (TOE) Overview

The Ciena Waveserver 5 (herein referred to as the TOE) provides the best transport economics for high-capacity, high-growth applications. It combines the industry's most advanced coherent technology with a simple, server-like operational model to drive down cost per bit and reduce energy consumption. Its industry-leading density, scale, and capacity per wavelength allow Internet Content Providers (ICPs), Data Center Operators (DCOs), and Communications Service Providers (CSPs) to deliver a high-performance, quality experience to their end-user customers.

1.1 TOE Description

The Ciena Waveserver 5 is a purpose-built, 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.

While not an exhaustive list, some of the leveraged security mechanisms include the following. For information on all 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.

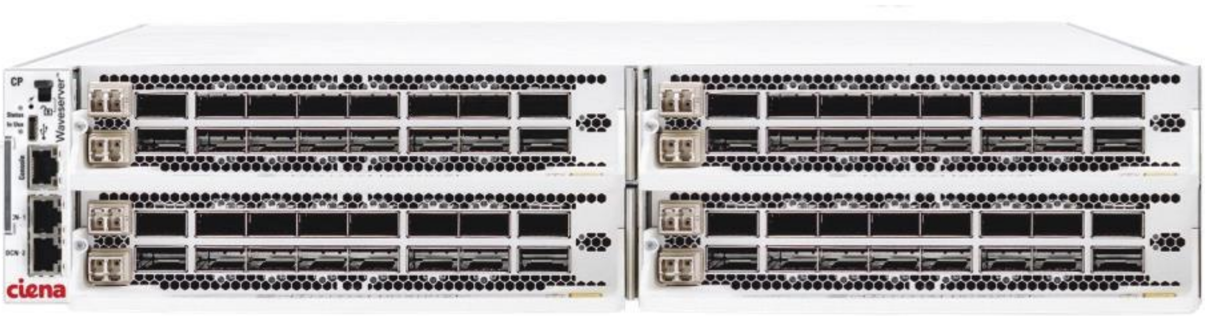
2. RADIUS via TLS: The Waveserver 5 is capable of using RADIUS authentication with TLS encryption, ensuring the secure transmission of login credentials and providing an added layer of protection for user authentication.

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.

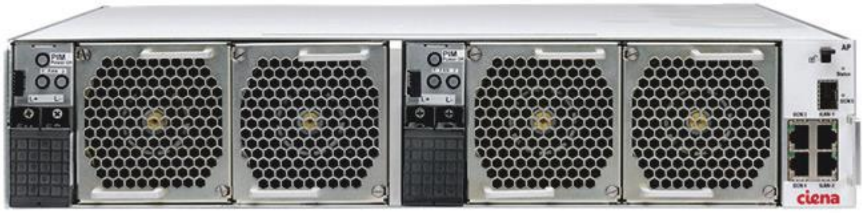
4. NTP with SHA Authentication: The Waveserver 5 supports the use of NTP with SHA authentication, providing a secure method for time synchronization across network devices and reducing the risk of time-based attacks.

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: AC power and fan modules



2 Assurance Activities Identification

The Assurance Activities contained in this document include all those defined within NDcPPv2.2E based on the core SFRs and those implemented based on selections within the Protection Profile (PP).

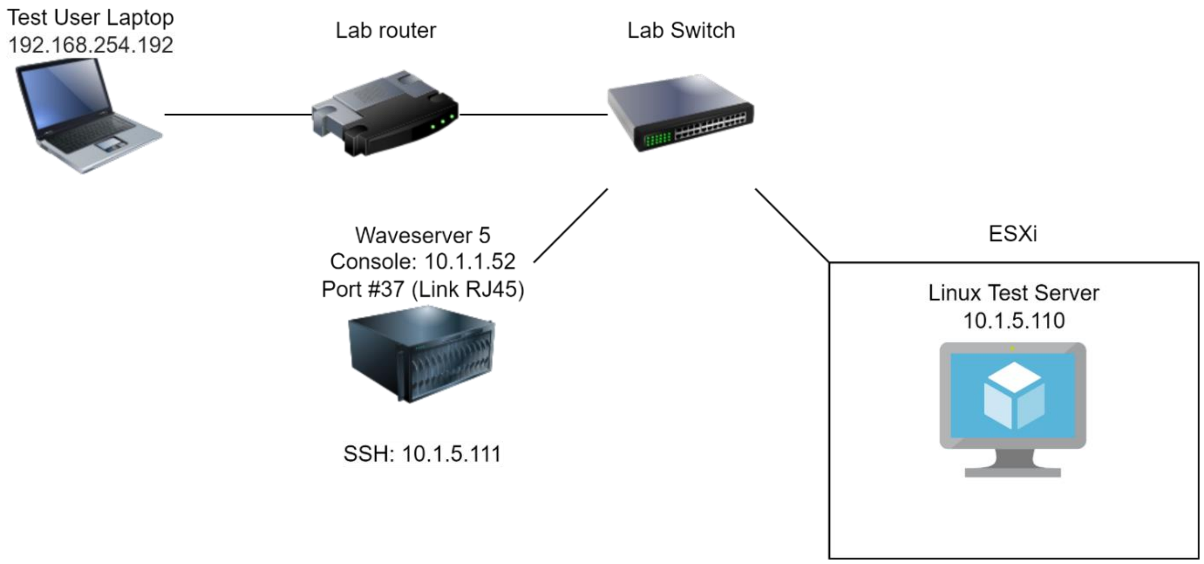
3 Test Equivalency Justification

The Waveserver 5 OS R2.3.12 is the only device evaluated.

4 Test Diagram

4.1 Testbed Diagram

Below is a visual representation of the components included in the test bed:



NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.

4.2 Test Time/Location

All testing was carried out at the Acumen Security office located at 2400 Research Boulevard, Rockville, Maryland 20850 Suite 395.

Testing was conducted as provided below:

•Formal testing for Common Criteria took place starting in September, 2022.

The TOE was located in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. At the end of each day, the device was turned off. All evaluation documentation was kept with the evaluator at all times. Testing was carried out by the evaluator with collaborative guidance from the customer on TOE functionality.

5 Detailed Test Cases (Auditing)

5.1 Test Cases (Auditing)

5.1.1 FAU_GEN.1 TSS 1

For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key.

5.1.1.1 Evaluator Findings

The evaluator examined the section 6 titled TOE Summary Specification for FAU_GEN.1 of the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that this section identified the following information was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys: “Administrative tasks of generating, deleting cryptographic keys contain the necessary audit information as mandated by FAU_GEN.1.1.

Audit events for deleting and 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

SSH Generate key:
eventlog: ssh [CienaWOS@1271.3 TIME-FORMAT="uTC" EVENT-ID="29- 013" EVENT-NAME="GenerateKey" EVENT-ORIGIN="ssh"] Ssh Generate Key

X509 device certificate installed:
eventlog: DeviceCertificateAdd [CienaWOS@1271.3 TIMEFORMAT="uTC" EVENT-ID="24-036" EVENTNAME="DeviceCertificateAdd" EVENT-ORIGIN="security"] X.509 Device Certificate Name test Installed

Based on these findings, this assurance activity is considered satisfied.

5.1.1.2 Verdict

Pass

5.1.2 FAU_GEN.1 Guidance 1

The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event– comprising the mandatory, optional and selection-based SFR sections as applicable – shall be provided from the actual audit record).

5.1.2.1 Evaluator Findings

The evaluator examined the guidance document “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance document” to determine if it lists all auditable events. The section 4.5 titled Auditable Events of

AGD was used to determine the verdict of this assurance activity. The evaluator first found an identification of each auditable event in Table 3 in the section titled "Auditable Events". The evaluator next compared this list of events to the auditable events listed in the NDcPP**.** Each event listed in the NDcPP is also listed in AGD. Next, the evaluator reexamined AGD and found that the section titled "Auditable Events" contains a listing and description of each of the fields in generated audit records that contain the information required in FAU_GEN.1.2.

Based on these findings, this assurance activity is considered satisfied.

5.1.2.2 Verdict

Pass

5.1.3 FAU_GEN.1 Guidance 2

The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.

5.1.3.1 Evaluator Findings

The evaluator examined the guidance documentation document "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine which administrative commands are relevant in the context of the cPP. The ST and AGD were used to determine the verdict of this assurance activity. The evaluator first examined the entirety of AGD to determine what administrative commands are associated with each administrative activity. The evaluator found the following are applicable,

Administrative Activity	Method (Command/GUI Configuration)	Section
Generating Keys (certificates)	ssh server key install user [user id]	6.2
Display system information	Software show	9.1
Creating Users	user create user <String: 1...32> access-level <limited | admin | super> [password <String: 8...128>]	6.7.1
Configuring Revocation Servers	syslog tls ocsp set default-responder <String: [1..255]> radsec ocsp set default-responder <String: [1..255]>	4.4 and 5.1
Generating CSRs	pkix certificates entity csr generate cert-name test1 tftpserver 1.2.3.4 key-type rsa2048 filename test1.cnf	6.5

Administrative Activity	**Method (Command/GUI Configuration)**	**Section**
Performing Software Updates	software activate version <version> [auto-commit] [delete-from-load]	9.1
Configuring Admin Timeout	System server set global-inactivity-timer on system server set global-inactivity-timeout <# of minutes>	11
Configuring the Audit Server	syslog tls <disable | enable>	4.4
Configuring Access Banner	system shell set login-banner-file <filename>	12.1
Setting Password Length	user set min-password-length [8..128]	6.1
Configuring SSH	No configuration is required	7.1
Configuring TLS	system server https mutual-authentication enable	7.2
Configuring Authentication Server Protocols (RADSec)	radsec add server <IP address or host name> [fingerprint <a SHA256 certificate fingerprint[95]] [priority <Number:1...8>] [port <Number:1...65535>] [trusted-dns <a fully qualified domain name that can accept a leading wildcard period>]	5

The audit record associated with the configuration was captured. The following table reflects the configurations that were found and identifies the specific method for invoking the functionality that generated the audit record.

Administrative Activity	**Method (Command/GUI Configuration)**
Audit behavior	Software show log
Logout	Exit
Generating Keys (certificates)	ssh server key install user [user id]
Display system information	Software show
Creating Users	user create user <String: 1...32> access-level <limited | admin | super> [password <String: 8...128>]
Configuring Revocation Servers	Syslog tls ocsp set default-responder <String: [1..255]> radsec ocsp set default-responder <String: [1..255]>
Generating CSRs	pkix certificates entity csr generate cert-name test1 tftpserver 1.2.3.4 key-type rsa2048 filename test1.cnf
Performing Software Updates	software activate version <version> [auto-commit] [delete-from-load]

Administrative Activity	**Method (Command/GUI Configuration)**
Setting the Time	system set date <Date: yyyy-mm-dd | yy-mm-dd | mm-dd>
Configuring Admin Timeout	System server set global-inactivity-timer on system server set global-inactivity-timeout <# of minutes>
Configuring the Audit Server	syslog tls <disable | enable>
Configuring Access Banner	system shell set login-banner-file <filename>
Setting Password Length	user set min-password-length [8..128]
Configuring Authentication Server Protocols (RADSec)	radsec add server <IP address or host name> [fingerprint <a SHA256 certificate fingerprint[95]] [priority <Number:1...8>] [port <Number:1...65535>] [trusted-dns <a fully qualified domain name that can accept a leading wildcard period>]

The above analysis illustrates that each of the relevant configuration methods were appropriately audited by the TOE. Based on these findings, this assurance activity is considered satisfied.

5.1.3.2 Verdict

Pass

5.1.4 FAU_GEN.1 Test 1

Item	**Data/Description**
Test ID	FAU_GEN.1_T1
Objective	*The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries.*
Test Flow	• Trigger each auditable event on the TOE • Verify that each audit record is generated and contains the required

	information
Pass/Fail Explanation	The audit records associated with each test case are recorded with each test case. A comparison of required audit records to the presented audit records was additionally performed. This analysis shows that each required audit record is generated by the TOE, meeting the test requirements.
Result	PASS

5.1.5 FAU_GEN.2

None – The evaluation of this SFR is tested in conjunction with the testing of FAU_GEN.1.

5.1.6 FAU_STG_EXT.1 TSS 1

The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.

5.1.6.1 Evaluator Findings

The evaluator examined the TSS to ensure that it describes the means by which audit data is transmitted to an external audit server, and how the trusted channel is provided. The TSS entry for FAU_STG_EXT.1 in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states that the TOE sends audit records to an external syslog server over TLS v1.2 or TLS v1.1 protocol using X509 certificates. To support this functionality, the TOE transports syslog records to a specified external syslog server. Only after a connection has been established, does the TOE push audit records to the external server.

Based on these findings, this assurance activity is considered satisfied.

5.1.6.2 Verdict

Pass

5.1.7 FAU_STG_EXT.1 TSS 2

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.

5.1.7.1 Evaluator Findings

The evaluator examined the TSS to determine if it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. The TSS entry for FAU_STG_EXT.1 in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states that the TOE stores up to 4 files each holding up to 10,000 audit data locally. The evaluator, next, found that, when the local audit storage on the TOE is full, the TOE shall overwrite the oldest file to allow new audit events to be created. Finally, the evaluator found that the TOE implements the following protection to protect against unauthorized access to local audit records: "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".

Based on these findings, this assurance activity is considered satisfied.

5.1.7.2 Verdict

Pass

5.1.8 FAU_STG_EXT.1 TSS 3

The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components

5.1.8.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator concluded that the TOE is standalone due to audit data being stored locally.

Based on these findings, this assurance activity is considered satisfied.

5.1.8.2 Verdict

Pass

5.1.9 FAU_STG_EXT.1 TSS 4

The evaluator shall examine the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behavior of the TOE shall also be detailed in the TSS.

5.1.9.1 Evaluator Findings

The evaluator examined the TSS to ensure that it details the behavior of the TOE when the storage space for audit data is full. The FAU_STG_EXT.1 SFR found in the section 5.2.1 titled "Class: Security Audit (FAU)" of the ST and the TSS entry for FAU_STG_EXT.1 in the section 6 titled "TOE Summary Specification" of ST were used to determine the verdict of this assurance activity. The evaluator found that "overwrite previous audit records according to the following rule: when the local storage space for audit data is full" was selected in the SFR. Next, the evaluator confirmed that the TSS provides a description of how the TOE implements this functionality. The TSS states "When the local data is full, the oldest audit events are overwritten to allow new audit events to be created". The evaluator found this description to be consist with the selection within the SFR.

Based on these findings, this assurance activity is considered satisfied.

5.1.9.2 Verdict

Pass

5.1.10 FAU_STG_EXT.1 TSS 5

The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in real-time or periodically. In case the TOE does not perform transmission in real-time the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible as well as acceptable frequency for the transfer of audit data.

5.1.10.1 Evaluator Findings

The evaluator examined the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in real-time or periodically. The FAU_STG_EXT.1 SFR found in the section 5.2.1 titled "Class: Security Audit (FAU)" of the ST and the TSS entry for FAU_STG_EXT.1 in the section 6 titled "TOE Summary Specification" of ST were used to determine the verdict of this assurance activity. The TSS states that "The TOE transmits audit data to an external syslog server in real time".

Based on these findings, this assurance activity is considered satisfied.

5.1.10.2 Verdict

Pass

5.1.11 FAU_STG_EXT.1 Guidance 1

The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.

5.1.11.1 Evaluator Findings

The evaluator examined the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine if it describes how to establish a trusted channel to an audit server. Section 4, titled "Using an Audit Server" of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD states that the TOE securely sends traffic to an external audit server via TLS v1.2 or TLS v1.1. Next, the evaluator found that AGD provides instructions for configuring the secure connection between the TOE and the remote audit server via CLI in the section

4.4 titled “Audit Server Configuration”. Finally, the evaluator found that AGD defines the following requirements for audit server to which the TOE connects:

- You must be logged in to Waveserver 5 using an account with at least admin access privileges.
- You have the server IP or host name and filename for the X.509 certificate files.
- Device certificate with private key and CA certificate has been installed on the TLS syslog server.
- You know the IP address or host name for the TLS syslog server.

Based on these findings, this assurance activity is considered satisfied.

5.1.11.2 Verdict

Pass

5.1.12 FAU_STG_EXT.1 Guidance 2

The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and “cleared” periodically by sending the data to the audit server.

5.1.12.1 Evaluator Findings

The evaluator examined the guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to determine the relationship between local and external audit data. The section 4.3 titled “System Behavior” of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD describes the relationship between local and external audit data, as follows: 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.

Based on these findings, this assurance activity is considered satisfied.

5.1.12.2 Verdict

Pass

5.1.13 FAU_STG_EXT.1. Guidance 3

The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.

5.1.13.1 Evaluator Findings

The evaluator examined the guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document ” to determine if it describes all possible configuration options for FAU_STG_EXT.1.3 and the TOE behavior for each possible configuration. The TSS entry for FAU_STG_EXT.1 in the section 6 titled “TOE Summary Specification” of ST and the section 4.3 titled “System Behavior” of AGD was used to determine the verdict of this assurance activity. The evaluator found that the TOE does not support the configuration of different methods of handling exhausted local audit storage. Next, the evaluator compared the exhausted local audit handling description found in AGD to the description provided by the TSS of the ST. The descriptions of the behavior found in AGD and ST are consistent.

Based on these findings, this assurance activity is considered satisfied.

5.1.13.2 Verdict

Pass

5.1.14 FAU_STG_EXT.1 Test 1

Item	**Data/Description**
Test ID	FAU_STG_EXT.1_T1
Objective	*The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided.* *The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.*
Test Flow	• *Configure the switch to communicate with a syslog via TLS* • *Generate audit events (the event itself does not matter)* • *Capture the traffic between the switch and the syslog server* • *Verify that the packets are TLS encrypted*
Pass/Fail Explanation	The TOE successfully sends all logs over an encrypted channel. This meets testing requirements.
Result	PASS

5.1.15 FAU_STG_EXT.1 Test 2

Item	**Data/Description**
Test ID	FAU_STG_EXT.1_T2
Objective	*Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies*

	that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: *2) The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option 'overwrite previous audit records' in FAU_STG_EXT.1.3)*
Test Flow	• Login as an administrator • Check the logs file • Clear the logs file • Generate new logs and verify that they are now replacing the logging buffer
Pass/Fail Explanation	When audit log files reach maximum size, a new audit log file is created and overwrites previous logs. This meets the testing requirements.
Result	PASS

5.2 Test Cases (Cryptographic Support)

5.2.1 FCS_CKM.1 TSS 1

The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

5.2.1.1 Evaluator Findings

The evaluator examined the TSS to determine if it identifies the key sizes supported by the TOE. The TSS entry for FCS_CKM.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. The evaluator found that the TSS states The TOE supports RSA key sizes of 2048 and 3072 bits. The RSA keys are used in support 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 Digital Signature Standard (DSS)", Appendix B.4. The Elliptic keys are used in support of ECDH key exchange. The TOE supports FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3. RSA and 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.

Based on these findings, this assurance activity is considered satisfied.

5.2.1.2 Verdict

Pass

5.2.2 FCS_CKM.1 Guidance 1

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.

5.2.2.1 Evaluator Findings

The evaluator examined guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document ” to determine if it instructs the administrator how to configure TOE to use the selected key generation schemes and key sizes. Upon investigation, the evaluator found that generating keys is addressed in section 6.2 and section 3 titled, “Configuring SSH Public Keys” and “Enabling CC-NDcPP Compliance”. In particular, the evaluator found that the TOE supports all NIST curves (P-256, P-384, P521) and Diffie-Hellman group 14 by default and cannot be configured. The following information was pulled from the AGD:

<u>Default cryptographic functionality for SSH:</u>

```
WS5_0195*# ssh algorithm show

+----------SSH Key Exchange Algorithms-----------------------+

| Algorithm Name                          | Admin State  |

+--------------------------------------------+--------------+

| ecdh-sha2-nistp521                      | Enabled      |

| ecdh-sha2-nistp384                      | Enabled      |

| ecdh-sha2-nistp256                      | Enabled      |

| diffie-hellman-group14-sha1             | Enabled      |

+--------------------------------------------+--------------+
```

<u>Default cryptographic functionality for TLS:</u>

```
WS5_0195*# ssl algorithm show

+-------------------- TLS Cipher Suites ------------------------+

| Cipher suite Name                          | Admin State  |

+-----------------------------------------------+--------------+

| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384       | Enabled      |

| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384       | Enabled      |

| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384         | Enabled      |

| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384         | Enabled      |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256          | Disabled     |
| TLS_RSA_WITH_AES_256_GCM_SHA384              | Disabled     |
| TLS_RSA_WITH_AES_256_CBC_SHA256              | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256      | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256      | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256        | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256        | Disabled     |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384          | Disabled     |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256          | Disabled     |
| TLS_RSA_WITH_AES_128_CBC_SHA256              | Disabled     |
+----------------------------------------------+--------------+
```

Based on these findings, this assurance activity is considered satisfied.

5.2.2.2 Verdict

Pass

5.2.3 FCS_CKM.1 Test 1

The evaluator shall verify the implementation of Key Generation by the TOE using the Key Generation test.

5.2.3.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the Key Generation test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.

5.2.3.2 CAVP Algorithm Certificate

A3284

5.2.3.3 Verdict

Pass

5.2.4 FCS_CKM.2 TSS 1 ***[TD0580]***

The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme (including whether the TOE acts as a sender, a recipient, or both).

5.2.4.1 Evaluator Findings

The evaluator examined the TSS to determine if the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. The TSS entries for FCS_CKM.1 and FCS_CKM.2 in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator compared the key establishment schemes listed in FCS_CKM.2 to the key generation schemes listed in FCS_CKM.1. Upon investigation, the evaluator found that FCS_CKM.2 do not introduce any key generation scheme not include in FCS_CKM.1.

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.

Based on these findings, this assurance activity is considered satisfied.

5.2.4.2 Verdict

Pass

5.2.5 FCS_CKM.2 Guidance 1

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).

5.2.5.1 Evaluator Findings

The evaluator examined the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document " to determine if it instructs the administrator how to configure TOE to use the selected key establishment schemes. Upon investigation, the evaluator found that using the selected keys is addressed in section 3 titled, "Enabling CC-NDcPP Compliance".

Based on these findings, this assurance activity is considered satisfied.

5.2.5.2 Verdict

Pass

5.2.6 FCS_CKM.2 ECC

The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE.

5.2.6.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the Key Agreement Scheme test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below. This test only applies to 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.”

5.2.6.2 CAVP Algorithm Certificate

A3284

5.2.6.3 Verdict

Pass

5.2.7 FCS_CKM.2 FFC

The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE.

5.2.7.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the Key Agreement Scheme test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below. This test only applies to 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.”

5.2.7.2 CAVP Algorithm Certificate

A3284

5.2.7.3 Verdict

Pass

5.2.8 FCS_CKM.4 TSS 1

The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.

5.2.8.1 Evaluator Findings

The evaluator examined the TSS to ensure that it lists each type of plaintext key material and its origin and storage location. The TSS entry for FCS_CKM.4 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. According to the TSS the following plaintext keys are stored in volatile memory:

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.
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.

The evaluator compared the list of keys to the keys which would be expected for the supported cryptographic protocols and found this list consistent with those keys.

Based on these findings, this assurance activity is considered satisfied.

5.2.8.2 Verdict

Pass

5.2.9 FCS_CKM.4 TSS 2

The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).

5.2.9.1 Evaluator Findings

The evaluator checked to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs). The section 6.2 titled, "Cryptographic Key Destruction" in ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that all keys used by the TOE are zeroized by overwriting the value with "zeros."

Based on these findings, this assurance activity is considered satisfied.

5.2.9.2 Verdict

Pass

5.2.10 FCS_CKM.4 TSS 3

Note that where selections involve 'destruction of reference' (for volatile memory) or 'invocation of an interface' (for non-volatile memory) then the relevant interface definition is examined by the evaluator to ensure that the interface supports the selection(s) and description in the TSS. In the case of non-volatile memory, the evaluator includes in their examination the relevant interface description for each media type on which plaintext keys are stored. The presence of OS-level and storage device-level swap and cache files is not examined in the current version of the Evaluation Activity.

5.2.10.1 Evaluator Findings

The evaluator examined the TSS to ensure that it contains a relevant interface definition that ensures the interface supports the selection by the TOE. The TSS entry for FCS_CKM.4 in section 6 titled "TOE Summary Specification" was used to determine the verdict of this assurance activity. The TSS states the following:

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.

Based on these findings, this assurance activity is considered satisfied.

5.2.10.2 Verdict

Pass

5.2.11 FCS_CKM.4 TSS 4

Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.

5.2.11.1 Evaluator Findings

The evaluator examined the TSS to ensure that it lists each type of plaintext key material and its origin and storage location. The TSS entry for FCS_CKM.4 in the section 6 titled "TOE Summary Specification" as well as section 6.2 titled "Cryptographic Key Destruction" of ST was used to determine the verdict of this assurance activity.

- Diffie-Hellman Shared Secret
  - Used for providing perfect forward secrecy
  - Key-encrypting key is overwritten with zeros.
- Passwords
  - Used for user authentication
  - Stored as salted hash in file system.
  - Waveserver 5 performs a Secure Erase feature that will reset the chassis to factory default
  - All content, including user credentials, will be removed as part of this operation
- Diffie Hellman Key Pair
  - Used to establish SSH sessions
  - Key encrypting key is overwritten with zeros.
- SSH Private Key
  - Used for SSH server on the TOE
  - Key-encrypting key is overwritten with zeros.
- AES Key
  - Used for encrypting and decrypting as well as X509 certificate passphrases
  - Key-encrypting key is overwritten with zeros.
- SSH Session Key
  - Used for SSH Server on the TOE
  - Key-encrypting key is overwritten with zeros.
- RNG Seed
  - Used to help seed the DRBG
  - Key-encrypting key is overwritten with zeros.
- TLS Session Key
  - Used for TLS syslog, RADsec and HTTPS connections
  - Key-encrypting key is overwritten with zeros

5.2.11.2 Verdict

Pass

5.2.12 FCS_CKM.4 TSS 5

The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.

5.2.12.1 Evaluator Findings

The TSS entry for FCS_CKM.4 in section 6 titled "TOE Summary Specification" Measures of ST was used to determine the verdict of this assurance activity in addition to Section 6.2, 'Cryptographic Key Destruction'. Upon investigation, the evaluator found that the TOE zeros all secrets, keys and associated values when they are no longer required. Hence no circumstances were found where destruction may be prevented or delayed.

Based on these findings, this assurance activity is considered satisfied.

5.2.12.2 Verdict

Pass

5.2.13 FCS_CKM.4 TSS 6

Where the ST specifies the use of "a value that does not contain any CSP" to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.

5.2.13.1 Evaluator Findings

Where the ST specifies the use of "a value that does not contain any CSP" to overwrite keys, the evaluator examined the entry for FCS_CKM.4 in section 6 of the ST: TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. Upon investigation, the evaluator found that the keys are only overwritten with zeros.

Based on these findings, this assurance activity is considered satisfied.

5.2.13.2 Verdict

Pass

5.2.14 FCS_CKM.4 Guidance 1

The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used).

5.2.14.1 Evaluator Findings

The evaluator reviewed the TSS and AGD documentation for the TOE and found no items that did not meet conformance to the key destruction requirement.

Based on these findings, the above requirement has been met.

5.2.14.2 Verdict

Pass

5.2.15 FCS_CKM.4 Guidance 2

The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.

5.2.15.1 Evaluator Findings

The evaluator reviewed the TSS and AGD and found no instance in which key destruction is delayed following the request for destruction. Based on these findings, the above requirement has been met.

5.2.15.2 Verdict

Pass

5.2.16 FCS_COP.1/DataEncryption TSS 1

The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.

5.2.16.1 *Evaluator Findings*

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.2.16.2 *Verdict*

Pass

5.2.17 FCS_COP.1/DataEncryption Guidance 1

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.

5.2.17.1 *Evaluator Findings*

The evaluator examined the section titled 7.1 SSH and 3.1 Enabling CC-NDPP Compliance Using the CLI interface in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD states the following:

No configuration is necessary on the TOE to enable the use of all selected modes and key sizes. The TOE only supports all claimed algorithms by default and all other algorithms are disabled.

Based on these findings, this assurance activity is considered satisfied.

5.2.17.2 *Verdict*

Pass

5.2.18 FCS_COP.1/DataEncryption Test 1

The evaluator shall verify the implementation of symmetric encryption supported by the TOE.

5.2.18.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the Encryption test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.

5.2.18.2 CAVP Algorithm Certificate

A3284 & A3283

5.2.14.3 Verdict

Pass

5.2.19 FCS_COP.1/SigGen TSS 1

The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.

5.2.19.1 *Evaluator Findings*

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.2.19.2 *Verdict*

Pass

5.2.20 FCS_COP.1/SigGen Guidance 1

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.

5.2.20.1 *Evaluator Findings*

The evaluator examined the section titled 3.1 Enabling CC-NDcPP Compliance Using the CLI Interface in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD states the following:

The following algorithms are supported by the TOE:

Default cryptographic functionality:

```
+----------SSH Public Key Authentication Algorithms----------+

| Algorithm Name                        | Admin State  |

+-------------------------------------------+--------------+

| ssh-rsa                         | Enabled      |

| ecdsa-sha2-nistp256                   | Enabled      |

| ecdsa-sha2-nistp384                   | Enabled      |

| ecdsa-sha2-nistp521                   | Enabled      |

+-------------------------------------------+--------------+
```

The TOE supports RSA key sizes of 2048, 3072 and 4096. RSA 4096 can only be used by the TOE if it is generated off-TOE and then imported. Section 6.2 in the AGD provides instructions on how to perform this action.

Default cryptographic functionality:

```
WS5_0195*# ssl algorithm show

+-------------------- TLS Cipher Suites ------------------------+

| Cipher suite Name                     | Admin State  |

+-----------------------------------------------+--------------+

| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384       | Enabled      |

| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384       | Enabled      |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384       | Enabled      |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384       | Enabled      |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256         | Disabled     |
| TLS_RSA_WITH_AES_256_GCM_SHA384             | Disabled     |
| TLS_RSA_WITH_AES_256_CBC_SHA256             | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256     | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256     | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256       | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256       | Disabled     |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384         | Disabled     |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256         | Disabled     |
| TLS_RSA_WITH_AES_128_CBC_SHA256             | Disabled     |
+---------------------------------------------+--------------+
```

Based on these findings, this assurance activity is considered satisfied.

5.2.20.2 *Verdict*

Pass

5.2.21 FCS_COP.1/SigGen Test 1

The evaluator shall verify the implementation of the digital signature algorithms supported by the TOE.

5.2.21.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the Digital Signature test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.

5.2.21.2 CAVP Algorithm Certificate

A3284

5.2.15.3 Verdict

Pass

5.2.22 FCS_COP.1/Hash TSS 1

The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.

5.2.22.1 Evaluator Findings

The evaluator examined the TSS to determine that the association of the hash function with other TSF cryptographic features is documented in the TSS. The TSS entry for FCS_COP.1/Hash in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes each of the associated TSF cryptographic functions for which hashing is associated with, as follows,

- SSH
- TLS

Based on these findings, this assurance activity is considered satisfied.

5.2.22.2 Verdict

Pass

5.2.23 FCS_COP.1/Hash Guidance 1

The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.

5.2.23.1 Evaluator Findings

The evaluator examined the guidance documents to determine if they describe any configuration that is required for the required hash sizes. The entire AGD was used to determine the verdict of this Assurance Activity. Upon investigation, the evaluator found that section 7 of the AGD states that no configuration is required and the required hash sizes are used automatically when the appropriate cryptographic function is invoked.

Based on these findings, this assurance activity is considered satisfied.

5.2.23.2 Verdict

Pass

5.2.24 FCS_COP.1/Hash Test 1

The evaluator shall verify the implementation of hashing supported by the TOE.

5.2.24.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the Hashing test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.

5.2.24.2 CAVP Algorithm Certificate

A3284

5.2.18.3 Verdict

Pass

5.2.25 FCS_COP.1/KeyedHash TSS 1

The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.

5.2.25.1 Evaluator Findings

The evaluator examined the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. The TSS entry for FCS_COP.1/KeyedHash in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator found the following information in the TSS for the supported HMACs:

- HMAC Algorithms: HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
- Hash function used: SHA-1, SHA-256, SHA-384, SHA-512
- Block size: 512-bit, 1024 bits
- Key Lengths: 256 bits, 384 bits, 512 bits
- MAC Lengths: 160 bits, 256 bits, 384 bits, 512 bits

Additionally, the evaluator compared the values provided in the TSS to the definition of the SFR in ST under section 5.2.2 titled "Class: Cryptographic Support (FCS)" and the operation of the TOE during testing. The evaluator found that values listed to be consistent with the implementation of the algorithm.

Based on these findings, this assurance activity is considered satisfied.

5.2.25.2 Verdict

Pass

5.2.26 FCS_COP.1/KeyedHash Guidance 1

The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.

5.2.26.1 *Evaluator Findings*

The evaluator examined the section titled 3 Enabling CC-NDcPP Compliance in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states that there is a default cryptography setting on the TOE that does not require any pre-configuration:

Default cryptographic functionality:

```
WS5_0195*# ssh algorithm show

+----------SSH Message Authentication Code Algorithms--------+

| Algorithm Name                    | Admin State  |

+---------------------------------------------+--------------+
| hmac-sha2-512                          | Enabled      |
| hmac-sha2-256                          | Enabled      |
+----------------------------------------------+--------------+
```

HMAC-SHA-384 is supported via the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ciphers automatically by the TOE in CC-Mode. The AGD states the following in section 3 in terms of default support for the HMAC algorithm:

```
WS5_0195*# ssl algorithm show
+-------------------- TLS Cipher Suites ------------------------+
| Cipher suite Name                          | Admin State  |
+-------------------------------------------------+--------------+
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384       | Enabled      |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384       | Enabled      |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384         | Enabled      |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384         | Enabled      |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256           | Disabled     |
| TLS_RSA_WITH_AES_256_GCM_SHA384               | Disabled     |
| TLS_RSA_WITH_AES_256_CBC_SHA256               | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256       | Disabled     |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256       | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256         | Disabled     |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256         | Disabled     |
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384           | Disabled     |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256           | Disabled     |
| TLS_RSA_WITH_AES_128_CBC_SHA256               | Disabled     |
+-----------------------------------------------+--------------+
```

Based on these findings, this assurance activity is considered satisfied.

5.2.26.2 *Verdict*

Pass

5.2.27 FCS_COP.1/KeyedHash Test 1

The evaluator shall verify the implementation of MACing supported by the TOE.

5.2.27.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the HMAC test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.

5.2.27.2 CAVP Algorithm Certificate

A3284

5.2.20.3 Verdict

Pass

5.2.28 FCS_RBG_EXT.1 TSS 1

The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.

5.2.28.1 Evaluator Findings

The entry for FCS_RBG_EXT.1 in section 6: TSS of ST states “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. https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/23”

Based on these findings, this assurance activity is considered satisfied.

5.2.28.2 Verdict

Pass

5.2.29 FCS_RBG_EXT.1 Guidance 1

The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.

5.2.29.1 Evaluator Findings

No configuration is required for implementation of the RNG functionality.

Based on these findings, this assurance activity is considered satisfied.

5.2.29.2 Verdict

Pass

5.2.30 FCS_RBG_EXT.1.1 Test 1

The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration.

If the RNG has prediction resistance enabled, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. “generate one block of random bits” means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP800-90A).

If the RNG does not have prediction resistance, each trial consists of (1) instantiate DRBG, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

Entropy input: the length of the entropy input value must equal the seed length.

Nonce: If a nonce is supported (CTR_DRBG with no Derivation Function does not use a nonce), the nonce bit length is one-half the seed length.

Personalization string: The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.

Additional input: the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.

5.2.30.1 Evaluator Findings

The implemented cryptographic module employed by the TOE has been subject to the DRBG test. The module passed each test. The individual algorithm implementations have been tested against the CAVP algorithm validation system. The associated certificate number is listed below.

5.2.30.2 CAVP Algorithm Certificate

A3284

5.2.23.3 Verdict

Pass

5.2.31 FCS_NTP_EXT.1.1 TSS 1

The evaluator shall examine the TSS to ensure it identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained.

5.2.31.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.2.31.2 Verdict

Pass

5.2.32 FCS_NTP_EXT.1.1 TSS 2

The TOE must support at least one of the methods or may use multiple methods, as specified in the SFR element 1.2. The evaluator shall ensure that each method selected in the ST is described in the TSS, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp.

5.2.32.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS describes each method selected in the ST, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp. Upon investigation, the evaluator found that the TSS states that 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 evaluator also verified the TOE supported NTPv4 (RFC 5905).

Based on these findings, this assurance activity is considered satisfied.

5.2.32.2 Verdict

Pass

5.2.33 FCS_NTP_EXT.1.1 Guidance 1

The evaluator shall examine the guidance documentation to ensure it provides the Security Administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST.

5.2.33.1 Evaluator Findings

The evaluator examined the section titled 11 Setting Time Using NTP Synchronization in the AGD to verify that it provides the administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST. Upon investigation, the evaluator found that the AGD states the following:

For CC-NDcPP compliance, time can also be synced to NTP servers. NTPv4 is used by default on the device. To enable NTP connections on the Waveserver, use the following commands:

1. Enable NTP

- ntp client enable

2. Add/Remove the NTP Server to Sync to:

- ntp client add/remove server X.X.X.X

3. To enable a secure connection to the NTP server using a SHA1 key, use the following command:

- ntp sha1-auth add key-id <id> sha1 <key-value>
- ntp client add server X.X.X.X key-id <id>

4. To verify the NTP servers enabled:

- ntp client show

5. Confirm the system time and date:

- system show time
- system show date

6. Save the provisioned setting to the configuration file:

- configuration save

Based on these findings, this assurance activity is considered satisfied.

5.2.33.2 Verdict

Pass

5.2.34 FCS_NTP_EXT.1.1 Test #1

Item	Data/Description
Test ID	FCS_NTP_EXT.1.1 T1
Objective	The version of NTP selected in element 1.1 and specified in the ST shall be verified by observing establishment of a connection to an external NTP server known to be using the specified version(s) of NTP. This may be combined with tests of other aspects of FCS_NTP_EXT.1 as described below.
Test Flow	• Note that TOE only supports NTP version 4 • On the TOE set clock to new time • On the TOE enable NTP service and add a new NTP server for time synchronization • Show TOE clock to verify time synchronization • Gather test log and capture packets • Verify test log that TOE is time synchronized with the server and packets show TOE NTP version supported.
Pass/Fail Explanation	TOE uses correct version of NTP to synchronize with an external NTP server.
Result	PASS

5.2.35 FCS_NTP_EXT.1.2 Guidance 1

For each of the secondary selections made in the ST, the evaluator shall examine the guidance document to ensure it instructs the Security Administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp.

5.2.35.1 Evaluator Findings

The evaluator examined the section titled 11 Setting Time Using NTP Synchronization in the AGD to verify that, for each of the secondary selections made in the ST, it instructs the administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp. Upon investigation, the evaluator found that the AGD states the following:

1. To enable a secure connection to the NTP server using a SHA1 key, use the following command:

- ntp sha1-auth add key-id <id> sha1 <key-value>
- ntp client add server X.X.X.X key-id <id>

Based on these findings, this assurance activity is considered satisfied.

5.2.35.2 Verdict

Pass

5.2.36 FCS_NTP_EXT.1.2 Test #1

Item	Data/Description
Test ID	FCS_NTP_EXT.1.2 T1
Objective	[Conditional] If the message digest algorithm is claimed in element 1.2, the evaluator will change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source. The evaluator shall use a packet sniffer to capture the network traffic between the TOE and the NTP server. The evaluator uses the captured network traffic, to verify the NTP version, to observe time change of the TOE and uses the TOE's audit log to determine that the TOE accepted the NTP server's timestamp update. The captured traffic is also used to verify that the appropriate message digest algorithm was used to authenticate the time source and/or the appropriate protocol was used to ensure integrity of the timestamp that was transmitted in the NTP packets.
Test Flow	• TOE only supports SHA1 to authenticate message digest algorithm • Show NTP server supported message digest algorithms • Configure TOE message digest algorithm to MD5 which does not match the configuration on the NTP server • Gather test and capture packets • Verify that TOE does not authenticate and sync time to NTP server • On the TOE set new time and configure TOE to support SHA1 message digest algorithm • Gather test log and capture packets • Verify test log and packet capture that TOE successfully synced to NTP server time

Pass/Fail Explanation	TOE successfully authenticates remote NTP server with valid message digest algorithm and denies authentication if presented with invalid message algorithm.
Result	PASS

5.2.37 FCS_NTP_EXT.1.3 Guidance 1

The evaluator shall examine the guidance documentation to ensure it provides the Security Administrator instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated.

5.2.37.1 Evaluator Findings

The evaluator examined the section titled 11 Setting Time Using NTP Synchronization in the AGD to verify that it provides instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. Upon investigation, the evaluator found that the AGD states the following:

Note: The Waveserver device does not accept broadcast and multicast NTP packets by default hence there are no provisioning steps.

Based on these findings, this assurance activity is considered satisfied.

5.2.37.2 Verdict

Pass

5.2.38 FCS_NTP_EXT.1.3 Test #1

Item	**Data/Description**
Test ID	FCS_NTP_EXT.1.3 T1
Objective	The evaluator shall configure NTP server(s) to support periodic time updates to broadcast and multicast addresses. The evaluator shall confirm the TOE is configured to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. The evaluator shall check that the time stamp is not updated after receipt of the broadcast and multicast packets.
Test Flow	• Configure NTP server(s) to support periodic time updates to broadcast and multicast addresses. • TOE is configured to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. • Gather test log and capture packets • Verify that TOE does not accept time updates from broadcast and multicast addresses
Pass/Fail Explanation	TOE does not accept NTP broadcast or multicast messages from an NTP server.

Result	PASS

5.2.39 FCS_NTP_EXT.1.4 Test #1

Item	**Data/Description**
Test ID	FCS_NTP_EXT.1.4 T1
Objective	The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is updated after receipt of the NTP packets. The purpose of this test to verify that the TOE can be configured to synchronize with multiple NTP servers. It is up to the evaluator to determine that the multi- source update of the time information is appropriate and consistent with the behaviour prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4. **TD0528 Has been applied**
Test Flow	• On the TOE add NTP SHA1 message authentication • Add 3 NTP servers • Set test time, enable NTP1, and verify that TOE is updated with NTP1 server time • Disable NTP1, set new test time and make sure the new NTP3 is selected and TOE time is updated • Disable NTP3, set new test time and make sure the new NTP2 is selected and that TOE time is updated
Pass/Fail Explanation	TOE successfully supports 3 NTP servers and that it accepts NTP packets that would result in the timestamp being updated from each of the NTP servers.
Result	PASS

5.2.40 FCS_NTP_EXT.1.4 Test #2

Item	**Data/Description**
Test ID	FCS_NTP_EXT.1.4 T2
Objective	Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers). The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system

	time. This rogue time source needs to be configured in a way (e.g. degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behaviour of a correctly-functioning NTP server. **TD0528 Has been applied**
Test Flow	• Configure and enable TOE as NTP client • Add an NTP server to the TOE • Set TOE test time • Using TCP replay utility to send NTP sync request to the TOE • Verify that TOE does not accept request from another NTP source
Pass/Fail Explanation	TOE does not accept NTP Sync Request from another NTP source.
Result	PASS

5.3 Test Cases (SSHS)

5.3.1 FCS_SSHS_EXT.1.2 TSS 1 ***[TD0631]***

The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims).

The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.

If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS

5.3.1.1 Evaluator Findings

The evaluator checked to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and ensure that password-based authentication methods are also allowed. The definition of FCS_SSHS_EXT.1 in section 5.2.2 titled "Class: Cryptographic Support (FCS)" in ST and the TSS entry for FCS_SSHS_EXT.1 in the section 6 titled "TOE Summary Specification" of ST were used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS identifies the following public key algorithms for authentication,

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

Next, the evaluator examined the definition of FCS_SSHS_EXT.1 in ST and found that the identified public key algorithms to be consistent with the public key algorithms specified in the TSS. Finally, the evaluator again reviewed the TSS of ST and found that the TSS states that password-based authentication is supported for SSH users. The evaluator also verified that the TSS consists of information pertaining to how the TOE establishes user identity when an SSH client presents a public key or X.509v3 certificate. The TSS states the following:

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

All algorithms listed in TSS for FCS_SSHS_EXT.1 line up with the claimed algorithms under FCS_COP.1/SigGen.

Based on these findings, this assurance activity is considered satisfied.

5.3.1.2 Verdict

Pass

5.3.2 FCS_SSHS_EXT.1.2 Test 1

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.2_T1
Objective	Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. **TD0631 has been applied**
Test Flow	• Open an SSH terminal • Connect to the TOE using the correct credentials • Verify that the connection is a success

Pass/Fail Explanation	The TOE can successfully authenticate a user after a successful login attempt. This meets testing requirements.
Result	PASS

5.3.3 FCS_SSHS_EXT.1.2 Test 2

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.2_T2
Objective	Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. **TD0631 has been applied**
Test Flow	• Create a user and assign ECDSA-256 public key • Attempt to login with different key • Gather test log and capture packets • Verify test log and packets capture that user is rejected.
Pass/Fail Explanation	The TOE does not allow access to the admin account over SSH with an unknown public key pair. This meets testing requirements.
Result	PASS

5.3.4 FCS_SSHS_EXT.1.2 Test 3

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.2_T3
Objective	Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client. **TD0631 has been applied**
Test Flow	• On the TOE create super user named test using password authentication method • Attempt to login the TOE using test account • Gather test log and verify that test user is successfully logged in the TOE

Pass/Fail Explanation	Use of correct credentials allows access to the TOE.
Result	PASS

5.3.5 FCS_SSHS_EXT.1.2 Test 4

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.2_T4
Objective	Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client. **TD0631 has been applied**
Test Flow	• Attempt to login using previously created su user with invalid password • Gather test log and verify that su user authentication fails.
Pass/Fail Explanation	Invalid credentials should result in unsuccessful authentication.
Result	PASS

5.3.6 FCS_SSHS_EXT.1.3 TSS 1

The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.

5.3.6.1 Evaluator Findings

The evaluator examined the TSS to determine if it describes how large packets are handled. The TSS entry for FCS_SSHS_EXT.1 in the section 6 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS of ST states that “The TOE accepts packet size up to 256K and meets the requirements of RFC 4253".

Based on these findings, this assurance activity is considered satisfied.

5.3.6.2 Verdict

Pass

5.3.7 FCS_SSHS_EXT.1.3 Test 1

Item	**Data/Description**

Test ID	FCS_SSHS_EXT.1.3_T1
Objective	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Note	*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.*
Test Flow	• Run Acumen tool to log in the TOE and then send a packet larger than 256K bytes. • Gather test log and verify that large packet dropped
Pass/Fail Explanation	TOE drops large packet than maximum size allowed and logs the error. This meets the testing requirements.
Result	PASS

5.3.8 FCS_SSHS_EXT.1.4 TSS 1

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.

5.3.8.1 Evaluator Findings

The evaluator examined the TSS to determine if optional SSH characteristics and supported encryption algorithms are specified. The definition of FCS_SSHS_EXT.1 in section 5.2.2 titled “Class: Cryptographic Support (FCS)” and TSS entry for FCS_SSHS_EXT.1 in the section 6 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity. The evaluator first examined the TSS of ST to identify the encryption algorithms supported for SSH connections by the TOE. The following algorithms are identified as supported within the TSS:

- AES128-CTR
- AES256-CTR
- AES128-GCM@openssh.com
- AES256-GCM@openssh.com

Next, the evaluator examined the definition of FCS_SSHS_EXT.1 in ST. The evaluator found that the symmetric encryption specified in the definition of the SFR are consistent with the description within the TSS of ST. Finally, the evaluator reviewed the TSS to ensure that any optional characteristics supported by the TOE are described. The evaluator found that the TSS describes the following optional characteristics for SSH connections described:

- No optional SSH characteristics are supported by the TOE

Based on this the assurance activity is considered satisfied.

5.3.8.2 Verdict

Pass

5.3.9 FCS_SSHS_EXT.1.4 Guidance 1

The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

5.3.9.1 Evaluator Findings

The evaluator examined the guidance document "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine if it contains instructions on configuring the TOE so that SSH conforms to the descriptions in the TSS. The section 7 titled "Cryptographic Protocols" was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that no configuration is required for SSH and the required algorithms are used automatically when the CC-NDcPP compliance is enabled.

Based on these findings, this assurance activity is considered satisfied.

5.3.9.2 Verdict

Pass

5.3.10 FCS_SSHS_EXT.1.4 Test 1

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.4_T1
Objective	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish a SSH connection. To verify this, the evaluator shall start session establishment for a SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.
Note	*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].
Test Flow	- From an SSH client, connect to the TOE using AES-256-CTR as the cipher - The connection succeeds - Verify by examining the packet capture that the connection succeeds using AES-CTR-256 - Repeat the above steps for any additional symmetric algorithms supported by the TOE
Pass/Fail Explanation	The TOE is able to use each of the claimed symmetric algorithms for SSH connections. This meets the testing requirements.
Result	PASS

*5.3.11 FCS_SSHS_EXT.1.5 TSS 1 **[TD0631]***

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component..

5.3.11.1 Evaluator Findings

The evaluator examined the TSS to determine supported public key algorithms. The definition of FCS_SSHS_EXT.1 in section 5.2.2 titled "Class: Cryptographic Support (FCS)" and TSS entry for FCS_SSHS_EXT.1 in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator first examined the TSS of ST to identify the public key algorithms supported for SSH connections by the TOE. The following public key algorithms are identified as supported within the TSS,

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

Next, the evaluator examined the definition of FCS_SSHS_EXT.1 in ST. The evaluator found that the public key algorithms specified in the definition of the SFR are consistent with the description within the TSS of ST.

Based on this the assurance activity is considered satisfied.

5.3.11.2 Verdict

Pass

5.3.12 FCS_SSHS_EXT.1.5 Guidance 1

The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

5.3.12.1 Evaluator Findings

The evaluator examined the guidance document "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine if it contains instructions on configuring the TOE so that SSH conforms to the descriptions in the TSS. The section 7 titled "Cryptographic Protocols" was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that no configuration is required for SSH and the required algorithms are used automatically by default.

Based on these findings, this assurance activity is considered satisfied.

5.3.12.2 Verdict

Pass

5.3.13 FCS_SSHS_EXT.1.5 Test 1

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.5_T1
Objective	Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. **TD0631 has been applied**
Note	*FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation [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.*
Test Flow	• Show supported public key algorithms • On TOE generate test public key and assign to a user • Remote login TOE using supported public key-based authentication • Supported key are: ecdsa256, ecdsa384, ecdsa521, ssh_rsa, rsa_sha256 and rsa_sha512. • Gather test log and capture packets • Verify test log and packets capture that user successfully authenticates with public key-based
Pass/Fail Explanation	TOE successfully authenticates user with all supported public keys: ecdsa256, ecdsa384, ecdsa521, ssh_rsa, rsa_sha256 and rsa_sha512

Result	PASS

5.3.14 FCS_SSHS_EXT.1.5 Test 2

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.5_T2
Objective	Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected. **TD0631 has been applied**
Test Flow	• On the TOE show public key supported • Create a user rsa4096 and assign RSA4096 to the user • Attempt to establish SSH connection with public key ssh-dss which the TOE does not support • Gather test log and capture packets • Verify connection fails
Pass/Fail Explanation	TOE denies user log in if presented with unsupported public key.
Result	PASS

5.3.15 FCS_SSHS_EXT.1.6 TSS 1

The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that list corresponds to the list in this component.

5.3.15.1 Evaluator Findings

The evaluator examined the TSS to ensure that it lists all supported data integrity algorithms. The definition of FCS_SSHS_EXT.1 in section 5.2.2 titled “Class: Cryptographic Support (FCS)” and TSS entry for FCS_SSHS_EXT.1 in the section 6 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity. The evaluator first examined the TSS of ST to identify the data integrity algorithms supported for SSH connections by the TOE. The following data integrity algorithms are identified as supported within the TSS,

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

Next, the evaluator examined the definition of FCS_SSHS_EXT.1 in ST. The evaluator found that the data integrity algorithms specified in the definition of the SFR are consistent with the description within the TSS of ST.

Based on this the assurance activity is considered satisfied.

5.3.15.2 Verdict

Pass

5.3.16 FCS_SSHS_EXT.1.6 Guidance 1

The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).

5.3.16.1 Evaluator Findings

The evaluator examined the guidance document "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document " to determine if it contains instructions on configuring the TOE so that SSH conforms to the descriptions in the TSS. The section 7 titled "Cryptographic Protocols" was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that no configuration is required for SSH and the required algorithms are used automatically when the CC-NDcPP compliance is enabled.

Based on these findings, this assurance activity is considered satisfied.

5.3.16.2 Verdict

Pass

5.3.17 FCS_SSHS_EXT.1.6 Test 1

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.6_T1
Objective	*(conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST)* *The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.* *Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.*
Note	*FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512] and [implicit] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).*
Test Flow	• From an SSH client, connect to the TOE using HMAC-SHA-2-256 as the data integrity algorithm ○ The connection succeeds • Verify by examining the packet capture that the connection succeeds using HMAC-SHA-2-256 • Repeat the above steps for any additional data integrity algorithm claimed to be supported by the TOE (*hmac-sha2-512, implicit)*

Pass/Fail Explanation	The TOE is able to make SSH connections with each claimed data integrity algorithm. This meets the testing requirements.
Result	PASS

5.3.18 FCS_SSHS_EXT.1.6 Test 2

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.6_T2
Objective	*(conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST)* *The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.* *Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*- gcm@openssh.com encryption algorithm is negotiated while performing this test.*
Note	*FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512] and [implicit] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).*
Test Flow	• Configure an SSH client to connect with the TOE using only the "HMAC-MD5" MAC • Attempt to connect to the TOE using the SSH client configured to only support "HMAC-MD5" MAC • Verify that the connection is rejected
Pass/Fail Explanation	The TOE rejects SSH connections using the hmac-md5 (a non-supported) MAC for data integrity. This meets the testing requirements.
Result	PASS

5.3.19 FCS_SSHS_EXT.1.7 TSS 1

The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that list corresponds to the list in this component.

5.3.19.1 Evaluator Findings

The evaluator examined the TSS to ensure that it lists the supported key exchange algorithms. The definition of FCS_SSHS_EXT.1 in section 5.2.2 titled "Class: Cryptographic Support (FCS)" and TSS entry for FCS_SSHS_EXT.1 in the section 6 titled "TOE Summary Specification" of ST was used to determine the verdict of this assurance activity. The evaluator first examined the TSS of ST to identify the key exchange algorithms supported for SSH connections by the TOE. The following key exchange algorithms are identified as supported within the TSS,

- diffie-hellman-group14-sha1

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Next, the evaluator examined the definition of FCS_SSHS_EXT.1 in ST. The evaluator found that the key exchange algorithms specified in the definition of the SFR are consistent with the description within the TSS of ST.

Based on this the assurance activity is considered satisfied.

5.3.19.2 Verdict

Pass

5.3.20 FCS_SSHS_EXT.1.7 Guidance 1

The evaluator shall also check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.

5.3.20.1 Evaluator Findings

The evaluator examined the guidance document "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document " to determine if it contains instructions on configuring the TOE so that SSH conforms to the descriptions in the TSS. The section 7 titled "Cryptographic Protocols" was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that no configuration is required for SSH and the required algorithms are used automatically when the CC-NDcPP compliance is enabled.

Based on these findings, this assurance activity is considered satisfied.

5.3.20.2 Verdict

Pass

5.3.21 FCS_SSHS_EXT.1.7 Test 1

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.7_T1
Objective	The evaluator shall configure an SSH client to only allow the diffiehellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Flow	• Configure an SSH client to connect with the TOE using only diffiehellman-group1-sha1 as the key exchange method • Attempt to connect to the TOE using the SSH client configured to only support diffiehellman-group1-sha1 as the key exchange method • Verify that the connection is rejected

Pass/Fail Explanation	The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements.
Result	PASS

5.3.22 FCS_SSHS_EXT.1.7 Test 2

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.7_T2
Objective	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Note	*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.*
Test Flow	• From an SSH client, connect to the TOE using diffie-hellman-group14-sha1 as the key exchange method a. The connection succeeds • Verify by examining the packet capture that the connection succeeds using diffie-hellman-group14-sha1 • Repeat the above steps for each additional key exchange method claimed to be supported by the TOE (*ecdh-sha2-nistp256,ecdh-sha2-nistp384 ecdh-sha2-nistp521)*
Pass/Fail Explanation	The TOE is able to make SSH connections with each claimed data key exchange method. This meets the testing requirements.
Result	PASS

5.3.23 FCS_SSHS_EXT.1.8 TSS 1

The evaluator shall check that the TSS specifies the following:

1. Both thresholds are checked by the TOE.

2. Rekeying is performed upon reaching the threshold that is hit first.

5.3.23.1 Evaluator Findings

The evaluator checked that the section 6 - TSS specifies the rekeying thresholds supported by the TOE. The FCS_SSHS_EXT.1 of the TSS of ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states, “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.

Based on these findings, this activity is considered satisfied.

5.3.23.2 Verdict

PASS

5.3.24 FCS_SSHS_EXT.1.8 Guidance 1

If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.

5.3.24.1 Evaluator Findings

The evaluator examined the guidance document “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document ” to determine if it contains instructions on configuring the threshold for SSH rekey, either time or volume. The section 3.2 titled “Configuring SSH Thresholds” was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found “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.
NOTE: There is no additional configuration necessary to enable SSH thresholds as it is supported by default.”

Based on these findings, this assurance activity is considered satisfied.

5.3.24.2 Verdict

Pass

5.3.25 FCS_SSHS_EXT.1.8 Test 1

Item	**Data/Description**
Test ID	FCS_SSHS_EXT.1.8_T1
Objective	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the traffic-based threshold. For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the

	threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time, but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8). 530 The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic, but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions). In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met: a. An argument is present in the TSS section describing this hardware-based limitation and b. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.
Note	*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 no more than (1GB) of transmitted data. After either of the thresholds are reached a rekey needs to be performed.*

Test Flow	- Send enough data to initiate a rekey - Verify the rekey occurred - Wait the time allotted to initiate a rekey - Verify the rekey occurred
Pass/Fail Explanation	Rekey was initiated by the TOE after the traffic threshold is met. This meets the testing requirements.
Result	PASS

5.4 Test Cases (TLSC)

5.4.1 FCS_TLSC_EXT.1.1 TSS 1

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

5.4.1.1 Evaluator Findings

The evaluator examined the TSS to ensure that the ciphersuites supported are specified. The definition of FCS_TLSC_EXT.1 in section 5.2.2 titled “Class: Cryptographic Support (FCS)” and TSS entry for FCS_TLSC_EXT.1 in the section 6 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity.

The evaluator first examined the TSS of ST to identify the ciphersuites supported by the TOE for TLS client connections. The following ciphersuites are identified as supported within the TSS,

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

Next, the evaluator examined the definition of FCS_TLSC_EXT.1 in ST. The evaluator found that the ciphersuites for TLS client connection specified in the definition of the SFR are consistent with the description within the TSS of ST.

Based on these findings, the assurance activity is considered satisfied.

5.4.1.2 Verdict

Pass

5.4.2 FCS_TLSC_EXT.1.1 Guidance 1

The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.

5.4.2.1 Evaluator Findings

The evaluator examined the operational guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to ensure that it contains instructions on configuring the TOE as a TLS client. The section 3 titled 'Enabling CC-NDcPP Compliance' of the AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that AGD indicates that no configuration is needed to enforce the ciphers being used by the TOE when the TOE acts as a TLS client.

Based on these findings, this assurance activity is considered satisfied.

5.4.2.2 Verdict

Pass

5.4.3 FCS_TLSC_EXT.1.1 Test #1

– FCS_TLSC_EXT.1.1 Test 1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T1
Objective	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Note	*FCS_TLSC_EXT.1.1 The TSF shall implement [selection: 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_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289* • *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289* • *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*
Test Flow	• Attempt to connect to a TLS server using OpenSSL • Test against all claimed ciphers • Verify all claimed ciphers are successful
Pass/Fail Explanation	The TOE allows a connection on all claimed cipher suites. This meets testing requirements.
Result	Pass

5.4.4 FCS_TLSC_EXT.1.1 Test #2

– FCS_TLSC_EXT.1.1 Test #2	
Item	**Data/Description**

Test ID	FCS_TLSC_EXT.1.1_T2
Objective	*Test 2: The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.*
Test Flow	• Create a server certificate that contains Server Authentication purpose in the exetendedKeyUsage field. • On the TOE configure TLS communication to the remote server. • Remote login TOE and trigger TLS connection to the remote server. • Gather and verify TLS connection establish on test log • Gather and verify TLS negotiation packets are successful. • Create a server certificate that does not contain Server Authentication purpose in the exetendedKeyUsage field. • Repeat above test and verify TLS connection is not established as indicated on test log and TLS negotiation packets failed to negotiate.
Pass/Fail Explanation	The TOE did not allow for a connection with a certificate with an invalid server authentication in the extendedKeyUsage field but allowed for a connection with a certificate with a valid server authentication in the extendedKeyUsage.
Result	PASS

5.4.5 FCS_TLSC_EXT.1.1 Test #3

– FCS_TLSC_EXT.1.1 Test #3	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T3
Objective	The evaluator shall send a server certificate in the TLS connection that does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite). The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Test Flow	• Attempt to the connect to the TOE with a mismatched cipher suite • Verify the TOE rejects the handshake message • Verify with PCAP that the connection does not establish
Pass/Fail Explanation	The TOE denied a connection when the server ciphersuite did not match. This meets testing requirements.
Result	PASS

5.4.6 FCS_TLSC_EXT.1.1 Test #4a

– FCS_TLSC_EXT.1.1 Test #4a	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T4a

Objective	*The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.*
Test Flow	• Configure a server to offer a TLS_NULL_WITH_NULL_NULL cipher suite during a TLS connection • Attempt to connect to the TOE from the server • Verify this connection fails
Pass/Fail Explanation	The TOE did not connect when there was a NULL cipher offered from the server. This meets testing requirements.
Result	PASS

5.4.7 FCS_TLSC_EXT.1.1 Test #4b

– FCS_TLSC_EXT.1.1 Test #4b	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T4b
Objective	*Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.*
Test Flow	• Execute Acumen tool in attempt to establish TLS connection with unsupported cipher-suite TLS_RSA_WITH_NULL_MD5 • Gather test log and capture packets. Verify TLS connection fails on test log and TLS negotiate packet fails.
Pass/Fail Explanation	TOE successfully denies TLS connection if server presented with unsupported Cipher-Suite TLS_RSA_WITH_NULL_MD5.
Result	PASS

5.4.8 FCS_TLSC_EXT.1.1 Test #4c

– FCS_TLSC_EXT.1.1 Test #4c	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T4c
Objective	*[conditional]: If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension** the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.*
Test Flow	• Execute Acumen test tool to establish TLS connection using a non-supported secp256k1 curve/group • Gather test log and capture negotiated packets • Verify TLS connection fails on both test log and packets capture.
Pass/Fail Explanation	TOE rejects TLS connection if server presented with non-supported SECP256K1 EC curve group.

Result	PASS

5.4.9 FCS_TLSC_EXT.1.1 Test #5a

– FCS_TLSC_EXT.1.1 Test #5a	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T5a
Objective	a) Change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Flow	• Run the Acumen TLSC tool. • Attempt to connect to the TOE using an unsupported TLS version 1.0. • Gather test log and packets capture. • Verify the TOE does not connect.
Pass/Fail Explanation	TOE rejects TLS connection when presented with unsupported TLS versions
Result	Pass

5.4.10 FCS_TLSC_EXT.1.1 Test #5b

– FCS_TLSC_EXT.1.1 Test #5b	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T5b
Objective	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Flow	• Run Acumen tool to modify signature in the server key exchange and attempt to establish TLS connection. • Gather test log and packet capture. • Verify TLS connection fails on test log and verify TLS negotiate packets fail.
Pass/Fail Explanation	TOE successfully rejects TLS connection if server presented certificate with modified signature
Result	Pass

5.4.11 FCS_TLSC_EXT.1.1 Test #6a

– FCS_TLSC_EXT.1.1 Test #6a	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T6a

Objective	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish and no application data flows.
Test Flow	• Execute Acumen tool to modify a byte in server finished packet and attempt to establish TLS connection • Gather test log and verify that TLS connection fail and that no application data transmitted. Note that modification to the finished packet is not visible on Wireshark.
Pass/Fail Explanation	TOE rejects TLS connection if remote server presented with impaired finished message.
Result	Pass

5.4.12 FCS_TLSC_EXT.1.1 Test #6b

– FCS_TLSC_EXT.1.1 Test #6b	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T6b
Objective	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows
Test Flow	• Execute Acumen test tool to send garble message after the server issues the ChangeCipherSpec message. • Gather test log and capture packets using Wireshark. • Verify that TLS connection fails and packets fail to negotiate.
Pass/Fail Explanation	TOE does not complete TLS handshake, and no application data flows after sending a garbled message.
Result	Pass

5.4.13 FCS_TLSC_EXT.1.1 Test #6c

– FCS_TLSC_EXT.1.1 Test #6c	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T6c
Objective	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE cipher-suite) or that the server denies the client's Finished handshake message.
Test Flow	• Run Acumen tool to modify a byte in the server's nonce in the server hello packet and attempt to establish TLS connection. • Gather test log and capture packet. Note that modified byte are not visible on Wireshark captured packet. • Verify test log that TLS connection fails, and TLS packets fail to negotiate.

Pass/Fail Explanation	TOE Client rejects client’s Finished handshake message.
Result	Pass

5.4.14 FCS_TLSC_EXT.1.2 TSS 1

The evaluator shall ensure that the TSS describes the client’s method of establishing all reference identifiers from the administrator/application configured reference identifier, including which types of reference identifiers are supported (e.g. application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.

5.4.14.1 Evaluator Findings

The evaluator checked the TSS to determine if it describes the client’s method of establishing reference identifiers. The TSS entry for FCS_TLSC_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that the TSS describes the client’s method of establishing reference identifiers. Specifically, the TSS states the following, “The reference identifiers supported are: DNS names or IP addresses.” The TSS also states 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.

Based on these findings, the Assurance Activity is considered satisfied.

5.4.14.2 Verdict

Pass

5.4.15 FCS_TLSC_EXT.1.2 TSS 3

If IP addresses are supported in the CN as reference identifiers, the evaluator shall ensure that the TSS describes the TOE’s conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order. The evaluator shall also ensure that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced.

5.4.15.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that, if IP addresses are supported in the CN as reference identifiers, the TSS describes the TOE’s conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order and whether canonical format is enforced. Upon investigation, the evaluator found that the TSS states that 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 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.

Based on these findings, this assurance activity is considered satisfied.

5.4.15.2 Verdict

Pass

5.4.16 FCS_TLSC_EXT.1.2 Guidance 1

The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE includes support for IP addresses, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.

5.4.16.1 Evaluator Findings

The evaluator examined the operational guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to ensure that it contains instructions on configuring the TOE as a TLS client. The section 6.4 titled 'Configuring Reference Identifiers' of AGD was used to determine the verdict of this assurance activity.

Upon investigation, the AGD states the following related to TLS configuration, "The TOE supports DNS name and IP addresses as its reference identifiers."

When the syslog client or RADsec 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 TLS server setup must match the Certificate identifier scheme configuration with DNS vs IP Address format that is intended to be used otherwise the certificate will be rejected.

i.e. When users expect the TLS server certificate with an IP address format reference identifier, users shall configure the TOE to add the TLS server using IP address format. When users expect the TLS server certificate with an DNS format reference identifier, users shall configure the TOE to add the TLS server using DNS format.

The evaluator can configure the reference identifier of the TOE using the following instructions found in sections 4.4 and 5.1:

Syslog - Create a collector for TLS syslog with the desired attributes to enable the TOE to communicate with syslog server:

syslog tls create collector <IP address or host name> [custom-prefix <String: 1...15>] [fingerprint <fingerprint>] [facility <Number: 0..24>] [port <Number: 1..65535>] [severity <emergency | alert | error | warning | notice | info | debug | all>] [trusted-dns <trusteddns>]

RADSec - Add a RADSec server to the Waveserver 5 system, specifying a priority for the server:

radsec add server <IP address or host name> [priority <Number:1...8>] [port <Number:1...65535>]

Based on these findings, this assurance activity is considered satisfied.

5.4.16.2 Verdict

Pass

5.4.17 FCS_TLSC_EXT.1.2 Test #1

– FCS_TLSC_EXT.1.2 Test #1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T1
Objective	The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. *Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.*
Note	
Test Flow	• Send a certificate to the TOE that contains a mismatched CN and reference identifier without a SAN • Attempt to connect to the TOE • Verify the connection is rejected
Pass/Fail Explanation	The TOE rejects the connection when there is no CN that matched the reference identifier and there is no SAN extension. This meets testing requirements.
Result	PASS

5.4.18 FCS_TLSC_EXT.1.2 Test #2

– FCS_TLSC_EXT.1.2 Test 2	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T2
Objective	*The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall*

	verify that the connection fails. The evaluator shall repeat this test for each supported SAN type. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.
Test Flow	• Attempt to connect to the TOE with no identifier in the SAN that matches the reference identifier • Verify when the TOE connects that there is a failure • Capture evidence with Wireshark
Pass/Fail Explanation	The TOE denies a connection when the certificate does not contain an identifier in the SAN that matches the reference identifier. This meets testing requirements.
Result	PASS

5.4.19 FCS_TLSC_EXT.1.2 Test #3

– FCS_TLSC_EXT.1.2 Test 3	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T3
Objective	If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted
Test Flow	• Present a certificate with a CN that matches the reference identifier but no SAN extension • Verify that the handshake is successful • Verify that the connection succeeds
Pass/Fail Explanation	The TOE successfully connected to the server when the CN matches the reference identifier and does not contain the SAN extension. This meets testing requirements.
Result	PASS

5.4.20 FCS_TLSC_EXT.1.2 Test #4

– FCS_TLSC_EXT.1.2 Test 4	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T4
Objective	The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).
Test Flow	• Attempt to connect to the TOE with a certificate with mismatched reference identifier and no SAN • Watch the handshake and verify that it succeeds

	- Verify that the TOE successfully connects
Pass/Fail Explanation	The TOE had a successful connection when the SAN matches the reference identifier while the CN does not. This meets testing requirements.
Result	PASS

5.4.21 FCS_TLSC_EXT.1.2 Test #5 (a)

– FCS_TLSC_EXT.1.2 Test #5 (a)	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T5a
Objective	The evaluator shall perform the following wildcard test with each supported type of reference identifier. The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
Test Flow	- Connect to the TOE with a wildcard in the wrong position - Attempt a handshake - Verify that the handshake fails
Pass/Fail Explanation	The TOE denied a connection when the wildcard was not in the proper position. This meets testing requirements.
Result	Pass

5.4.22 FCS_TLSC_EXT.1.2 Test #5 (b)

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T5b
Objective	The evaluator shall perform the following wildcard test with each supported type of reference identifier. The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds. The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.come) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Flow	- Connect to the TOE with a wildcard in the leftmost position - Verify success - Connect to the TOE with no wildcard - Verify failure

	• Connect to the TOE with two left most identifiers • Verify failure
Pass/Fail Explanation	The TOE made a successful connection when there was one single left-most label in the reference identifier. When there were two left most label, the TOE refused connection. This meets testing requirements.
Result	Pass

5.4.23 FCS_TLSC_EXT.1.2 Test #6

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T6
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT**. [conditional] If IP address identifiers are supported in the SAN or CN, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with a wildcard asterisk (*) (e.g. CN=*.168.0.1 when connecting to 192.168.0.1, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g. IPv4, IPv6). This negative test corresponds to the following section of the Application Note 64/105: "The exception being, the use of wildcards is not supported when using IP address as the reference identifier." [TD0790 applied] Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 6.
Test Flow	• Create server certificates with invalid CN IPv4 and IPv6 where one of the groups of the address has been placed with * • On the TOE create RADSEC & syslog configuration. • Attempt to login TOE to trigger TLS connection. • Gather test log and capture packets. • Verify test log and negotiate packets that TLS connection fails.
Pass/Fail Explanation	TOE rejects TLS connection if server presented its certificate’s CN field that contains * in its IP address group.
Result	Pass

5.4.24 FCS_TLSC_EXT.1.3 Test #1

– FCS_TLSC_EXT.1.3 Test #1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.3_T1
Objective	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Test Flow	• Duplicate test case FIA_X509_EXT_1.1 Test#1a (valid chain)
Pass/Fail Explanation	When there was a valid path, the test succeeded. This meets testing requirements.
Result	Pass

5.4.25 FCS_TLSC_EXT.1.3 Test #2

– FCS_TLSC_EXT.1.3 Test #2	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.3_T2
Objective	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
Test Flow	• Duplicate test case FIA_X509_EXT_1.1 Test#1b (broken chain), FIA_X509_EXT_1.1 Test#2 (expired certificate) and FIA_X509_EXT_1.1 Test #3 (Revoked certificate)
Pass/Fail Explanation	The TOE denied a connection when there was no valid certificate path. This meets testing requirements.
Result	Pass

5.4.26 FCS_TLSC_EXT.1.4 TSS 1

The evaluator shall verify that TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured.

5.4.26.1 Evaluator Findings

The evaluator verified that TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. The TSS entry for FCS_TLSC_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that the TSS provides full details regarding the TOE support for ECDH parameters, as follows, "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."

Based on these findings, this assurance activity is considered satisfied.

5.4.26.2 Verdict

Pass

5.4.27 FCS_TLSC_EXT.1.4 Guidance 1

If the TSS indicates that the Supported Elliptic Curves Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves Extension

5.4.27.1 Evaluator Findings

The evaluator examined the operational guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to ensure that it contains instructions on configuring the supported Elliptic Curves Extension. Upon investigation, the evaluator found that section 3 "Enabling CC-NDcPP Compliance" of AGD provides the Supported Elliptic Curves Extension configured on the TOE when the CC-NDcPP compliance is enabled. The AGD states the following:

The following EC curves are supported by default on the device and no other curves are allowed or enabled:

- secp256r1
- secp384r1
- secp521r1

Based on these findings, this assurance activity is considered satisfied.

5.4.27.2 Verdict

Pass

5.4.28 FCS_TLSC_EXT.1.4 Test #1

– FCS_TLSC_EXT.1.4 Test #1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.4_T1
Objective	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.

Test Flow	- For each EC support secp256r1_kex, secp384r1_kex and secp521r1_kex, and perform the followings: - Create certificate using each EC curve. - Configure TOE to support RADSEC. - Start remote TLS server. - Attempt to login TOE to trigger TLS connection. - Gather test log and capture packets. - Verify test log and negotiate packets that TLS connection succeeds
Pass/Fail Explanation	TOE successfully establishes TLS connection to both RADSEC and SYSLOG servers using CE curves secp256r1, secp384r1 and secp521r1.
Result	Pass

5.4.29 FCS_TLSC_EXT.2.1 TSS 1

The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.

5.4.29.1 Evaluator Findings

The evaluator ensured that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. The FCS_TLSC_EXT.2.1 entry of TSS within the section 6 of the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS includes a description of the TLS Mutual authentication handshake used by the TOE for connections. The TSS states the following:

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.

Based on these findings, this assurance activity is considered satisfied.

5.4.29.2 Verdict

Pass

5.4.30 FCS_TLSC_EXT.2.1 Guidance 1

If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication.

5.4.30.1 Evaluator Findings

The evaluator verified that the AGD guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” includes instructions for configuring the client-side certificates for TLS mutual authentication. The entirety of the AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that the guidance documentation provides instructions for configuring client-side certificates in the section 5 “Configuring RADsec Authentication” and section 4.4

“Audit Server Configuration.” The certificates are then used for client-side connection for TLS mutual authentication. The sections state the following:

RADsec:

1. Install the X.509 certificate for RADSec:
    - certificates entity install cert-name <String: cert_name> {default-ftp-server | default-sftp-server | default-tftpserver | default-server | default-scp-server | sftpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftpserver <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]> certpassphrase [certificate-only]

    - For example:
        - certificates entity **install cert-name <Entity Name> default-scp-server filename <Path/File.p12> certpassphrase ************
        - **certificates entity install cert-name <Entity Name> scp-server <IP address> login-id <user-name> password <password> filename <Path/File.p12> cert-passphrase ************

2. Optionally, display the installed certificate:
    - **certificates authorities show**
    - **certificates entity show**

3. Specify the global RADSec settings:
    - **radsec set [cert-name <String: cert_name>] [timeout <Seconds: 1..30>]**

Syslog:

1. To use an audit server:
   create a private key and install a device trusted CA certificate as follows:
    - **certificates authorities install {default-ftp-server | default-sftp-server | default-tftserver | defaultserver | default-scpserver | sftp-server <IP address or host name>**
      login-id <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scp-server <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]>

- For example**: certificates authorities install cert-name <CA Name> default-scp-server filename <Path/File>**

2. Set the TLS syslog certificate name to the certificate you installed in step 1:
    - **syslog tls set cert-name <String: cert_name> For example: syslog tls set cert-name tlssyslogcert**

Based on these findings, this assurance activity is considered satisfied.

5.4.30.2 Verdict

Pass

5.4.31 FCS_TLSC_EXT.2.1 Test #1

– FCS_TLSC_EXT.2.1 Test #1	
Item	**Data/Description**
Test ID	FCS_TLSC_EXT.2.1_T1
Objective	**TD0670** The evaluator shall establish a connection to a peer server that is configured for mutual authentication (i.e. sends a server Certificate Request (type 13) message). The evaluator observes that the TOE TLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages during its negotiation of a TLS channel and that Application Data is sent.
Test Flow	• Create Certificates for both client and server • Configure TOE to support RADSEC & syslog • Add TLS server openssl verify option to request client to send certificate for mutual authentication. • Attempt to remote login to TOE to trigger TLS connection. • Gather test log and capture packets • Verify that TLS connection is established on test log. • Verify captured packets for mutual authentication.
Pass/Fail Explanation	The TOE successfully establishes TLS connection if remote server is configured for mutual authentication.
Result	Pass

5.5 Test Cases (TLSS)

5.5.1 FCS_TLSS_EXT.1.1 TSS 1

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.

5.5.1.1 Evaluator Findings

The evaluator first examined the entry for FCS_TLSS_EXT.1.1 in section 6 - TSS of ST to identify the ciphersuites supported by the TOE for TLS server connections. The following ciphersuites are identified as supported within the TSS,

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

Next, the evaluator examined the definition of FCS_TLSS_EXT.2 in section 5.2.2 of the ST. The evaluator found that the ciphersuites for TLS client connection specified in the definition of the SFR are consistent with the description within the TSS of ST.

Based on this the assurance activity is considered satisfied.

5.5.1.2 Verdict

Pass

5.5.2 FCS_TLSS_EXT.1.1 Guidance 1

The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

5.5.2.1 Evaluator Findings

The evaluator examined the operational guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to ensure that it contains instructions on configuring the TOE as a TLS server. The section 7 titled ‘Cryptographic Protocols’ of AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that AGD identifies the method for configuring TLS server communications on the TOE.

Based on these findings, this assurance activity is considered satisfied.

5.5.2.2 Verdict

Pass

5.5.3 FCS_TLSS_EXT.1.1 Test #1

Item	***Data/Description***

Test ID	*FCS_TLSS_EXT.1.1 Test #1*
Objective	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Flow (generic test steps)	• Attempt to connect to the client from the TOE with all claimed ciphersuites • Verify all correct ciphersuites are used in the process • Capture evidence with Wireshark
Pass/Fail Explanation	The TOE allowed for only claimed ciphers to connect. This meets testing requirements.
Result	PASS

5.5.4 FCS_TLSS_EXT.1.1 Test #2

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.1 Test #2
Objective	The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
Test Flow (generic test steps)	• Attempt to connect to the TOE using an invalid ciphersuite • Verify that the TOE denies a connection • Verify that there is failure
Pass/Fail Explanation	• The TOE denied a connection due to a weak cipher. This meets testing requirements.
Result	PASS

5.5.5 FCS_TLSS_EXT.1.1 Test #3a

Item	***Data/Description***
Test ID	*FCS_TLSS_EXT.1.1 Test #3a*
Objective	The evaluator shall perform the following modifications to the traffic: Modify a byte in the Client Finished handshake message, and verify that the server rejects the connection and does not send any application data.
Test Flow (generic test steps)	• Run the acumenTLSS tool • Show the output of the test • Show packet capture

Pass/Fail Explanation	TOE Server rejects the connection with a modified byte on Client Finished handshake message.
Result	PASS

5.5.6 FCS_TLSS_EXT.1.1 Test #3b

Item	***Data/Description***
Test ID	*FCS_TLSS_EXT.1.1 Test #3b*
Objective	(Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.) The evaluator shall use one of the claimed cipher-suites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent. The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.
Test Flow (generic test steps)	• Run Acumen test tool to establish TLS connection with a supported cipher-suite. • Verify TLS connection successfully established. • Capture packets Verify finished message is encrypted.
Pass/Fail Explanation	TOE Server TLS implementation correctly make use of the key exchange and authentication algorithms.
Result	PASS

5.5.7 FCS_TLSS_EXT.1.2 TSS 1

The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.

5.5.7.1 Evaluator Findings

The evaluator ensured that the TSS contains a description of the denial of old SSL and TLS versions. The FCS_TLSS_EXT.2 entry of section 6 - TSS within the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states that, “The TOE denies connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1.” The TSS also states that, “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.”

Based on these findings, this assurance activity is considered satisfied.

5.5.7.2 Verdict

Pass

5.5.8 FCS_TLSS_EXT.1.2 Guidance 1

The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.

5.5.8.1 Evaluator Findings

The evaluator examined the operational guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to ensure that it contains instructions on configuring the TOE as a TLS server. The section 4.3 titled ‘System Behavior’ of AGD was used to determine the verdict of this assurance activity. Upon investigation, the AGD states that the TOE supports TLS v1.2. No configuration is necessary to enforce TLSv1.2 connection due to the device denying connections from clients requesting any lower SSL versions.

Based on these findings, this assurance activity is considered satisfied.

5.5.8.2 Verdict

Pass

5.5.9 FCS_TLSS_EXT.1.2 Test #1

Item	***Data/Description***
Test ID	*FCS_TLSS_EXT.1.2 Test #1*

Objective	*The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.*
Note	*FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [TLS 1.1].*
Test Flow (generic test steps)	• Connect to the TOE using an older version of TLS • Verify when there is a connection attempt with an old TLS version, a description of denial is sent
Pass/Fail Explanation	The TOE successfully denied a connection with an unsupported protocol version. This meets testing requirements.
Result	PASS

5.5.10 FCS_TLSS_EXT.1.3 TSS 1 **[TD0635]**

If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14.

5.5.10.1 Evaluator Findings

The evaluator ensured that the TSS describes the key agreement parameters of the server Key Exchange message. The FCS_TLSS_EXT.1 entry of section 6 - TSS within the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS states that, “The TOE performs key establishment for TLS using ECDHE curves: secp256r1, secp384r1, secp521r1.”

Based on these findings, this assurance activity is considered satisfied.

5.5.10.2 Verdict

Pass

5.5.11 FCS_TLSS_EXT.1.3 Guidance 1

The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.

5.5.11.1 Evaluator Findings

The evaluator verified that the AGD guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” includes instructions for configuring the RSA keys. The entirety of the AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that section 7 of the guidance documentation "Cryptographic Protocols" contains the command to enable mutual authentication and no further configuration is needed for TLS.

Based on these findings, this assurance activity is considered satisfied.

5.5.11.2 Verdict

Pass

5.5.12 FCS_TLSS_EXT.1.3 Test #1a

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.1.3 Test# 1a*
Objective	[conditional] If ECDHE ciphersuites are supported: a) The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.
Test Flow (generic test steps)	• Run Acumen tool to establish TLS connection using the following EC curves (secp256r1, secp384r1, and secp521r1) • Capture TLS packets • Verify that TLS connections successfully establish using supported EC curves.
Pass/Fail Explanation	TOE successfully establishes TLS connections using supported EC curves SECP256R1, SECP384R1, and SECP521R1.
Result	PASS

5.5.13 FCS_TLSS_EXT.1.3 Test #1b

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.1.3 Test# 1b*
Objective	[conditional] If ECDHE ciphersuites are supported: b) The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established
Test Flow (generic test steps)	• Run Acumen test tool to initiate TLS connection to the TOE using unsupported EC curve SECP256K1 • Gather test log and capture packets • Verify TLS connection fails and server does not reply with Server Hello message.

Pass/Fail Explanation	TOE rejects TLS connection if client presented with Client Hello message with unsupported EC curve SECP256K1.
Result	PASS

5.5.14 FCS_TLSS_EXT.1.3 Test #2

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.1.3 Test# 2*
Objective	[conditional] If DHE ciphersuites are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).
Test Flow (generic test steps)	N/A – The TOE does not support DHE ciphersuites
Pass/Fail Explanation	N/A – The TOE does not support DHE ciphersuites
Result	N/A

5.5.15 FCS_TLSS_EXT.1.3 Test #3

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.1.3 Test# 3*
Objective	If **RSA key establishment ciphersuites** are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.
Test Flow (generic test steps)	N/A – The TOE does not support RSA key establishment ciphersuites
Pass/Fail Explanation	N/A – The TOE does not support RSA key establishment ciphersuites
Result	N/A

5.5.16 FCS_TLSS_EXT.1.4 TSS 1

The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).

5.5.16.1 Evaluator Findings

The evaluator examined the section titled 5.2.2.14 in the Security Target. Upon investigation, the evaluator found that the ST states that the TSF shall support no session resumption or session tickets.

Based on these findings, this assurance activity is considered satisfied.

5.5.16.2 Verdict

Pass

5.5.17 FCS_TLSS_EXT.1.4 Test #1

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.1.4 Test# 1*
Objective	[conditional]: If the TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077, the evaluator shall perform the following test: a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket. b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake). c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps: Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID. d) The client completes the TLS handshake and captures the SessionID from the ServerHello. e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session using the SessionID captured in step d). f) The client verifies the TOE (1) implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data. *Remark: If multiple contexts are supported for session resumption, the session ID or session ticket may be obtained in one context for resumption in another context. It is possible that one or more contexts may only permit the construction of sessions to be reused in other contexts but not actually permit resumption themselves. For contexts which do not permit resumption, the evaluator is required to verify this behaviour subject to the description provided in the TSS. It is not mandated that the session establishment and session resumption share context. For example, it is acceptable for a control channel to establish and application channel to resume the session.*
Test Flow (generic test steps)	a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket. b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake). c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps: Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID. d) The client completes the TLS handshake and captures the SessionID from the ServerHello.

	e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session using the SessionID captured in step d). f) The client verifies the TOE: a. implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or b. terminates the connection in some way that prevents the flow of application data.
Pass/Fail Explanation	The TOE does not use session resumption or session tickets, and this meets requirement.
Result	Pass

5.5.18 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 TSS 1

The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.

5.5.18.1 Evaluator Findings

The evaluator ensured that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. The FCS_TLSS_EXT.2 entry of section 6 - TSS within the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS includes a description of the TLS Mutual authentication handshake used by the TOE for connections.

Based on these findings, this assurance activity is considered satisfied.

5.5.18.2 Verdict

Pass

5.5.19 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 TSS 2

The evaluator shall verify the TSS describes how the TSF uses certificates to authenticate the TLS client. The evaluator shall verify the TSS describes if the TSF supports any fallback authentication functions (e.g. username/password, challenge response) the TSF uses to authenticate TLS clients that do not present a certificate. If fallback authentication functions are supported, the evaluator shall verify the TSS describes whether the fallback authentication functions can be disabled.

5.5.19.1 Evaluator Findings

The evaluator ensured that the TSS description required per FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 includes how the TSF uses certificates to authenticate the TLS client. The evaluator also ensured that the description provides details on if the TSF supports any fallback authentication function. The FCS_TLSS_EXT.2 entry of section 6 – TSS within the ST was used to determine the verdict of these activities. Upon investigation, the evaluator found that the TSS includes the following:

The TOE supports TLS v1.2 protocol with mutual authentication for use with X.509v3 based authentication.

The TOE does not support any fallback authentication for new TLS connections.

Based on these findings, this assurance activity is considered satisfied.

5.5.19.2 Verdict

Pass

5.5.20 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Guidance 1

If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication.

5.5.20.1 Evaluator Findings

The evaluator verified that the AGD guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” includes instructions for configuring the client-side certificates for TLS mutual authentication. The entirety of the AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that the guidance documentation provides instructions for configuring client-side certificates in the section 6.3 titled, “Configuring X509 Certification Authentication for TLS Mutual Authentication".

Based on these findings, this assurance activity is considered satisfied.

5.5.20.2 Verdict

Pass

5.5.21 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Guidance 2

The evaluator shall verify the guidance describes how to configure the TLS client certificate authentication function. If the TSF supports fallback authentication functions, the evaluator shall verify the guidance provides instructions for configuring the fallback authentication functions. If fallback authentication functions can be disabled, the evaluator shall verify the guidance provides instructions for disabling the fallback authentication functions.

5.5.21.1 Evaluator Findings

The evaluator verified that the AGD guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” includes instructions for configuring the client-side certificates for TLS mutual authentication. The entirety of the AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that the guidance documentation provides instructions for configuring client-side certificates in the section 6.3 titled, “Configuring X509 Certification Authentication for TLS Mutual Authentication". The evaluator also found in the same section mentioned that “The Waveserver device does not support any fallback authentication for new TLS connections.”

Based on these findings, this assurance activity is considered satisfied.

5.5.21.2 Verdict

Pass

5.5.22 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #1a

Item	*Data/Description*
Test ID	FCS_TLSS_EXT.2.1 and 2.2_T1a
Objective	*If the **TOE requires or can be configured to require a client certificate**, the evaluator shall configure the TOE to require a client certificate and send a Certificate Request to the client. The evaluator shall attempt a connection while sending a certificate list structure with a length of zero in the Client Certificate message. The evaluator shall verify that the handshake is not finished successfully and no application data flows.*
Test Flow (generic test steps)	• Create and install CA, ICA, and Entity certificates on the TOE • Configure TOE to support HTTPS • Configure TOE to support mutual authentication • On test VM initiate HTTPS connection without entity certificate • Gather test log and capture packet • Verify test log and packets capture that TOE rejects TLS connection
Pass/Fail Explanation	TOE denies certificate authentication if client presents with zero length certificate.
Result	PASS

5.5.23 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #2

Item	*Data/Description*
Test ID	FCS_TLSS_EXT.2.1 and 2.2_T2
Objective	*Test 2[conditional]: If TLS1.2 is claimed for the TOE, the evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied."*
Test Flow (generic test steps)	• Reuse test configuration and certificates from previous test. • Create client certificates with different key • Run Acumen tool and present server with unsupported signature • Gather test log and capture packets • Verify test and packets capture that connection fails
Pass/Fail Explanation	The TOE rejects mutually authenticated TLS connection attempts from a client whose certificate contains an unsupported signature algorithm. This meets testing requirements.
Result	PASS

5.5.24 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #3

Item	*Data/Description*
Test ID	FCS_TLSS_EXT.2.1 and 2.2_T3
Objective	*The aim of this test is to check the response of the server when it receives a client identity certificate that is signed by an impostor CA (either Root CA or intermediate CA).* *To carry out this test the evaluator shall configure the client to send a client identity certificate with an issuer field that identifies a CA recognised by the TOE as a trusted CA, but where the key used for the signature on the client certificate does not correspond to the CA certificate trusted by the TOE (meaning that the client certificate is invalid because its certification path does not terminate in the claimed CA certificate).* *The evaluator shall verify that the attempted connection is denied.*
Test Flow (generic test steps)	• Create client certificate that is signed from an intermediate CA with different key. • From Client initiate connection and present server with invalid key certificate. • Gather test log and capture packets • Verify test log and packets capture that connection fails
Pass/ Fail Explanation	TOE reject TLS connection if client presents a signed certificate with different key.
Result	PASS

5.5.25 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #4

Item	*Data/Description*
Test ID	FCS_TLSS_EXT.2.1 and 2.2_T4
Objective	*The evaluator shall configure the client to send a certificate with the Client Authentication purpose in the extendedKeyUsage field and verify that the server accepts the attempted connection. The evaluator shall repeat this test without the Client Authentication purpose and shall verify that the server denies the connection. Ideally, the two certificates should be identical except for the Client Authentication purpose.*
Test Flow (generic test steps)	• Generate a TLS client certificate that has the Client Authentication purpose in the extendedKeyUsage field. • Attempt to open a TLS connection from OpenSSL (openssl s_client) to the TOE using the previously generated TLS client certificate • Verify that the TOE accepts the TLS connection attempt. • Generate a TLS client certificate that does not have the Client Authentication purpose in the extendedKeyUsage field. • Attempt to open a TLS connection from OpenSSL (openssl s_client) to the TOE using the previously generated TLS client certificate • Verify that the TOE rejects the TLS connection attempt.
Pass/Fail Explanation	The TOE accepts TLS client certificates if they contain the Client Authentication purpose, and rejects them if they do not.

Result	PASS

5.5.26 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #5a

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.2.1 and 2.2_T5a*
Objective	*Configure the server to require mutual authentication and then connect to the server with a client configured to send a client certificate that is signed by a Certificate Authority trusted by the TOE. The evaluator shall verify that the server accepts the connection.*
Test Flow (generic test steps)	• Create client certificate which signed by a CA trusted by TOE • On client initiate HTTPS/TLS connection • Gather packets capture and verify connection succeeds
Pass/Fail Explanation	The TOE accepts a connection when a certificate is properly signed by a trusted Certificate Authority.
Result	Pass

5.5.27 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #5b

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.2.1 and 2.2_T5b*
Objective	*Configure the server to require mutual authentication and then modify a byte in the signature block of the client's Certificate Verify handshake message (see RFC5246 Sec 7.4.8). The evaluator shall verify that the server rejects the connection.*
Test Flow (generic test steps)	• Reuse TOE HTTPS Configuration and certificates from previous test • Run Acumen tool modify a byte in the signature of client certificate. • Gather test log and capture packets • Verify test log and packets capture that connection fails
Pass/Fail Explanation	TOE rejects TLS connection if client presents with a certificate which has modified byte in the signature
Result	Pass

5.5.28 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #6

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.2.1 and 2.2_T6*
Objective	*Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.*
Test Flow	• *Reuse TOE HTTPS configuration and enable OCSP validation* • *On remote client server reuse certificates from previous test and start OCSP responders*

(generic test steps)	• *On remote client server initiate TLS connection to the TOE* • *Capture packets and verify the connection is successful*
Pass/Fail Explanation	TOE successfully validates the presented certificates used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Result	PASS

5.5.29 FCS_TLSS_EXT.2.1 and FCS_TLSS_EXT.2.2 Test #7

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.2.1/2.2 Test #7*
Objective	*The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.*
Test Flow (generic test steps)	• *Configure TOE to support HTTPS* • *Create a client certificate with invalid CN identifier and no SAN* • *Create a client certificate with valid CN but invalid DNS SAN* • *Create an expired client certificate* • *Create a client certificate with revoke status enabled* • *Create client certificates with incomplete CA chain (Root CA is removed from the chain* • *On client initiate connection using each certificate above* • *Gather test log and capture packets* • *Verify test log and packet capture that connection fails*
Pass/Fail Explanation	TOE rejects TLS connection if client presents a certificate with: invalid CN no SAN, valid CN invalid SAN DNS, expired certificate, revoked certificate, or incomplete CA chain.
Result	PASS

5.5.30 FCS_TLSS_EXT.2.3 TSS 1

The evaluator shall verify that the TSS describes which types of identifiers are supported during client authentication (e.g. Fully Qualified Domain Name (FQDN)). If FQDNs are supported, the evaluator shall verify that the TSS describes that corresponding identifiers are matched according to RFC6125. For all other types of identifiers, the evaluator shall verify that the TSS describes how these identifiers are parsed from the certificate, what the expected identifiers are and how the parsed identifiers from the certificate are matched against the expected identifiers.

5.5.30.1 Evaluator Findings

The evaluator ensured that the TSS describes how the DN or SAN in the certificate is compared to the expected identifier. The FCS_TLSS_EXT.2 entry of section 6 - TSS within the ST was used to determine the verdict of this activity. Upon investigation, the evaluator found that the TSS includes a description of how the DN or SAN in the certificate is compared to the expected identifier.

Based on these findings, this assurance activity is considered satisfied.

5.5.30.2 Verdict

Pass

5.5.31 FCS_TLSS_EXT.2.3 Guidance 1

The evaluator shall ensure that the AGD guidance describes the configuration of expected identifier(s) for X.509 certificate-based authentication of TLS clients. The evaluator ensures this description includes all types of identifiers described in the TSS and, if claimed, configuration of the TOE to use a directory server.

5.5.31.1 Evaluator Findings

The evaluator verified that the AGD guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" includes instructions for configuring the Reference Identifiers. The entirety of the AGD was used to determine the verdict of this assurance activity.

Upon investigation, the evaluator found that the guidance documentation section 6.4 titled, "Configuring Reference Identifiers" states that the client will compare the reference identifier with SAN if available or with CN The AGD states that, "The TOE supports DNS name and IP addresses as its reference identifiers".

Based on these findings, this assurance activity is considered satisfied.

5.5.31.2 Verdict

Pass

5.5.32 FCS_TLSS_EXT.2.3 Test #1

Item	*Data/Description*
Test ID	*FCS_TLSS_EXT.2.3 Test #1*
Objective	*The evaluator shall send a client certificate with an identifier that does not match an expected identifier and verify that the server denies the connection.*
Note	*FCS_TLSS_EXT.2.3 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.*
Test Flow (generic test steps)	• Generate a TLS client certificate with a CN that is not recognized as a reference identifier by the TOE. • Attempt to open a TLS connection to the TOE using the OpenSSL with the previously generated TLS client certificate.

	- Verify that the connection attempt fails.
Pass/Fail Explanation	The TOE rejects an attempt to open a mutually authenticated TLS connection if the client certificate has an unexpected CN. This meets testing requirements. Reference ID check is verified on FCS_TLSS_EXT.2.1&2 Test#7
Result	PASS

5.6 Test Cases (HTTPS)

5.6.1 FCS_HTTPS_EXT.1 TSS 1

The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.

5.6.1.1 Evaluator Findings

The evaluator examined the entry for FCS_HTTPS_EXT.1 in section 6 - TSS to determine that it describes RFC 2818 as HTTP over TLS. The TSS further states "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."
Based on these findings, this assurance activity is considered satisfied.

5.6.1.2 Verdict

Pass

5.6.2 FCS_HTTPS_EXT.1.1 Guidance 1

The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.

5.6.2.1 Evaluator Findings

The evaluator examined the section titled 3.1 Enabling CC-NDcPP Compliance Using the CLI Interface in the AGD to verify that it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server. Upon investigation, the evaluator found that the AGD states the following:

Setup HTTPs

- system server https set cert-name <Entity Name>

Based on these findings, this assurance activity is considered satisfied.

5.6.2.2 Verdict

Pass

5.7 Test Cases (Identification and Authentication)

5.7.1 FIA_AFL.1 TSS 1

The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.

5.7.1.1 Evaluator Findings

The evaluator reviewed the section 6 - TSS within the Security Target and found under the row for FIA_AFL.1, it stated that the TOE will lockout the user account after the configured number of unsuccessful authentication attempts occurs. The range as defined within the Security Target TSS is between 2-10 attempts. The account will be locked and prevented from successfully authenticating until defined time period has elapsed. Based on these findings, the above requirement has been met.

5.7.1.2 Verdict

Pass

5.7.2 FIA_AFL.1 TSS 2

The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).

5.7.2.1 Evaluator Findings

The evaluator reviewed the entry for FIA_AFL.1 in the TSS and found that under the Section 6 TOE Summary Specification, it states that, “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”.

Based on these findings, the above requirement has been met.

5.7.2.2 Verdict

Pass

5.7.3 FIA_AFL.1 Guidance 1

The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each “action” specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.

5.7.3.1 Evaluator Findings

The evaluator examined the guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified. Under the section 6.6 titled "Authentication Failure Handling", the evaluator found that the threshold for the number of authentication failures before lockouts, as well as how to clear a lock out, can be configured.

Based on these findings, the above requirement has been met.

5.7.3.2 Verdict

Pass

5.7.4 FIA_AFL.1 Guidance 2

The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.

5.7.4.1 Evaluator Findings

The evaluator examined the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. The section 6.6 titled "Authentication Failure Handling" within the guidance document was used to determine the verdict of this activity.

Upon investigation, the evaluator found that the AGD describes the ability to access the TOE after logout, as follows, "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."

Based on these findings, the above requirement has been met.

5.7.4.2 Verdict

Pass

5.7.5 FIA_AFL.1 Test #1 & Test #2

Item	**Data/Description**
Test ID	FIA_AFL.1_T1 & 2
Objective	*FIA_AFL.1 Test #1* *The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the*

	authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful. *FIA_AFL.1 Test #2* *After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows.* *If the administrator action selection in FIA_AFL.1.2 is included in the ST then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).* *If the time period selection in FIA_AFL.1.2 is included in the ST then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorization attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorization attempt using valid credentials results in successful access.*
Note	*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* *NOTE: the default value is 5.* *FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall prevent the offending remote Administrator from successfully authenticating until an Administrator defined time period has elapsed].*
Test Flow	• The evaluator configures the numbers of times successive unsuccessful login attempts, as well as a time period that must elapse before access is re-enabled (lockout period). • The evaluator attempts to login with incorrect credentials until the authentication attempts limit is reached. • The evaluator will verify that following authentication attempts with valid credentials are no longer successful. • The evaluator attempts to login with invalid credentials, reaching the limit for unsuccessful authentication attempts. • The evaluator waits until just less than the time period has elapsed before attempting to login using valid credentials, verifying that it does not result in access. • Then, the evaluator waits until after the time period has elapsed before attempting to login using valid credentials, verifying that access is granted.

Pass/Fail Explanation	The TOE denies a session after invalid credentials are entered but accepts the session if the lockout interval has been surpassed and valid credentials are being used. This meets testing requirements.
Result	PASS

5.7.6 FIA_PMG_EXT.1.1 TSS 1

The evaluator shall check that the TSS lists the supported special character(s) for the composition of administrator passwords.

The evaluator shall check the TSS to ensure that the minimum_password_length parameter is configurable by a Security Administrator.

The evaluator shall check that the TSS lists the range of values supported for the minimum_password_length parameter. The listed range shall include the value of 15.

[TD0792 applied]

5.7.6.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.7.6.2 Verdict

Pass

5.7.7 FIA_PMG_EXT.1.1 Guidance 1

The evaluator shall examine the guidance documentation to determine that it:

a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and

b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.

5.7.7.1 Evaluator Findings

The evaluator examined the AGD “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to determine if it provides guidance on the composition of strong passwords. The section 6.1 titled “Password Management” of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD provides instructions to administrative users regarding strong passwords. In particular, the evaluator found that AGD identifies that at minimum passwords must be 15 characters. The evaluator found that AGD provide instructions for configuring passwords via CLI.

Based on these findings, this assurance activity is considered satisfied.

5.7.7.2 Verdict

Pass

5.7.8 FIA_PMG_EXT.1 Test 1

Item	***Data/Description***
Test ID	FIA_PMG_EXT.1.1_T1
Objective	*The evaluator shall compose passwords that either meet the requirements, or fail to meet the requirements, in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, rule characteristics, and a minimum length listed in the requirement are supported, and justify the subset of those characters chosen for testing.*
Note	*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 [128] characters.* *NOTE: default is 8 characters*
Test Flow	• Verify that there is a password policy in place • Attempt to create an invalid password (non-supported lengths/ characters) • Verify that the TOE does not support the password
Pass/Fail Explanation	The TOE was able to create users with good passwords and reject user creation with bad passwords. This meets the testing requirements.

Result	PASS

5.7.9 FIA_PMG_EXT.1 Test 2

Item	***Data/Description***
Test ID	FIA_PMG_EXT.1.1_T2
Objective	*The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.*
Note	*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 [128] characters.* *NOTE: default is 8 characters*
Test Flow	• The evaluator creates some passwords that do not meet the password requirements supported by the TOE. • The evaluator verifies that the TOE does not support these passwords.
Pass/Fail Explanation	The TOE rejected passwords that did not meet the requirements.
Result	PASS

5.7.10 FIA_UIA_EXT.1 TSS 1

The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”.

5.7.10.1 Evaluator Findings

The evaluator examined the TSS to determine that it describes the logon process for each logon method. The TSS entry for FIA_UIA_EXT.1 in the section 6 titled “TOE Summary Specification” of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS identifies the following authentication methods for the users of the TOE,

- 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
- Remotely connecting to appliance WebUI via HTTPS/TLS

NOTE: The web browser is not in scope of the evaluation but the secure HTTPS/TLS connection to the WebUI was evaluated and tested.

Further, the evaluator found that each description in the TSS includes the authentication parameters username/password , the protocol the authentication takes place over, and a description of "successful login."

Based on these findings, this assurance activity is considered satisfied.

5.7.10.2 Verdict

Pass

5.7.11 FIA_UIA_EXT.1 TSS 2

The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.

5.7.11.1 Evaluator Findings

The evaluator examined the TSS to determine that it describes which actions are allowed before user identification and authentication. The TSS entry for FIA_UAU_EXT.1 under section 6 was used to determine the verdict of this activity. Upon investigation, the evaluator found that "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."

Based on these findings, this assurance activity is considered satisfied.

5.7.11.2 Verdict

Pass

5.7.12 FIA_UIA_EXT.1 Guidance 1

The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.

5.7.12.1 Evaluator Findings

The evaluator examined the operational guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to determine that any necessary preparatory steps to logging in are described. Several relevant sections were used to determine the verdict of this assurance activity. The evaluator found that AGD provides instructions for configuring user authentication on the TOE in the following sections:

Remotely connecting to appliance WebUI via HTTPS/TLS

- Section 3 – Enabling CC-NDcPP Compliance
  - Setup HTTPs
    - system server https set cert-name <Entity Name>
- Section 6.3 - Configuring X.509 Certiifcate Authentication for TLS Mutual Authentication
  - System server https mutual-authentication enable

Remotely connecting to each appliance via SSHv2 or RADSec via TLS

- Section 6.2 – Configuring SSH Public Keys
  - Create a user:
    - user create user rsa4096 access-level super password **********
  - Create the public key using Linux ssh-keygen (The key file name should be the same as user name) on the remote server.
    - ssh-keygen -t rsa -b 4096 -f Documents/rsa4096ssh-keygen -t rsa-sha2-256 -f Documents/rsa4096_sha2
    - ssh-keygen -t rsa-sha2-512 -f Documents/rsa4096_sha2512
    - ssh-keygen -t ecdsa-sha2-nistp256 -f Documents/rsa4096_ecd
    - ssh-keygen -t ecdsa-sha2-nistp384 -f Documents/rsa4096_ecd384
    - ssh-keygen -t ecdsa-sha2-nistp521 -f Documents/rsa4096_ecd521
  - Install the public key associating with the pre-created user
  - ssh server key install user rsa4096 sftp-server <IP address> login-id <user> password *********
- Section 5 – Configuring RADsec authentication
  2. Install the X.509 certificate for RADSec:
     - certificates entity install cert-name <String: cert_name> {default-ftp-server | default-sftp-server | default-tftpserver | default-server | default-scp-server | sftpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftpserver <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]> certpassphrase [certificate-only]

     - For example:
       - certificates entity **install cert-name <Entity Name> default-scp-server filename <Path/File.p12> certpassphrase ***********

- ○ **certificates entity install cert-name <Entity Name> scp-server <IP address> login-id <user-name> password <password> filename <Path/File.p12> cert-passphrase** **********

4. Optionally, display the installed certificate:
   - **certificates authorities show**
   - **certificates entity show**

5. Specify the global RADSec settings:
   - **radsec set [cert-name <String: cert_name>] [timeout <Seconds: 1..30>]**

6. Add a RADSec server to the Waveserver 5 system, specifying a priority for the server:
   - **radsec add server <IP address or host name> [priority <Number:1...8>] [port <Number:1...65535>]**

Note 1: Repeat step 5 for each RADSec server you want to add. You can add up to eight RADSec servers. Note 2: For the [priority] attribute, 1 is the highest priority. Note 3: The default value for the [port] attribute is 2083.

7. It is recommended that OCSP be used to perform real time certificate status checks when validating a RADSec server's X.509 certificate. Enable RADSec with OCSP:
   - **radsec ocsp enable**

8. Set the default OCSP responder:
   - **radsec ocsp set default-response <String: [1..255]>**

Note: The default value for the [default-responder] attribute is blank.

9. Set the OCSP responder preference.
   - **radsec ocsp set responder-preference <aia | default-responder>**

Note: The default value for the [responder-preference] attribute is aia.

10. Set whether you want the OCSP responders to contain nonce:
    - **radsec ocsp set nonce <on | off>**

Note: The default value for the [nonce] attribute is on.

11. Set the order of available authentication providers:
    - **user auth set order radsec [,radius][,local]**

Note: Set RADIUS and/or local authentication as a backup provider to ensure access to the Waveserver 5 in the event that RADSec services are unavailable.

12. Set RADSec as the authentication method for all remote connections over SSH:
    - **user auth set method radsec scope remote**

13. Configuring RADSec for both remote and local connections:
    - **user auth set method radsec scope all**

14. Optionally, view RADSec summary or statistics information for all configured RADSec servers:
    - **radsec show [statistics]**

Note: RADSec servers are listed by priority, with the highest priority server displayed first.

15. Save the provisioned settings to the configuration file:
    - **configuration save**

<u>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.</u>

- Section 2 – Using Local Access
  - Initially make sure the TOE is in an active state up and running.
  - For direct access of the TOE, connect a USB type-C port one to the TOE and other to the management/user's laptop.
  - Power up the laptop and navigate to the section "This PC" by following the steps Windows -> Documents -> This PC.
  - Under the Devices and drives section you can find the TOE connected to the laptop as a device.
  - The above can also be done with the help of connecting a console cable between the TOE and User's system.

Authentication may be configured via CLI. The instructions provided by AGD place the TOE in a configuration that requires authentication for all administrative access.

Based on these findings, this assurance activity is considered satisfied.

5.7.12.2 Verdict

Pass

5.7.13 FIA_UIA_EXT.1 Test #1

Item	**Data/Description**

Test ID	FIA_UIA_EXT.1.1_T1
Objective	The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
Note	*FIA_UIA_EXT.1.1 The TSF shall require the following actions prior to allowing the non-TOE entity to initiate the identification and authentication process:* • *Display the warning banner in accordance with FTA_TAB.1;* • *[no other actions].*
Test Flow	• Configure the TOE to support authentication • Attempt to login from a local connection with incorrect credentials ○ Confirm that access was denied • Log into the TOE from a local connection with correct credentials ○ Confirm that access was granted • Verify that an audit records were generated showing the both login failure and success • Attempt to login from a remote CLI connection with incorrect credentials ○ Confirm that access was denied • Log into the TOE from a remote CLI connection with correct credentials ○ Confirm that access was granted • Verify that an audit records were generated showing the both login failure and success
Pass/Fail Explanation	Presenting incorrect authentication credentials results in denied access to the TOE. Presenting correct authentication credentials results in access being allowed to the TOE. This meets the testing requirements.
Result	PASS

5.7.14 FIA_UIA_EXT.1 Test #2

Item	**Data/Description**
Test ID	FIA_UIA_EXT.1.1_T2
Objective	The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
Note	No services are available prior to authentication. As the previous test showed the only functionality available prior to authentication on both the local CLI and the remote GUI is the ability to enter a login and password.

Test Flow	• At the remote authentication prompt attempt to execute authenticated commands • Verify that no functionality is available
Pass/Fail Explanation	No system services are available to an unauthenticated user connecting remotely. This meets the testing requirements.
Result	PASS

5.7.15 FIA_UIA_EXT.1 Test #3

Item	**Data/Description**
Test ID	FIA_UIA_EXT.1.1_T3
Objective	For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
Note	No services are available prior to authentication. As the previous test showed the only functionality available prior to authentication on the local CLI is the ability to enter a login and password.
Test Flow	• At the directly connected console authentication prompt attempt to execute authenticated commands • Verify that no functionality is provided
Pass/Fail Explanation	No system services are available to an unauthenticated user via the directly connected console except viewing of Login Banner and password input. This meets the testing requirements.
Result	PASS

5.7.16 FIA_UAU_EXT.2

None – The evaluation of this SFR is tested in conjunction with the testing of FIA_UIA_EXT.1.

5.7.17 FIA_UAU.7 Guidance 1

The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.

5.7.17.1 Evaluator Findings

No Preparatory steps are needed to ensure authentication data is not revealed while entering for each local login.

Based on these findings, this assurance activity is considered satisfied.

5.7.17.2 Verdict

Pass

5.7.18 FIA_UAU.7 Test #1

Item	***Data/Description***
Test ID	*FIA_UAU.7.1_T1*
Objective	The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
Note	*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.*
Test Flow	At the directly connected login prompt, enter incorrect authentication credentials • Verify that at most obscured feedback is provided At the directly connected login prompt, enter correct authentication credentials • Verify that at most obscured feedback is provided At the remote login prompt, enter incorrect authentication credentials • Verify that at most obscured feedback is provided At the remote login prompt, enter correct authentication credentials Verify that at most obscured feedback is provide
Pass/Fail Explanation	At both the directly connected and remote login prompt, the TOE does not provide anything more than obscured feedback. This meets the testing requirements.
Result	PASSs

5.7.19 FIA_X509_EXT.1/Rev TSS 1

The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not sufficient to verify the status of a X.509 certificate only when it's loaded onto the device. It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).

5.7.19.1 Evaluator Findings

The evaluator examined the TSS to determine where certificate validation occurs. The TSS entry for FIA_X509_EXT.1 under section 6 reveals: “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, 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 CA certificates and verify the validity of the certificates. These checks are done prior to loading the certificates onto the TOE".

Per the TSS, the evaluator found that revocation checking is performed by the TOE. "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. Revocation checking is performed when the TOE receives a server certificate from a TLS server. 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."

Based on these findings, this assurance activity is considered satisfied.

5.7.19.2 Verdict

Pass

5.7.20 FIA_X509_EXT.1/Rev TSS 2

The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.

5.7.20.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that 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. 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.

Based on these findings, this assurance activity is considered satisfied.

5.7.20.2 Verdict

Pass

5.7.21 FIA_X509_EXT.1/Rev Guidance 1

The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.

5.7.21.1 Evaluator Findings

The evaluator examined the section titled 4.4 Audit Server Configuration in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD states the following:

It is recommended that OCSP be used to perform real time certificate status checks when validating a Syslog server's X.509 certificate.

1. Enable Syslog with OCSP:

➢ syslog tls ocsp enable

2. Set the default OCSP responder:

➢ syslog tls ocsp set default-responder <String: [1..255]>

3. To set the OCSP responder preference

➢ syslog tls ocsp set responder-preference <aia | default responder>

4. To set whether you would like the OCSP responders to contain nonce:

➢ syslog tls ocsp set nonce <on | off>

5. Optionally, retrieve TLS syslog OCSP settings:

➢ syslog tls ocsp show

Note: OCSP revocation status checks take place wherever a TLS certificate connection is implemented (RADsec and Audit server).

Based on these findings, this assurance activity is considered satisfied.

5.7.21.2 Verdict

Pass

5.7.22 FIA_X509_EXT.1/Rev Test 1

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T1
Objective	*The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when*

	performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. *Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the certificate to be used in the function and shall use this chain to demonstrate that the function succeeds.* *Test 1b: The evaluator shall then delete one of the certificates in the presented chain (i.e. the root CA certificate or other intermediate certificate, but not the end-entity certificate), and show that an attempt to validate an incomplete chain fails..*
Test Flow	• Attempt to make a connection with the TOE using a digital certificate. Ensure that a full certificate path is present for the digital certificate used in the communication • Verify that this attempt succeeds • Re-Attempt to make a connection with the TOE using a digital certificate without a valid certificate path • Verify that this attempt fails
Pass/Fail Explanation	When a complete certificate trust chain is present, the TOE can make a successful connection. When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection. This meets the testing requirements.
Result	PASS

5.7.23 FIA_X509_EXT.1/Rev Test 2

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T2
Objective	*The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.* *The evaluator shall demonstrate that validating an expired certificate results in the function failing.*
Test Flow	• Attempt to make a connection with the TOE using a digital certificate without a valid certificate path • Verify that this attempt fails
Pass/Fail Explanation	The TOE denied the connection because of the expired certificate. This meets the testing requirements.
Result	PASS

5.7.24 FIA_X509_EXT.1/Rev Test 3

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T3
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall test that the TOE can properly handle revoked certificates-– conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails. No testing is required if no revocation method is selected.
Note	*FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with 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*
Test Flow	• Attempt a connection between the TOE and a peer for which the peer certificate is revoked • Verify that the connection fails • Un-revoke the peer certificate • Re-attempt the connection between the TOE and the peer • Verify that the connection succeeds • Revoke an intermediary CA certificate for the peer • Re-attempt the connection between the TOE and the peer • Verify that the connection fails because of the revoked intermediary certificate
Pass/Fail Explanation	The TOE communications with peers that either have a revoked certificate or one of their Intermediary CA certificates are revoked. When presented non-revoked certificates, the TOE accepts the certificate. This meets the testing requirements.
Result	PASS

5.7.25 FIA_X509_EXT.1/Rev Test 4

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T4
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set, and verify that validation of the CRL fails.
Test Flow	• Configure a connection with a peer on the TOE, • Ensure that digital certificates are used for authentication • Ensure that the peer certificate identifies an OCSP server • Attempt a connection with the peer • Configure the OCSP responder such that the response does not have the OCSP signing purpose • Verify that the connection does not complete
Pass/Fail Explanation	The TOE rejected the OCSP request when the OCSP signing bit was not set. This meets testing requirements.

Result	PASS

5.7.26 FIA_X509_EXT.1/Rev Test 5

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T5
Objective	*The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE.* *The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)*
Test Flow	• Configure a connection with a peer on the TOE, • Ensure that digital certificates are used for authentication • Ensure that the peer certificate identifies an OCSP server • During session establishment modify a byte in the first eight bytes of the certificate • Verify that the connection does not complete
Pass/Fail Explanation	The TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the testing requirements.
Result	PASS

5.7.27 FIA_X509_EXT.1/Rev Test 6

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T6
Objective	*Test 6: The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)*
Test Flow	• TOE and remote server are to reuse general certificate chain from previous test for this test • Remove existing RADSEC configuration and reconfigure RADSEC configuration • On remote server run Acumen tool to modify a byte in the certificate signature • Gather test log and capture packets • Verify that TLS connection fails Repeat test steps above for remote SYSLOG configuration
Pass/Fail Explanation	TOE denies TLS connection if certificate presented with impaired signature.

Result	PASS

5.7.28 FIA_X509_EXT.1/Rev Test 7

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T7
Objective	*The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)*
Test Flow	• Configure a connection with a peer on the TOE, ◦ Ensure that digital certificates are used for authentication • During session establishment modify a byte in the public key of the certificate • Verify that the connection does not complete
Pass/Fail Explanation	The TOE rejects connections when the public of the certificate is modified. This meets the testing requirements.
Result	Pass

5.7.29 FIA_X509_EXT.1/Rev Test 8a

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T8a
Objective	*Test 8a: (Conditional on TOE ability to process CA certificates presented in certificate message) The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.* **TD0527 Has been applied**
Test Flow	• The evaluator shall generate a valid chain of EC certificates (as supported by FCS_COP.1/SigGen) which terminate in a trusted CA certificate, this chain of EC certificates shall have the elliptic curve parameters specified as a named curve. • The evaluator confirms that the TOE validates the certificate chain.
Pass/Fail Explanation	TOE does not support this condition **(Conditional on TOE ability to process CA certificates presented in certificate message).**
Result	N/A

5.7.30 FIA_X509_EXT.1/Rev Test 8b

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T8b
Objective	*Test 8b: (Conditional on TOE ability to process CA certificates presented in certificate message) The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.* **TD0527 Has been applied**
Test Flow	• The evaluator shall generate a valid chain of EC certificates (as supported by FCS_COP.1/SigGen) which terminate in a trusted CA certificate, this chain of EC certificates will have the intermediate certificate use an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA. • The evaluator confirms that the TOE treats the certificate as invalid.
Pass/Fail Explanation	Not Support. TOE does not support this condition: **(Conditional on TOE ability to process CA certificates presented in certificate message)**
Result	N/A

5.7.31 FIA_X509_EXT.1/Rev Test 8c

Item	**Data/Description**
Test ID	FIA_X509_EXT.1/Rev_T8c
Objective	*Test 8c: The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store.* **TD0527 Has been applied**

Test Flow	- Upload a Root EC certificate to the TOE and then attempt to load a subordinate intermediate CA where the elliptic curve parameters are specified as a named curve - The evaluator verifies the TOE allows the certificate to be loaded into the trust store - The evaluator shall generate a valid chain of EC certificates (as supported by FCS_COP.1/SigGen) which terminate in a trusted CA certificate, this chain of EC certificates will have the intermediate certificate use an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA. - The evaluator attempts to load the certificate into the trust store and observes that it is rejected, and is not added to the TOE's trust store.
Pass/Fail Explanation	TOE rejects to store certificate with invalid EC curve.
Result	Pass

5.7.32 FIA_X509_EXT.1.2/Rev Test 1

Item	**Data/Description**
Test ID	FIA_X509_EXT.1.2/Rev_T1
Objective	Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: (i) as part of the validation of the leaf certificate belonging to this chain; (ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).
Test Flow	- Configure the TOE to support digital certificates - Configure the certificate used by the TOE such that, - The certificate of the CA issuing the TOE's certificate does not contain the basicConstraints extension - Verify that the TOE identifies that the signing CA certificate does not contain the basicConstraints extension - Ensure the TOE rejects the certificate
Pass/Fail Explanation	The TOE rejects certificates signed by a CA that does not contain the basicConstraints extension. This meets the testing requirements.
Result	PASS

5.7.33 FIA_X509_EXT.1.2/Rev Test 2

Item	Data/Description
Test ID	FIA_X509_EXT.1.2/Rev_T2
Objective	*Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points:* *(i) as part of the validation of the leaf certificate belonging to this chain;* *(ii) when attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).*
Test Flow	• Configure the TOE to support digital certificates • Configure the certificate used by the TOE such that, • The certificate of the CA issuing the TOE's certificate has the cA flag in the basicConstraints extension set to FALSE • Verify that the TOE identifies that the signing CA certificate has the cA flag in the basicConstraints extension set to FALSE • Ensure the TOE rejects the certificate
Pass/Fail Explanation	The TOE rejects certificates signed by a CA that has the cA flag in the basicConstraints extension set to FALSE. This meets the testing requirements.
Result	PASS

5.7.34 FIA_X509_EXT.2 TSS 1

The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates.

5.7.34.1 Evaluator Findings

The evaluator examined the TSS to determine if it describes how the TOE chooses which certificates to use. The TSS entry for FIA_X509_EXT.2 in the section 6 titled TOE summary specification of ST and the section titled "Configuring X509 Certificate Authentication for TLS Mutual Authentication" of AGD were used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes how the TOE chooses the certificates to use for communications. The TSS states that the following criteria is used,

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 for authentication.

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 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.)

Next, the evaluator examined AGD. The evaluator found that AGD provides guidance regarding what is necessary to for the TOE to be configured to use digital certificates.

Based on these findings, this assurance activity is considered satisfied.

5.7.34.2 Verdict

Pass

5.7.35 FIA_X509_EXT.2 TSS 2

The evaluator shall examine the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.

5.7.35.1 Evaluator Findings

The evaluator examined the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The TSS entry for FIA_X509_EXT.2 in the section titled 6 TOE summary specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes how the TOE handles scenarios where the TOE cannot determine the validity of the peer certificate. Specifically, the TSS states that the TOE handles these scenarios, as follows,

- 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 evaluator found that this behavior is applicable to the following connections,

- HTTPS
- TLS

Based on these findings, this assurance activity is considered satisfied.

5.7.35.2 Verdict

Pass

5.7.36 FIA_X509_EXT.2 Guidance 1

The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.

5.7.36.1 Evaluator Findings

The evaluator examined the section titled 4.4 Audit Server Configuration in the AGD. Upon investigation, the evaluator found that the AGD states that:

1. Create a private key and install a device certificate.

2. Install a trusted CA certificate:

- ➢ certificates authorities install {default-ftp-server | default-sftp-server | default-tftp-server | default-server | default-scpserver | sftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scp-server <IP address or host name> login-id <String [1..32]> password <String [1..128] | ftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]>

- ➢ For example: certificates authorities install cert-name <CA Name> default-scp-server filename <Path/File>

3. Set the TLS syslog certificate name to the certificate you installed in step 1:

- syslog tls set cert-name <String: cert_name> For example: syslog tls set cert-name tlssyslogcert

4. Set the global administrative state of TLS syslog message logging: syslog tls <disable | enable>

5. Create a collector for TLS syslog with the desired attributes to enable the TOE to communicate with syslog server:

- syslog tls create collector <IP address or host name> [custom-prefix <String: 1...15>] [fingerprint <fingerprint>] [facility <Number: 0..24>] [port <Number: 1..65535>] [severity <emergency | alert | error | warning | notice | info | debug | all>] [trusted-dns <trusteddns>]

It is recommended that OCSP be used to perform real time certificate status checks when validating a Syslog server's X.509 certificate.

6. Enable Syslog with OCSP:

- syslog tls ocsp enable

7. Set the default OCSP responder:

- syslog tls ocsp set default-responder <String: [1..255]>

8. To set the OCSP responder preference

- syslog tls ocsp set responder-preference <aia | default responder>

9. To set whether you would like the OCSP responders to contain nonce:

- syslog tls ocsp set nonce <on | off>

10. Optionally, retrieve TLS syslog OCSP settings:

- syslog tls ocsp show

11. Save the provisioned settings to the configuration file:

➢ configuration save

Information on how to setup RADIUS can be found in section 5, “Configuring RADsec authentication,” where the following is stated:

1. Install the X.509 certificate for RADSec:

• certificates entity install cert-name <String: cert_name> {default-ftp-server | default-sftp-server | default-tftpserver | default-server | default-scp-server | sftpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scpserver <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftpserver <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]> certpassphrase [certificate-only]

• For example:

o certificates entity install cert-name <Entity Name> default-scp-server filename <Path/File.p12> certpassphrase **********

o certificates entity install cert-name <Entity Name> scp-server <IP address> login-id <user-name> password <password> filename <Path/File.p12> cert-passphrase **********

2. Optionally, display the installed certificate:

• certificates authorities show

• certificates entity show

3. Specify the global RADSec settings:

• radsec set [cert-name <String: cert_name>] [timeout <Seconds: 1..30>]

4. Add a RADSec server to the Waveserver 5 system, specifying a priority for the server:

• radsec add server <IP address or host name> [priority <Number:1...8>] [port <Number:1...65535>]

Note 1: Repeat step 5 for each RADSec server you want to add. You can add up to eight RADSec servers. Note 2: For the [priority] attribute, 1 is the highest priority. Note 3: The default value for the [port] attribute is 2083.

5. It is recommended that OCSP be used to perform real time certificate status checks when validating a RADSec server's X.509 certificate. Enable RADSec with OCSP:

- radsec ocsp enable

6. Set the default OCSP responder:

- radsec ocsp set default-response <String: [1..255]>

Note: The default value for the [default-responder] attribute is blank.

7. Set the OCSP responder preference.

- radsec ocsp set responder-preference <aia | default-responder>

Note: The default value for the [responder-preference] attribute is aia.

8. Set whether you want the OCSP responders to contain nonce:

- radsec ocsp set nonce <on | off>

Note: The default value for the [nonce] attribute is on.

9. Set the order of available authentication providers:

- user auth set order radsec [,radius][,local]

Note: Set RADIUS and/or local authentication as a backup provider to ensure access to the Waveserver 5 in the event that RADSec services are unavailable.

10. Set RADSec as the authentication method for all remote connections over SSH:

- user auth set method radsec scope remote

11. Configuring RADSec for both remote and local connections:

- user auth set method radsec scope all

12. Optionally, view RADSec summary or statistics information for all configured RADSec servers:

- radsec show [statistics]

Note: RADSec servers are listed by priority, with the highest priority server displayed first.

13. Save the provisioned settings to the configuration file:

- configuration save

Section 3.1, "Enabling CC-NDPP Compliance Using the CLI Interface," provides the following detail on setting up a secure HTTPS/TLS connection for admins to access the TOE GUI:

Setup HTTPs

- system server https set cert-name <Entity Name>

The AGD also states in section 6.3 that when a connection can't be established during the validity check, the administrator should do the following:

If a connection can't be established to the OCSP responder, the TOE will not accept the certificate and the administrator must reattempt the connection when the responder is back online.

Based on these findings, this assurance activity is considered satisfied.

5.7.36.2 Verdict

Pass

5.7.37 FIA_X509_EXT.2 Test #1

Item	**Data/Description**
Test ID	FIA_X509_EXT.2_T1
Objective	The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.
Note	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].

Test Flow	• Configure a connection with a peer on the TOE, ◦ Ensure that digital certificates are used for authentication • During session establishment ensure that the TOE cannot verify the validity of the peer certificate • Verify that the certificate is rejected
Pass/Fail Explanation	The TOE does not accept a certificate without checking for its validity. This meets the testing requirements.
Result	PASS

5.7.38 FIA_X509_EXT.3 TSS 1

If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.

5.7.38.1 Evaluator Findings

The ST does not select "device-specific information". Therefore, a description is not required.

5.7.38.2 Verdict

Pass

5.7.39 FIA_X509_EXT.3 Guidance 1

The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certification Requests. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request.

5.7.39.1 Evaluator Findings

The evaluator examined the guidance document “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to determine if instructions for requesting certificates from a CA are provided. The section 6.5 titled “Generation of a Certificate Signing Request” of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD provides instructions for generating CSRs. The evaluator found that these instructions include the complete set of steps necessary to configure a fully formed CSR containing each of the fields described in FIA_X509_EXT.3. Finally, the evaluator found that AGD provides instructions for generating CSRs from the CLI.

Based on these findings, this assurance activity is considered satisfied.

5.7.39.2 Verdict

Pass

5.7.40 FIA_X509_EXT.3 Test #1

Item	**Data/Description**

Test ID	FIA_X509_EXT.3_1
Objective	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated request and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
Note	*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].*
Test Flow	• From the TOE, generate a CSR • Examine the CSR contents • Ensure the CSR contains the following fields
Pass/Fail Explanation	The TOE is able to generate a CSR with all of the requisite information. This meets the testing requirements.
Result	PASS

5.7.41 FIA_X509_EXT.3 Test #2

Item	**Data/Description**
Test ID	FIA_X509_EXT.3_T2
Objective	The evaluator shall demonstrate that validating a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the response message, and demonstrate that the function succeeds.
Note	*FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.*
Test Flow	• From the TOE, generate a CSR request • Generate a signed certificate based on the generated CSR from an external CA • Ensure that the full trust chain for the signed CA is not present on the TOE • Attempt to load the signed certificate on the TOE • Verify that the TOE rejects the certificate because the full trust chain of the CA is not present • Add the intermediary certificates to the TOE certificate store to ensure that the signing CA now has a full certificate path • Re-attempt to load the signed certificate on the TOE • Verify that the TOE accepts the certificate because the path validation succeeded • Remove the signing CA intermediary certificates from the TOE certificate store • Verify that the TOE now identifies the signed certificate as invalid

Pass/Fail Explanation	The TOE does not install CSR responses signed by a CA without a full trust path. The TOE does install a CSR response signed by a CA with a full trust path. This meets the testing requirements.
Result	Pass

5.8 Test Cases (Security Management)

5.8.1 FMT_MOF.1/ManualUpdate Guidance 1

The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).

5.8.1.1 Evaluator Findings

The evaluator examined the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine that any necessary steps to perform manual update are described. The AGD section 9 titled, "Performing Manual Software Updates on the TOE" was used to determine the verdict of this activity. Upon investigation, the evaluator found that section 9.1 of the AGD (steps 1-5) describe the process of manually updating the software on the TOE.

Based on these findings, the above requirement has been met.

5.8.1.2 Verdict

Pass

5.8.2 FMT_MOF.1/ManualUpdate Test #1

Item	**Data/Description**
Test ID	FMT_MOF.1/ManualUpdate_T1
Objective	The evaluator shall try to perform the update using a legitimate update image without prior authentication as security administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Flow	• Attempt to update the TOE from an unprivileged user • Verify that the update attempt fails • Verify that an admin can update the TOE Audit Log
Pass/Fail Explanation	The ability to update the TOE is restricted to the privileged administrators. This meets the testing requirements.
Result	PASS

5.8.3 FMT_MOF.1/ManualUpdate Test #2

Item	**Data/Description**
Test ID	FMT_MOF.1/ManualUpdate_T2
Objective	The evaluator shall try to perform the update with prior authentication as security administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Pass/Fail Explanation	This test is covered by FPT_TUD_EXT.1
Result	Pass

5.8.4 FMT_MOF.1/Functions TSS 1

For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).

5.8.4.1 Evaluator Findings

The evaluator examined the TSS and ensured that, for non-distributed TOEs, it details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).

The relevant information is found in the following section(s): TOE Summary Specification FMT_MOF.1/Functions.

Upon investigation, the evaluator found that the TSS states that:

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.

Based on these findings, the above requirement has been met

5.8.4.2 Verdict

Pass

5.8.5 FMT_MOF.1/Functions AGD 1

For non-distributed TOEs, the evaluator shall also ensure the AGD describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings

5.8.5.1 Evaluator Findings

The evaluator examined the AGD and ensured that, for non-distributed TOEs, it describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.

The AGD provides instructions on how the security administrator determines or modifies the behaviour of transmitting audit data, handling audit data and audit functionality when local storage is full in section 4 Using an Audit Server.

Upon investigation, the evaluator found that the AGD activity states the following:

- You must be logged in to Waveserver 5 using an account with at least admin access privileges.
- The audit server must be a Syslog server that supports TCP and TLS v1.1 or TLS v1.2.
- The TOE stores audit data locally. When a file is full, a new file is created. When the local data is full, the oldest file is overwritten to allow new audit events to be created.
- 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.

5.8.5.2 Verdict

Pass

5.8.6 FMT_MOF.1/Services TSS 1

For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

5.8.6.1 Evaluator Findings

The evaluator examined the TSS and ensured that, for non-distributed TOEs, it lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

The relevant information is found in the following section(s): TOE Summary Specification FMT_MOF.1/Services.

Upon investigation, the evaluator found that the TSS states that: the following details are provided in relation to 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

Based on these findings, the above requirement has been met.

5.8.6.2 Verdict

Pass

5.8.7 FMT_MOF.1/Services AGD

For non-distributed TOEs, the evaluator shall also ensure the AGD describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

5.8.7.1 Evaluator Findings

The evaluator examined the AGD and ensured that, for non-distributed TOEs, it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.

Section 6.7 Role Based Access Control (RBAC), Section 4 Using an Audit Server, Section 5 Configuring RADsec authentication, Setting Time Using NTP Synchronization

Upon investigation, the evaluator found that the AGD activity states that:

The Security administrator has the ability to start and stop any services surrounding Syslog, RADsec, SSH and NTP.

5.8.7.2 Verdict

Pass

5.8.8 FMT_MOF.1/Services Test #1

Item	Data/Description
Test ID	FMT_MOF.1/Services_T1

Objective	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable this service/these services can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator
Test Flow	• Non security admin (Limited user) attempts to disable logging messages • Verify that operation fails • Collect test log
Pass/Fail Explanation	TOE does not allow limited user to disable system logging service.
Result	PASS

5.8.9 FMT_MOF.1/Services Test #2

Item	**Data/Description**
Test ID	FMT_MOF.1/Services_T2
Objective	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
Test Flow	• The evaluator logs into the TOE using an authenticated Security administrator account. • The evaluator attempts to enable or disable the security logging service (same as the tested feature of Test #1), this attempt should be successful.
Pass/Fail Explanation	TOE allows security admin to enable/disable system logging service
Result	PASS

5.8.10 FMT_MTD.1/CoreData TSS 1

The evaluator shall examine the TSS to determine that, for each administrative function identified in the operational guidance; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.

5.8.10.1 Evaluator Findings

The evaluator examined the TSS to determine what administrative functions are accessible prior to administrator log-in. The TSS entry for FMT_MTD.1/CoreData in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS states that no administrative functionality is available prior to administrative login. Based on these findings, this assurance activity is considered satisfied.

5.8.10.2 Verdict

Pass

5.8.11 FMT_MTD.1/CoreData TSS 2

If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.

5.8.11.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specification in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that the TOE implements Role Based Access Control (RBAC). Administrative users are required to login before being provided with access to any administrative functions. The Security administrator is the only one authorized to perform actions like import, export and delete certificates and also manage trusted CAs.

Based on these findings, this assurance activity is considered satisfied.

5.8.11.2 Verdict

Pass

5.8.12 FMT_MTD.1/CoreData Guidance 1

The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.

5.8.12.1 Evaluator Findings

The evaluator examined the operational guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine if configuration information is provided to ensure that only administrators have access to TSF-data manipulating functions. Upon investigation, the evaluator found that AGD describes how administrative users are able to configure the TSF-data manipulating functions for the TOE. The evaluator found that the configuration of the following functionality is described within AGD:

- Enabling CC-NDcPP Compliance – section 3
- Authentication Failure Handling – section 6.6
- Audit Server Configuration – section 4.4
- Authentication – section 6
- Setting Time Manually– section 10
- Automatic Logout due to Session Inactivity – section 12
- Setting Login Banners – section 13
- Performing Manual Software Updates on the TOE – section 9
- Configuring X.509 Certificate Authentication for TLS Mutual Authentication – section 6.3

The evaluator found that this encompasses all of the TSF-data manipulating functionality required by the NDcPP.

Based on these findings, this assurance activity is considered satisfied.

5.8.12.2 Verdict

Pass

5.8.13 FMT_MTD.1/CoreData Guidance 2

If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor.

5.8.13.1 Evaluator Findings

The evaluator examined the section titled 4.4 Audit Server Configuration in the AGD to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD states that:

6. Install a trusted CA certificate:

➢ certificates authorities install {default-ftp-server | default-sftp-server | default-tftp-server | default-server | default-scpserver | sftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scp-server <IP address or host name> login-id <String [1..32]> password <String [1..128] | ftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128]} filename <String [1..127]>

- ➢ For example: certificates authorities install cert-name <CA Name> default-scp-server filename <Path/File>

The evaluator examined the section titled 3.1 Enabling CC-NDCPP Using the CLI Interface in the AGD to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD states that:

Install CA chain and Entity certificates.

- ➢ certificates authorities install cert-name <CA Name> default-scp-server filename <Path/File>
- ➢ certificates entity install cert-name <Entity Name> default-scp-server filename <Path/File.p12> cert-passphrase **********

Based on these findings, this assurance activity is considered satisfied.

5.8.13.2 Verdict

Pass

5.8.14 FMT_MTD.1/CryptoKeys TSS 1

For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.

5.8.14.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states the following:

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 all aspects of 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.

Based on these findings, this assurance activity is considered satisfied.

5.8.14.2 Verdict

Pass

5.8.15 FMT_MTD.1/CryptoKeys Guidance 1

For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.

5.8.15.1 Evaluator Findings

The evaluator examined the section titled 6.2 Configuring SSH Public Keys, 4.4 Audit Server Configuration, and 6.1 Password Management in the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD states that:

Use the commands in this section to create a new public key for SSH user authentication. You can use this key instead of the password to authenticate the remote user.

<u>SSH Public Keys:</u>

1. Create a user:
   - **user create user rsa4096 access-level super password** **********
2. Create the public key using Linux ssh-keygen (The key file name should be the same as user name) on the remote server.
   - ssh-keygen -t rsa -b 4096 -f Documents/rsa4096ssh-keygen -t rsa-sha2-256 -f Documents/rsa4096_sha2
   - ssh-keygen -t rsa-sha2-512 -f Documents/rsa4096_sha2512
   - ssh-keygen -t ecdsa-sha2-nistp256 -f Documents/rsa4096_ecd
   - ssh-keygen -t ecdsa-sha2-nistp384 -f Documents/rsa4096_ecd384
   - ssh-keygen -t ecdsa-sha2-nistp521 -f Documents/rsa4096_ecd521
3. Install the public key associating with the pre-created user
   - **ssh server key install user rsa4096 sftp-server <IP address> login-id <user> password** *********

X509 Certificates and Certificate Authorities:

2. To use an audit server:
   create a private key and install a device trusted CA certificate as follows:
   - **certificates authorities install {default-ftp-server | default-sftp-server | default-tftserver | defaultserver | default-scpserver | sftp-server <IP address or host name>**
     login-id <String [1..32]> password <String [1..128] | tftp-server <IP address or host name> | scp-server <IP address or host name> loginid <String [1..32]> password <String [1..128] | ftp-server <IP address or host name> login-id <String [1..32]> password <String [1..128]}
     filename <String [1..127]>

   - For example**: certificates authorities install cert-name <CA Name> default-scp-server**
     filename <Path/File>

Passwords:

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

The TOE is capable of configuring strong passwords, such as those with at least 15 characters long and the following complexity rules:

- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

Minimum password lengths shall be configurable to 8 characters to maximum of 128 characters. The default minimum password length is 8 characters. The TOE only supports the creation of strong passwords.

1. To create a user account and setting of the password use the following command:
   - **user create user <String: 1...32> access-level <limited | admin | super> [password <String: [8...128>]**

2. To set the minimum password length, use the following command:
   - **user set min-password-length [8..128]**

Based on these findings, this assurance activity is considered satisfied.

5.8.15.2 Verdict

Pass

5.8.16 FMT_MTD.1/CryptoKeys Test #1

Item	**Data/Description**
Test ID	*FMT_MTD.1/CryptoKeys Test #1*
Objective	*The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.*
Test Flow	• Using Limited user account and attempt to generate cryptographic key • Collect log and verify that operation fails
Result	TOE does not allow Limited user to generate cryptographic key.
Verdict	Pass

5.8.17 FMT_MTD.1/CryptoKeys Test #2

Item	**Data/Description**
Test ID	*FMT_MTD.1/CryptoKeys Test #2*
Objective	*The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.*
Test Flow	• The evaluator attempts to perform at least one of the following actions effecting cryptographic keys; modify, delete, generate/import. This attempt will be executed using a Security Administrator account. • The evaluator logs that this attempt succeeds.
Result	TOE allows Security Administrator to generate cryptographic key.

Verdict	Pass

5.8.18 FMT_SMF.1 TSS 1 & 2

The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local. The evaluator shall examine the TSS, Guidance Documentation and the TOE as observed during all other testing and shall confirm that the management functions specified in FMT_SMF.1 are provided by the TOE. The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).

5.8.18.1 Evaluator Findings

The evaluator examined the TSS, Guidance Documentation and the TOE as observed during all other testing and shall confirm that the management functions specified in FMT_SMF.1 are provided by the TOE. The ST, AGD, and TOE itself was used to determine the verdict of this activity. Upon investigation, the evaluator found that following management activities,

- Local/Remote administration
- Login banner configuration
- Session inactivity timer configuration
- Firmware updates
- Authentication failure configuration
- Crypto configuration
- PKI/digital certification configuration
- Audit configuration

The evaluator confirmed that each of the functionalities were available and described in the ST/TSS, AGD, and on the TOE itself.

Based on these findings, this activity is considered satisfied.

5.8.18.2 Verdict

PASS

5.8.19 FMT_SMF.1 Test #1

Item	**Data/Description**
Test ID	*FMT_SMF.1 Test #1*
Objective	*The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.*

Note	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; o Ability to configure audit behavior; o Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1; o Ability to configure the cryptographic functionality; o Ability to configure thresholds for SSH rekeying; o Ability to re-enable an Administrator account; o Ability to set the time which is used for time-stamps; o Ability to configure the reference identifier for the peer;
Result	Throughout the various security functionality testing of the TOE, FMT_SMF.1 Specification of Management Functions requirements have been met. Therefore, this test Passed.
Verdict	Pass

5.8.20 FMT_SMR.2 TSS 1

The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.

5.8.20.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.8.20.2 Verdict

Pass

5.8.21 FMT_SMR.2 Guidance 1

The evaluator shall review the operational guidance to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.

5.8.21.1 Evaluator Findings

The evaluator examined the operational guidance “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to determine if instructions for administering the TOE locally and remotely are included. The section 3 titled “Enabling CC-NDcPP Compliance” of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD describes the configuration necessary to administer the TOE from a variety of interfaces, as follows,

- Local console CLI
- Remote SSH CLI

For remote administration, the evaluator found that AGD describes all configurations necessary to connect to the TOE.

Based on these findings, this assurance activity is considered satisfied.

5.8.21.2 Verdict

Pass

5.8.22 FMT_SMR.2 Test

In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team’s test activities.

5.8.22.1 Evaluator Findings

In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team’s test activities.

The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces. This test has passed.

5.8.22.2 Verdict

Pass

5.9 Test Cases (Protection of the TSF)

5.9.1 FPT_SKP_EXT.1 TSS 1

The evaluator shall examine the TSS to determine that it details how an pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

5.9.1.1 Evaluator Findings

The evaluator examined the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. The TSS entry for FPT_SKP_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes the methods keys are store within the TOE. The methods described in the TSS include the following,

- The TOE stores all private keys in a secure storage and is not accessible through an interface to administrators.

Based on these findings, this assurance activity is considered satisfied.

5.9.1.2 Verdict

Pass

5.9.2 FPT_APW_EXT.1 TSS 1

The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored.

5.9.2.1 Evaluator Findings

The TSS entry for FPT_APW_EXT.1 under section 6 states that "All passwords are stored in a secure directory that is not readily accessible to administrators. The passwords are stored as SHA-512 salted hash." This ensures that administrators will not have access to plain-text passwords. There are no administrative interfaces that allow administrative users to view passwords as they are encrypted.

Based on these findings, this assurance activity is considered satisfied.

5.9.2.2 Verdict

Pass

5.9.3 FPT_APW_EXT.1 TSS 2

The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.

5.9.3.1 Evaluator Findings

The evaluator examined the TSS to determine if passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. The TSS entry for FPT_APW_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS explicitly states that all passwords are stored in a secure directory that is not readily accessible to administrators. The passwords are stored as SHA-512 salted hash.

Based on these findings, this assurance activity is considered satisfied.

5.9.3.2 Verdict

Pass

5.9.4 *FPT_STM_EXT.1* TSS 1

The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time. The TSS provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.

5.9.4.1 Evaluator Findings

The evaluator examined the TSS to determine if it lists each security function that makes use of time. The TSS entry for FPT_STM.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS states that time is used for the following services,

- Audit events
- Session inactivity
- X509 certificate expiration validation

Next, the evaluator reviewed the TSS and found that the TSS describes the method for maintaining time on the TOE. Finally, the evaluator reviewed the TSS and found that a rationale is provided regarding why the time is considered reliable.

Based on these findings, this assurance activity is considered satisfied.

5.9.4.2 Verdict

Pass

5.9.5 *FPT_STM_EXT.1* Guidance 1

The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.

5.9.5.1 Evaluator Findings

The evaluator examined AGD “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to determine if it instructs administrators how to set the time. Section 10, “Setting Time” describes the method for configuring time on the TOE. Section 11, “Setting Time Using NTP Synchronization,” provides details on the configuration of the NTP server on the TOE to support communication.

Based on these findings, this assurance activity is considered satisfied.

5.9.5.2 Verdict

Pass

5.9.6 FPT_STM_EXT.1 Test #1

Item	**Data/Description**
Test ID	FPT_STM_EXT.1.1_T1
Objective	If the TOE supports direct setting of the time by the Security Administrator then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Flow	• If the TOE supports direct setting of the time by the Security Administrator, then the evaluator uses the guidance documentation to set the time. • The evaluator shall then use an available interface to observe that the time was set correctly. • The evaluator shall check the logs
Pass/Fail Explanation	The TOE allows the administrative user to configure the time on the TOE. This meets the testing requirements.
Result	PASS

5.9.7 FPT_STM_EXT.1 Test #2

Item	**Data/Description**
Test ID	FPT_STM_EXT.1.1_T2
Objective	If the TOE supports the use of an NTP server; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Test Flow	1. The evaluator shall use the guidance documentation to configure the NTP client on the TOE and set up a communication path with the NTP server. 2. The evaluator shall observe that the NTP server has set the time to what is expected. 3. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Pass/Fail Explanation	This test was performed in conjunction with test case: **FCS_NTP_EXT.1.1 Test #1**
Result	Pass

5.9.8 *FPT_TST_EXT.1.1* TSS 1

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF on start-up; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used).

5.9.8.1 Evaluator Findings

The evaluator examined the TSS to determine if it details the self-tests that are run by the TSF on start-up. The TSS entry for FPT_TST_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS states that the following self-test are run by the TOE,

- Software integrity test
- AES Known Answer Test
- HMAC Known Answer Test
- SHA-256/384/512 Known Answer Test
- RSA Signature Known Answer Test
- ECDSA Signature Known Answer Test
- RNG Known Answer Test

Based on these findings, this assurance activity is considered satisfied.

5.9.8.2 Verdict

Pass

5.9.9 *FPT_TST_EXT.1.1* TSS 2

The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

5.9.9.1 Evaluator Findings

The evaluator examined the TSS to determine if it makes an argument for why the tests are sufficient to demonstrate that the TSF is operating correctly. The TSS entry for FPT_TST_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS provides an argument that the included self-tests sufficiently demonstrate that the TSF is operating correctly. The TSS states “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.”

Based on these findings, this assurance activity is considered satisfied.

5.9.9.2 Verdict

Pass

5.9.10 FPT_TST_EXT.1.1 Guidance 1

The evaluator shall also ensure that the operational guidance describes the possible errors that may result from such tests and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.

5.9.10.1 Evaluator Findings

Section 8 in the AGD, "Self-Tests" describes possible errors that may result from self-testing as well as actions the administrator should take in response. The AGD states that "When Waveserver Ai 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 Ai does not resolve the issue, then the administrator should contact their next level of support or their Ciena support group for further assistance". These errors also correspond to those described in the TSS.

Based on these findings, this assurance activity is considered satisfied.

5.9.10.2 Verdict

Pass

5.9.11 FPT_TST_EXT.1.1 Test #1

Item	**Data/Description**
Test ID	FPT_TST_EXT.1.1_T1
Objective	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this. For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.
Test Flow	• Power on the TOE • Observer the output of the TOE start up • Ensure that evidence of the execution of self-tests are provided • Reboot waveserver to examine the self-tests (typically takes about 2 minutes to reboot) //created a user account to access the wavserver
Pass/Fail Explanation	The TOE performs all claimed self-tests. This meets the testing requirements.
Result	PASS

5.9.12 FPT_TUD_EXT.1 TSS 1

The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.

5.9.12.1 Evaluator Findings

The evaluator reviewed Section 6 – TSS of the ST to determine the verdict of this requirement. Under the entry for FPT_TUD_EXT.1, the evaluator found that "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". The AGD, under Section 9, provide specific instructions on how these actions can be performed. The TOE does not support delayed activation.

Based on these findings, the above requirement has been met.

5.9.12.2 Verdict

Pass

5.9.13 FPT_TUD_EXT.1 TSS 2

The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software. The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.

5.9.13.1 Evaluator Findings

The evaluator verified that the TSS describes all TSF software update mechanisms for updating the system software. The TSS entry for FPT_TUD_EXT.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS describes the software update mechanism of the TOE. The TSS states that the TOE uses a digital signature to verify the integrity of software updates. The evaluator also found that the TSS describes the behavior of the TOE if the integrity test over the software update fails. Specifically, the software update is discarded and an audit record is generated. Finally, the evaluator verified that the TSS describes the method that software updates are obtained by the administrative user of the TOE.

Based on these findings, this assurance activity is considered satisfied.

5.9.13.2 Verdict

Pass

5.9.14 FPT_TUD_EXT.1 Guidance 1

The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version.

5.9.14.1 Evaluator Findings

The evaluator verified that the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" describes how to query the currently active version. Section 9 of AGD, "Performing Manual Software Updates on the TOE" was used to determine the verdict of this activity. Upon investigation, the evaluator found that, the administrator must run command "software show" to query the currently active version.

Based on these findings, the activities are considered satisfied.

5.9.14.2 Verdict

Pass

5.9.15 FPT_TUD_EXT.1 Guidance 2

The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.

5.9.15.1 Evaluator Findings

The evaluator examined the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine if it describes how the verification of the authenticity of updates is performed. The section 9 titled 'Performing Manual Software Updates on the TOE' of AGD were used to determine the verdict of this assurance activity. Upon investigation the evaluator found that AGD describe the software update procedures for the TOE. These procedures include a description of the determination of a successful or unsuccessful verification. Finally, the evaluator compared the description in AGD to the description found in the TSS of ST. The evaluator found that the descriptions were consistent. In addition, Section 9 of the AGD states that verification of the updated software is done as follows: 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. 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 then the image will be loaded onto the TOE. If the images cannot be verified, the image will not be loaded onto the TOE.

Based on these findings, this assurance activity is considered satisfied.

5.9.15.2 Verdict

Pass

5.9.16 FPT_TUD_EXT.1 Test #1

Item	**Data/Description**
Test ID	FPT_TUD_EXT.1_T1
Objective	The evaluator performs the version verification activity to determine the current version of the product. If a trusted update can be installed on the TOE with a delayed activation, the evaluator shall also query the most recently installed version). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version. (disregard) After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.
Test Flow	• Verify the current version of the TOE • Perform the image update • Verify the new version of the TOE ○ The version should now be the new software version
Pass/Fail Explanation	The TOE software was able to be updated when an image that passes the integrity test is used. This meets the testing requirements.
Result	PASS

5.9.17 FPT_TUD_EXT.1 Test #2

Item	**Data/Description**
Test ID	*FPT_TUD_EXT.1_T2*
Objective	The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 1) A modified version (e.g. using a hex editor) of a legitimately signed update

	2) An image that has not been signed 3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature)
Test Flow	• Log into the TOE and verify the current software version installed on the TOE Attempt to install an image in which the binary is corrupted • Verify that the version did not change • Audit Log (Failure):
Pass/Fail Explanation	The TOE actively rejects software updates that are corrupt. This meets the testing requirements
Result	PASS

5.9.18 FPT_TUD_EXT.1 Test #2(d)

Item	**Data/Description**
Test ID	FPT_TUD_EXT.1_T1
Objective	*(if digital signatures are used): The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:* *4) If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.*
Pass/Fail Explanation	Delayed activation is not supported by the TOE.
Result	N/A

5.10 Test Cases (TOE Access)

5.10.1 FTA_SSL_EXT.1 TSS 1

The evaluator shall examine the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings.

5.10.1.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS identifies whether local administrative session locking or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that the TOE will terminate the session after a Security Administrator defined period of inactivity.

Based on these findings, this assurance activity is considered satisfied.

5.10.1.2 Verdict

Pass

5.10.2 FTA_SSL_EXT.1 Guidance 1

The evaluator shall confirm that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period.

5.10.2.1 Evaluator Findings

The evaluator confirmed that the guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. The section 12 titled “Automatic Logout due to Session Inactivity” of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local console CLI interface. The default value is 10 minutes for the local console CLI interface. The configuration of inactivity periods is a global parameter for the chassis and it get applied to all connections. Each connection has its own count down but the timeout value is global. 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.

Based on these findings, this assurance activity is considered satisfied.

5.10.2.2 Verdict

Pass

5.10.3 FTA_SSL_EXT.1 Test #1

Item	Data/Description
Test ID	FTA_SSL_EXT.1.1_T1
Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For

	each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Note	FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [• terminate the session] after a Security Administrator-specified time period of inactivity
Test Flow	• On the TOE configure three minutes inactivity time out period • Remote login TOE and let the TOE idle out by not perform any operation • Verify that TOE exit out current session after three minutes time • Repeat above test steps by setting inactivity timeout to five minutes
Pass/Fail Explanation	The local administrative inactivity was able to be set to multiple values. In each instance, the TOE logged the user out after the configured time. This meets the testing requirements.
Result	PASS

5.10.4 FTA_SSL.3 TSS 1

The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.

5.10.4.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specification in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.10.4.2 Verdict

Pass

5.10.5 FTA_SSL.3 Guidance 1

The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.

5.10.5.1 Evaluator Findings

The evaluator confirmed that the guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. The section 12 titled “Automatic Logout due to Session Inactivity” of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD states that “A Security Administrator can configure maximum inactivity times for administrative sessions through the remote SSH CLI interfaces. The default value is 10 minutes for the remote SSH CLI interfaces. The configuration of inactivity periods is a global parameter for the chassis and it get applied to all connections. Each connection has its own count down but the timeout value is global. 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.”

Based on these findings, this assurance activity is considered satisfied.

5.10.5.2 Verdict

Pass

5.10.6 FTA_SSL.3 Test #1

Item	***Data/Description***
Test ID	*FTA_SSL.3_T1*
Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Flow	• Configure a remote CLI time out period of 2 minutes on administrative sessions • Connect to the TOE from the remote CLI • Let the remote CLI connection set idle for 2 minutes • Verify that the session was terminated • Configure a remote CLI out period of 5 minutes on administrative sessions • Connect to the TOE from the remote CLI • Let the remote CLI connection set idle for 5 minutes • Verify that the session was terminated

Pass/Fail Explanation	Both the remote administrative time out periods can be set by the administrative user. The TOE enforces the configured inactivity period in each instance. This meets the testing requirements.
Result	PASS

5.10.7 FTA_SSL.4 TSS 1

The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.

5.10.7.1 Evaluator Findings

The evaluator examined the section titled 6 TOE Summary Specifications in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that 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.

Based on these findings, this assurance activity is considered satisfied.

5.10.7.2 Verdict

Pass

5.10.8 FTA_SSL.4 Guidance 1

The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.

5.10.8.1 Evaluator Findings

The evaluator confirmed that the guidance documentation "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" states how to terminate a local or remote interactive session. The section 6.8 titled, 'Logging out of the local CLI and remote SSH interfaces' of AGD was used to determine the verdict of this activity.

Upon investigation, the evaluator found the method for terminating a session was defined for CLI (remote and local).

Based on these findings, this assurance activity is considered satisfied.

5.10.8.2 Verdict

Pass

5.10.9 FTA_SSL.4 Test #1

Item	**Data/Description**
Test ID	FTA_SSL.4.1_T1

Objective	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Flow	• Log onto the TOE through a directly connected interface • Using the instructions provided by the user guide, log off of the TOE
Pass/Fail Explanation	The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.
Result	Pass

5.10.10 FTA_SSL.4 Test #2

Item	***Data/Description***
Test ID	*FTA_SSL.4.1_T2*
Objective	*The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.*
Test Flow	• Log onto the TOE through each remote interface type • Using the instructions provided by the user guide, log off of the TOE
Pass/Fail Explanation	The TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.
Result	PASS

5.10.11 FTA_TAB.1 TSS 1

The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).

5.10.11.1 Evaluator Findings

The evaluator examined the TSS to determine if it details each method of access available to the administrator. The TSS entry for FTA_TAB.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that each of the methods to access the TOE are described in the TSS. Specifically, the evaluator found that the TSS identifies the following methods of administrative access where the banner is shown to the user when logging into the TOE:

- Local CLI
- Remote CLI

This banner will be displayed prior to allowing Security Administrator access through those interfaces.

Based on these findings, this assurance activity is considered satisfied.

5.10.11.2 Verdict

Pass

5.10.12 FTA_TAB.1 Guidance 1

The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.

5.10.12.1 Evaluator Findings

The evaluator shall check the guidance documentation “Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document” to ensure that it describes how to configure the banner message. Under section 13 “Setting Login Banners” of the AGD, a privileged administrator can configure the login message with the command “system shell set login-banner-file” followed by the desired banner message. The evaluator confirmed this information to be present and consistent with the requirement in the ST.

Based on these findings, the above requirement has been met.

5.10.12.2 Verdict

Pass

5.10.13 FTA_TAB.1 Test #1

Item	**Data/Description**
Test ID	FTA_TAB.1_T1
Objective	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Flow	• Using the guidance documentation, configure an access banner for each administrative interface • Log into the TOE via each administrative interface o This includes both directly connected and remote administrative interfaces • Verify that the administrative access banner is displayed • Change the access banner for each administrative interface

	• Re-log into the TOE via each administrative interface • Verify that the newly configured access banner is displayed rather then the originally configured banner
Pass/Fail Explanation	An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements.
Result	PASS

5.11 Test Cases (Trusted Path/Channels)

5.11.1 FTP_ITC.1 TSS 1

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint.

5.11.1.1 Evaluator Findings

The evaluator examined the TSS to determine if communications mechanisms are identified for all communications with authorized IT entities. The TSS entry for FTP_ITC.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that the TSS identifies connections with the following authorized IT entities,

- Syslog server
- RADIUS server

Next, the evaluator verified that for each communication identified in the TSS a description of the secure communication mechanism is provided. Specifically, the evaluator found that "The TOE uses TLS v1.2 or TLS v1.1 protocol with X.509 certificate-based authentication".

Based on these findings, this assurance activity is considered satisfied.

5.11.1.2 Verdict

Pass

5.11.2 FTP_ITC.1 TSS 2

The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.

5.11.2.1 Evaluator Findings

The evaluator examined the TSS to determine if all listed protocols in the TSS are included in the ST requirements. The definition of FTP_ITC.1 in section 5.2.7 and TSS entry for FTP_ITC.1 in the section 6 titled TOE Summary Specification of ST was used to determine the verdict of this assurance activity. First, the evaluator reviewed the TSS of ST to identify the protocols described for remote communications.

Upon investigation, the evaluator found that the TSS identifies Syslog server and RADIUS server for remote communications.

Next, the evaluator compared the list identified in the TSS to the definition of the SFR in ST. The evaluator found the identified protocols to be consistent. The protocol supported for RADIUS and syslog connections is TLS.

Based on these findings, this assurance activity is considered satisfied.

5.11.2.2 Verdict

Pass

5.11.3 FTP_ITC.1 Guidance 1

The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.

5.11.3.1 Evaluator Findings

The evaluator confirmed that the operational guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. The only allowed protocols are TLS v1.1 or TLS v1.2; the AGD addresses this in section 6.3 Configuring X.509 Certificate Authentication for TLS Mutual Authentication and section 3.1 Enabling CC-NDPP Compliance Using the CLI Interface. The AGD states the following:

For all the servers that use TLS, the Admin provisions the server information and the TOE automatically creates the TLS connection to the server. When a connection is severed then the TOE will detect that state and will automatically re-connect and perform retry attempts as needed. The administrator does not need to perform any actions. This applies to RADsec and TLS-Syslog. If the IT entity server is non-functional then that equipment and application will need to be recovered.

Based on these findings, this assurance activity is considered satisfied.

5.11.3.2 Verdict

Pass

5.11.4 FTP_ITC.1 Test #1, 2, 3

Item	**Data/Description**
Test ID	FTP_ITC.1_T1/2/3
Objective	The vendor shall provide to the evaluator application layer configuration settings for all secure communication mechanisms specified by the FTP_ITC.1 requirement. This information should be sufficiently detailed to allow the evaluator to determine the application layer timeout settings for each

	cryptographic protocol. There is no expectation that this information must be recorded in any public-facing document or report. Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful. Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE. Test3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Flow	• Configure the TOE to connect with an authorized IT entity • This will configure a secure channel between the TOE and the IT entity • Initiate the connection between the TOE and the IT entity • Perform a packet capture of the traffic between the TOE and the IT entity • Verify that the connection is not sent plaintext
Pass/Fail Explanation	External connections from the TOE are sent via an encrypted channel. This meets the testing requirements.
Result	PASS

5.11.5 FTP_ITC.1 Test #4

Item	**Data/Description**
Test ID	FTP_ITC.1_T4
Objective	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations: i) a duration that exceeds the TOE's application layer timeout setting, ii) a duration shorter than the application layer timeout but of sufficient length to interrupt the MAC layer. The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext. In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.

Test Flow	• Configure the TOE to connect with an authorized IT entity • This will configure a secure channel between the TOE and the IT entity • Initiate the connection between the TOE and the IT entity • Perform a packet capture of the traffic between the TOE and the IT entity • Verify that the connection is not sent plaintext • Disconnect the remote entity from the network • From the TOE, continue to send data • Verify that the data sent from the TOE is not sent plaintext • Reconnect the remote entity to the network • From the TOE, continue to send data • Verify that the data sent from the TOE is not sent plaintext
Pass/Fail Explanation	The TOE does not send plaintext traffic when disconnected from the external entity. This meets the testing requirements.
Result	PASS

5.11.6 FTP_TRP.1/Admin TSS 1

The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected.

5.11.6.1 Evaluator Findings

The evaluator examined the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The FTP_TRP.1 entry in TSS under section 6 was used to determine the verdict of this activity. Per the TSS, "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."

Based on these findings, this assurance activity is considered satisfied.

5.11.6.2 Verdict

Pass

5.11.7 FTP_TRP.1/Admin TSS 2

The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST

5.11.7.1 Evaluator Findings

The evaluator confirmed that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST. The FTP_TRP.1 entry in section 6 - TSS and the SFR definitions in section 5.2.7 of ST were used to determine the verdict of this activity. Upon investigation, the evaluator found that the ST specifies SSH and HTTPS/TLS, which corresponds to the details of the TSS under FTP_TRP.1.

Based on these findings, this assurance activity is considered satisfied.

5.11.7.2 Verdict

Pass

5.11.8 FTP_TRP.1/Admin Guidance 1

The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.

5.11.8.1 Evaluator Findings

The evaluator examined the operational guidance "Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document" to determine if it contains instructions for establishing remote administrative sessions. The section 6.3 and 3 titled "Configuring X.509 Certificate Authentication for TLS Mutual Authentication" and "Enabling CC-NDcPP Compliance" of AGD was used to determine the verdict of this assurance activity. Upon investigation, the evaluator found that AGD provides instructions for configuring the remote administration of the TOE. In particular, the evaluator found that these instructions include configuration of the protocols used to secure remote administrative session. Specifically, AGD provides instructions for configuring the following protocols,

HTTPS/TLS

Based on these findings, this assurance activity is considered satisfied.

5.11.8.2 Verdict

Pass

5.11.9 FTP_TRP.1/Admin Test #1, 2

Item	Data/Description
Test ID	FTP_TRP.1_T1/2
Objective	The evaluators shall ensure that communications using each specified (in the operational guidance) remote administration method is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Test Flow	• Configure the TOE to support remote administration • This will configure a secure channel between the TOE and the remote administrator • Initiate a remote administrative session with the TOE • Perform a packet capture of the traffic between the TOE and the remote administrator • Verify that the connection is not sent plaintext

Pass/Fail Explanation	Remote administrative access to the TOE is over secure protected channels. This meets the testing requirements.
Result	PASS

6 Security Assurance Requirements

6.1 ADV Assurance Activities

6.1.1 ADV_FSP.1

The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.

The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.

The evaluator shall examine the interface documentation to develop a mapping of the interfaces to SFRs.

6.1.1.1 Evaluator Findings

Per this cPP, the Evaluation Activities for this family focus on understanding the interfaces presented in the TSS in response to the functional requirements and the interfaces presented in the AGD documentation. No additional 'functional specification' documentation is necessary to satisfy the Evaluation Activities specified in the ST.

6.1.1.2 Verdict

Pass

6.2 ASE_CCL.1 Conformance Claims

6.2.1 ASE_CCL.1.8.C

The evaluator shall check that the statements of security problem definition in the PP and ST are identical.

6.2.1.1 Evaluator Findings

The evaluator checked that the statements of security problem definition in the PP and ST are identical. The section titled Security Problem Definition of ST and section 4 of the NDcPP were used to determine the verdict of this work unit. Upon investigation, the evaluator found that the SPD defined in the NDcPP and the SDP defined in the ST are identical.

Based on these findings, this work unit is considered satisfied.

6.2.1.2 Verdict

Pass

6.2.2 ASE_CCL.1.9.C

The evaluator shall check that the statements of security objectives in the PP and ST are identical.

6.2.2.1 Evaluator Findings

The evaluator checked that the statements of security objectives in the PP and ST are identical. The section titled Security Objectives of ST and section 5 of the NDcPP were used to determine the verdict of this work unit. Upon investigation, the evaluator found that the Objectives defined in the NDcPP and the Objectives defined in the ST are identical.

Based on these findings, this work unit is considered satisfied.

6.2.2.2 Verdict

Pass

6.2.3 ASE_CCL.1.9.C Test 1

The evaluator shall check that the statements of security requirements in the ST include all the mandatory SFRs in the cPP, and all of the selection-based SFRs that are entailed by selections made in other SFRs (including any SFR iterations added in the ST).

6.2.3.1 Evaluator Findings

The evaluator shall check that the statements of security requirements in the ST include all the mandatory SFRs in the cPP, and all of the selection-based SFRs that are entailed by selections made in other SFRs. The section titled Security Requirements of ST and section 6 of the NDcPP were used to determine the verdict of this work unit. Upon investigation, the evaluator found that all required SFRs (both mandatory and selection-based) are included in the ST. The following table compares the SFRs found in the ST to the SFRs found in the PP.

SFR found in the Security Target	**SFR found in the Protection Profile**
FAU_GEN.1	FAU_GEN.1
FAU_GEN.2	FAU_GEN.2
FAU_STG_EXT.1	FAU_STG_EXT.1
FCS_CKM.1	FCS_CKM.1
FCS_CKM.2	FCS_CKM.2
FCS_CKM.4	FCS_CKM.4
FCS_COP.1(1)	FCS_COP.1(1)
FCS_COP.1(2)	FCS_COP.1(2)
FCS_COP.1(3)	FCS_COP.1(3)
FCS_COP.1(4)	FCS_COP.1(4)
FCS_RBG_EXT.1	FCS_RBG_EXT.1
FIA_AFL.1	FIA_AFL.1
FIA_PMG_EXT.1	FIA_PMG_EXT.1
FIA_UIA_EXT.1	FIA_UIA_EXT.1
FIA_UAU_EXT.2	FIA_UAU_EXT.2
FIA_UAU.7	FIA_UAU.7
FIA_X509_EXT.1	FIA_X509_EXT.1
FIA_X509_EXT.2	FIA_X509_EXT.2
FIA_X509_EXT.3	FIA_X509_EXT.3

SFR found in the Security Target	SFR found in the Protection Profile
FMT_MOF.1/Manual Update	FMT_MOF.1/Manual Update
FMT_MTD.1/CoreData	FMT_MTD.1/CoreData
FMT_SMF.1	FMT_SMF.1
FMT_SMR.2	FMT_SMR.2
FPT SKP EXT.1	FPT SKP EXT.1
FPT APW EXT.1	FPT APW EXT.1
FPT_STM.EXT.1	FPT_STM.1
FPT TUD EXT.1	FPT TUD EXT.1
FPT TST EXT.1	FPT TST EXT.1
FTA_SSL_EXT.1	FTA_SSL_EXT.1
FTA_SSL.3	FTA_SSL.3
FTA_SSL.4	FTA_SSL.4
FTA_TAB.1	FTA_TAB.1
FTP_ITC.1	FTP_ITC.1
FTP_TRP.1	FTP_TRP.1
FCS_SSHS_EXT.1	FCS_SSHS_EXT.1
FCS_TLSC_EXT.2	FCS_TLSC_EXT.2
FCS_TLSS_EXT.2	FCS_TLSS_EXT.2
FCS_HTTPS_EXT.1	FCS_HTTPS_EXT.1

Based on these findings, this work unit is considered satisfied.

6.2.3.2 Verdict

Pass

6.2.4 ASE_CCL.1.9.C Test 2

The evaluator shall check that if any other SFRs are present in the ST (apart from iterations of SFRs in the cPP) then these are taken only from the list of optional SFRs specified in the cPP (the cPP will not necessarily include optional SFRs, but may do so).

6.2.4.1 Evaluator Findings

The evaluator checked if any other SFRs are present in the ST (apart from iterations of SFRs in the cPP) then these are taken only from the list of optional SFRs specified in the cPP (the cPP will not necessarily include optional SFRs, but may do so). The section titled Security Requirements of ST and section 6 of the NDcPP were used to determine the verdict of this work unit. The evaluator compared the SFRs found in ST to the SFRs found in the NDcPP and found that no additional SFRs are included in the ST that are not included in the NDcPP.

Based on these findings, this work unit is considered satisfied.

6.2.4.2 Verdict

Pass

6.3 AGD_OPE.1 Operational User Guidance

6.3.1 AGD_OPE.1

The evaluator shall ensure the Operational guidance documentation is distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.

The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.

The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.

TD0536 Applied Below

The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

The documentation must describe the process for verifying updates to the TOE by verifying a digital signature. The evaluator shall verify that this process includes the following steps: Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).

Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature.

The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.

6.3.1.1 Evaluator Findings

Sections 2, 3, and 9 of AGD provides instructions for configuring the TOE into its CC configuration. As part of this configuration, all cryptographic algorithms are limited to only the allowed algorithms.

The section titled "Performing Manual Software Updates on the TOE" of AGD provides instructions to the Administrator for performing an update. Step by step instructions are provided for the administrator to follow including downloading the image, copying it to the TOE and installing it. This includes integrity verification.

The entirety of the guidance documentation identifies the evaluated capabilities of the TOE by describing how to configure each for Common Criteria.

6.3.1.2 Verdict

Pass

6.4 AGD_PRE.1 Preparative Procedures

6.4.1 AGD_PRE.1

The evaluator shall examine the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).

The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.

The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.

The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.

The preparative procedures must a) include instructions to provide a protected administrative capability; and b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.

6.4.1.1 Evaluator Findings

The evaluator used the guidance documentation when configuring the TOE. The completeness of the documentation is addressed by its use in the AA's carried out in the evaluation.

6.4.1.2 Verdict

Pass

6.5 ALC Assurance Activities

6.5.1 ALC_CMC.1

When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.

6.5.1.1 Evaluator Findings

The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.

6.5.1.2 Verdict

Pass

6.5.2 ALC_CMS.1

When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.

6.5.2.1 Evaluator Findings

The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing.

6.5.2.2 Verdict

Pass

6.6 ATE_IND.1 Independent Testing – Conformance

6.6.1 ATE_IND.1

The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4.

The evaluator should consult Appendix B when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.

6.6.1.1 Evaluator Findings

The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities.

6.6.1.2 Verdict

Pass

6.7 AVA_VAN.1 Vulnerability Survey

6.7.1 AVA_VAN.1 Test #1 ***(TD0564)***

The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.

Evaluator Findings

The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement.

Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include:

- CN9130
- Waveserver 5
- SSHv2
- X.509v3
- TLSv1.2
- NTPv4
- HTTPS “Ciena”
- Linux Kernel v4.14
- Ciena Waveserver 5 Crypto Library 1
- R2.3.12
- WolfSSL v5.2.0-commercial-fips-ready

The evaluation lab examined each result provided from nvd.nist.gov and cve.mitre.org to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. The vulnerability searches were performed on the 6th of September 2023, October 12th 2023, 9th of November 2023 and a follow up search on the 27th of November 2023. All information pertaining to AVA_VAN.1 can be found in the Vulnerability Assessment for Ciena Waveserver 5 version 1.5.

6.7.1.1 Verdict

Pass

7 Technical Decisions

The following Technical Decisions apply to the NDcPPv2.2e:

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	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
0670 – NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
0639 – NIT Technical Decision for Clarification for NTP MAC Keys	Yes	
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	

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
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.
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	

8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document