Assurance Activity Report for
Ciena 6500 Packet Optical Platform
Version 15.6

Ciena 6500 Packet Optical Platform Security Target
Version 1.0

collaborative Protection Profile for Network Devices, Version 2.2e

AAR Version 0.8, January 2025

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

The Author of the Security Target:
Acumen Security

The TOE Evaluation was Sponsored by:
Ciena Corporation

Evaluation Personnel:
Furukh Siddique
Akshay Jain
Shaina Rae

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

REVISION HISTORY

VERSION	DATE	CHANGES
0.1	January 2024	Draft of TSS
0.2	April 2024	Updates to TSS and draft of Guidance
0.3	September 2024	Updates to Guidance and Check-out QA
0.4	October 2024	New template, Check-Out Ready
0.5	October 2024	Peer Review Updates
0.6	November 2024	Peer Review Updates
0.7	December 2024	ECR Comment Updates
0.8	January 2025	Minor Updates

CONTENTS

1 TOE OVERVIEW

The TOE is the Ciena 6500 Packet Optical Platform running software version 15.6 and is developed by Ciena Corporation. The Ciena 6500 Packet Optical Platform, the Target of Evaluation (TOE), is a family of standalone hardware devices that run VxWorks and provide OSI Layers 1 and 2 network traffic management services. The security functions provided by the TOE include security auditing, cryptographic support, identification and authentication, security management, protection of TSF, TOE access controls, and trusted communications. The appliance provides the TL1 interface to the TOE's security management functionality. The TOE enables users to direct traffic to designated ports, giving them control of network availability for specific services. The system features an agnostic switch fabric that is capable of switching SONET/SDH, OTN, and Ethernet/MPLS networks. The switching behavior is beyond the scope of the claimed Protection Profile.

2 ASSURANCE ACTIVITIES IDENTIFICATION

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e based upon the core SFRs and those implemented based on selections within the PPs/EPs.

3 TEST EQUIVALENCY JUSTIFICATION

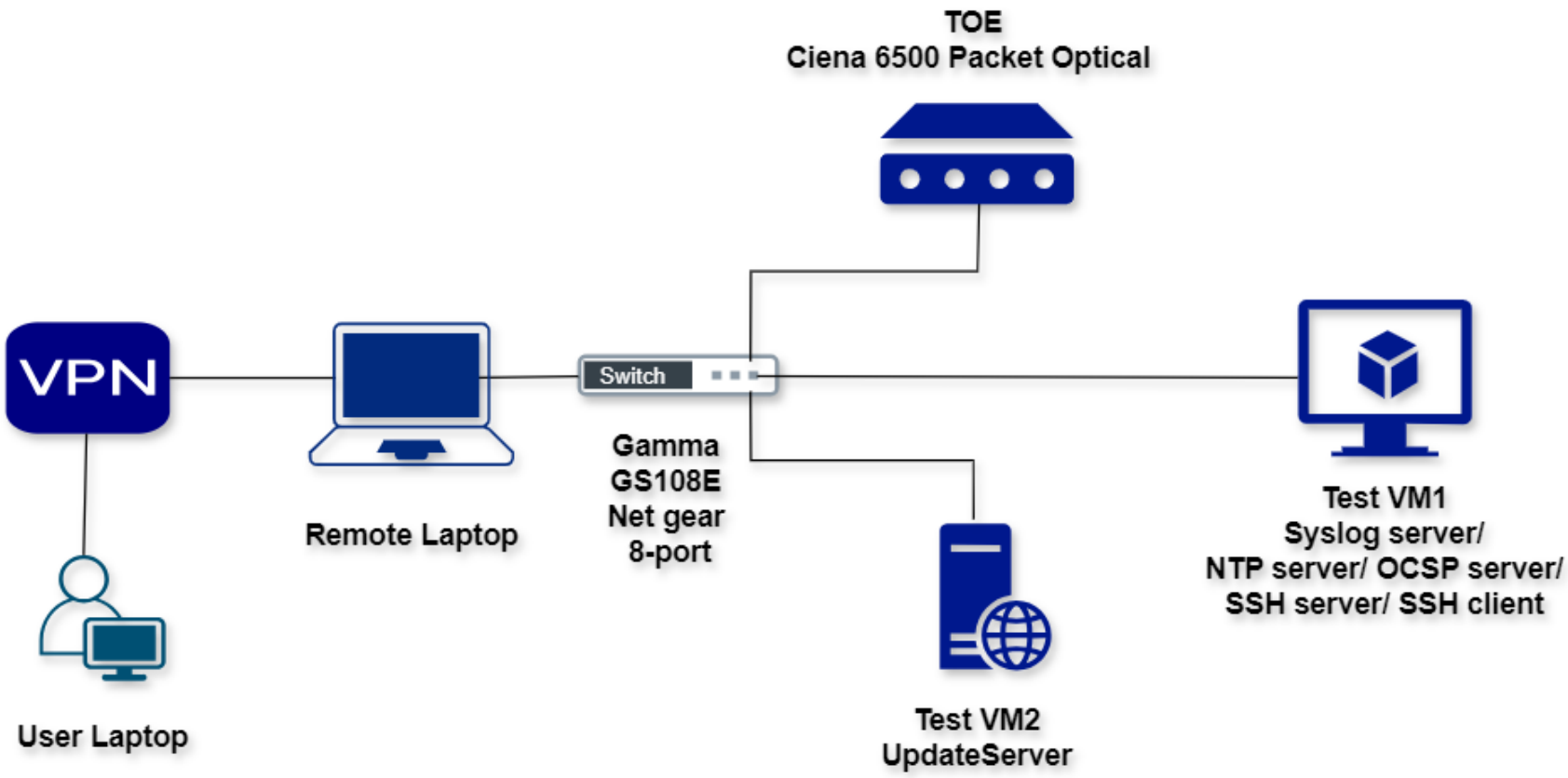
A detailed equivalency report can be found in the document called Equivalency Analysis for 6500 Packet Optical (22 April 2024). The hardware devices for this evaluation are nearly identical with the exception of their shelf sizes. The 6500 has four shelf variants which range in size from 2RU to 32RU. Each variant has the same software image loaded onto it and therefore each has the same security functionality across the family.

All hardware devices in this evaluation compile and execute the same binary update file of 15.6. Because of this, all platforms are equivalent between processor families and provide the same TOE Security Functionality. A full suite of testing will be performed on devices listed below running software 15.6:

- 6500 Packet Optical SP3 processor card installed on the 7-Slot device (NTK503PA)
  - QorIQ T1042 Quad Core processor with VxWorks 6.9
- 6500 Packet Optical SPAP3 processor card installed on the 2-Slot Type 2 device (NTK503LA)
  - QorIQ T1022 Dual Core processor with VxWorks 6.9

4 TEST BED DESCRIPTIONS

4.1 TEST BED



4.2 CONFIGURATION INFORMATION

The following table provides configuration information about each device in the test environment.

Device Details		Network Details		System Details		
Device Name	**Function**	**MAC Address**	**Protocols**	**OS, including version**	**Timing Source**	**Software & Tools, including version**
Ciena 6500 Packet Optical SPAP3	TOE	40:B2:C8:00:0A:36	SSH/TLS/OCSP/ NTP/SFTP	VxWorks Version 6.9 Version 15.6	Manually set and verified	N/A
Ciena 6500 Packet Optical SP3	TOE	2C:39:C1:A4:84:38	SSH/TLS/OCSP/ NTP/SFTP	VxWorks Version 6.9 Version 15.6	Manually set and verified	N/A
Remote Laptop	Remote Laptop	E8-EA-6A-49-F0-7F	SSH/TLS	Windows 11 22H2	Manually set and verified	MobaXterm (23.2), OpenSSL (1.1.1f), Hex editor (Version 2.5.0.0)
User Laptop	Tester's Laptop	02-00-4C-4F-4F-50	RDP	Windows 10	Manually set and verified	XCA (2.1.1), RDP
Test VM1	Syslog Server/ OCSP Server	1a:15:e3:7e:74:e5	TLS/OCSP	Ubuntu 22.04.3	Manually set and verified	OpenSSL (1.1.1f), acumen-tlsc, acumen-tlsc-v2.2e, X509-mod

	SSH client/ SSH server	1a:15:e3:7e:74:e5	SSH	Ubuntu 22.04.3	Manually set and verified	acumen-sshc, acumen-sshs
	NTP server	1a:15:e3:7e:74:e5	NTP	Ubuntu 22.04.3	NTP	N/A
		a6:e7:42:b2:7f:52		Ubuntu 23.10		
		3a:43:ce:46:8c:ed		Ubuntu 23.10		
		d6:45:b0:91:eb:14		Ubuntu 23.10		
Test VM2	Update server	fe:30:65:14:a5:00	SFTP	Ubuntu 22.04.3	Manually set and verified	N/A
Gamma GS108E Net gear 8-Port	L2 Switch	N/A	N/A	N/A	N/A	N/A

4.3 TEST TIME AND LOCATION

All Testing was done remotely from the Acumen lab with some on-site testing performed at the vendor facility for the SPAP3 and SP3 platform. The remote testing was carried out from Acumen Security offices located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from October 2023 to December 2024.

The on-site (local) testing for SPAP3 and SP3 platform was performed at the vendor's main production facility located at 7035 Ridge Road in Hanover, Maryland 21076 from 01/24/24 – 01/31/24. Follow up on-site retesting took place on 07/23/2024, 11/14/2024 and 12/17/2024.

The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each testing day, the test bed was verified to ensure that it was not compromised. Evidence collected during on-site testing was then securely uploaded to the Acumen repository at the end of each day. All evaluation documentation and evidence was always kept in a secure repository at the Acumen facility.

5 DETAILED TEST CASES (TSS AND AGD ACTIVITIES)

5.1 MANDATORY REQUIREMENTS

5.1.1 SECURITY AUDIT (FAU)

5.1.1.1 FAU_GEN.1 AUDIT DATA GENERATION

5.1.1.1.1 FAU_GEN.1 TSS

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.

Evaluator Findings:
The evaluator examined the TSS section 7 in the ST and ensured that it identifies what information is logged to identify the relevant cryptographic key during generating/import, changing, or deleting. The relevant information is found in the following section(s): TOE Summary Specification FAU_GEN.1. Upon investigation, the evaluator found that the TSS states that: The generation of an audit record for the creation, importing and deletion of the SSH key pair contains the id of the device, date and time, USERID, SOURCE, PRIORITY, STATUS, KEYSIZE and KEYTYPE. There is only ever one SSH key pair associated with the TOE. A similar audit record is generated for TLS keys when importing or deleting X509 certificates. The audit record contains the DN, SERIALNUMBER, ISSUER and Validity date of the certificate.

For distributed TOEs the evaluator shall examine the TSS and ensured that it describes which of the overall required auditable events defined in FAU_GEN.1.1 are generated and recorded by which TOE components.

Evaluator Findings:
The TOE is not a distributed TOE; hence this assurance activity is not applicable.

The evaluator shall ensure that the mapping of audit events to TOE components accounts for, and is consistent with, information provided in Table 1, as well as events in Tables 2, 4, and 5 (as applicable to the overall TOE). The evaluator confirmed that all components defined as

generating audit information for a particular SFR contributed to that SFR as defined in the mapping of SFRs to TOE components, and that the audit records generated by each component covered all the SFRs that it implements.

Evaluator Findings:
The TOE is not a distributed TOE; hence this assurance activity is not applicable.

Verdict:
PASS.

5.1.1.1.2 FAU_GEN.1 AGD

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).

Evaluator Findings:
The evaluator checked the AGD and ensured 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, was provided from the actual audit record). The relevant information is found in the following section(s): Section 11 'Auditing'. Upon investigation, the evaluator found that the AGD provides a list of auditable events in Table 3: Ciena 6500 Auditable Events. Due to table size it should be referenced in the AGD itself. The AGD also specifies the following: The TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The audit records will display in different formats depending on where the audit record originated from. Each audit record generated contains all the required information (date and time of the event, type of event, subject identity, and the outcome of the event).

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.

Evaluator Findings:
The evaluator made a determination of the administrative actions related to TSF data related to configuration changes. The evaluator examined the AGD and made 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 relevant information is found in the following section(s): Section 7.4 '**Disable Insecure Services**,' Section 8 '**Enabling CC-NDCPP Compliance**,' Section 9 '**Secure Management of the TOE**,' Section 10 '**Cryptographic Protocols**,' section 11 '**Auditing,**' and section 12 '**Operational Modes**.' **Section 7.4** relates to the disabling of insecure services on the TOE that are not allowed in the evaluated configuration. **Section 8** relates to the enabling of CC-NDCPP mode which restricts algorithms to those claimed in the Security Target. **Section 9** relates to the secure management of the TOE and provides the administrator steps to ensure the TOE is in the proper evaluated configuration. For example, this section specifies how to use SSH public/private key pairs, configure authentication lockout periods, configuring X.509 Certificate authentication for TLS, password enforcement, and session termination when a user idles at the command line/Site Manager on the TOE. **Section 10** of the AGD provides details on the cryptographic protocols and how to enable and disable these services. **Section 11** of the AGD provides information on all the logs generated on the TOE within the evaluated configuration. **Section 12** of the AGD provides a high-level overview of what the administrator should do to put the TOE in an evaluated configuration. All these activities 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.

Evaluator Findings:
The evaluator documented 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 AGD satisfies the requirements related to it.

The relevant information is found in the following section(s): Section 9 'Secure Management of the TOE'.

Upon investigation, the evaluator used the same rationale from the previous activity. Please reference the table in the previous AA. All activities listed are related to TSF configuration changes.

Verdict:
PASS.

5.1.1.2 FAU_GEN.2 USER IDENTITY ASSOCIATION

5.1.1.2.1 TSS & AGD

The TSS and Guidance Documentation requirements for FAU_GEN.2 are already covered by the TSS and AGD requirements for FAU_GEN.1.

5.1.1.3 FAU_STG_EXT.1 PROTECTED AUDIT EVENT STORAGE

5.1.1.3.1 FAU_STG_EXT.1 TSS

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.

Evaluator Findings:
The evaluator examined the TSS for FAU_STG_EXT.1 and ensured that it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. The relevant information is found in the following section(s): TOE Summary Specification FAU_STG_EXT.1. Upon investigation, the evaluator found that the TSS states that: in the evaluated configuration, the TOE simultaneously transmits all audit events to the audit server over a TLS trusted channel.

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.

Evaluator Findings:
The evaluator examined the TSS and ensured 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 relevant information is found in the following section(s): TOE Summary Specification FAU_STG_EXT.1. Upon investigation, the evaluator found that the TSS states that for SP3, the syslog file holds a maximum of 1000 records of 800KB. For SPAP3, the syslog file holds a maximum of 3000 records or 2.5MB. The TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The security log is the record of events such as login/authentication, authorized commands, changes made in the network configuration. The AO contains the detailed information about the event such as what parameters were used. The maximum audit size is approximate as the TSF limits the audit logs based on the number of records per log file or a combined file size of approximately 7MB of data. When a locally stored audit file has reached its defined maximum number of records allowed, or has reached the maximum file size, the oldest record is overwritten with new audit data. The TOE does not provide a user mechanism to delete or modify the locally-stored audit data and the filesystem is not accessible by any user of the TOE.

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.

Evaluator Findings:
The TOE is not a distributed TOE. The TSS for FAU_STG_EXT.1 states that the TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The security log is the record of events such as login/authentication, authorized commands, changes made in the network configuration. The AO contains the detailed information about the event such as what parameters were used. The TOE aggregates both the security log and the AO files into the local audit records file. The local audit record file contains all the information required to satisfy the PP requirements and is therefore the file that is subject to export to the external audit server. The evaluator examined the Security Target to verify that, for distributed TOEs, the TSS contains a list of TOE components that store audit data locally. Upon investigation, the evaluator found that the TOE is not distributed. The evaluation examined the Security Target to verify that, for distributed TOEs that contain component which do not store audit data locally, the TSS contains a mapping between transmitting and storing TOE component. Upon investigation, the evaluator found that the TOE is not distributed.

The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally.

Evaluator Findings:
TOE is not a distributed TOE hence this assurance activity is not applicable.

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.

Evaluator Findings:
The TOE is not a distributed TOE; hence this assurance activity is not applicable.

The evaluator shall examine the TSS to ensure that it details the behaviour 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 behaviour of the TOE shall also be detailed in the TSS.

Evaluator Findings:
The evaluator examined the TSS for FAU_STG_EXT.1 and ensured that it details the behaviour 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 behaviour of the TOE is detailed in the TSS. The relevant information is found in the following section(s): TOE Summary Specification FAU_STG_EXT.1 Upon investigation, the evaluator found that the TSS states that: When a locally stored audit file has reached its defined maximum number of records allowed, or has reached the maximum file size, the oldest record is overwritten with new audit data. The TOE does not provide a user mechanism to delete or modify the locally-stored audit data and the filesystem is not accessible by any user of the TOE.

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 acceptable frequency for the transfer of audit data.

Evaluator Findings:
The evaluator examined the TSS for FAU_STG_EXT.1 and ensured that it details whether the transmission of audit information to an external IT entity can be done in real-time, periodically, or both. In the case where the TOE is capable of performing transmission periodically, the evaluator verified that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data. The relevant information is found in the following section(s): TOE Summary Specification FAU_STG_EXT.1. Upon investigation, the evaluator found that the TSS states that: In the evaluated configuration, the TOE simultaneously transmits all audit events to the audit server over a TLS trusted channel.

For distributed TOEs the evaluator shall examine the TSS to ensure it describes to which TOE components this SFR applies and how audit data transfer to the external audit server is implemented among the different TOE components (e.g. every TOE components does its own transfer or the data is sent to another TOE component for central transfer of all audit events to the external audit server).

Evaluator Findings:
The TOE is not a distributed; TOE hence this assurance activity is not applicable.

For distributed TOEs the evaluator shall examine the TSS to ensure it describes which TOE components are storing audit information locally and which components are buffering audit information and forwarding the information to another TOE component for local storage. For every component the TSS shall describe the behaviour when local storage space or buffer space is exhausted.

Evaluator Findings:
The TOE is not a distributed; TOE hence this assurance activity is not applicable.

Verdict:
PASS.

5.1.1.3.2 FAU_STG_EXT.1 AGD

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.

Evaluator Findings:
The evaluator examined the guidance documentation section 11.1 titled **'Syslog server Configuration'** and ensured 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. The relevant information is found in the following section(s): Section 11.1 titled **'Syslog server Configuration'.** Upon investigation, the evaluator found that the AGD provides the information for how the admin needs to use the T1 Command builder to configure the syslog server and how to set the appropriate privilege level. The server protocol also includes loading CA certificates into the TOE's trust store which is noted in step 4 of the configuration instructions. The final step is the command for pointing the TOE to the appropriate syslog server to connect. When all these steps are completed the connection is configured in a way that it is considered a trusted channel.

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.

Evaluator Findings:
The evaluator also examined the guidance documentation section titled 11.2 **'Audit Storage'** and determined that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. The relevant information is found in the following section(s): Section 11.2 **'Audit Storage'** Upon investigation, the evaluator found that the AGD states that: < the TOE stores audit data locally in three distinct files: security log, autonomous outputs (AO) log, and syslog. The security log is the record of events such as login/authentication, authorized commands, changes made in the network configuration. The AO contains the detailed information about the event such as what parameters were used. The TOE aggregates both the security log and the AO files into the syslog records file. The syslog file contains all the information required to satisfy the PP requirements and is therefore the file that is subject to export to the external audit server. The TOE simultaneously transmits all audit events to the audit server over a TLS trusted channel. In the evaluated configuration, the syslog file is periodically pulled to a remote audit server, via an automated script, using SFTP over an SSH trusted channel.

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

Evaluator Findings:
The evaluator ensured that the AGD describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behaviour of the TOE for each possible configuration. The description of possible configuration options and resulting behaviour correspond to those described in the TSS. The relevant information is found in the following section(s): Section 11.2 **'Audit Storage'** and 11 **'Auditing'** Upon investigation, the evaluator found that the AGD states that: when a locally stored audit file has reached its defined maximum number of records allowed, or has reached the maximum file size, the oldest record is overwritten with new audit data. This matches the claimed requirement selection for FAU_STG_EXT.1.3.

Verdict:
PASS.

5.1.2 CRYPTOGRAPHIC SUPPORT (FCS)

5.1.2.1 FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION

5.1.2.1.1 FCS_CKM.1 TSS

The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE.

Evaluator Findings:
The evaluator ensured that the TSS for FCS_CKM.1 identifies the key sizes supported by the TOE. The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.1. Upon investigation, the evaluator found that the TSS states that: That the TOE generates 2048 asymmetric keys for RSA providing support for SSHv2 and TLS according to FIPS PUB 186-4.

If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.

Evaluator Findings:
The evaluator examined the TSS for FCS_CKM.1 and verified that it identifies the usage for each scheme. The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.1. Upon investigation, the evaluator found that the TSS states that: The TOE generates 2048 asymmetric keys for RSA support for SSHv2 and TLS according to FIPS PUB 186-4. The TOE also generates ECC keys over NIST curves P-256, P-384, and P-521 in accordance with FIPS PUB 186-4 Appendix B.4. ECC keys are used in support of SSH and TLS.

Verdict:
PASS.

5.1.2.1.2 FCS_CKM.1 AGD

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.

Evaluator Findings:
The evaluator verified that the AGD section titled 7.3 **'Cryptographic Configuration Notice'** 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. The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice'** Upon investigation, the evaluator found that the AGD states that: the administrator installing the TOE is expected to perform all of the operations in Sections 7.1 and 7.2 of the AGD. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements. The TOE is preconfigured to enforce the use of the selected DRBG, key generation and key establishment schemes, key sizes, hash sizes, and ciphersuites listed below: • Encryption using AES-128-CBC, AES-256-CBC, AES-128-CTR and AES-256-CTR • Public key user and host authentication: RSA-SHA2-256 or RSA-SHA2-512 • Integrity using HMAC-SHA2-256 and HMAC-SHA2-384 • Key exchange using ECDH over NIST P-256 with SHA2, ECDH over NIST P-384 with SHA2 or ECDH over NIST P-521

Verdict:
PASS.

5.1.2.2 FCS_CKM.2 CRYPTOGRAPHIC KEY ESTABLISHMENT

5.1.2.2.1 FCS_CKM.2 TSS **[TD0580]**

The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1.

Evaluator Findings:
The evaluator ensured that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. The relevant information is found in the following section(s): TOE Summary Specification for FCS_CKM.2.

Upon investigation, the evaluator found that the TSS states that: the TOE implements ECC key establishment in accordance with SP 800-56Ar3. This key establishment scheme is used in support of SSH and TLS trusted channels. This corresponds to the scheme claimed 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. It is sufficient to provide the scheme, SFR, and service in the TSS.

Evaluator Findings:

The evaluator examined the TSS for FCS_CKM.1 to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.

The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.2.

Upon investigation, the evaluator found that the TSS states that usage for each scheme is as noted in the chart below:

Key Generation	SFR	Usage
Elliptic curve	FCS_SSHC_EXT.1, FCS_SSHS_EXT.1, FCS_TLSC_EXT.1	SSH Server for administration and SSH Client for connections to an update server TLS Client for connections to an update server.

Verdict:
PASS.

5.1.2.2.2 FCS_CKM.2 AGD

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

Evaluator Findings:
The evaluator verified that the AGD guidance section 7.3 **'Cryptographic Configuration Notice'** instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice'** Upon investigation, the evaluator found that the AGD states that: the administrator installing the TOE is expected to perform all of the operations in Sections 7.1, 7.2, 7.4 and 8. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements. The TOE is preconfigured to enforce the use of the selected DRBG, key generation and key establishment schemes, key sizes, hash sizes, and ciphersuites to conform to the Common Criteria selections.

Verdict:
PASS.

5.1.2.3 FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION

5.1.2.3.1 FCS_CKM.4 TSS

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 for2). 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.

Evaluator Findings:
The evaluator examined the TSS for FCS_CKM.4 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. The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.4

Upon investigation, the evaluator found that the TSS states that: the Diffie-Hellman Shared Secret, Diffie Hellman private exponent, and SSH session key are generated by the TOE and stored in volatile memory (RAM). These keys are destroyed by a single direct overwrite consisting of zeroes and is read back to verify the success of the zeroization prior to releasing the memory free(). These keys are zeroized immediately after they are no longer needed (i.e. connection terminated or re-key) and when the TOE is shut down as well as when power is lost.

The X.509v3 private keys and SSH private key are encrypted with a 256 bit AES key before being stored in non-volatile storage. This symmetric key is stored as two halves. One half is stored in flash on the shelf-processor, the other half is stored in another device on the backplane, separate from the shelf processor. If the INIT-ZEROIZE TL1 command is invoked by the Security Administrator, the AES encryption key is destroyed by a single direct overwrite consisting of zeroes and is read back to verify the success of the zeroization. This effectively destroys the SSH keys as the encrypted SSH private key is not recoverable. There are no known instances where key destruction does not happen as defined. X.509v3 private keys are destroyed by logically addressing the storage location with zeroization using a single overwrite of zero's. Further detail can be referenced in Table 14 of the ST labeled 'Cryptographic Key Destruction Table'.

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).

Evaluator Findings:

The evaluator confirmed 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, the evaluator checked that the claim not to store plaintext keys in non-volatile memory is consistent with the operation of the TOE.

The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.4 .

Upon investigation, the evaluator found that the TSS states that: The X.509v3 private keys and SSH private key are encrypted before being stored in non-volatile storage. Further detail can be referenced in Table 14 of the ST labeled 'Cryptographic Key Destruction Table'. This is consistent with the claims.

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.

Evaluator Findings:
The evaluator checked to ensure the TSS for FCS_CKM.4 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 relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.4 Upon investigation, the evaluator found that the TSS states that: The X.509v3 private keys and SSH private key are encrypted before being stored in non-volatile storage. This symmetric key is stored as two halves. One half is stored in flash on the shelf-processor, the other half is stored in another device on the backplane, separate from the shelf processor. If the INIT-ZEROIZE TL1 command is invoked by the Security Administrator, the AES encryption key is destroyed by a single direct overwrite consisting of zeroes and is read back to verify the success of the zeroization. This effectively destroys the SSH keys as the encrypted SSH private key is not recoverable. There are no known instances where key destruction does not happen as defined.

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.

Evaluator Findings:
Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator checked that the TSS for FCS_CKM.4 identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is destroyed by a method included under FCS_CKM.4. The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.4. Upon investigation, the evaluator found that the TSS states that: the TSS provides the information which confirms that keys stored in non-plaintext form are encrypted using AES and the key-encrypting-key (AES key) is securely stored in two halves in flash on the shelf-processor and the other half on another device on the backplane separate from the shelf-processor. The destruction method for these keys is well-defined with zeroization being verified for the destruction method. This is in line with the claims made for FCS_CKM.4.

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.

Evaluator Findings:
The evaluator checked that the TSS for FCS_CKM.4 identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.4. Upon investigation, the evaluator found that the TSS states that: here are no known instances where key destruction does not happen as defined.

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.

Evaluator Findings:
Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examined the TSS for FCS_CKM.4 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. The relevant information is found in the following section(s): TOE Summary Specification FCS_CKM.4 . Upon investigation, the evaluator found that the TSS states that: keys are overwritten with zeroes. This is considered a consistent value and the use of zeroes is a non-CSP-containing value.

Verdict:
PASS.

5.1.2.3.2 FCS_CKM.4 AGD

A TOE may be subject to situations that could prevent or delay key destruction in some cases. 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).

Evaluator Findings:
The evaluator checked that the guidance documentation section 7.3 **'Cryptographic Configuration Notice'** 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). The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice'** Upon investigation, the evaluator found that the AGD states that: the Diffie-Hellman Shared Secret, Diffie Hellman private exponent, and SSH session key are generated by the TOE and stored in volatile memory (RAM). These keys are destroyed by a single direct overwrite consisting of zeroes and is read back to verify the success of the zeroization prior to releasing the memory free(). These keys are zeroized immediately after they are no longer needed (i.e. connection terminated or re-key) and when the TOE is shut down as well as when power is lost. As the keys are zeroized immediately there are no delays in key destruction to note.

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

For example, when the TOE does not have full access to the physical memory, it is possible that the storage may be implementing wear-levelling and garbage collection. This may result in additional copies of the key that are logically inaccessible but persist physically. Where available, the TOE might then describe use of the TRIM command3 and garbage collection to destroy these persistent copies upon their deletion (this would be explained in TSS and Operational Guidance).

Evaluator Findings:
The evaluator checked that the guidance documentation section 7.3 'Cryptographic Configuration Notice' provides guidance on situations where key destruction may be delayed at the physical layer. The relevant information is found in the following section(s): 7.3 'Cryptographic Configuration Notice'

Upon investigation, the evaluator found that the AGD states that: As the keys are zeroized immediately there are no delays in key destruction to noted.

Verdict:
PASS.

5.1.2.4 FCS_COP.1/DATAENCRYPTION CRYPTOGRAPHIC OPERATION (AES DATA ENCRYPTION/DECRYPTION)

5.1.2.4.1 FCS_COP.1/DATAENCRYPTION TSS

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.

Evaluator Findings:
The evaluator examined the TSS for FCS_COP.1/DataEncryption to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. The relevant information is found in the following section(s): TOE Summary Specification FCS_COP.1/DataEncryption. Upon investigation, the evaluator found that the TSS states that: The TOE provides symmetric encryption and decryption capabilities using AES in CBC and CTR modes with 128 and 256-bit keys in support of SSH functionality. The TOE implements AES with 128-bit or 256-bit keys in GCM or CBC modes in support of TLS functionality.

Verdict:
PASS.

5.1.2.4.2 FCS_COP.1/DATAENCRYPTION AGD

EThe 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.

Evaluator Findings:
The evaluator verified that the AGD guidance for 7.3 **'Cryptographic Configuration Notice'** 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.

The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice'** and 7.1 **'Initial Configuration'**

Upon investigation, the evaluator found that the AGD states that: the administrator installing the TOE is expected to perform all of the operations in Sections 7.1, 7.2, 7.4 and 8 of the AGD. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements. The TOE is preconfigured to enforce the use of the selected DRBG, key generation and key establishment schemes, key sizes, hash sizes, and ciphersuites. These configurations use AES-128-CBC, AES-256-CBC, AES-128-CTR, AES-256-CTR, AES-128-GCM, and AES-256-GCM for encryption/decryption.

Verdict:
PASS.

5.1.2.5 FCS_COP.1/SIGGEN CRYPTOGRAPHIC OPERATION (SIGNATURE GENERATION AND VERIFICATION)

5.1.2.5.1 FCS_COP.1/SIGGEN TSS

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

Evaluator Findings:

The evaluator examined the TSS for FCS_COP.1/SigGen to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.

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

Upon investigation, the evaluator found that the TSS states that: the TOE provides RSA and ECDSA signature generation and verification. RSA keys are 2048, while ECDSA keys are 256, 384, or 521 bits. These keys are used in support of SSH and TLS.

Verdict:
PASS.

5.1.2.5.2 FCS_COP.1/SIGGEN AGD

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.

Evaluator Findings:
The evaluator verified that the AGD guidance section 7.3 **'Cryptographic Configuration Notice'** 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. The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice'** Upon investigation, the evaluator found that the AGD states that: the administrator installing the TOE is expected to perform all of the operations in Sections 7.1, 7.2, 7.4 and 8 of this document. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements. The TOE is preconfigured to enforce the use of the selected DRBG, key generation and key establishment schemes, key sizes, hash sizes, and ciphersuites as follows: • Encryption using AES-128-CBC, AES-256-CBC, AES-128-CTR, AES-256-CTR, AES-128-GCM, and AES-256-GCM • Public key user and host authentication: RSA-SHA2-256 or RSA-SHA2-512 • Integrity using HMAC-SHA2-256 and HMAC-SHA2-384 • Key exchange using ECDH over NIST P-256 with SHA2, ECDH over NIST P-384 with SHA2 or ECDH over NIST P-521 with SHA2.

Verdict:
PASS.

5.1.2.6 FCS_COP.1/HASH CRYPTOGRAPHIC OPERATION (HASH ALGORITHM)

5.1.2.6.1 FCS_COP.1/HASH TSS

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.

Evaluator Findings:
The evaluator checked that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS for FCS_COP.1/Hash.

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

Upon investigation, the evaluator found that the TSS states that: the TOE provides SHA2-256, SHA2-384 and SHA2-512 hashing services in support of TLS.

The TOE provides SHA2-256 and SHA2-512 hashing services, offering 256 or 512 bit output MAC sizes, in support of SSH services. These are also used to compute the software integrity checksum.

Verdict:
PASS.

5.1.2.6.2 FCS_COP.1/HASH AGD

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

Evaluator Findings:

The evaluator checked the AGD documents section 7.3 **'Cryptographic Configuration Notice'** to determine that any configuration that is required to configure the required hash sizes is present.

The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice'**

Upon investigation, the evaluator found that the AGD states that: the administrator installing the TOE is expected to perform all of the operations in Sections 7.1, 7.2, 7.4 and 8. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements. The TOE is preconfigured to enforce the use of the selected DRBG, key generation and key establishment schemes, key sizes, hash sizes, and ciphersuites as integrity using HMAC-SHA2-256 and HMAC-SHA2-384 which is consistent with that is defined in the Security Target.

Verdict:
PASS.

5.1.2.7 FCS_COP.1/KEYEDHASH CRYPTOGRAPHIC OPERATION (KEYED HASH ALGORITHM)

5.1.2.7.1 FCS_COP.1/KEYEDHASH TSS

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.

Evaluator Findings:

The evaluator examined the TSS for FCS_COP.1/KeyedHash 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 relevant information is found in the following section(s): TOE Summary Specification FCS_COP.1/KeyedHash.

Upon investigation, the evaluator found that the TSS states that: the TOE provides keyed hashing using HMAC-SHA2-256 and HMAC-SHA2-384 used for TLS and SSH. The key, block and digest sizes for HMAC-SHA-256 and HMAC-SHA2-384 are included in the chart below:

Algorithm	Block Size	Key Size	Digest Size
HMAC-SHA-256	512 bits	256 bits	256 bits
HMAC-SHA2-384	1024 bits	384 bits	384 bits

Verdict:
PASS.

5.1.2.7.2 FCS_COP.1/KEYEDHASH AGD

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.

Evaluator Findings:

The evaluator verified that the AGD guidance section 7.3 titled **'Cryptographic Configuration Notice'** 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.

The relevant information is found in the following section(s): 7.3 titled **'Cryptographic Configuration Notice'**

The administrator installing the TOE is expected to perform all of the operations as mentioned in Sections 7.1, 7.2, 7.4 and 8 of this document. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE's cryptographic engine as the TOE already becomes pre-configured to meet many of the Common Criteria requirements. The TOE is preconfigured to enforce the use of the selected DRBG, key generation and key establishment schemes, key sizes, hash sizes, and ciphersuites as defined in the Security Target.

- Encryption algorithms: AES-128-cbc, AES-256-cbc, AES-128-ctr, AES-256-ctr, AES-128-gcm, and AES-256-gcm
- Public key algorithm: RSA-SHA2-256 or RSA-SHA2-512
- MAC algorithms: HMAC-sha-256 and HMAC-SHA-384
- Key exchange using ECDH over NIST P-256 with SHA2, ECDH over NIST P-384 with SHA2 or ECDH over NIST P-521 with SHA2.

Verdict:
PASS.

5.1.2.8 FCS_RBG_EXT.1 EXTENDED: CRYPTOGRAPHIC OPERATION (RANDOM BIT GENERATION)

5.1.2.8.1 FCS_RBG_EXT.1 TSS

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.

Evaluator Findings:

The evaluator examined the TSS for FCS_RBG_EXT.1 and determined 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.

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

Upon investigation, the evaluator found that the TSS states that: the TOE implements a NIST-approved deterministic random bit generator (DRBG) as specified in ISO/IEC 18031:2011. The DRBG used by the TOE is the CTR_DRBG (AES). The TOE models provide an FPGA hardware-based entropy source as described in the proprietary Entropy Analysis Report (EAR). The DRBG is seeded with a minimum of 256 bits of entropy so that it is sufficient to ensure full entropy.

Verdict:
PASS.

5.1.2.8.2 FCS_RBG_EXT.1 AGD

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

Evaluator Findings:
The evaluator confirmed that the guidance documentation section 10.3 titled **'Crypto Configuration'** and 7.3 **'Cryptographic Configuration'** contains appropriate instructions for configuring the RNG functionality. The relevant information is found in the following section(s): 10.3 titled **'Crypto Configuration'** and 7.3 **'Cryptographic Configuration'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDCPP compliance. RNG functionality is specified in this section of the AGD (10.3) and should be further referenced in section 7.3 **'Cryptographic Configuration'**. This section states that the TOE implements a NIST-approved deterministic random bit generator (DRBG) as specified in ISO/IEC 18031:2011. The DRBG used by the TOE is the CTR_DRBG (AES).

Verdict:
PASS.

5.1.3 IDENTIFICATION AND AUTHENTICATION (FIA)

5.1.3.1 FIA_AFL.1 AUTHENTICATION FAILURE MANAGEMENT

5.1.3.1.1 FIA_AFL.1 TSS

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.

Evaluator Findings:
The evaluator examined the TSS and determined 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 also describes the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability. The relevant information is found in the following section(s): TOE Summary Specification FIA_AFL.1. Upon investigation, the evaluator found that the TSS states that: the TOE uses a counter to keep track of the number of unsuccessful authentication attempts that occur per user. The authentication failure threshold is configurable by a Security Administrator with UPC >=4 and can be set between 2 and 20. Once the authentication failure threshold is reached, the TOE prevents further authentication attempts by locking that users account. The TOE will prevent the user from successfully authenticating until a Security Administrator with a UPC >=4 unlocks the accounts or the account is automatically unlocked after a configurable period of between 0 and 300 seconds, with 0 meaning no automatic locking, i.e. user account is not locked out. The counter is reset to zero upon a successful authentication provided it is accomplished prior to the authentication failure threshold being met and the account being locked. Security Administrators with a UPC>=4 are exempt from being locked out over the local connection to ensures that remote authentication failures cannot cause a denial of service.

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).

Evaluator Findings:
The evaluator examined 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). The relevant information is found in the following section(s): TOE Summary Specification FIA_AFL.1. Upon investigation, the evaluator found that the TSS states that: a Security Administrators with a UPC>=4 are exempt from being locked out over the local connection to ensures that remote authentication failures cannot cause a denial of service

Verdict:
PASS.

5.1.3.1.2 FIA_AFL.1 AGD

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.

Evaluator Findings:
The evaluator examined 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. The relevant information is found in the following section(s): 9.3 **'Failed Authentication Lockout'** Upon investigation, the evaluator found that the AGD states that: in the evaluated configuration, the TOE will lock a remote administrative account when an administrator configured number of successive invalid login attempts have been made within an administrator configured time period. This applies to the remote TL1 interface, and the default values for the failed attempts is between 2 and 20 unsuccessful remote authentication attempts within 15 minutes. The TOE prevents further authentication attempts until a Security Administrator with a UPC Level of 4 or higher (UPC >=4) unlocks the accounts or the account is automatically unlocked after a configurable period of between 0 and 7200 seconds, with 0 meaning no automatic locking, i.e. user account is not locked out. The TOE ensures that remote authentication failures do not prevent another Administrator from accessing the TOE thus preventing a denial of service attack from taking place. By default, this is achieved by exempting Security Administrators with a UPC >=4 from being locked out on local connections.

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.

Evaluator Findings:
The evaluator examined 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. The relevant information is found in the following section(s): 9.4 **'Failed Authentication Lockout'** Upon investigation, the evaluator found that the AGD states that: The TOE ensures that remote authentication failures do not prevent another Administrator from accessing the TOE thus preventing a denial of service attack from taking place. By default, this is achieved by exempting Security Administrators with a UPC >=4 from being locked out on local connections.

Verdict:
PASS.

5.1.3.2 FIA_PMG_EXT.1 PASSWORD MANAGEMENT

5.1.3.2.1 FIA_PMG_EXT.1 TSS **[TD0792]**

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

Evaluator Findings:
The evaluated examined the TSS and verified that it lists the supported special character(s) for the composition of administrator passwords. The relevant information is found in the following section(s): TOE Summary Specification FIA_PMG_EXT.1. Upon investigation, the evaluator found that the TSS states that: the passwords can be composed of any combination of upper and lower-case letters, numbers, and special characters. The supported special characters include "!", "@", "#", "$", "%", "^", "*", "(", ")", "", "", "+", "-", "_", "/", "<", "=", ">", "{", "}", "\" and "~". A Security Administrator has the ability to set the minimum length that is permitted to any value between 8 and 128. In the evaluated configuration passwords must be set to 8 characters or greater. The TOE supports three local password rules: Standard, Complex and Custom. The default is Standard for the 6500.

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

Evaluator Findings:
The evaluated examined the TSS and verified that the minimum_password_length parameter is configurable by a Security Administrator. The relevant information is found in the following section(s): TOE Summary Specification FIA_PMG_EXT.1. Upon investigation, the evaluator found that the TSS states that: A Security Administrator has the ability to set the minimum length that is permitted to any value between 8 and 128. In the evaluated configuration passwords must be set to 8 characters or greater. The TOE supports three local password rules: Standard, Complex and Custom. The default is Standard for the 6500.

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.

Evaluator Findings:
The evaluated examined the TSS and verified that it lists the range of values supported for the minimum_password_length parameter. The listed range includes the value of 15. The relevant information is found in the following section(s): TOE Summary Specification FIA_PMG_EXT.1. Upon investigation, the evaluator found that the TSS states that: A Security Administrator has the ability to set the minimum length that is permitted to any value between 8 and 128. In the evaluated configuration passwords must be set to 8 characters or greater. The TOE supports three local password rules: Standard, Complex and Custom. The default is Standard for the 6500.

Verdict:
PASS.

5.1.3.2.2 FIA_PMG_EXT.1 AGD

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

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

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

Evaluator Findings:
The evaluator examined 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. The relevant information is found in the following section(s): 9.8 **'Password Management'** Upon investigation, the evaluator found that the AGD states that: a Security Administrator has the ability to set the minimum length that is permitted to any value between 8 and 128. In the evaluated configuration, the passwords must have minimum length of 8 characters or greater. The accepted characters include upper and lower case letters, numbers, and the special characters "!", "@", "#", "$", "%", "^", "*", "(", ")", "", "", "+", "-", "_", "/", "<", "=", ">", "{", "}", "\" and "~". In order to minimize the risk of account compromise, it is recommended to use a password that includes a mixture of uppercase, lowercase, numeric, and special characters and is not a common word or phrase. The TOE supports three local password rules: Standard, Complex and Custom. The default is Standard for the Ciena 6500. When a password is set to the above specifications it is considered an appropriate password of sufficient strength.

Verdict:
PASS.

5.1.3.3 FIA_UIA_EXT.1 USER IDENTIFICATION AND AUTHENTICATION

5.1.3.3.1 FIA_UIA_EXT.1 TSS

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".

Evaluator Findings:
The evaluator examined the TSS for FIA_UIA_EXT.1 determine that it describes the logon process for remote authentication mechanism (e.g. SSH public key, Web GUI password, etc.) and optional local authentication mechanisms supported by the TOE. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon".

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

Upon investigation, the evaluator found that the TSS states that: the TOE requires the use of locally-defined authentication credentials. The TOE supports remote authentication using SSH public keys. Local authentication is handled with username/password.

Users are not allowed to perform any security-relevant functions on the TOE without first being successfully identified and authenticated by the TOE's authentication method, with the exception of viewing the warning banner. At initial login, via the TL1 ACT-USER command, the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and credential are correct) or indicates that the login was unsuccessful. The TOE stores username and password hash data in the local storage for the TL1 interfaces.

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.

Evaluator Findings:
The evaluator examined the TSS for FIA_UIA_EXT.1 and determined that it describes which actions are allowed before administrator identification and authentication. The description shall cover authentication and identification for local and remote TOE administration. The relevant information is found in the following section(s): TOE Summary Specification FIA_UIA_EXT.1. Upon investigation, the evaluator found that the TSS states that: users are not allowed to perform any security-relevant functions on the TOE without first being successfully identified and authenticated by the TOE's authentication method, with the exception of viewing the warning banner and the TOE will respond to ICMP echo requests with an ICMP echo response.

For distributed TOEs the evaluator shall examine that the TSS details how Security Administrators are authenticated and identified by all TOE components. If not, all TOE components support authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2, the TSS shall describe how the overall TOE functionality is split between TOE components including how it is ensured that no unauthorized access to any TOE component can occur.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

For distributed TOEs, the evaluator shall examine the TSS to determine that it describes for each TOE component which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration. For each TOE component that does not support authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2 the TSS shall describe any unauthenticated services/services that are supported by the component.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

Verdict:
PASS.

5.1.3.3.2 FIA_UIA_EXT.1 AGD

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.

Evaluator Findings:
The evaluator examined the guidance documentation sections 9.4 titled **'User Accounts and User Management'**, 9.2 titled **'Generating, Configuring and Uploading SSH Public/Private key on TOE'** and Section 7.4 **'Disable Insecure Services'** and determined 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. The relevant information is found in the following section(s): 9.4 titled **'User Accounts and User Management'**, 9.2 titled **'Generating, Configuring and Uploading SSH Public/Private key on TOE'** and Section 7.4 **'Disable Insecure Services'**

Upon investigation, the evaluator found that the AGD states that: the TOE requires the use of locally defined authentication credentials. Users are not allowed to perform any security-relevant functions on the TOE without first being successfully identified and authenticated by the TOE's authentication method. At initial login, via a TL1 ACT-USER command, the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and credential are correct) or indicates that the login was unsuccessful.

Section 9.2 titled 'Generating, Configuring and Uploading SSH Public/Private key on TOE' provides instructions on how to generate SSH key pairs to allow users to authenticate to the TOE. This is a prerequisite that must be completed prior to setting the SSH Server authentication method to public key as seen in section 8. At least one SSH/SFTP User with public key (authorized user entry) must be configured before public key authentication can be used by the SSH/SFTP Server (i.e., before setting SSH Server "Server Auth" to Public Key).

Section 7.4 titled 'Disabling Insecure Services' provides information and instruction for additional configuration that the admin performs as part of initial installation. In the evaluated configuration, certain services will need to be configured off on the TOE. The Security Administrator will need to disable these services by performing the appropriate TL1 commands. Detailed commands and services that can be disabled are located in this section of the AGD and can be referenced in greater detail there.

Section 9.4 titled 'User Accounts and Management' provides instructions on how to authenticate to the TOE locally. The TOE has two physical connections for security management: a local console (RJ-45 Craft ethernet port) for direct connections and a Central Office Local Area Network (COLAN) ethernet port for remote connections. An administrator can access the TL1 interface using either a local workstation connected directly to the TOE's Craft ethernet port or a remote workstation that can connect to the TOE over the COLAN ethernet via SSH.

Verdict:
PASS.

5.1.3.4 FIA_UAU_EXT.2 PASSWORD-BASED AUTHENTICATION MECHANISM

Evaluation Activities for this requirement are covered under those for FIA_UIA_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA_UIA_EXT.1.

5.1.3.5 FIA_UAU.7 PROTECTED AUTHENTICATION FEEDBACK

5.1.3.5.1 FIA_UAU.7 TSS

None.

5.1.3.5.2 FIA_UAU.7 AGD

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.

Evaluator Findings:
The evaluator examined the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. The relevant information is found in the following section(s): 9.4 titled **'User Accounts and User Managements'** and 9.9 **'Protected Authentication Feedback'** Upon investigation, the evaluator found that the AGD states that: At initial login, via a TL1 ACT-USER command, the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and credential are correct) or indicates that the login was unsuccessful. Section 9.9 of the AGD states that the TOE does not provide any feedback for the password characters entered. This is by default and does not require any configuration.

Verdict:
PASS.

5.1.4 SECURITY MANAGEMENT (FMT)

5.1.4.1 FMT_MOF.1/MANUALUPDATE

5.1.4.1.1 FMT_MOF.1/MANUALUPDATE TSS

For distributed TOEs see chapter 2.4.1.1. There are no specific requirements for non-distributed TOEs.

Evaluator Findings:
The TOE is not a distributed TOE and there are no specific requirements for non-distributed TOES; hence, this assurance activity is not applicable.

Verdict:
PASS.

5.1.4.1.2 FMT_MOF.1/MANUALUPDATE AGD

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).

Evaluator Findings:
The evaluator examined the guidance documentation section 9.13 **'Secure Updates'** and determined that any necessary steps to perform manual update are described. The guidance documentation > also provides warnings regarding functions that may cease to operate during the update (if applicable). The relevant information is found in the following section(s): 9.13 **'Secure Updates'** Upon investigation, the evaluator found that the AGD states that: the TOE provides the ability for a Security Administrator with UPC >=4 to update its software from the TL1 interface. Step-by-step process for this is included in the AGD in this section. The evaluator examined the same section in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD states that the TOE does not provide any warnings regarding functions that may cease to operate during the update procedure.

For distributed TOEs the guidance documentation shall describe all steps how to update all TOE components. This shall contain description of the order in which components need to be updated if the order is relevant to the update process. The guidance documentation shall also provide warnings regarding functions of TOE components and the overall TOE that may cease to operate during the update (if applicable).

Evaluator Findings:
The TOE is not a distributed TOE; hence, this assurance activity is not applicable.

Verdict:
PASS.

5.1.4.2 FMT_MTD.1/COREDATA MANAGEMENT OF TSF DATA

5.1.4.2.1 FMT_MTD.1/COREDATA TSS

The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; 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.

Evaluator Findings:
The evaluator confirmed that the TSS for FMT_MOF.1/CoreData details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. The relevant information is found in the following section(s): TOE Summary Specification FMT_MOF.1/CoreData. Upon investigation, the evaluator found that the TSS states that: The TOE restricts access to the management functions to Security Administrators. No management function of TSF data is available prior to login. Non-administrative users are not allowed to manipulate the TSF data at any time.

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.

Evaluator Findings:
If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator examined the TSS for FMT_MOF.1/CoreData and determined that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. The relevant information is found in the following section(s): TOE Summary Specification FMT_MOF.1/CoreData. Upon investigation, the evaluator found that the TSS states that: the TOE restricts access to the x.509v3 certificate trust store to security administrators and no other users.

Verdict:
PASS.

5.1.4.2.2 FMT_MTD.1/COREDATA AGD

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 c PP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.

Evaluator Findings:
The evaluator reviewed the guidance documentation section 9 **'Secure Management of the TOE'** and 6 **'Evaluated Configuration of the TOE'** and determined 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. The relevant information is found in the following section(s): 9 **'Secure Management of the TOE'** and 6 **'Evaluated Configuration of the TOE'** Upon investigation, the evaluator found that the AGD states that: that TOE restricts access to the management functions to Security Administrators. Non-administrative users are not allowed to manipulate the TSF data at any time.

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.

Evaluator Findings:
If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator reviewed the guidance documentation and determined 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 reviewed the guidance documentation and determined that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator also reviewed the guidance documentation and determined that it explains how to designate a CA certificate a trust anchor. The relevant information is found in the following section(s): 11.1 **'Syslog server Configuration'** and 9.6 **'Configuring X.509 Certificate Authentication'** and 9.6.1 **'Addition of the certificate'**

Upon investigation, the evaluator found that the AGD states that: that section 11.1 **'Syslog server Configuration'** of the AGD provides instructions on how to load CA certificates into the TOE's trust store. This is specifically in step 4 of the instructions in this section.

The evaluator examined the section 9.6 titled **'Configuring X.509 Certificate Authentication'** 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 9.6.1 labeled 'Addition of the certificate' provides instructions for designating the trust anchor.

Verdict:
PASS.

5.1.4.3 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

5.1.4.3.1 FMT_SMF.1 TSS (CONTAINING ALSO REQUIREMENTS ON GUIDANCE DOCUMENTATION AND TESTS)

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.

Evaluator Findings:

The evaluator examined the TSS for FMT_SMF.1, the Guidance Documentation 9.4 **'User Accounts and User Management'** the TOE as observed during all other testing and confirmed that the management functions specified in FMT_SMF.1 are provided by the TOE.

The relevant information is found in the following section(s): TOE Summary Specification FMT_SMF.1 of the Security Target and section 9.4 **'User Accounts and User Management'** of the AGD

Upon investigation, the evaluator found that the TSS states that: **t**he TOE provides all the capabilities necessary to securely manage the TSF. The TOE includes an SSH and TL1 interface to administer the functions associated with day-to-day operations of the TOE. The TL1 interface can

be accessed locally or via the Site Manager graphical front-end that resides on a remote PC and connects to the TOE via SSH. The Site Manager translates user activity into equivalent TL1 commands.

The following management functions are supported by the TOE:

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

The evaluator also found that the AGD states that: section 9.5 titled **'User Accounts and User Management'** of the AGD states that Security administrators can perform activities from both the local craft port interface or remote interface. The TL1 interface can be accessed via SSH only. If administering the TOE locally via TL1 is desired, the management workstation should be placed on a dedicated local network as 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).

Evaluator Findings:
The evaluator confirmed that the TSS for FMT_SMF.1 details which security management functions are available through which interface(s) (local administration interface, remote administration interface).

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

Upon investigation, the evaluator found that the TSS states that: **t**he TOE provides all the capabilities necessary to securely manage the TSF. The TOE includes an SSH and TL1 interface to administer the functions associated with day-to-day operations of the TOE. The TL1 interface can be accessed locally or via the Site Manager graphical front-end that resides on a remote PC and connects to the TOE via SSH. The Site Manager translates user activity into equivalent TL1 commands.

The following management functions are supported by the TOE:

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

The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.

Evaluator Findings:
The evaluator examined the TSS for FMT_SMF.1 and the Guidance Documentation 9.4 **'User Accounts and User Management' in the AGD** to verify they both describe the local administrative interface.

The relevant information is found in the following section(s): TOE Summary Specification FMT_SMF.1 in the Security Target and 9.4 titled **'User Accounts and User Management' in the AGD**

Upon investigation, the evaluator found that the AGD states that: Security administrators can perform activities from both the local craft port interface or remote interface. The TL1 interface can be accessed via SSH only. If administering the TOE locally via TL1 is desired, the management workstation should be placed on a dedicated local network as the TOE.

The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.

Evaluator Findings:
The evaluator ensured the Guidance Documentation section 9.4 **'User Accounts and User Management'** includes appropriate warnings for the administrator to ensure the interface is local. The relevant information is found in the following section(s): 9.4 titled **'User Accounts and User Management'** and 7.5 **'Login Banner'** Upon investigation, the evaluator found that the AGD states that: Security administrators can perform activities from both the local craft port interface or remote interface. The TL1 interface can be accessed via SSH only. If administering the TOE locally via TL1 is desired, the management workstation should be placed on a dedicated local network as the TOE. The evaluator examined the section titled 7.5 **'Login Banner'** in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD states that the TOE displays a configurable warning banner on the local and remote console prior to a user supplying their authentication credentials. Remote authentication requires the use of SSH. The warning banner is configured by a Security Administrator with a UPC >=4.

For distributed TOEs with the option 'ability to configure the interaction between TOE components' the evaluator shall examine that the ways to configure the interaction between TOE components is detailed in the TSS and Guidance Documentation.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

Verdict:
PASS.

5.1.4.3.2 FMT_SMF.1 AGD

See section 2.4.4.1.

Evaluator Findings:
See section 5.1.4.3.1 of this document for AGD activities.

Verdict:
PASS.

5.1.4.4 FMT_SMR.2 RESTRICTIONS ON SECURITY ROLES

5.1.4.4.1 FMT_SMR.2 TSS

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.

Evaluator Findings:
The evaluator examined the TSS for FMT_SMR.2 and determined that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE. The relevant information is found in the following section(s): TOE Summary Specification FMT_SMR.2. Upon investigation, the evaluator found that the TSS states that: the Security Administrator role, as defined by the NDcPP, is met through the Security Administrator role with a UPC between 1 and 5 that is defined for the TL1 interface and remote administration over SSH. Each of the five Security Administrator roles, has a fixed set of allowed operations based on the UPC value assigned to the Security Administrator. A larger UPC value provides more capabilities for the Security Administrator. These Security Administrators manage the TOE locally and remotely using SSH via the TL1 interface of the TSF.

Verdict:
PASS.

5.1.4.4.2 FMT_SMR.2 AGD

The evaluator shall review the guidance documentation 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.

Evaluator Findings:
The evaluator reviewed the AGD section 9 **'Secure Management of the TOE'** and 9.1 **'Authentication the TOE via SSH'** and 9.4 **'User Accounts and user Management'** and ensured 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. The relevant information is found in the following section(s): 9 **'Secure Management of the TOE',**9.1 **'Authentication the TOE via SSH' and 9.4 'User Accounts and User Management'** Upon investigation, the evaluator found that the AGD s provides instructions for administering the TOE both locally and remotely including the configuration that needs to be performed on the client in remote cases. Section 9 of the AGD notes that the instructions in this chapter are specific to the evaluated configuration of the TOE in relation to how the security administrator is the only entity that can manage the TSF data off the TOE. Section 9.4 of the AGD states that an administrator can access the TL1 interface using either a local workstation connected directly to the TOE's Craft ethernet port or a remote workstation that can connect to the TOE over the COLAN ethernet via SSH. Section 9.1 titled 'Authenticating to the TOE via SSH' provides the instructions for a remote connection. This includes the use of client side login.

Verdict:
PASS.

5.1.5 PROTECTION OF THE TSF (FPT)

5.1.5.1 FPT_SKP_EXT.1 PROTECTION OF TSF DATA (FOR READING OF ALL PRE-SHARED, SYMMETRIC AND PRIVATE KEYS)

5.1.5.1.1 FPT_SKP_EXT.1 TSS

The evaluator shall examine 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. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.

Evaluator Findings:
The evaluator examined the TSS for FPT_SKP_EXT.1 and determined 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. If these values are not stored in plaintext, the TSS describes how they are protected/obscured. The relevant information is found in the following section(s): TOE Summary Specification FPT_SKP_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE does not provide a mechanism to view secret keys and key material. The fingerprint of the public key data that is stored on the TOE can be viewed by a Security Administrator depending on their UPC level: node SSH public key (UPC>=1), SSH server host keys (UPC>=2), and SSH client authorized keys or the X.509v3 certificates used for TLS authentication (UPC>=4). In the case of the public key with known hosts, only the fingerprint of the key is observable. Key data that is resident in volatile memory cannot be accessed by an administrative command. Any persistent key data is stored in the underlying filesystem of the OS on internal flash memory. The TOE's management interfaces do not provide any direct access to the file system therefore, there is no administrative method of accessing this data. The X.509v3 private keys and SSH private key are encrypted with a 256 bit AES key before being stored in non-volatile storage (filesystem).

Verdict:
PASS.

5.1.5.2 FPT_APW_EXT.1 PROTECTION OF ADMINISTRATOR PASSWORDS

5.1.5.2.1 FPT_APW_EXT.1 TSS

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. 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.

Evaluator Findings:
The evaluator examined 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. The TSS also detailed 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. The relevant information is found in the following section(s): TOE Summary Specification FPT_APW_EXT.1. Upon investigation, the evaluator found that the TSS states that: Administrator passwords are not stored in plaintext on the TOE. All administrative passwords are hashed using SHA-256 and the hash is what is stored on the TOE. The evaluator also examined the TSS in the Security Target to verify that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that there is no function provided by the TOE to display a password value in plaintext.

Verdict:
PASS.

5.1.5.3 FPT_TST_EXT.1 TSF TESTING

5.1.5.3.1 FPT_TST_EXT.1 TSS

The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; 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).

Evaluator Findings:
The evaluator examined the TSS for FPT_TST_EXT.1 and ensured that it details the self-tests that are run by the TSF; 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" is used). The relevant information is found in the following section(s): TOE Summary Specification FPT_TST_EXT.1.

Upon investigation, the evaluator found that the TSS states that: the TOE runs a series of self-tests during initial start-up to verify its correct operation. As part of the startup of the TOE, the TOE will perform a series of known answer tests, pair-wise consistency tests, continuous random number generator tests, SP 800-90B health tests to verify the correct functionality of the cryptographic functions.

- Known answer tests - A cryptographic algorithm is run on data for which the correct output is already known. The calculated output is compared with the known answer. If they are not identical, the KAT test fails.
- Pair-wise consistency tests - The test is run when a RSA or ECDSA asymmetrical key pair is generated. The system uses the private key to sign the specific data, and then uses the public key to authenticate the signed data. If the authentication is successful, the test succeeds.
- Continuous random number generator tests - Runs when a random number is generated. The system compares the generated random number with the previously generated random number. If the two numbers are the same, the test fails.
- SP800-90B health tests
  - Repetition Count Test (RCT) – the goal of the Repetition Count Test is to quickly detect catastrophic failures that cause the noise source to become “stuck” on a single output value for a long period of time.
  - Adaptive Proportion Test (APT) – the Adaptive Proportion Test is designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source.

Additionally, the TOE performs a software integrity check using SHA2-256. The TOE calculates a SHA2-256 hash of the installed firmware and compares it with the known value to verify the software integrity during power-up.

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

Evaluator Findings:

The evaluator ensured that the TSS for FPT_TST_EXT.1 makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.

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

Upon investigation, the evaluator found that the TSS states that: in the event that a cryptographic self-test or the software integrity check fails, the TOE will create a log to indicate which self-test failed. These tests and the responses to failures are sufficient to ensure that the TSF is functioning in the manner that is described in the ST because they will detect unauthorized modified of the TOE software image and detect improperly functioning cryptography which could lead to insecure trusted channels.

For distributed TOEs the evaluator shall examine the TSS to ensure that it details which TOE component performs which self-tests and when these self-tests are run.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

Verdict:
PASS.

5.1.5.3.2 FPT_TST_EXT.1 AGD

The evaluator shall also ensure that the guidance documentation 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.

Evaluator Findings:
The evaluator also ensured that the guidance documentation section 7.2 **'Power-On Self Tests'** describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors correspond to those described in the TSS. The relevant information is found in the following section(s): 7.2 **'Power-On Self Tests'** Upon investigation, the evaluator found that the AGD states that: in the event that a POST fails, the TOE will create a log to indicate which self-test failed. The TOE will attempt to reboot to resolve the issue. If the TOE has been corrupted or the hardware has failed such that rebooting will not resolve the issue, an Administrator will need to contact Ciena support as per the guidance in Section 13 of the AGD. Section 13 states that Ciena provides technical support for its products if needed. Customers can register for a support account at http://my.ciena.com/CienaPortal/. Additionally, customers can open a ticket with Ciena support by calling +1 (800) 243-6224 (U.S. and Canada only). Please visit https://www.ciena.com/support/ for international phone numbers.

For distributed TOEs the evaluator shall ensure that the guidance documentation describes how to determine from an error message returned which TOE component has failed the self-test.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

Verdict:
PASS.

5.1.5.4 FPT_TUD_EXT.1 TRUSTED UPDATE

5.1.5.4.1 FPT_TUD_EXT.1 TSS

The evaluator shall verify that the TSS describes 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.

Evaluator Findings:
The evaluator verified that the TSS for FPT_TUD_EXT.1 describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS describes how and when the inactive version becomes active. The evaluator verified this description. The relevant information is found in the following section(s): TOE Summary Specification FPT_TUD_EXT.1. Upon investigation, the evaluator found that the TSS states that: the Security Administrator can query the currently executing version and most recently installed version using the following commands after authenticating to the TOE: • RTRV-RELEASE:::CTAG; • RTRV-SW-VER:::CTAG; The TOE supports delayed activation for trusted updates only when a valid update file is downloaded from the update server. The TOE performs a check on the image when it is fetched from the update server via SFTP. If the update file is an illegitimate image, the TOE will not load the image into flash memory and it will generate an error log. If the update file is legitimate, the administrator will have to commit the upgrade manually after a successful fetch of the image.

The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software).

Evaluator Findings:
The evaluator verified that the TSS describes all TSF software update mechanisms for updating the system firmware and software. The relevant information is found in the following section(s): TOE Summary Specification FPT_TUD_EXT.1. Upon investigation, the evaluator found that the TSS states that: The TOE provides the ability for a Security Administrator with UPC >=4 to update its software from the TL1 interface. The TOE, acting as the SSH client, will use SFTP via SSH to retrieve software updates from an update server. This can be a server maintained by Ciena or one maintained by the organization operating the TOE, in which case updates are shipped

on read-only physical media when made available by Ciena and then loaded onto the update server, which must support SFTP via SSH, in the Operational Environment. Updates are digitally signed and verified using ECDSA using the P-521 elliptic curve with SHA-384. Once the update has been loaded on the TOE, the digital signature of the software upgrade is verified. The upgrade process will stop if the digital signature verification fails and the downloaded software release will be flushed from the device's temporary memory. After successful digital signature validation, the Security Administrator must load the update into flash memory, by executing the LOAD-UPGRD command, where it remains until invoked. Invoking the update requires the Security Administrator to execute the INVK-UPGRD command to install the upgrade onto the shelf processor and then forces the TOE to reboot. The Security Administrator will then need to reauthenticate the TOE and commit the upgrade using the CMMT-UPGRD command.

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.

Evaluator Findings:

The evaluator verified 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 details this mechanism instead of the digital signature verification mechanism.

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

Upon investigation, the evaluator found that the TSS states that: the upgrade process will stop if the digital signature verification fails and the downloaded software release will be flushed from the device's temporary memory.

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.

Evaluator Findings:

The evaluator verified 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.

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

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

The TOE, acting as the SSH client, will use SFTP via SSH to retrieve software updates from an update server. This can be a server maintained by Ciena or one maintained by the organization operating the TOE, in which case updates are shipped on read-only physical media when made available by Ciena and then loaded onto the update server, which must support SFTP via SSH, in the Operational Environment.

Updates are digitally signed and verified using ECDSA using the P-521 elliptic curve with SHA-384. Once the update has been loaded on the TOE, the digital signature of the software upgrade is verified. The upgrade process will stop if the digital signature verification fails and the downloaded software release will be flushed from the device's temporary memory. After successful digital signature validation, the Security Administrator must load the update into flash memory, by executing the LOAD-UPGRD command, where it remains until invoked. Invoking the update requires the Security Administrator to execute the INVK-UPGRD command to install the upgrade onto the shelf processor and then forces the TOE to reboot. The Security Administrator will then need to reauthenticate to the TOE and commit the upgrade using the CMMT-UPGRD command.
Note: The update will not be completed if the digital verification fails

If the options 'support automatic checking for updates' or 'support automatic updates' are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.

Evaluator Findings:
The TOE does not make a claim for automatic updates.

For distributed TOEs, the evaluator shall examine the TSS to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component. Alternatively, this description can be provided in the guidance documentation. In that case the evaluator should examine the guidance documentation instead.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update

is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.

Evaluator Findings:
'Published hash' is not claimed but uses the TOE uses a 'digital signature' instead.

Verdict:
PASS.

5.1.5.4.2 FPT_TUD_EXT.1 AGD

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.

Evaluator Findings:
The evaluator verified that the guidance documentation section 9.13 **'Secure Updates** 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 describes how to query the loaded but inactive version. The relevant information is found in the following section(s): 9.13 **'Secure Updates'** Upon investigation, the evaluator found that the AGD states that: the administrator can query the currently executing version and most recently installed version. The instructions for querying the current version of the TOE is in step 2 listed in this section and reads as follows: "Execute the following commands to output the current running and most recently installed TOE software version: RTRV-RELEASE:::CTAG; RTRV-SW-VER:::CTAG;"

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.

Evaluator Findings:
The evaluator verified that the guidance documentation section 9.13 **'Secure Updates'** describes how the verification of the authenticity of the update is performed (digital signature verification). The description includes the procedures for successful and unsuccessful verification. The description corresponds to the description in the TSS. The relevant information is found in the following section(s): 9.13 **'Secure Updates'** Upon investigation, the evaluator found that the AGD states that: Updates are digitally signed and verified using ECDSA using the P-521 elliptic curve with SHA-512. Once the update has been uploaded to the TOE, the digital signature of the software upgrade is verified. If the digital signature verification fails, the upgrade process will stop and the downloaded software release will be flushed from the device's temporary memory. After successful digital signature validation, the Security Administrator must load the update into flash memory, by executing the LOADUPGRD command, where it remains until invoked. Invoking the update requires the Security Administrator to execute the INVK-UPGRD command to install the upgrade on the shelf processor resulting in the TOE rebooting. The Security Administrator will then need to reauthenticate to the TOE and commit the upgrade using the CMMT-UPGRD command. Step 9 in this section of the AGD requests that the admin repeat step 2 in order to verify that the update has been installed.

If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.

Evaluator Findings:
Published hash is not claimed.

For distributed TOEs the evaluator shall verify that the guidance documentation describes how the versions of individual TOE components are determined for FPT_TUD_EXT.1, how all TOE components are updated, and the error conditions that may arise from checking or applying the update (e.g. failure of signature verification, or exceeding available storage space) along with appropriate recovery actions. The guidance documentation only has to describe the procedures relevant for the Security Administrator; it does not need to give information about the internal communication that takes place when applying updates.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

If this was information was not provided in the TSS: For distributed TOEs, the evaluator shall examine the Guidance Documentation to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component.

Evaluator Findings:
The TOE is not a distributed TOE hence this assurance activity is not applicable.

If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.

Evaluator Findings:
The TOE does not use a certificate based mechanism for digital signature verification related to software updates.

Verdict:
PASS.

5.1.5.5 FPT_STM_EXT.1 RELIABLE TIME STAMPS

5.1.5.5.1 FPT_STM_EXT.1 TSS **[TD0632]**

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

Evaluator Findings:
The evaluator examined the TSS for FPT_STM_EXT.1 and ensured that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. The relevant information is found in the following section(s): TOE Summary Specification FPT_STM_EXT.1.

Upon investigation, the evaluator found that the TSS states that: the TOE provides source date and time information for use in audit timestamps, tracking administrator session inactivity for session termination, automatically unlocking an account after the administrator defined period of time, X.509 certificate expiry, and for determining when SSH rekeying should occur. The clock function is reliant on the system clock provided by the underlying hardware.
A Security Administrator with UPC >=4 has the ability to manually set the time.
Additionally, the administrator (UPC>=3)can configure the TOE to accept time from as many as three NTP servers, authenticated using SHA2-256.

If "obtain time from the underlying virtualization system" is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.

Evaluator Findings:
If "obtain time from the underlying virtualization system" is selected, the evaluator examined the TSS for FPT_STM_EXT.1 and ensured that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay. The relevant information is found in the following section(s): TOE Summary Specification FPT_STM_EXT.1. Upon investigation, the evaluator found that the TSS states that: The TOE does not rely on any underlying virtual system for time updates as the TOE is a standalone hardware product.

Verdict:
PASS.

5.1.5.5.2 FPT_STM_EXT.1 AGD **[TD0632]**

The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time.

Evaluator Findings:
The evaluator examined the guidance documentation 9.12 **'System Time Configuration',** 9.12.1 **'Setting System Time Manually'** and 9.12.2 **'Setting System Time via NTP'** and ensured that it instructs the administrator how to set the time.

The relevant information is found in the following section(s): 9.12 **'System Time Configuration',** 9.12.1 **'Setting System Time Manually'** and 9.12.2 **'Setting System Time via NTP'**

Upon investigation, the evaluator found that the AGD states that: The TOE has an underlying hardware clock that is used for time keeping. In the evaluated configuration of the TOE, the system time is expected to be manually set or automatically updated via NTP synchronization. The Security Administrator with UPC >=4 can configure all aspects of the clock using the local or remote TL1.
Section 9.12.1 titles '**Setting System Time Manually'** provides instructions for manually setting the system time by the admin.

Section 9.12.2 titled **'Setting System Time via NTP'** provides instructions for the admin to set the time from an NTP server.

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.

Evaluator Findings:

The evaluator examined the guidance documentation section 9.12.2 **'Setting System Time via NTP'** and ensured that it 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.

The relevant information is found in the following section(s): 9.12.2 **'Setting System Time via NTP'**

Upon investigation, the evaluator found that the AGD section 9.12.2 **'Setting System Time via NTP'** provides instruction for setting up NTPv4 authentication on the TOE using SHA256.

If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the guidance documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the guidance documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the guidance documentation informs the administrator of the maximum possible delay.

Evaluator Findings:
The TOE only acquires the time from manual configuration or from an NTP server. Please see other AGD activities for more detail on this functionality.

Verdict:
PASS.

5.1.6 TOE ACCESS (FTA)

5.1.6.1 FTA_SSL_EXT.1 TSF-INITIATED SESSION LOCKING

5.1.6.1.1 FTA_SSL_EXT.1 TSS

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.

Evaluator Findings:
The evaluator examined the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings. The relevant information is found in the following section(s): TOE Summary Specification FTA_SSL_EXT.1. Upon investigation, the evaluator found that the TSS states that: the Security Administrator with UPC >=4 can configure maximum inactivity times for both local and remote administrative sessions. The idle timeout value is set for each individual user account as opposed to being globally defined for all users. This is specified using the 'Timeout Interval' field when the user is created or modified using the TL1 interface. By default, a user account will be logged out if idle for 30 minutes, but the value can be set to anything between 1 and 99 minutes. When a local session is inactive for the configured period of time the TOE will terminate the session, requiring the Security Administrator to establish a new session, including authenticating to the TOE.

Verdict:
PASS.

5.1.6.1.2 FTA_SSL_EXT.1 AGD

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.

Evaluator Findings:
The evaluator confirmed that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. The relevant information is found in the following section(s): 9.11 **'Session Termination', 9.11.1 'Admin Logout'** and 9.11.2 **'Termination from Inactivity'** Upon investigation, the evaluator found that the AGD: breaks down the functionality for this requirement into two sections: section 9.11.1 **'Admin Logout'** the TOE provides the ability for administrators to manually terminate their own sessions. Both the TL1 interface and Site Manager use the CANC-USER command. These commands apply to both local and remote usage. Section 9.11.2 **'Termination from Inactivity'** states that a Security Administrator with UPC >=4 can configure maximum inactivity times for both local and remote administrative sessions. The idle timeout value is set for each individual user account as opposed to being globally defined for all users. This is specified using the 'Timeout Interval' field when the user is created or modified using the TL1 interface (TMOUT=XXX parameter). By default, a user account will be logged out if idle for 30 minutes, but the value can be set to anything between 1 and 99 minutes. This applies to both local and remote connections

Verdict:
PASS.

5.1.6.2 FTA_SSL.3 TSF-INITIATED TERMINATION

5.1.6.2.1 FTA_SSL.3 TSS

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

Evaluator Findings:
The evaluator examined the TSS and determined that it details the administrative remote session termination and the related inactivity time period.

The relevant information is found in the following section(s): TOE Summary Specification FTA_SSL.3.

Upon investigation, the evaluator found that the TSS states that: the Security Administrator with UPC >=4 can configure maximum inactivity times for both local and remote administrative sessions. The idle timeout value is set for each individual user account as opposed to being globally defined for all users. This is specified using the 'Timeout Interval' field when the user is created or modified using the TL1 interface. By default, a user account will be logged out if idle for 30 minutes, but the value can be set to anything between 1 and 99 minutes. The TOE will terminate a remote TL1 session after a Security Administrator-defined period of inactivity. Additionally, there is an inactivity timer for SSH with a default of 30 minutes.

Verdict:
PASS.

5.1.6.2.2 FTA_SSL.3 AGD

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

Evaluator Findings:

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

The relevant information is found in the following section(s): 9.11.2 **'Termination from Inactivity'**

Upon investigation, the evaluator found that the AGD states that: a Security Administrator with UPC >=4 can configure maximum inactivity times for both local and remote administrative sessions. The idle timeout value is set for each individual user account as opposed to being globally defined for all users. This is specified using the 'Timeout Interval' field when the user is created or modified using the TL1 interface (TMOUT=XXX parameter). By default, a user account will be logged out if idle for 30 minutes, but the value can be set to anything between 1 and 99 minutes. This applies to both local and remote connections.

Verdict:
PASS.

5.1.6.3 FTA_SSL.4 USER-INITIATED TERMINATION

5.1.6.3.1 FTA_SSL.4 TSS

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

Evaluator Findings:
The evaluator examined the TSS and determined that it details how the remote administrative session (and if applicable the local administrative session) are terminated. The relevant information is found in the following section(s): TOE Summary Specification FTA_SSL.4. Upon investigation, the evaluator found that the TSS states that: The TOE provides the ability for administrators to manually terminate their own sessions. Both the TL1 interface and Site Manager use the CANC-USER command. These commands apply to both local and remote usage. Additionally, when managing the TOE remotely, the terminal application used on the management workstation will terminate the SSH session if the application itself is closed.

Verdict:
PASS.

5.1.6.3.2 FTA_SSL.4 AGD

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

Evaluator Findings:
The evaluator confirmed that the guidance documentation states how to terminate a remote interactive session (and if applicable the local administrative session). The relevant information is found in the following section(s): 9.11.1 **'Admin Logout'** Upon investigation, the evaluator found that the AGD states that: The TOE provides the ability for administrators to manually terminate their own sessions. Both the TL1 interface and Site Manager use the CANC-USER command. These commands apply to both local and remote usage. Additionally, when managing the TOE remotely, the terminal application used on the management workstation will terminate the SSH session if the application itself is closed.

Verdict:
PASS.

5.1.6.4 FTA_TAB.1 DEFAULT TOE ACCESS BANNERS

5.1.6.4.1 FTA_TAB.1 TSS

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).

Evaluator Findings:
The evaluator checked the TSS and ensured that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The relevant information is found in the following section(s): TOE Summary Specification FTA_TAB.1. Upon investigation, the evaluator found that the TSS states that: the TOE displays a configurable warning banner on the local and remote interface prior to a user supplying their authentication credentials. Remote authentication requires the use of SSH. Local authentication requires the use of the RJ-45 craft ethernet port.

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).

Evaluator Findings:
The evaluator checked the TSS and ensured 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). The relevant information is found in the following section(s): TOE Summary Specification FTA_TAB.1.

Upon investigation, the evaluator found that the TSS states that: The TOE displays a configurable warning banner on the local and remote interface prior to a user supplying their authentication credentials. Remote authentication requires the use of SSH. Local authentication requires the use of the RJ-45 craft ethernet port. The warning banner is configured by a Security Administrator with a UPC >=4.

Verdict:
PASS.

5.1.6.4.2 FTA_TAB.1 AGD

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

Evaluator Findings:
The evaluator examined the guidance documentation and ensured that it describes how to configure the banner message. The relevant information is found in the following section(s): 9.10 **'Login Banner'** Upon investigation, the evaluator found that the AGD states that: the TOE displays a configurable warning banner on the local and remote console prior to a user supplying their authentication credentials. Remote authentication requires the use of SSH. The warning banner is configured by a Security Administrator with a UPC >=4. Configuring instructions for the banners are available in this section using either the TL1 command or the Site Manager.

Verdict:
PASS.

5.1.7 TRUSTED PATH (FTP)

5.1.7.1 FTP_ITC.1 INTER-TSF TRUSTED CHANNEL

5.1.7.1.1 FTP_ITC.1 TSS

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.

Evaluator Findings:

The evaluator examined the TSS and determined 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.

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

Upon investigation, the evaluator found that the TSS states that: the TOE provides the ability to secure sensitive data in transit to and from the Operational Environment. In the evaluated configuration, the TOE, acting as the TLS client, pushes audit data periodically to a remote audit server. The identity of the audit server is verified by checking the administrator-configured reference identifier. Additionally, the TOE, acting as an SSH client, retrieves software updates via the update server using SFTP protected by SSH.

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.

Evaluator Findings:

The evaluator also confirmed 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.

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

Upon investigation, the evaluator found that the TSS states that: In the evaluated configuration, the TOE, acting as the TLS client, pushes audit data periodically to a remote audit server. The identity of the audit server is verified by checking the administrator-configured reference identifier. Additionally, the TOE, acting as an SSH client, retrieves software updates via the update server using SFTP protected by SSH. The table below shows the usage of these protocols and which SFR they map to:

Protocol	Usage
SSH	FCS_SSHC_EXT.1

	TLS	FCS_TLSC_EXT.1 FIA_X509_EXT.1

The TOE relies on the CAVP-validated cryptographic algorithm implementation used to establish these trusted channels.

Verdict:
PASS.

5.1.7.1.2 FTP_ITC.1 AGD

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.

Evaluator Findings:

The evaluator confirmed that the AGD 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 relevant information is found in the following section(s): **9.2.4 'Configuring SSH Server and Client Parameter', 9.2.5 'SSH/SFTP Server & Client (System) RSA Keys',** 10.2 **'TLS',** 11.1 **'Syslog Server Configuration'** and **9.13 'Secure Updates'**

Upon investigation, the evaluator found that the AGD states that: There are no special actions required in the event of a communications outage.

In section 9.2.4 **'Configuring SSH Server and Client Parameter'** and 9.13 **'Secure Updates'** of the AGD provides instructions on connection to the SFTP server for update files.

In section 9.2.5 **'SSH/SFTP Server & Client (System) RSA Keys'** states that there are no special actions required in the event of a communications outage. If the SSH/SFTP connection for the update server is broken, simply re-establish the SSH connection while logged in as the security administrator.

In section 10.2 **'TLS'** of the AGD, in the case of a TLS connection being broken the TOE will automatically attempt to re-establish an unintentionally disrupted channel to the remote Syslog server indefinitely. During this time, audit messages continue to be stored locally on the

TOE. Once the disruption has been corrected, the syslog client on the TOE will automatically attempt to re-negotiate the TLS channel upon the next retry.

In section 11.1 **'Syslog Server Configuration'** the AGD provides configuration instructions for connection to the syslog via TLS for remote syslog use.

Verdict:
PASS.

5.1.7.2 FTP_TRP.1/ADMIN TRUSTED PATH

5.1.7.2.1 FTP_TRP.1/ADMIN TSS

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

Evaluator Findings:
The evaluator examined the TSS and determined that the methods of remote TOE administration are indicated, along with how those communications are protected. The relevant information is found in the following section(s): TOE Summary Specification FTP_TRP.1/Admin. Upon investigation, the evaluator found that the TSS states that: all remote administrative communications, regardless of which logical interface they originate from, take place over a secure encrypted SSHv2 session. For these secure connections the TOE acts as a SSH server and is compliant with FCS_SSHS_EXT.1. The TOE relies on the CAVP-validated cryptographic algorithm implementation used to establish these trusted channels.

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.

Evaluator Findings:
The evaluator also 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 relevant information is found in the following section(s): TOE Summary Specification FTP_TRP.1/Admin.

Upon investigation, the evaluator found that the TSS states that: All remote administrative communications, regardless of which logical interface they originate from, take place over a secure encrypted SSHv2 session. For these secure connections the TOE acts as a SSH server and is compliant with FCS_SSHS_EXT.1.

Verdict:
PASS.

5.1.7.2.2 FTP_TRP.1/ADMIN AGD

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

Evaluator Findings:

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

The relevant information is found in the following section(s): 9.1 **'Authenticating to the TOE via SSH'**

Upon investigation, the evaluator found that the AGD provides the following steps for establishing a remote administrative session:

1. Authenticate the TOE via SSH using the Site Manager client on machine.
2. Specify the IP address of the TOE.
3. Authenticate using the default credentials (case sensitive):

Username: ADMIN
Password: ADMIN

Note: per instructions in section 7.1 of the AGD, the admin is expected to change the default password, so the default password is expected to be changed when creating the admin account.

Verdict:
PASS.

5.2 OPTIONAL REQUIREMENTS

No optional requirements claimed.

5.3 SELECTION-BASED REQUIREMENTS

5.3.1 CRYPTOGRAPHIC SUPPORT (FCS)

5.3.1.1 FCS_NTP_EXT.1 NTP PROTOCOL

5.3.1.1.1 FCS_NTP_EXT.1.1 TSS

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.

Evaluator Findings:
The evaluator examined 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. The relevant information is found in the following section(s): TOE Summary Specification FCS_NTP_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE implements NTP version 4, in accordance with RFC 5905. The TOE verifies that the received timestamp is from an authenticated time server by using SHA2-256 as the authentication algorithm.

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.

Evaluator Findings:
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. The relevant information is found in the following section(s): TOE Summary Specification FCS_NTP_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE implements NTP version 4. The TOE verifies that the received timestamp is from an authenticated time server by using SHA2-256 as the authentication algorithm.

Verdict:
PASS.

5.3.1.1.2 FCS_NTP_EXT.1.1 AGD

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.

Evaluator Findings:
The evaluator examined the AGD 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. The relevant information is found in the following section(s): 9.12.2 **'Setting System Time via NTP'** Upon investigation, the evaluator found that the AGD states that: instructions are present to set the system clock using the specified NTP server. This is a one-time operation and does not cause the clock to be kept in sync on an ongoing basis. If authentication key is present, then request will be sent with authentication parameters (key number, keys file), by default authentication is disabled.

Verdict:
PASS.

5.3.1.1.3 FCS_NTP_EXT.1.2 AGD

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.

Assurance Activity Note:
Each primary selection in the SFR contains selections that specify a cryptographic algorithm or cryptographic protocol. For each of these secondary selections made in the ST, the evaluator shall examine the guidance documentation to ensure that the documentation instructs the Security Administrator how to configure the TOE to use the chosen option(s).

Evaluator Findings:
The evaluator examined the AGD and ensured that, for each of the secondary selections made in the ST, 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. The relevant information is found in the following section(s): 9.12.2 **'Setting System Time via NTP'** Upon investigation, the evaluator found that the AGD states that: the TOE polls the server at 60 minute intervals and is kept in sync on an ongoing basis. If authentication key is present, then request will be sent with authentication parameters (key number, keys file). Steps to configure the TOE are present in this section. Step 3 specifically addresses adding authentication keys which is used to verify authenticity of the timestamps.

Verdict:
PASS.

5.3.1.1.4 FCS_NTP_EXT.1.3 AGD

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.

Evaluator Findings:
The evaluator examined the AGD 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. The relevant information is found in the following section(s):9.12.2 '**Setting System Time via NTP** '

Upon investigation, the evaluator found that the AGD notes in section 9.12.2 that the NTP implementation does not accept broadcast or multicast NTP packets in the TOE. No configuration is required.

Verdict:
PASS.

5.3.1.2 FCS_SSHC_EXT.1.1 SSH CLIENT

5.3.1.2.1 FCS_SSHC_EXT.1.2 TSS **[TD0636]**

The evaluator shall check to ensure that the TSS contains a list of the public key algorithms that are acceptable for use for user authentication and that this list is consistent with asymmetric key generation algorithms selected in FCS_CKM.1, hashing algorithms selected in FCS_COP.1/Hash, and signature generation algorithms selected in FCS_COP.1/SigGen.

Evaluator Findings:

The evaluator checked and ensured that the TSS contains a list of the public key algorithms that are acceptable for use for user authentication and that this list is consistent with asymmetric key generation algorithms selected in FCS_CKM.1, hashing algorithms selected in FCS_COP.1/Hash, and signature generation algorithms selected in FCS_COP.1/SigGen.

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

Upon investigation, the evaluator found that the TSS states that: the TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms which conforms to selections made in FCS_SSHC_EXT.1.5. When acting as an SSH client, the TOE supports using either public key or password-based authentication.

The TSS section for FCS_COP.1/Hash states that the TOE provides SHA2-256 and SHA2-512 hashing services, offering 256 or 512 bit output MAC sizes, in support of SSH services. This is consistent with sizes claimed in FCS_SSHC_EXT.1.

The TSS section for FCS_COP.1/SigGen states that The TOE provides RSA and ECDSA signature generation and verification. RSA keys are 2048,

while ECDSA keys are 256, 384, or 521 bits. P-256 and P-384 are used for TLS protocols whereas sizes P-256 and P-512 are used for SSH protocols.

It is important to note that while 384 bit is claimed in FCS_COP.1/Hash and FCS_COP.1/SigGen, that size is limited to TLS and not SSH.

The evaluator shall confirm the TSS is unambiguous in declaring the TOE's ability to authenticate itself to a remote endpoint with a user-based public key.

Evaluator Findings:

The evaluator confirmed the TSS is unambiguous in declaring the TOE's ability to authenticate itself to a remote endpoint with a user-based public key.

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

Upon investigation, the evaluator found that the TSS states that: When acting as an SSH client, the TOE supports using either public key or password-based authentication.

If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then the evaluator shall confirm it is also described in the TSS.

Evaluator Findings:

The evaluator confirmed password-based authentication is also described in the TSS.

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

Upon investigation, the evaluator found that the TSS states that the TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms which conforms to selections made in FCS_SSHC_EXT.1.5. When acting as an SSH client, the TOE supports using either public key or password-based authentication.

Verdict:
PASS.

5.3.1.2.2 FCS_SSHC_EXT.1.3 TSS

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

Evaluator Findings:
The evaluator checked that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that: The TOE drops packets larger than 32,768 bytes meeting the requirements of RFC 4253.

Verdict:
PASS.

5.3.1.2.3 FCS_SSHC_EXT.1.4 TSS

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.

Evaluator Findings:
The evaluator checked the description of the implementation of this protocol in the TSS and ensured that optional characteristics are specified, and the encryption algorithms supported are specified as well. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1.

Upon investigation, the evaluator found that the TSS states that: the TOE implementation of SSHv2 supports AES-128-CBC, AES-256-CBC, AES-128-CTR and AES-256-CTR for its transport algorithms.

These algorithms are consistent with selections made in the SFR. No additional optional characteristics are claimed and as the TOE is not distributed there are no additional components that need listing.

The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.

Evaluator Findings:

The evaluator checked the TSS and ensured that the encryption algorithms specified are identical to those listed for this component.

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

Upon investigation, the evaluator has checked the claims made in the TSS for this requirement and has checked it against the claims made in the SFR and has determined the encryption algorithms to be consistent in both locations of the Security Target.

Verdict:
PASS.

5.3.1.2.4 FCS_SSHC_EXT.1.5 TSS **[TD0636]**

The evaluator shall confirm the TSS describes how a host-key public key (i.e., SSH server's public key) is associated with the server identity.

Evaluator Findings:

The evaluator confirmed the TSS describes how a host-key public key (i.e., SSH server's public key) is associated with the server identity.

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

Upon investigation, the evaluator found that the TSS states that: The TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms (and has an associated identity).

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the host-key public key algorithms supported by the TOE are specified as well.

Evaluator Findings:
The evaluator checked the description of the implementation of this protocol in the TSS and ensured that optional characteristics are specified, and the host-key public key algorithms supported by the TOE are specified as well. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that: These algorithms are consistent with selections made in the SFR. No additional optional characteristics are claimed.

The evaluator shall check the TSS to ensure that the host-key public key algorithms specified are identical to those listed for this component.

Evaluator Findings:
The evaluator checked the TSS and ensured that the host-key public key algorithms specified are identical to those listed for this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that: These algorithms are consistent with selections made in the SFR. No additional optional characteristics are claimed.

If x509v3-based public key authentication algorithms are claimed, the evaluator shall confirm that the TSS includes the description of how the TOE establishes the server's identity and how this identity is confirmed with the one that is presented in the provided certificate. For example, the TOE could verify that a server's configured IP address matches the one presented in the server's x.509v3 certificate.

Evaluator Findings:
If x509v3-based public key authentication algorithms are claimed, the evaluator confirmed that the TSS includes the description of how the TOE establishes the server's identity and how this identity is confirmed with the one that is presented in the provided certificate. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that: X509 selection was not made for this SFR. The TOE uses rsa-sha2-256 and rsa-sha2-512 as its public key algorithms.

Verdict:
PASS.

5.3.1.2.5 FCS_SSHC_EXT.1.6 TSS

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

Evaluator Findings:
The evaluator checked the TSS and ensured that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that data integrity is assured using HMAC-SHA2-256. This corresponds with the selected claim.

Verdict:
PASS.

5.3.1.2.6 FCS_SSHC_EXT.1.7 TSS

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

Evaluator Findings:
The evaluator checked the TSS and ensured that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE uses ECDH-SHA2-NISTp256 or ECDH-SHA2-NISTp384 as the key exchange algorithms. This corresponds with the selections made for this SFR.

Verdict:
PASS.

5.3.1.2.7 FCS_SSHC_EXT.1.8 TSS

The evaluator shall check that the TSS specifies the following:

a. Both thresholds are checked by the TOE.
b. Rekeying is performed upon reaching the threshold that is hit first.

Evaluator Findings:
The evaluator checked that the TSS specifies the following: a. Both thresholds are checked by the TOE. b. Rekeying is performed upon reaching the threshold that is hit first. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHC_EXT.1. Upon investigation, the evaluator found that the TSS states that: the SSH connection will rekey before 1 hour has elapsed or 500 MB of data has been transmitted using that key, whichever occurs first.

Verdict:
PASS.

5.3.1.2.8 FCS_SSHC_EXT.1.2 AGD **[TD0636]**

The evaluator shall check the guidance documentation to ensure that it contains instructions to the administrator on how to ensure that only the allowed mechanisms are used in SSH connections initiated by the TOE.

Evaluator Findings:
The evaluator checked the AGD to ensure that it contains instructions to the administrator on how to ensure that only the allowed mechanisms are used in SSH connections initiated by the TOE. The relevant information is found in the following section(s): 10.1 **'SSH'**

Upon investigation, the evaluator found that the AGD states that: No configuration is required other than enabling CC-NDcPP compliance in accordance with section 8 and section 9.2, no other configurations or mechanisms are able to be used.

Verdict:
PASS.

5.3.1.2.9 FCS_SSHC_EXT.1.4 AGD

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).

Evaluator Findings:
The evaluator also checked the AGD and ensured 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). The relevant information is found in the following section(s): 9.2.4 **'Configuring SSH Server and Client Parameters'** Upon investigation, the evaluator found that the AGD states that: If the SSH Server is set to perform Public Key based authentication, at least one SSH/SFTP Users (authorized user) entry must be configured. Similarly, if the SSH Client is set to perform host validation, at least one SSH/SFTP Hosts (known host) entry must be configured. Instructions for configuring the SSH client parameters is also included in section 9.2.4.

Verdict:
PASS.

5.3.1.2.10 FCS_SSHC_EXT.1.5 AGD

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).

Evaluator Findings:
The evaluator also checked the AGD 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).

The relevant information is found in the following section(s): 9.2.4 titled **'Configuring SSH Server and Client Parameters'** and section 10.1 **'SSH'**

Upon investigation, the evaluator found that the AGD provides detailed instructions on configuring the settings of the SSH server and client. No configuration is required other than enabling CC-NDcPP compliance in accordance with section 8 and section 9.2.4. The TOE implements SSHv2 that complies with the following RFCs: 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308 Section 3.1, and 8332. The TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms, and ECDH-SHA2-NISTp256 or ECDH-SHA2-NISTp384 as the key exchange algorithms.

Verdict:
PASS.

5.3.1.2.11 FCS_SSHC_EXT.1.6 AGD

The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security 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).

Evaluator Findings:

The evaluator also checked the AGD and ensured that it contains instructions to the Security 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).

The relevant information is found in the following section(s): 9.1 titled **'Authenticating to the TOE via SSH'** and 10.1 **'SSH'**

Upon investigation, the evaluator found that the AGD states that: the only MAC algorithms allowed is hmac-sha2-256 and all other MAC algorithms are rejected and "none" is not allowed.

Further, section 10.1 titled 'SSH" notes that no configuration is required other than enabling CC-NDcPP compliance.

Verdict:
PASS.

5.3.1.2.12 FCS_SSHC_EXT.1.7 AGD

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

Evaluator Findings:
The evaluator also checked the AGD and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. The relevant information is found in the following section(s): 10.1 **'SSH'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDcPP compliance mode. Instructions for enabling CC-NDcPP compliance mode can be referenced in section 8 of the AGD titled **'Enabling CC-NDcPP Compliance'**.

Verdict:
PASS.

5.3.1.2.13 FCS_SSHC_EXT.1.8 AGD

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.

Evaluator Findings:
If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator checked that the AGD describes how to configure those thresholds. Either the allowed values are specified in the AGD 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 relevant information is found in the following section(s): 10.1 **'SSH'** Upon investigation, the evaluator found that the AGD states that: the SSH connection will rekey before 1 hour has elapsed or 500 MB of data has been transmitted using that key, whichever occurs first. No other thresholds are claimed.

The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.

Evaluator Findings:
The evaluator checked that the AGD describes that the TOE reacts to the first threshold reached. The relevant information is found in the following section(s): 10.1 **'SSH'** Upon investigation, the evaluator found that the AGD states that: the SSH connection will rekey before 1 hour has elapsed or 500 MB of data has been transmitted using that key, whichever occurs first.

Verdict:
PASS.

5.3.1.3 FCS_SSHS_EXT.1. SSH SERVER

5.3.1.3.1 FCS_SSHS_EXT.1.2 TSS **[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).

Evaluator Findings:
The evaluator checked and ensured 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 relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms. This is consistent with the 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.

Evaluator Findings:
The evaluator confirmed 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. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: Once the public key is verified the admin can login.

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.

Evaluator Findings:
If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator confirmed its role in the authentication process is described in the TSS. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: when the TOE acts as an SSH server, only public key authentication is supported. The TOE SSH server functionality is for remote administrative connections over SSHv2. The TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms.

Verdict:
PASS.

5.3.1.3.2 FCS_SSHS_EXT.1.3 TSS

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

Evaluator Findings:
The evaluator checked that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE drops packets larger than 32,768 bytes meeting the requirements of RFC 4253.

Verdict:
PASS.

5.3.1.3.3 FCS_SSHS_EXT.1.4 TSS

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.

Evaluator Findings:
The evaluator checked the description of the implementation of this protocol in the TSS and ensured that optional characteristics are specified, and the encryption algorithms supported are specified as well. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE implementation of SSHv2 supports AES-128-CBC, AES-256-CBC, AES-128-CTR and AES-256-CTR for its encryption algorithms.

The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.

Evaluator Findings:
The evaluator checked the TSS and ensured that the encryption algorithms specified are identical to those listed for this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1.

Upon investigation, the evaluator found that the TSS states that: the TOE implementation of SSHv2 supports AES-128-CBC, AES-256-CBC, AES-128-CTR and AES-256-CTR for its algorithms. These are identical to the claims made for this component.

Verdict:
PASS.

5.3.1.3.4 FCS_SSHS_EXT.1.5 TSS **[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.

Evaluator Findings:
The evaluator checked the description of the implementation of this protocol in the TSS and ensured that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: The TOE implementation of SSHv2 only supports RSA-SHA2-256 or RSA-SHA2-512 as its public key algorithms. These algorithms are identical to those selected for in the SFR for this component.

Verdict:
PASS.

5.3.1.3.5 FCS_SSHS_EXT.1.6 TSS

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

Evaluator Findings:
The evaluator checked the TSS and ensured that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1.

Upon investigation, the evaluator found that the TSS states that: data integrity is assured using HMAC-SHA2-256. This is identical to claims made in the SFR and no other sizes have been selected for. These algorithms are identical to those selected for in the SFR for this component.

Verdict:
PASS.

5.3.1.3.6 FCS_SSHS_EXT.1.7 TSS

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

Evaluator Findings:
The evaluator checked the TSS and ensured that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_SSHS_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE uses ECDH-SHA2-NISTp256 or ECDH-SHA2-NISTp384 as the key exchange algorithms. These are consistent with claims made in the SFR for this component.

Verdict:
PASS.

5.3.1.3.7 FCS_SSHS_EXT.1.8 TSS

The evaluator shall check that the TSS specifies the following:

a. Both thresholds are checked by the TOE.
b. Rekeying is performed upon reaching the threshold that is hit first.

Evaluator Findings:
The evaluator checked that the TSS specifies the following: a. Both thresholds are checked by the TOE. b. Rekeying is performed upon reaching the threshold that is hit first.

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

Upon investigation, the evaluator found that the TSS states that: the SSH connection will rekey before 1 hour has elapsed or 500 MB of data has been transmitted using that key, whichever occurs first.

Verdict:
PASS.

5.3.1.3.8 FCS_SSHS_EXT.1.4 AGD

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).

Evaluator Findings:

The evaluator also checked the AGD and ensured 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).

The relevant information is found in the following section(s): 10.1 **'SSH' and 8 'Enabling CC-NDcPP Compliance'**

Upon investigation, the evaluator found that the AGD states that: The TOE SSH server functionality is for remote administrative connections over SSHv2. When the TOE acts as an SSH server, only public key authentication is supported. No configuration is required other than enabling CC-NDcPP compliance.
Instructions for enabling CC-NDcPP compliance mode can be referenced in section 8 of the AGD titled **'Enabling CC-NDcPP Compliance'**.

Verdict:
PASS.

5.3.1.3.9 FCS_SSHS_EXT.1.5 AGD

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).

Evaluator Findings:
The evaluator also checked the AGD and ensured 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). The relevant information is found in the following section(s): 10.1 **'SSH' and 8 'Enabling CC-NDcPP'** Upon investigation, the evaluator found that the AGD states that: No configuration is required other than enabling CC-NDcPP compliance. The claims are detailed in this section of the AGD and the specified implementations have been checked against the claims in the ST to assure consistency. Instructions for enabling CC-NDcPP compliance mode can be referenced in section 8 of the AGD titled **'Enabling CC-NDcPP Compliance'**.

Verdict:
PASS.

5.3.1.3.10 FCS_SSHS_EXT.1.6 AGD

The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security 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).

Evaluator Findings:
The evaluator also checked the AGD and ensured that and ensured that it contains instructions to the Security 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). The relevant information is found in the following section(s): 10 **'SSH'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDcPP compliance mode. Instructions for enabling CC-NDcPP compliance mode can be referenced in section 8 of the AGD titled **'Enabling CC-NDcPP Compliance'**.

Verdict:
PASS.

5.3.1.3.11 FCS_SSHS_EXT.1.7 AGD

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

Evaluator Findings:
The evaluator also checked the AGD and ensured that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. The relevant information is found in the following section(s): 10.1 **'SSH',** 8 **'Enabling CC-NDcPP Compliance'** and section 9.1 **'Authentication to the TOE via SHH'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDcPP compliance mode. Instructions for enabling CC-NDcPP compliance mode can be referenced in section 8 of the AGD titled **'Enabling CC-NDcPP Compliance'**. Section 9.1 titled 'Authenticating to the TOE via SSH' states that the only key exchange methods supported are ecdh-sha2-nistp256 or ecdh-sha2-nistp384.

Verdict:
PASS.

5.3.1.3.12 FCS_SSHS_EXT.1.8 AGD

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.

Evaluator Findings:
If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator checked that the AGD describes how to configure those thresholds. Either the allowed values are specified in the AGD 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 relevant information is found in the following section(s): 10.1 **'SSH',** 8 **'Enabling CC-NDcPP Compliance'** and section 9.2 **'Generating, Configuring and Uploading SSH Public/Private key on TOE'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDcPP compliance in accordance with section 8 and section 9.2 of the AGD.

The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.

Evaluator Findings:
The evaluator checked that the AGD describes that the TOE reacts to the first threshold reached. The relevant information is found in the following section(s): 10.1 **'SSH'** Upon investigation, the evaluator found that the AGD states that: The SSH connection will rekey before 1 hour has elapsed or 500 MB of data has been transmitted using that key, whichever occurs first. The TOE authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key as specified in RFC 4251 Section 4.1.

Verdict:
PASS.

5.3.1.4 FCS_TLSC_EXT.1 EXTENDED: TLS CLIENT PROTOCOL WITHOUT MUTUAL AUTHENTICATION

5.3.1.4.1 FCS_TLSC_EXT.1.1 TSS

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

Evaluator Findings:
The evaluator checked the description of the implementation of this protocol in the TSS and ensured that the ciphersuites supported are specified. The relevant information is found in the following section(s): TOE Summary Specification FCS_TLSC_EXT.1. Upon investigation, the evaluator found that the TSS states that: the TOE supports the following ciphersuites: • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.

Evaluator Findings:
The evaluator checked the TSS and ensured that the ciphersuites specified include those listed for this component. The relevant information is found in the following section(s): TOE Summary Specification FCS_TLSC_EXT.1. Upon investigation, the evaluator has compared the list of the ciphersuites in the TSS to the list selected for in the SFR for this requirement and have found them to be consistent for this component.

Verdict:
PASS.

5.3.1.4.2 FCS_TLSC_EXT.1.2 TSS

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.

Evaluator Findings:
The evaluator ensured 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. The relevant information is found in the following section(s): TOE Summary Specification FCS_TLSC_EXT.1. Upon investigation, the evaluator found that the TSS states that: The TOE uses administrator-configured reference identifiers according to RFC 6125 section 6, as well as IPv4 Address in CN or SAN, IPv6 Address in CN or SAN. Wildcards are supported.

Note that where a TLS channel is being used between components of a distributed TOE for FPT_ITT.1, the requirements to have the reference identifier established by the user are relaxed and the identifier may also be established through a "Gatekeeper" discovery process. The TSS should describe the discovery process and highlight how the reference identifier is supplied to the "joining" component. Where the secure channel is being used between components of a distributed TOE for FPT_ITT.1 and the ST author selected attributes from RFC 5280, the evaluator shall ensure the TSS describes which attribute type, or combination of attribute types, are used by the client to match the presented identifier with the configured identifier. The evaluator shall ensure the TSS presents an argument how the attribute type, or combination of attribute types, uniquely identify the remote TOE component; and the evaluator shall verify the attribute type, or combination of attribute types, is sufficient to support unique identification of the maximum supported number of TOE components.

Evaluator Findings:
Upon investigation, the evaluator found that the TOE is not distributed and this activity is considered complete.

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.

Evaluator Findings:
If IP addresses are supported in the CN as reference identifiers, the evaluator ensured 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 relevant information is found in the following section(s): TOE Summary Specification FCS_TLSC_EXT.1. Upon investigation, the evaluator found that the TSS states that: IP addresses are converted to binary in network byte order using standard decimal-to-binary encoding, which is then encoded in hex according to the canonical format defined in RFC 3986 and RFC 5952.

The evaluator shall also ensure that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced.

Evaluator Findings:
The evaluator also ensured that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced. The relevant information is found in the following section(s): TOE Summary Specification FCS_TLSC_EXT.1. Upon investigation, the evaluator found that the TSS states that: IP addresses are converted to binary in network byte order using standard decimal-to-binary encoding, which is then encoded in hex according to the canonical format defined in RFC 3986 and RFC 5952.

Verdict:
PASS.

5.3.1.4.3 FCS_TLSC_EXT.1.4 TSS

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

Evaluator Findings:
The evaluator verified that TSS describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behaviour is performed by default or may be configured. The relevant information is found in the following section(s): TOE Summary Specification FCS_TLSC_EXT.1.

Upon investigation, the evaluator found that the TSS states that: the supported Elliptic Curve groups/extensions are supported by default and require no additional configuration.

Verdict:
PASS.

5.3.1.4.4 FCS_TLSC_EXT.1.1 AGD

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.

Evaluator Findings:
The evaluator checked the AGD and ensured that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. The relevant information is found in the following section(s): 10.2 **'TLS'** and 8 **'Enabling CC-NDcPP Compliance'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDcPP compliance mode. Instructions for enabling CC-NDcPP compliance mode can be referenced in section 8 of the AGD titled **'Enabling CC-NDcPP Compliance'**.

Verdict:
PASS.

5.3.1.4.5 FCS_TLSC_EXT.1.2 AGD

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.

Evaluator Findings:
The evaluator ensured that the AGD 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). The evaluator ensured that

the AGD provides a set of warnings and/or CA policy recommendations that would result in secure TOE use when the identifier scheme implemented by the TOE includes support for IP addresses.

The relevant information is found in the following section(s): 10.2.1 **'Reference Identifiers'**

Upon investigation, the evaluator found that the AGD states that: it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s), and provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. Upon investigation, the evaluator found that the AGD states that the reference identifier for the syslog server is configured by the administrator using the available administrative commands in the CLI.

Note: The reference identifiers must be an IPv4 address, IPv6 address, or a hostname.

When the reference identifier is a hostname, the TOE compares the hostname against all the DNS Name entries in the Subject Alternative Name extension (SAN). If the hostname does not match any of the DNS Name entries, then the verification fails. If the certificate does not contain any DNS entries, the TSF will compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both dNSName and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.

When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary, IPv6 addresses are converted as specified in RFC 5952. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. The TLS channel is terminated if verification fails.

Where the secure channel is being used between components of a distributed TOE for FPT_ITT.1, the SFR selects attributes from RFC 5280, and FCO_CPC_EXT.1.2 selects "no channel"; the evaluator shall verify the AGD provides instructions for establishing unique reference identifiers based on RFC5280 attributes.

Evaluator Findings:
The evaluator examined Security Target. The TOE is not claimed as a distributed TOE. No additional AGD information required.

Verdict:
PASS.

5.3.1.4.6 FCS_TLSC_EXT.1.4 AGD

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

Evaluator Findings:
The evaluator verified that the AGD includes configuration of the Supported Elliptic Curves/Supported Groups Extension. The relevant information is found in the following section(s): 10.2 **'TLS'** and 8 **'Enabling CC-NDcPP Compliance'** Upon investigation, the evaluator found that the AGD states that: no configuration is required other than enabling CC-NDcPP compliance mode. Section 8 of the AGD titled "Configuring CC-NDcPP Compliance provides instructions for enabling this mode. The syslog TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve ciphersuites no additional configuration is required. The TOE also supports key agreement using the server's RSA public key.

Verdict:
PASS.

5.3.2 IDENTIFICATION AND AUTHENTICATION (FIA)

5.3.2.1 FIA_X509_EXT.1/REV X.509 CERTIFICATE VALIDATION

5.3.2.1.1 FIA_X509_EXT.1/REV TSS

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 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).

Evaluator Findings:

The evaluator ensured 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).

The relevant information is found in the following section(s): TOE Summary Specification FIA_X509_EXT.1/Rev.

Upon investigation, the evaluator found that the TSS states that: Because the TOE is only a TLS client, the TOE performs certificate validation when RootCA and IntermediaryCA certificates are first installed on the TOE for its own use in validating trust chains, and when peer certificates are presented to the TOE during authentication steps. The TOE does not have or present a certificate of its own.
Certificates are validated to ensure that they have the correct basicConstraints for the certificate type, and that all presented certificates terminate in a root of Trust. The peer certificate gets checked for SAN and CN while the validating CA certificate uses basicConstraints checking. Validation includes:

- That the presented certificates terminate in a root of trust. If the peer does not present its entire trust chain, the TOE will use its installed CA certificates to validate the peer. If the peer's identity does not match the configured reference identifier set by the administrator, the connection is refused.
- That the current date and time lies between the validity dates for all certificates in the trust chain.
- That the basicConstraints extension is included, with the CA flag set to "TRUE", for all CA certificates in the chain of trust
- That the extendedKeyUsage field in the peer's certificate has the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1)
- That the digital signatures are correct for all certificates, and there has been no loss in transit
- That none of the certificates in the trust chain are revoked.

Certificate revocation checking is performed using the OCSP as specified in RFC 6960; if the TOE cannot reach the revocation server, the TOE will reject the certificate and deny the connection.

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.

Evaluator Findings:
The TSS describes when revocation checking is performed and on what certificates. Any differences where revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented is summarized in the TSS section and explained in the Guidance. The relevant information is found in the following section(s): TOE Summary Specification FIA_X509_EXT.1/Rev. Upon investigation, the evaluator found that the TSS states that: certificate revocation checking is performed using the OCSP as specified in RFC 6960. The certificate is checked on each TLS client connection and if the TOE cannot reach the revocation server then the TOE will reject the certificate and deny the connection.

Verdict:
PASS.

5.3.2.1.2 FIA_X509_EXT.1/REV AGD

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.

Evaluator Findings:
The evaluator also ensured that the AGD 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. The relevant information is found in the following section(s): 9.5 **'X.509 Certificate'**

Upon investigation, the evaluator found that the AGD states that: The TOE performs X.509 certificate validation at the following points:
•The certification path must terminate with a trusted CA certificate designated as a trust anchor.
•The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
•The TSF shall validate the revocation status of the certificate using [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
The TOE validates certificates in accordance with the following rules:

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

Certificate revocation checking is performed on the leaf and intermediate CA certificates using OCSP responders as part of the authentication step. There is no difference in handling of revocation checking during authentication irrespective of whether a full certificate chain or only a leaf certificate is being presented. The OCSP signing certificate must have the OCSP signing purpose in the extendedKeyUsage extension.

Verdict:
PASS.

5.3.2.2 FIA_X509_EXT.2 X.509 CERTIFICATE AUTHENTICATION

5.3.2.2.1 FIA_X509_EXT.2 TSS

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.

Evaluator Findings:
The evaluator checked the TSS and ensured that it describes how the TOE chooses which certificates to use, and any necessary instructions in the AGD for configuring the operating environment so that the TOE can use the certificates. The relevant information is found in the following section(s): TOE Summary Specification FIA_X509_EXT.2. Upon investigation, the evaluator found that the TSS states that: X.509v3 certificates are only used for TLS, in which the TOE acts as a client. The TOE has no certificates of its own, except certificates installed to validate peers.

The evaluator shall examine the TSS and confirmed 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.

Evaluator Findings:
The evaluator examined the TSS and confirmed 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 relevant information is found in the following section(s): TOE Summary Specification FIA_X509_EXT.2. Upon investigation, the evaluator found that the TSS states that: when a connection to the OCSP server cannot be established, the TOE will reject the presented certificate and deny the connection.

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 AGD contains instructions on how this configuration action is performed.

Evaluator Findings:
The evaluator verified that any distinctions between trusted channels are described. The evaluator ensured that the guidance documentation contains instructions on how the administrator is able to specify the default action. The relevant information is found in the following section(s): TOE Summary Specification FIA_X509_EXT.2.

Upon investigation, the evaluator found that the TSS states that: X.509v3 certificates are only used for TLS, in which the TOE acts as a client. The TOE has no certificates of its own, except certificates installed to validate peers. When a connection to the OCSP server cannot be established, the TOE will reject the presented certificate and deny the connection.

Verdict:
PASS.

5.3.2.2.2 FIA_X509_EXT.2 AGD

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.

Evaluator Findings:

The evaluator also ensured that the AGD describes the configuration required in the operating environment so the TOE can use the certificates. The AGD also includes any required configuration on the TOE to use the certificates.

The relevant information is found in the following section(s): 9.7 **'OCSP Configuration', 9.6.1 'Authentication', 9.6.1 'Addition of the Certificate'** and 9.6.2 **'Deletion of the Certificate'**

Upon investigation, the evaluator found that the AGD states that Compliance requires OCSP certificate revocation to create a syslog connection using the TLS protocol. The OCSP Server, provided by the operational environment, must be loaded with the following certificates:

- Self-certificate (system cert) signed by the issuer (CA authority).
- Root certificate who signed the system certificate.
- Root certificate of the client who is trying to initiate the connection.

Instructions for these actions can be in section 9.6.1 titled **'Addition of the Certificate'** and subsections 9.6.1 and 9.6.2 which establish trusted authorities on the TOE to properly validate certificates

Additional instruction in case the OCSP responder cannot be contacted are also available in section 9.7 titled '**OCSP Configuration'**. OCSP is used to determine whether the certificate is revoked or not. If the OCSP responder cannot be contacted, then the TOE will choose to automatically reject the certificate in this case.

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.

Evaluator Findings:
The AGD also describes 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. The relevant information is found in the following section(s): **9.6 .1 'Addition of the Certificate'** and 9.7 **'OCSP Configuration'** Upon investigation, the evaluator found that the AGD states that: Instructions for these actions can be in section 9.6.1 titled **'Addition of the Certificate'**. Additional instruction in case the OCSP responder cannot be contacted are also available in section 9.7 titled '**OCSP Configuration'**. OCSP is used to determine whether the certificate is revoked or not. If the OCSP responder cannot be contacted, then the TOE will choose to automatically reject the certificate in this case.

Verdict:
PASS.

5.3.3 SECURITY MANAGEMENT (FMT)

5.3.3.1 FMT_MOF.1/FUNCTIONS MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

5.3.3.1.1 FMT_MOF.1/FUNCTIONS TSS

For distributed TOEs see Section 2.4.1.1.

Evaluator Findings:
The TOE is not distributed; hence, this requirement is not applicable.

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).

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 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 TOE restricts the management of audit data functionality to Security Administrators. This includes the transmission of audit data to the audit server. Security administrators are defined by their UPC levels, which are shown below:

Level	Functions Permitted
1	(monitoring only – no provisioning, maintenance or administration) – Retrieve allows retrieve and report related commands to be executed.
2	(maintenance but no provisioning) – Control allows access to control and retrieve commands but not to provisioning. Maintenance access provides the ability to reset performance monitoring counts.
3	(provisioning but no administration) – Provisioning allows access to provision, test, edit and retrieve commands.
4	(provisioning and administration) – Administration allows complete access to all commands.
5	(provisional and administration) – Surveillance allows complete access to all commands.

The TSS also states the following as it pertains to the details on how the Security Administrator determines or modifies the behaviour of transmitting audit data to an external IT entity: The ability to determine the behavior of and modify the behavior of transmission of audit data to an external IT entity is restricted to administrators with a UPC level of >=4. The administrator is able to configure the IP, reference identifiers and trusted certificate authorities for remote syslog connections by using the TL1 command interface or Site Manager via SSH or local craft ethernet port.

Verdict:
PASS.

5.3.3.1.2 FMT_MOF.1/FUNCTIONS AGD

For distributed TOEs see Section 2.4.1.2.

Evaluator Findings:
The TOE is not distributed; hence, this requirement is not applicable.

For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation 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.

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 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 relevant information is found in the following section(s): 11.1 **'Syslog server Configuration'**, 6 **'Evaluated Configuration of the TOE'** and 7 **'Secure Acceptance, Installation and Configuration'** Upon investigation, the evaluator found that the AGD states that: while the TOE is in CC NDCPP compliant mode, the TOE is understood to have its auditing functions turned on. Disabling CC mode on the TOE would put the TOE in a noncompliant state. To be compliant with Common Criteria, the TOE audits the events in the Table 3: Ciena 6500 Auditable Events. Performing the steps in Sections 6 and 7 of these documents are all the steps required for the TOE to generate the required audit records, store them locally, and send them to an external SFTP Server. The AGD also provides instructions on 'Configuring the syslog server on the TOE using TL1' and 'Configuring the syslog server on the TOE using Site Manager' in section 11.1. Section 6 titled **'Evaluated Configuration of the TOE'** and section 7 titled **'Secure Acceptance, Installation and Configuration'** provide the relevant instructions.

Verdict:
PASS.

5.3.3.2 FMT_MOF.1/SERVICES MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

5.3.3.2.1 FMT_MOF.1/SERVICES TSS

For distributed TOEs see Section 2.4.1.1.

Evaluator Findings:
The TOE is not distributed; hence, this requirement is not applicable.

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.

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 TOE restricts the ability to enable and disable the remote syslog service and SSH service to Security Administrators with (UPC>=4). The enabling and disabling of the remote syslog service affects the audit behavior

and is covered under the FMT_SMF.1 selection of “ability to configure audit behavior”. The enabling and disabling of the SSH service affects remote administrative access and obtaining update files from the remote repository.

Disabling SSH services can be accomplished with the following command:

- ED-SH:6500SP3::CTAG:::,,SERVER=DISABLED,,,,,,,,;

Enabling SSH services can be accomplished with the following command:

- ED-SH:6500SP3::CTAG:::,,SERVER=ENABLED,,,,,,,,;

Disabling remote syslog service can be accomplished with the following command:

- SET-SYSLOG-SERVER:6500SP3::CTAG::SERVER1:STATE=DISABLE,,,,,,,

Enabling remote syslog service can be accomplished with the following command:

- SET-SYSLOG-SERVER:6500SP3::CTAG::SERVER1:STATE=ENABLED,,,

Verdict:
PASS.

5.3.3.2.2 FMT_MOF.1/SERVICES AGD

For distributed TOEs see Section 2.4.1.2.

Evaluator Findings:
The TOE is not distributed; hence, this requirement is not applicable.

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

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. The relevant information is found in the following section(s): 11 **‘Auditing’**, 11.1 **‘Syslog server Configuration’,** 10.1 **‘SSH’,** and 10.2 **‘TLS’**

Upon investigation, the evaluator found that the AGD states that: while the TOE is in CC-NDCPP Compliant Mode, the TOE is understood to have its auditing functions turned on. Disabling CC mode on the TOE would put the TOE in a noncompliant state.

The managing of CC-NDCPP Compliance Mode would be the best practice for starting/stopping services. Further detail as to how this could be done can be referenced in section 8 'Enabling CC-NDCPP Compliance' in the AGD.

11.1 'Syslog server Configuration' gives more detailed instructions related to remote auditing activities and the admin's ability to manage them.

In 10.1 **'SSH'** the AGD states that the TOE restricts the ability to enable and disable the SSH service to Security Administrators with (UPC>=4). The enabling and disabling of the SSH service affects remote administrative access and obtaining update files from the remote repository. Here are instructions on how to start and stop the SSH service for Security Administrators:

Disabling SSH services can be accomplished with the following command:

- Execute the command: ED-SSH:6500SP3::CTAG:::,,SERVER=DISABLED,,,,,,,,;

Enabling SSH services can be accomplished with the following command:

- Execute the command: ED-SSH:6500SP3::CTAG:::,,SERVER=ENABLED,,,,,,,,;

In 10.2 **'TLS'** the AGD provides instructions for enabling and disabling Syslog (TLS).

Disabling TLS services can be accomplished with the following command:

- Execute the command: SET-SYSLOG-SERVER:6500SP3::CTAG::SERVER1:STATE=DISABLE,,,,,,,

Enabling TLS services can be accomplished with the following command:

- Execute the command: SET-SYSLOG-SERVER:6500SP3::CTAG::SERVER1:STATE=ENABLED,,,

Verdict:
PASS.

5.3.3.3 FMT_MTD.1/CRYPTOKEYS MANAGEMENT OF TSF DATA

5.3.3.3.1 FMT_MTD.1/CRYPTOKEYS TSS

For distributed TOEs see Section 2.4.1.1.

Evaluator Findings:
The TOE is not distributed; hence, this requirement is not applicable.

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.

Evaluator Findings:
The evaluator examined the TSS and ensured that, for non-distributed TOEs, 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. The relevant information is found in the following section(s): TOE Summary Specification FMT_MTD.1/CryptoKeys. Upon investigation, the evaluator found that the TSS states that: only the Security Administrator can manage cryptographic keys. This includes key generation for symmetric and asymmetric keys and key destruction/zeroization. Secret and private keys cannot be seen by Security Administrators. SSH Public keys are also managed by Security Administrators for users authenticating to the TOE. TLS and X509 keys are managed by the security administrator for the purpose of syslog functions. All supported keys and their purposes can be found in Table 14 – **'Cryptographic Key Destruction Table** of the Security Target. The table has been included below. The table includes the list of all keys, their method of generation and deletion. The list below is an iteration of the keys

listed in the chart:

- SSH Server RSA Private Key
- SSH Client RSA Private Key
- SSH Session Encryption Key
- SSH Session ECDH Key
- SSH Session ECDH Key
- TLS Client Session Keys

All keys and their options are shown below:

Option Available	Key Type
Generate	TLS, X509, SSH
Import	TLS, X509, SSH
Modify	TLS, X509, SSH
Delete	TLS, X509, SSH

Verdict:
PASS.

5.3.3.3.2 FMT_MTD.1/CRYPTOKEYS AGD

For distributed TOEs see Section 2.4.1.2.

Evaluator Findings:
The TOE is not distributed; hence, this requirement is not applicable.

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.

Evaluator Findings:
The evaluator examined the AGD and ensured that, for non-distributed TOEs, 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 those operations are performed. The relevant information is found in the following section(s): 7.3 **'Cryptographic Configuration Notice',** 9.2 **'Generating, Configuring and Uploading SSH Public/Private key on TOE'**, and 9.6 **'Configurating X.509 Certificate Authentication'** Upon investigation, the evaluator found that the AGD provides the information that the administrator installing the TOE is expected to have performed all of the operations referenced in 7.3 of the AGD. This will result in the TOE's cryptographic operations being limited to the claims made within the Common Criteria evaluation. The admin needs to perform initial setup tasks and enable NDcPP compliant mode. Instructions for enabling NDcPP compliant mode can be found in section 8 "Enabling CC-NDcPP Compliance". By enabling this mode cryptographic settings are automatically configured, and those settings can be viewed in section 7.3 "Cryptographic Configuration Notice". For the breadth of keys (SSH, TLS, X509) optional instruction is available for the admin. Section 9.2 '**Generating, Configuring and Uploading SSH Public/Private key on TOE'** has SSH keys instruction is available for admin set up. Section 9.6 '**Configurating X.509 Certificate Authentication'** provides the same instructions for X509 TLS keys for the admin.

Verdict:
PASS.

Security Assurance Requirements

5.4 ADV: DEVELOPMENT

5.4.1 BASIC FUNCTIONAL SPECIFICATION (ADV_FSP.1)

5.4.1.1 (5.2.1.1) EVALUATION ACTIVITY

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.

In this context, TSFI are deemed security relevant if they are used by the administrator to configure the TOE, or to perform other administrative functions (e.g. audit review or performing updates). Additionally, those interfaces that are identified in the ST, or guidance documentation, as adhering to the security policies (as presented in the SFRs), are also considered security relevant. The intent is that these interfaces will be

adequately tested and having an understanding of how these interfaces are used in the TOE is necessary to ensure proper test coverage is applied.

The set of TSFI that are provided as evaluation evidence are contained in the Administrative Guidance and User Guidance.

Evaluator Findings:
TOE Design information that can be made public is available in the guidance documentation and in the ST. Any sensitive or proprietary information required by this protection profile is not to be made public. It is not necessary to provide a complete specification of the TSFIs. For NDcPP, additional "functional specification" documentation is not necessary because this requirement is satisfied by multiple other documents (AGD, TSS, and Testing). All associated activities are covered in the Test Report, ST, and AGD documents. NDcPP2.2e, section 7.2.1 states that: "For 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." All of the above information is applicable to the ADV Evaluation Activities (5.2.1.1, 5.2.1.2, and 5.2.1.3) in NDcPP2.2e-SD. The evaluator examined the ST (Security Target) and the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all the AGD Evaluation Activities. During testing, the evaluator used the product and its interfaces extensively and did not find any areas that were deficient.

Verdict:
PASS.

5.4.1.2 (5.2.1.2) EVALUATION ACTIVITY

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.

Evaluator Findings:
The evaluator checked the interface documentation (AGD) and ensured it identifies and describes the parameters for each TSFI that is identified as being security relevant. This is covered in the previous evaluation activity above.

Verdict:
PASS.

5.4.1.3 (5.2.1.3) EVALUATION ACTIVITY

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

The evaluator uses the provided documentation and first identifies, and then examines a representative set of interfaces to perform the EAs presented in Section 2, including the EAs associated with testing of the interfaces.

It should be noted that there may be some SFRs that do not have an interface that is explicitly "mapped" to invoke the desired functionality. For example, generating a random bit string, destroying a cryptographic key that is no longer needed, or the TSF failing to a secure state, are capabilities that may be specified in SFRs, but are not invoked by an interface.

However, if the evaluator is unable to perform some other required EA because there is insufficient design and interface information, then the evaluator is entitled to conclude that an adequate functional specification has not been provided, and hence that the verdict for the ADV_FSP.1 assurance component is a 'fail'.

Evaluator Findings:
The evaluator examined the interface documentation to develop a mapping of the interfaces to SFRs. The evaluator used the provided documentation to first identify, and then examine a representative set of interfaces to perform the EAs presented in Section 2, including the EAs associated with testing of the interfaces. This is covered in the previous evaluation activity above.

Verdict:
PASS.

5.5 AGD: GUIDANCE DOCUMENTS

5.5.1 OPERATIONAL USER GUIDANCE (AGD_OPE.1)

5.5.1.1 (5.3.1.1) EVALUATION ACTIVITY

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

Evaluator Findings:
The evaluator checked the requirements above are met by the AGD. The AGD 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. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org.

Verdict:
PASS.

5.5.1.2 (5.3.1.2) EVALUATION ACTIVITY

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.

Evaluator Findings:
The evaluator ensured that the AGD is provided for every Operational Environment that the product supports as claimed in the Security Target. The section 6.1 titled 'TOE Components' of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are: • VXWorks 6.9 for SP3 and SPAP3

Verdict:
PASS.

5.5.1.3 (5.3.1.3) EVALUATION ACTIVITY

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.

Evaluator Findings:
The evaluator ensured that the AGD contains instructions for configuring any cryptographic implementation associated with the evaluated configuration of the TOE. It provides a warning to the administrator that use of other cryptographic implementations was not evaluated nor tested during the CC evaluation of the TOE.

Verdict:
PASS.

5.5.1.4 (5.3.1.4) EVALUATION ACTIVITY

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.

Evaluator Findings:
The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section 9 titled 'Secure Management of the TOE' specifies features that are not assessed and tested by the EAs. The evaluator ensured the AGD makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.

Verdict:
PASS.

5.5.1.5 (5.3.1.5) EVALUATION ACTIVITY **[TD0536]**

In addition, the evaluator shall ensure that the following requirements are also met:

- The AGD 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.

- **[TD0536]** The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. 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 AGD shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.

Evaluator Findings:
The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Test #3. The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2. The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4.

Verdict:
PASS.

5.5.2 PREPARATIVE PROCEDURES (AGD_PRE.1)

5.5.2.1 (5.3.2.1) EVALUATION ACTIVITY

The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security 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 documentation should be in an informal style and should be written with sufficient detail and explanation that they can be understood and used by the target audience (which will typically include IT staff who have general IT experience but not necessarily experience with the TOE product itself).

Evaluator Findings:

The evaluator examined 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. The evaluator reviewed the sections 6.2 titled **'Supporting Environmental Components'** of the AGD. The evaluator found that these sections describe how the Operational Environment must meet:

The following table lists components and applications in the environment that the TOE relies upon to function properly:

Component	Definition
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications. Alternatively, the workstation can physically connect to the TOE using the craft port, which is an Ethernet port through which the TOE can be managed locally using a SSH Client.
Syslog server	A properly configured audit data storage server implementing the Syslog over TLS protocol.
Update Server	A server running the secure file transfer protocol (SFTP) server that is used as a location for storing product updates that can be transferred to the TOE.
Site Manager	The Site Manager software provides a graphical interface to the TL1 interface for managing the TOE. The Site Manager software is installed on the Management workstation and uses an SSH channel to connect to the TOE.

Evaluated Components of the Operational Environment

Verdict:
PASS.

5.5.2.2 (5.3.2.2) EVALUATION ACTIVITY

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.

Evaluator Findings:

The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment, including:

- VxWorks 6.9 for the SP3 and SPAP3 shelf processors

The section 6.1 titled 'TOE Components' of AGD identifies the following supported platform:

The TOE is 6500 Packet Optical Platform, running software version Release 15.6. 6500 Packet Optical Platform are standalone hardware network appliances that run VxWorks. This is a family of products that contains the following hardware models:

MODEL TYPE	MODEL PART #	SP3 Shelf Processor Card	SPAP3 Shelf Processor Card
2-slot Type 2	NTK503LA	NO	YES
4-slot Type	NTK503HA	YES	NO
7-slot	NTK503PA	YES	NO
7-slot type 2	NTK503KA	NO	YES
6500-7	NTK503RA	YES	NO
14-slot	NTK503BA NTK503CA NTK503CC NTK503GA NTK503AD NTK503BD NTK503CD NTK503SA	YES	NO
32-slot	NTK603AA	YES	NO

		NTK603AB			

Verdict:
PASS.

5.5.2.3 (5.3.2.3) EVALUATION ACTIVITY

The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.

Evaluator Findings:
The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the instructions necessary to install and configure the TOE to work in the target operating environment, including: • Secure Acceptance, Installation and Configuration of the TOE • Enabling CC-NDcPP Compliance • Secure Management of the TOE • Cryptographic Protocols • Auditing • Operational Modes • Additional Support • TL1 Commands

Verdict:
PASS.

5.5.2.4 (5.3.2.4) EVALUATION ACTIVITY

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.

Evaluator Findings:
The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Test #3

Verdict:
PASS.

5.5.2.5 (5.3.2.5) EVALUATION ACTIVITY

In addition, the evaluator shall ensure that the following requirements are also met. 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.

Evaluator Findings:
The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The section 9.4 titled **'User Accounts and User Management'** were used to determine the verdict of this work unit. The AGD refers to "Local password management" and "Setting/changing/removing the supervisory password" in security document named "Ciena 6500 Packet-Optical Platform Administration and Security Release 15.6" to change the password or disable the default accounts.

Verdict:
PASS.

5.6 AVA: VULNERABILITY ASSESSMENT

5.6.1 VULNERABILITY SURVEY (AVA_VAN.1)

5.6.1.1 (5.6.1.1) EVALUATION ACTIVITY (DOCUMENTATION) **[TD0547]**

In addition to the activities specified by the CEM in accordance with Table 2, the evaluator shall perform the following activities.

The evaluator shall examine the documentation outlined below provided by the developer to confirm that it contains all required information. This documentation is in addition to the documentation already required to be supplied in response to the EAs listed previously.

The developer shall provide documentation identifying the list of software and hardware components that compose the TOE. Hardware components should identify at a minimum the processors used by the TOE. Software components include applications, the operating system and other major components that are independently identifiable and reusable (outside of the TOE), for example a web server, protocol or cryptographic libraries, (independently identifiable and reusable components are not limited to the list provided in the example). This additional documentation is merely a list of the name and version number of the components and will be used by the evaluators in formulating vulnerability hypotheses during their analysis.

The TOE is not distributed.

Evaluator Findings:
The evaluator collected this information from the developer which was used to feed into the Public Domain Search. Refer to evaluator findings in the evaluation activity below.

Verdict:
PASS.

5.6.1.2 (5.6.1.2) EVALUATION ACTIVITY

The evaluator formulates hypotheses in accordance with process defined in Appendix A. The evaluator documents the flaw hypotheses generated for the TOE in the report in accordance with the guidelines in Appendix A.3. The evaluator shall perform vulnerability analysis in accordance with Appendix A.2. The results of the analysis shall be documented in the report according to Appendix A.3.

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 evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below: • https://nvd.nist.gov/vuln/search • https://www.cve.org/ • https://www.cvedetails.com/vulnerability-search.php

The search was performed on following dates:

- July 24th, 2024
- November 8th, 2024
- December 13th, 2024

The evaluator performed the public domain vulnerability searches using the following key words.

- Ciena 6500 Packet Optical
- Packet Optical
- Ciena 6500
- Ciena
- VxWorks
- Ciena SP3
- Ciena SPAP3
- Digicert TrustCore Version GA0521-U2
- QorIQ T1042
- QorIQ T1022

The evaluation lab examined each result provided from NVD 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.

Verdict:
PASS.

5.6.1.3 AVA FUZZ TESTING

The evaluators performed the following fuzz testing in compliance with AVA_VAN.1. The results can be found in the table below:

Evaluator Findings:

The evaluator shall perform the following activities to generate type 4 flaw hypotheses:

- Fuzz testing
    - Examine effects of sending:
        - mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443)
        - mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE.

    Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.

Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well-formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.

ICMPv4

- Perform fuzz testing for each type and code of the ICMP header using the acumen-fuzzer tool.
- Verify via packet capture that each type and code has been fuzzed and the TOE behaviour was not adversely affected.

IPv4

- Perform fuzz testing for each protocol of the IPv4 header using the acumen-fuzzer tool.
- Verify via packet capture that each protocol has been fuzzed and the TOE behaviour was not adversely affected.

ICMPv6

- Perform fuzz testing for each type and code of the ICMP header using the acumen-fuzzer tool.
- Verify via packet capture that each type and code has been fuzzed and the TOE behaviour was not adversely affected.

IPv6

- Perform fuzz testing for each protocol of the IPv6 header using the acumen-fuzzer tool.
- Verify via packet capture that each protocol has been fuzzed and the TOE behaviour was not adversely affected.

The TOE was not adversely affected by the impaired traffic.

6 DETAILED TEST CASES (TEST ACTIVITIES)

6.1 AUTH

6.1.1 FIA_AFL.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): 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.
Notes	The NiT has issued a technical decision (TD0570) for clarification about FIA_AFL.1. 1. FIA_AFL.1 is a mandatory SFRs that the TOE will need to meet. 2. FIA_AFL.1 requires at least one remote administrative interface support password authentication.

	3. If SSH is the TOE's only remote administrative interface, it needs to support password authentication. If there is another administrative interface (e.g. a web GUI) that supports password authentication, SSH does not need to support password authentication and, by extension, FIA_AFL.1. The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.
Test Steps	• The evaluator configured the max number of logins attempts to 4 and the lockout time of 5 minutes before re-enabling access. • The evaluator attempted to login with incorrect login credentials four times to reach the attempt limit. • Verify that the login fails due to incorrect login credentials. • Login to the TOE with correct login credentials. • The evaluator verified through the logs that following authentication attempt with valid credentials were unsuccessful.
Pass/Fail with Explanation	Pass, The TOE denied access with valid credentials after the number of invalid authentication attempts is reached. This meets the testing requirements.

6.1.2 FIA_AFL.1 TEST #2A

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): 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).
Notes	The NiT has issued a technical decision (TD0570) for clarification about FIA_AFL.1. 1. FIA_AFL.1 is a mandatory SFRs that the TOE will need to meet. 2. FIA_AFL.1 requires at least one remote administrative interface support password authentication. 3. If SSH is the TOE's only remote administrative interface, it needs to support password authentication. If there is another administrative interface (e.g. a web GUI) that supports password authentication, SSH does not need to support password authentication and, by extension, FIA_AFL.1. The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.

Test Steps	• Login for the user “READONLY” to the TOE via SSH using incorrect password. • Verify that the Login fails due to incorrect login credentials. • Verify that the logs that the user gets locked. • Login to the TOE as the Administrator. • Execute the following command to manually unlock the user. • Verify from the logs that user “READONLY’ gets unlocked. • Login with the user “READONLY” to the TOE with correct login credentials. • Verify that the user is unlocked, and login is successful. • Verify from the logs that the login is successful with correct login credentials.
Pass/Fail with Explanation	Pass, when a user is locked out due to unsuccessful authentication attempts, the user can be unlocked successfully using an admin account. This meets the testing requirements. This meets the testing requirements.

6.1.3 FIA_AFL.1 TEST #2B

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: 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 authorisation 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 authorisation attempt using valid credentials results in successful access.
Notes	The NiT has issued a technical decision (TD0570) for clarification about FIA_AFL.1. 1. FIA_AFL.1 is a mandatory SFRs that the TOE will need to meet.

	2. FIA_AFL.1 requires at least one remote administrative interface support password authentication. 3. If SSH is the TOE's only remote administrative interface, it needs to support password authentication. If there is another administrative interface (e.g. a web GUI) that supports password authentication, SSH does not need to support password authentication and, by extension, FIA_AFL.1. The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.
Test Steps	• The evaluator configured the time period before allowing access with valid credentials at 5 minutes. • The evaluator attempted to login with incorrect credentials four times to reach the attempt limit. • Verify that the login attempt fails with the incorrect login credentials. • The evaluator confirmed that a further authentication attempt with valid credentials just before the time of 5 minute was unsuccessful. • Verify that the login fails with valid login credentials just before five minutes. • Verify from the logs that the login attempt with valid and Invalid login credentials were made. • The evaluator attempts to login into the TOE with valid credentials just 5 minutes after the last unsuccessful attempt. • Verify through the logs that the next authentication attempt using valid credentials just after 5 minutes was successful.
Pass/Fail with Explanation	Pass. TOE correctly allowed or did not allow authorization attempts depending on the time period. This meets the testing requirements.

6.1.4 FIA_PMG_EXT.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests. Test 1: The evaluator shall compose passwords that 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, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing.
Notes	The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. 2. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.

Test Steps	• Set the minimum password requirements.
	  ○ Minimum 8-character length.
	  ○ Minimum 1 upper case.
	  ○ Minimum 1 lower case.
	  ○ Minimum 1 digit.
	  ○ Minimum 1 special character.
	  ○ Minimum 1 character that should differ from previous password.
	• Authenticate to the TOE via the Site Manager as the Administrator.
	• Click the “Security” drop down menu and select “User Profiles”
	• Select the “Add” and attempt to create a new user with username “GOOD” and enter the password “A'B1C+D7-E!a@bc1de”
	• Verify the username “GOOD” with correct password requirements are created.
	• Select the “Add” and attempt to create a new user with username “GOOD2” and enter the password “U{V5W\X1}Y(u)vw5xy”
	• Verify the username “GOOD2” with correct password requirements are created.
	• Select the “Add” and attempt to create a new user with username “GOOD3” and enter the password “P=Q>4RS$T-p*qr4st”

	• Verify the username “GOOD3” with correct password requirements are created. • Select the “Add” and attempt to create a new user with username “GOOD4” and enter the password “ZA6>B<C2`D!z%ab6cd” • Verify the username “GOOD4” with correct password requirements are created. • Verify through logs that all the users are created with the assigned username and password.
Pass/Fail with Explanation	Pass. TOE supported passwords that meet the requirement in the ST and allowed authentication to the TOE. This meets the testing requirements.

6.1.5 FIA_PMG_EXT.1 TEST #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests. Test 2: 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.
Notes	The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. 2. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.
Test Steps	• Authenticate to the TOE via the Site Manager as the Administrator. • Click the “Security” drop down menu and select “User Profiles” • Select the “Add” and Attempt to create a user with a missing upper case character in the password with username “BAD” and password “ab1cd7e!a@bc1de” • Verify that the user could not be created.

	• Select the “Add” Attempt to create a user with missing lowing case character in password with username “BAD2” and password “FG2HI8J#F$GH2IJ” • Verify that the user could not be created. • Select the “Add” and Attempt to create a user with missing digits in the password with username “BAD3” and password “KLmMNra%k^lmsno” • Verify that the user could not be created. • Select the “Add” and Attempt to create a user with a missing special character in the password with username “BAD4” and password “PQ4RS0T2prqr4st” • Verify that the user could not be created. • Select the “Add” and Attempt to create a user with less than 8 characters in password username “BAD5” and password “UV5@wX1” • Verify that the user could not be created. • Verify through logs that the users are not created with the assigned username and password.
Pass/Fail with Explanation	Pass. The TOE rejected passwords that did not meet the requirements and no users are created with the bad password. This meets the testing requirements.

6.1.6 FIA_UIA_EXT.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: 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.s

Test Steps	Local console (Craft Ethernet): • Initiate a connection to the TOE via Craft Ethernet through the site manager. • Verify that the login is successful. • Verify that the TOE successfully authenticated and that audit logs were generated reflecting the login. • Initiate a connection to the TOE via Craft Ethernet through the site manager using an invalid username and valid password. • Verify that the login fails due to incorrect login credentials • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. • Initiate a connection to the TOE via Craft Ethernet through the site manager using a valid username and an invalid password. • Verify that the login fails due to incorrect login credentials • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. • Initiate a connection to the TOE via Craft Ethernet and then authenticate to the TOE via Site manager using an invalid username and an invalid password. • Verify that the login fails due to incorrect login credentials. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. Remote SSH (TL1): • Initiate a connection to the TOE via SSH and then authenticate to the TOE via Site manager using the following command for valid username and valid password: • Verify that the login is successful. • Verify that the TOE successfully authenticated and that audit logs were generated reflecting the login. • Initiate a connection to the TOE via SSH and then authenticate to the TOE via Site manager using the following command an invalid username and valid password: • Verify that the Login fails. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. • Initiate a connection to the TOE via SSH and then authenticate to the TOE via Site manager using a valid username and an invalid password. • Verify that the Login fails. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. • Initiate a connection to the TOE via SSH and then authenticate to the TOE via Site manager using an invalid username and an invalid password. • Verify that the login fails. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. Remote SSH (public/private key based): • Authenticate the TOE via SSH via Site manager using a valid username and private key (valid).

	• Verify that the login is successful. • Verify that the TOE successfully authenticated at audit logs were generated reflecting the login. • Authenticate the TOE via SSH via Site manager using an invalid username and a private key (valid). • Verify that the login fails. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. • Authenticate the TOE via SSH via Site manager using a valid username and a private key (invalid). • Verify that the login fails. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure. • Authenticate the TOE via SSH via Site manager using an invalid username and a private key(invalid). • Verify that the login fails. • Verify that the TOE failed to authenticate and that audit logs were generated reflecting the failure.
Pass/Fail with Explanation	Pass. The TOE successfully authenticates users with correct credentials and login fails when incorrect credentials are used. This meets the testing requirements.

6.1.7 FIA_UIA_EXT.1 TEST #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 2: 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.
Test Steps	• Authenticate to the TOE via the SSH. • Verify that the login banner is displayed prior to authentication to the TOE. • Verify through the log that the login was successful. • Ping to the TOE for ICMP echo.

	• Verify via pcap that the ICMP request and ICMP response packet.
Pass/Fail with Explanation	Pass. The TOE allows only banner to be visible prior to log in. This meets the testing requirements.

6.1.8 FIA_UIA_EXT.1 TEST #3

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 3: 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.
Test Steps	• Reuse existing login banner from previous test. • Authenticate to the TOE via the local console (Craft Ethernet) • Verify that the warning banner is displayed prior to authentication to the TOE. • Verify the TOE appropriately responds to ICMP echo requests • Verify that no other services are available prior to authentication by entering a privileged command to attempt to retrieve syslog data prior to authentication.
Pass/Fail with Explanation	Pass. The TOE allows banner to be visible prior to log in and respond to the ping. This meets the testing requirements.

6.1.9 FIA_UIA_EXT.1 TEST #4

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 4: For distributed TOEs where not all TOE components support the authentication of Security Administrators according to FIA_UIA_EXT.1 and FIA_UAU_EXT.2, the evaluator shall test that the components authenticate Security Administrators as described in the TSS.
Pass/Fail with Explanation	N/A. This test is not applicable since the TOE is not a distributed TOE.

6.1.10 FIA_UIA_EXT.1 TEST #1

Item	Data
Test Assurance Activity	Evaluation Activities for this requirement are covered under those for FIA_UIA_EXT.1. If other authentication mechanisms are specified, the evaluator shall include those methods in the activities for FIA_UIA_EXT.1.
Notes	The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. 2. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.

Pass/Fail with Explanation	Pass, this test is covered under FIA_UIA_EXT.1.

6.1.11 FIA_UAU.7 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each method of local login allowed: Test 1: 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.
Test Steps	• Attempt to login TOE on locally via site manager • Verify that authentication information, such as the password being obscured • Attempt to login TOE through ssh via site manager • Verify that authentication information, such as the password being obscured
Pass/Fail with Explanation	Pass. No feedback is shown for the password. This meets the testing requirements.

6.1.12 FMT_MOF.1/MANUALUPDATE TEST #1

Item	Data
Test Assurance Activity	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 Steps	• Log into TOE as a user that does not have Security Administrator privilege(UPC<=2). • Verify the logs on the TOE to ensure "READONLY" user is logged in with Read-Only permission. • Execute the following commands to output the current running and most recently installed TOE software version. • Fetch the legitimate update by executing the following command. • Verify from the logs that the update fails.
Pass/Fail with Explanation	Pass. The TOE does not allow a user without administrator privileges to update the image. This meets the testing requirements.

6.1.13 FMT_MOF.1/MANUALUPDATE TEST #2

Item	Data
Test Assurance Activity	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 with Explanation	Pass. This test has been completed as part of the requirements specified in FPT_TUD_EXT.1 Test#1. This meets the testing requirements.

6.1.14 FMT_MOF.1/FUNCTIONS (1) TEST #1

Item	Data
Test Assurance Activity	Test 1 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters 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 modify the security related parameters 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 Steps	• Authenticate to the TOE as a user with limited privileges (UPC = 2) • Attempt to execute the following command: SET-SYSLOG-SETTINGS:::1:::PRTCL=5424,SYSLOGFAC=16,SYSLOGSEV=7,SYSLOGTYPES=ALL,HOSTIPFMT=IPV4; • Verify from the logs that the command fails to execute due to insufficient privileges.
Pass/Fail with Explanation	Pass. TOE does not allow limited Privilege user to modify audit data of an external IT entity. This meets the testing requirements.

6.1.15 FMT_MOF.1/FUNCTIONS (1)TEST #2

Item	Data
Test Assurance Activity	Test 2 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the

	transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.
Test Steps	• Login to the TOE as a user with Administrator privileges (UPC = 4). • Attempt to execute the following command: SET-SYSLOG SETTINGS:::1:::PRTCL=5424,SYSLOGFAC=16,SYSLOGSEV=7,SYSLOGTYPES=ALL,HOSTIPFMT=IPV4**;** • Verify from logs that the command has been executed successfully.
Pass/Fail with Explanation	Pass. The TOE allows security admin to modify audit data of an external server. This meets the testing requirements.

6.1.16 FMT_MOF.1/FUNCTIONS (2) TEST #1

Item	Data
Test Assurance Activity	Test 1 (if **'handling of audit data'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters 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 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. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.

Pass/Fail with Explanation	N/A. The ST does not select 'audit functionality when Local Audit Storage Space is full'.

6.1.17 FMT_MOF.1/FUNCTIONS (2) TEST #2

Item	Data
Test Assurance Activity	Test 2 (if **'handling of audit data'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace. The evaluator does not necessarily have to test all possible values of the security related parameters for configuration of the handling of audit data but at least one allowed value per parameter.
Pass/Fail with Explanation	N/A. The ST does not select 'audit functionality when Local Audit Storage Space is full'.

6.1.18 FMT_MOF.1/FUNCTIONS (3) TEST #1

Item	Data
Test Assurance Activity	(if **'audit functionality when Local Audit Storage Space is full**' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This attempt 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 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.
Pass/Fail with Explanation	N/A. The ST does not select 'audit functionality when Local Audit Storage Space is full'.

6.1.19 FMT_MOF.1/FUNCTIONS (3) TEST #2

Item	Data
Test Assurance Activity	(if **'audit functionality when Local Audit Storage Space is full**' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full with prior authentication as Security Administrator. This attempt should be successful. The effect of the change shall be verified. The evaluator does not necessarily have to test all possible values for the behaviour when Local Audit Storage Space is full but at least one change between allowed values for the behaviour

Pass/Fail with Explanation	N/A. The ST does not select 'audit functionality when Local Audit Storage Space is full'.

6.1.20 FMT_MOF.1/FUNCTIONS TEST #3

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall 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 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.
Pass/Fail with Explanation	Pass. This test has been completed as part of the requirements specified in FMT_MOF.1/Functions (1) Test#1. This meets the testing requirements.

6.1.21 FMT_MOF.1/FUNCTIONS TEST #4

Item	Data
Test Assurance Activity	Test 4 (if in the first selection 'determine the behaviour of' has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection with prior authentication as Security Administrator. This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions with Security Administrator authentication shall be successful.
Pass/Fail with Explanation	Pass. This test has been completed as part of the requirements specified in FMT_MOF.1/Functions (1) Test#2. This meets the testing requirements.

6.1.22 FMT_MOF.1/SERVICES TEST #1

Item	Data
Test Assurance Activity	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 Steps	• Login to the TOE as a user with limited privileges (UPC = 2). • Attempt to execute the following command to disable the syslog service: SET-SYSLOG-SERVER:6500SPAP3::CTAG::SERVER1:STATE=DISABLED,,,TLSSTATE=ENABLED,,,,; • Attempt to execute the following command to enable the syslog service: SET-SYSLOG-SERVER:6500SPAP3::CTAG::SERVER1:STATE=ENABLED,,,TLSSTATE=ENABLED,,,,;

	• Verify via logs that the user “READONLY” fails to execute due to insufficient privilege. • Attempt to execute the following command to disable the SSH service: ED-SSH:6500SPAP3::CTAG:::,,SERVER=DISABLED,,,,,,,,; • Attempt to execute the following command to enable the SSH service: ED-SSH:6500SPAP3::CTAG:::,,SERVER=ENABLED,,,,,,,,; • Verify via logs that the user “READONLY” fails to execute due to insufficient privilege.
Pass/Fail with Explanation	PASS. TOE does not allow limited user to disable and enable syslog and SSH service. This meets the testing requirements.

6.1.23 FMT_MOF.1/SERVICES TEST #2

Item	Data
Test Assurance Activity	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 Steps	• Login to the TOE as a user with Administrator privileges (UPC = 4). • Attempt to execute the following command to disable the syslog service: SET-SYSLOG-SERVER:6500SPAP3::CTAG::SERVER1:STATE=DISABLED,,,TLSSTATE=ENABLED,,,,; • Attempt to execute the following command to enable the syslog service: SET-SYSLOG-SERVER:6500SPAP3::CTAG::SERVER1:STATE=ENABLED,,,TLSSTATE=ENABLED,,,,; • Verify via logs that the user “ADMIN” is able to enable and disable the syslog service. • Attempt to execute the following command to disable the SSH service: ED-SSH:6500SPAP3::CTAG:::,,SERVER=DISABLED,,,,,,,,; • Attempt to execute the following command to enable the SSH service: ED-SSH:6500SPAP3::CTAG:::,,SERVER=ENABLED,,,,,,,,; • Verify via logs that the user “ADMIN” is able to enable and disable the SSH service.
Pass/Fail with Explanation	Pass. TOE allows security admin to disable and enable the syslog and SSH service. This meets the testing requirements.

6.1.24 FMT_MTD.1/COREDATA TEST #1

Item	Data
Test Assurance Activity	No separate testing for FMT_MTD.1/CoreData is required unless one of the management functions has not already been exercised under any other SFR.
Pass/Fail with Explanation	Pass. This Test is covered under FMT_SMF.1 Test #1. This meets the testing requirements.

6.1.25 FMT_MTD.1/CRYPTOKEYS TEST #1

Item	Data
Test Assurance Activity	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 Steps	• Login to the TOE as a user with limited privileges (UPC = 2). • Attempt to execute the following command: CRTE-SSH-KEYS:::CTAG:::KEYSIZE=2048,KEYTYPE=RSA; • Verify via logs that the user “READONLY” fails to execute due to insufficient privileges.

Pass/Fail with Explanation	PASS. The TOE does not allow Limited user to generate cryptographic key. This meets the testing requirements.

6.1.26 FMT_MTD.1/CRYPTOKEYS TEST #2

Item	Data
Test Assurance Activity	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 Steps	• Login to the TOE as a user with Administrator privileges (UPC = 4). • Execute the following command: CRTE-SSH-KEYS:::CTAG:::KEYSIZE=2048,KEYTYPE=RSA; • Verify via logs that the user “ADMIN” can generate cryptographic key.
Pass/Fail with Explanation	PASS. TOE allows Security Administrator to generate cryptographic key. This meets the testing requirements.

6.1.27 FMT_SMF.1 TEST #1

Item	Data
Test Assurance Activity	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.

Notes	The NiT has issued a technical decision (TD0571) for Guidance on how to handle FIA_AFL.1. 1. FIA_UAU_EXT.2.1 applies solely to how the administrator logs in at the local console. Passwords were made selection based to allow TOEs that have difficulty determining whether an incoming connection is local or remote to provide a mechanism to prevent administrative lockout. As FIA_AFL.1 is a mandatory SFR, it is expected that the TOE provides at least one remote password-based authentication mechanism using credentials managed by the TOE. 2. FIA_PMG_EXT.1, FIA_AFL.1, and FMT_SMF.1 are all mandatory SFRs that the TOE will need to meet.
Pass/Fail with Explanation	PASS. All tests management functions as part of testing the SFRs identified as required. This meets the testing requirements.

6.1.28 FMT_SMR.2 TEST #1

Item	Data
Test Assurance Activity	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.
Pass/Fail with Explanation	PASS. The TOE successfully supports both local and remote access. This meets the testing requirements.

6.1.29 FTA_SSL.3 TEST #1

Item	Data
Test Assurance Activity	For each method of remote administration, the evaluator shall perform the following test: Test 1: 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 Steps	• Go to User Profile under the Security tab and click on EDIT to change the timeout value to 2 minutes. • Authenticate to the TOE via SSH. Note: The logs show the timestamp of login and timeout session. • Verify through the logs that the session gets terminated. • Go to User Profile under the Security tab and click on EDIT to change the timeout value to 5 minutes. • Authenticate to the TOE via SSH. Note: The logs show the timestamp of login and timeout session. • Verify through the logs that the session gets terminated.
Pass/Fail with Explanation	Pass. TOE correctly terminates remote session after the configured inactivity time period has elapsed. This meets the testing requirements.

6.1.30 FTA_SSL.4 TEST #1

Item	Data
Test Assurance Activity	For each method of remote administration, the evaluator shall perform the following tests:

	Test 1: 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 Steps	• Authenticate to the TOE via the local console. • Execute the following command to terminate the session: CANC-USER::<username>:CTAG; • Verify that user successfully exits out local console.
Pass/Fail with Explanation	Pass. The TOE allows the user to terminate the directly connected administrative session. This meets the testing requirements.

6.1.31 FTA_SSL.4 TEST #2

Item	Data
Test Assurance Activity	For each method of remote administration, the evaluator shall perform the following tests: Test 2: 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 Steps	• Remote login to the TOE using SSH. • Execute the following command to terminate the session: CANC-USER::<username>:CTAG; • Verify via logs that user successfully exits out remote session.
Pass/Fail with Explanation	Pass. The TOE allows the user to terminate the remote administrative session. This meets the testing requirements.

6.1.32 FTA_SSL_EXT.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test: Test 1: 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.
Test Steps	• Go to User Profile under the Security tab and click on EDIT to change the Local timeout value to 2 minutes. • Authenticate to the TOE via Craft Ethernet. • Verify through the logs that the session gets terminated. • Go to User Profile under the Security tab and click on EDIT to change the Local timeout value to 4 minutes. • Authenticate to the TOE via Craft Ethernet. • Verify through the logs that the session gets terminated.
Pass/Fail with Explanation	Pass. TOE ends the user session on the local console after the inactivity time limit is reached. This meets the testing requirements.

6.1.33 FTA_TAB.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall also perform the following test:

	Test 1: 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 Steps	• Authenticate to the TOE via the SSH. • On the opening screen, click the "Edit" button at the bottom. • Modify the text of the banner to read "THIS IS A WARNING BANNER!!!" • Click "Apply" and then "OK". • Log out of the Site Manager. • Attempt to authenticate to the TOE using the Site Manager application via SSH. • Validate that the warning banner configured in the TOE is presented prior to authentication. • Attempt to authenticate the TOE via Craft Ethernet port using the Site Manager. • Validate that the warning banner configured in the TOE is presented prior to authentication. • Authenticate the TOE via SSH using command line and validate that the warning banner is presented prior to authentication.
Pass/Fail with Explanation	PASS. TOE successfully displayed login and welcome banner messages to the user.

6.1.34 FTP_TRP.1/ADMIN TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 1: The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.

	For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.
Test Steps	• Log into the TOE via SSH. • Verify audit logs that the user is successfully log in to the TOE. • Verify that the session was established, and data is encrypted via packet capture.
Pass/Fail with Explanation	Pass. Users are successfully able to access the TOE via SSH connection. This meets the testing requirements.

6.1.35 FTP_TRP.1/ADMIN TEST #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 2: The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext. For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of trusted paths to TOE components in the Security Target.
Pass/Fail with Explanation	Pass. Refer to FTP_TRP.1/Admin Test #1 for encrypted channel data. This meets the testing requirements.

6.2 AUDIT

6.2.1 FAU_GEN.1 TEST #1

Item	Data
Test Assurance Activity	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. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Notes	**NIT Technical Decision (TD0639) for Clarification for NTP MAC Keys.** The SFRs FAU_GEN.1, FCS_CKM.4 and FPT_SKP_EXT.1 shall be applied to all cryptographic keys that are related to secure communication (i.e. related to FTP_TRP.1, FTP_ITC.1, FPT_ITT.1). The NTP requirements have been introduced in NDcPP V2.1 as a rather 'standalone' set of requirements with 'no audit requirements' specified in the ECD section for FCS_NTP_EXT.1 and no dependencies on FCS_CKM - in contrast to the corresponding sections for secure communication protocols like TLS. As NTP keys are not intended to be used for encryption of sensitive information, the level of protection is different compared to other pre-shared keys. It has therefore not been intended that NTP keys are treated as other pre-shared keys in the context of NDcPP.
Test Steps	• 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.

	• 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. • 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.
Pass/Fail with Explanation	Pass. 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. This meets the testing requirements.

6.2.2 FAU_GEN.1 TEST #2

Item	Data
Test Assurance Activity	For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of auditable events to TOE components in the Security Target. For all events involving more than one TOE component when an audit event is triggered, the evaluator has to check that the event has been audited on both sides (e.g. failure of building up a secure communication channel between the two components). This is not limited to error cases but includes also events about successful actions like successful build up/tear down of a secure communication channel between TOE components. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Notes	**NIT Technical Decision (TD0639) for Clarification for NTP MAC Keys.** The SFRs FAU_GEN.1, FCS_CKM.4 and FPT_SKP_EXT.1 shall be applied to all cryptographic keys that are related to secure communication (i.e. related to FTP_TRP.1, FTP_ITC.1, FPT_ITT.1). The NTP requirements have been introduced in NDcPP V2.1 as a rather 'standalone' set of requirements with 'no audit requirements' specified in the ECD section

	for FCS_NTP_EXT.1 and no dependencies on FCS_CKM - in contrast to the corresponding sections for secure communication protocols like TLS. As NTP keys are not intended to be used for encryption of sensitive information, the level of protection is different compared to other pre-shared keys. It has therefore not been intended that NTP keys are treated as other pre-shared keys in the context of NDcPP.
Pass/Fail with Explanation	N/A , The TOE is not distributed; hence, this activity is not applicable.

6.2.3 FAU_GEN.2 TEST #1

Item	Data
Test Assurance Activity	This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.
Pass/Fail with Explanation	Pass. FAU_GEN.1 Test#1 covers this requirement. This meets the testing requirements.

6.2.4 FAU_GEN.2 TEST #2

Item	Data
Test Assurance Activity	For distributed TOEs the evaluator shall verify that where auditable events are instigated by another component, the component that records the event associates the event with the identity of the instigator. The evaluator shall perform at least one test on one component where another component instigates an auditable event. The evaluator shall verify that the event is recorded by the component as expected and the event is associated with the instigating component. It is assumed that an event instigated by another component can at least be generated for building up a secure channel between two TOE components. If for some reason

	(could be e.g. TSS or Guidance Documentation) the evaluator would come to the conclusion that the overall TOE does not generate any events instigated by other components, then this requirement shall be omitted.
Pass/Fail with Explanation	N/A, The TOE is not distributed; hence, this activity is not applicable.

6.2.5 FAU_STG_EXT.1 TEST #1

Item	Data
Test Assurance Activity	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement: Test 1: 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 Steps	• Show the Openssl version. • Configure the TOE to ENABLE Syslog server service with correct port and server address. • Configure the TOE to upload the trust certificates (ROOT_CA and ICA). • Start the Syslog service. • Verify the logs generated on the TOE. • Verify the logs seen on the remote Syslog server are the same. • Verify that the logs are encrypted with packet capture.

Pass/Fail with Explanation	Pass. The TOE passes all audit traffic to the remote audit server through a secure channel without admin interference. This meets the testing requirements.

6.2.6 FAU_STG_EXT.1 TEST #2 (A)

Item	Data
Test Assurance Activity	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement: 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: The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option 'drop new audit data' in FAU_STG_EXT.1.3).
Pass/Fail with Explanation	N/A. The option 'drop new audit data' is not selected in the ST.

6.2.7 FAU_STG_EXT.1 TEST #2 (B)

Item	Data
Test Assurance Activity	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement: 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:tThe 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 Steps	• Authenticate to the TOE via SSH. • Execute the following command: RTRV-SYSLOG:6500A-SPAP3::CTAG:::,,; • Note the date and time of the oldest log. • Perform some action in the TOE and execute the following command again to retrieve the audit logs in the TOE: RTRV-SYSLOG:6500A-SPAP3::CTAG:::,,; • Verify that the oldest log is being overwritten.
Pass/Fail with Explanation	Pass. The test is passed because once the limit was reached the oldest audit record was overwritten. This meets the testing requirements.

6.2.8 FAU_STG_EXT.1 TEST #2 (C)

Item	Data
Test Assurance Activity	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement: 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:vThe TOE behaves as specified (for the option '**other action**' in FAU_STG_EXT.1.3).
Pass/Fail with Explanation	N/A, the ST does not select other action.

6.2.9 FAU_STG_EXT.1 TEST #3

Item	Data
Test Assurance Activity	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement: Test 3: If the TOE complies with FAU_STG_EXT.2/LocSpace the evaluator shall verify that the numbers provided by the TOE according to the selection for FAU_STG_EXT.2/LocSpace are correct when performing the tests for FAU_STG_EXT.1.3
Pass/Fail with Explanation	N/A, the ST does not select FAU_STG_EXT.2/LocSpace.

6.2.10 FAU_STG_EXT.1 TEST #4

Item	Data
Test Assurance Activity	Testing of the trusted channel mechanism for audit will be performed as specified in the associated assurance activities for the particular trusted channel mechanism. The evaluator shall perform the following additional tests for this requirement: Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.
Pass/Fail with Explanation	N/A. This test is not applicable since the TOE is not a distributed TOE.

6.2.11 FCS_NTP_EXT.1.1 TEST #1

Item	Data
Test Assurance Activity	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 Steps	Note: The TOE only supports NTP version 4. • On the TOE set clock to new time by executing the following command: ED-DAT:6500A-SPAP3::CTAG::YY-MM_DD, HH-MM-SS; • Show the new time in the TOE by executing the following command: RTRV-DAT:6500A-SPAP3::CTAG; • On the TOE enable NTP service and add a new NTP server for time synchronization and then click apply. • Click on Synchronize for time synchronization in the TOE. • Show TOE clock to verify time synchronization. • Verify the log that TOE is time synchronized with the server. • Verify packets to show that NTP version is supported.
Pass/Fail with Explanation	PASS. TOE uses the correct version of NTPv4 to synchronize with an external NTP server. This meets the testing requirements.

6.2.12 FCS_NTP_EXT.1.2 TEST #1

Item	Data
Test Assurance Activity	The cryptographic algorithms selected in element 1.2 and specified in the ST will have been specified in an FCS_COP SFR and tested in the accompanying Evaluation Activity for that SFR. Likewise, the cryptographic protocol selected in in element 1.2 and specified in the ST will have been specified in an FCS SFR and tested in the accompanying Evaluation Activity for that SFR. [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.
Notes	**NIT Technical Decision (TD0639) for Clarification for NTP MAC Keys.** The SFRs FAU_GEN.1, FCS_CKM.4 and FPT_SKP_EXT.1 shall be applied to all cryptographic keys that are related to secure communication (i.e. related to FTP_TRP.1, FTP_ITC.1, FPT_ITT.1). The NTP requirements have been introduced in NDcPP V2.1 as a rather 'standalone' set of requirements with 'no audit requirements' specified in the ECD section for FCS_NTP_EXT.1 and no dependencies on FCS_CKM - in contrast to the corresponding sections for secure communication protocols like TLS. As NTP keys are not intended to be used for encryption of sensitive information, the level of protection is different compared to other pre-shared keys. It has therefore not been intended that NTP keys are treated as other pre-shared keys in the context of NDcPP.
Test Steps	• Upload the supported message digest algorithm in the TOE. • Verify that the keys are uploaded. • Configure the NTP server with a supported message digest algorithm by the TOE. • Configure the TOE with the supported algorithm and NTP server address. • ON the NTP connection in the TOE for time synchronization with the server. • Verify the connection is established via logs. • Verify the connection is established via packet capture. • Configure the NTP server with a non-supported message digest algorithm by the TOE. • Configure the TOE with the supported algorithm and NTP server address. • ON the NTP connection in the TOE for time synchronization with the server. • Verify the connection is refused via packet capture. • Verify the connection failure through logs.

Pass/Fail with Explanation	Pass. The TOE is in sync with NTP Server when supported message digest algorithm is configured on NTP Server and does not sync when an unsupported message digest algorithm is used,. This meets testing requirements.

6.2.13 FCS_NTP_EXT.1.3 TEST #1

Item	Data
Test Assurance Activity	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 Steps	Broadcast: • Check the time on the TOE. • Set NTP server to broadcast to 10.41.79.255 • Verify with a capture that broadcast packets are sent by the NTP server. • Verify that the time on the TOE is not modified. Multicast: • Check the time on the TOE. • Set NTP server to multicast to 224.0.1.1 • Verify with a capture that multicast packets are sent by the NTP server. • Verify that the time on the TOE is not modified.
Pass/Fail with Explanation	Pass. The TOE does not sync with an NTP server that sends out broadcast and multicast updates. This meets testing requirements.

6.2.14 FCS_NTP_EXT.1.4 TEST #1 **[TD0528]**

Item	Data
Test Assurance Activity	Test 1: 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 Steps	• Verify the current time on the TOE. • Configure at least 3 NTP time sources. • Update the TOE according to the configured NTP servers. <u>Server 1</u> • Verify with packet capture. • Verify the time sync with the configured NTP server via logs. <u>Server 2</u> • Verify with packet capture. • Verify the time sync with the configured NTP server via logs. <u>Server 3</u> • Verify with packet capture. • Verify the time sync with the configured NTP server via logs.
Pass/Fail with Explanation	Pass. The TOE is able to update the time using three NTP servers. This meets the testing requirement.

6.2.15 FCS_NTP_EXT.1.4 TEST #2 **[TD0528]**

Item	Data
Test Assurance Activity	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 steps	• Verify the time on the TOE. • Configure the NTP server 1 in the TOE. • Sync the TOE with NTP server 1. • Verify that TOE is synced to NTP server 1. • Verify with packet capture that the TOE synced with the NTP server 1. • Verify with logs that TOE synced to NTP server 1. • Configure the NTP server 2 to which the TOE syncs. • Verify that TOE synced to NTP server 2. • Verify with logs that TOE synced to NTP server 2. • Verify the time on the TOE. • Replay the packets from the NTP server 1 which were captured during earlier sync. • Verify the TOE does not sync with the NTP server 2.
Pass/Fail with Explanation	Pass. The TOE is accepting valid NTP server as time source while rejecting rouge NTP server as tine source. This meets the testing requirements.

6.2.16 FPT_STM_EXT.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 1: 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. If the audit component of the TOE consists of several parts with independent time information, then the evaluator shall verify that the time information between the different parts are either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously.
Test Steps	• Authenticate to the TOE. • Use the following TL1 command to edit the date and time: ED-DAT:::CTAG::[yy-mm-dd],[hh-mm-ss]; • Verify that the date and time was set by entering the following TL1 command: RTRV-DAT:::CTAG; • Log out of the TOE. • Log into the TOE and show the system time for verification.
Pass/Fail with Explanation	Pass, The TOE successfully saves the configured time and date by the administrator. This meets testing requirements.

6.2.17 FPT_STM_EXT.1 TEST #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests:

	Test 2: 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. cIf the audit component of the TOE consists of several parts with independent time information, then the evaluator shall verify that the time information between the different parts are either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously.
Test Steps	• On the TOE set clock to new time by executing the following command: ED-DAT:6500A-SPAP3::CTAG::YY-MM_DD, HH-MM-SS; • Show the new time in the TOE by executing the following command: RTRV-DAT:6500A-SPAP3::CTAG; • On the TOE enable NTP service and add a new NTP server for time synchronization and then click apply. • Click on Synchronize for time synchronization in the TOE. • Show TOE clock to verify time synchronization. • Verify test log that TOE is time synchronized with the server. • Verify packets to show that NTP version is supported.
Pass/Fail with Explanation	Pass. The TOE was successfully able to synchronize with the NTP server. This meets the testing requirements.

6.2.18 FPT_STM_EXT.1 TEST #3 **[TD0632]**

Item	**Data**
Test Assurance Activity	Test 3: [conditional] If the TOE obtains time from the underlying VS, the evaluator shall record the time on the TOE, modify the time on the underlying VS, and verify the modified time is reflected by the TOE. If there is a delay between the setting the time on the VS and when the time is reflected on the TOE, the evaluator shall ensure this delay is consistent with the TSS and Guidance.

	TD0632 has been applied.
Pass/Fail with Explanation	N/A, This test is not claimed in the ST.

6.2.19 FTP_ITC.1 TEST #1

Item	Data
Test Assurance Activity	The developer 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. The evaluator shall perform the following tests: 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. For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Notes	The NiT has issued a technical decision (TD0572) for Restricting FTP_ITC.1 to only IP address identifiers. DNS resolution is not mandatory to support FTP_ITC.1. There are no resolution mandates or requirements in RFC 6125.

	The use of the dnsName identifiers in X.509 certificates must be supported by TOEs that claim FCS_DTLSC_EXT or FCS_TLSC_EXT when associated with FTP_ITC.1. Inability to parse dnsName identifiers shall be considered a failure to meet these requirements.
Test Steps	FCS_SSHC_EXT.1.2 TEST #1, FAU_STG_EXT.1 Test #1 and FCS_TLSC_EXT.1 Test #1 cover this test requirement. The TOE is not distributed so there are no additional components to test.
Pass/Fail with Explanation	Pass. TOE successfully communicates to an Update and Syslog server with an encrypted channel. The connection can be initiated by the TOE. This meets the testing requirements.

6.2.20 FTP_ITC.1 TEST #2

Item	Data
Test Assurance Activity	The developer 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. The evaluator shall perform the following tests: 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. For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Notes	The NiT has issued a technical decision (TD0572) for Restricting FTP_ITC.1 to only IP address identifiers.

	DNS resolution is not mandatory to support FTP_ITC.1. There are no resolution mandates or requirements in RFC 6125. The use of the dnsName identifiers in X.509 certificates must be supported by TOEs that claim FCS_DTLSC_EXT or FCS_TLSC_EXT when associated with FTP_ITC.1. Inability to parse dnsName identifiers shall be considered a failure to meet these requirements.
Test Steps	FCS_SSHC_EXT.1.2 TEST #1, FAU_STG_EXT.1 Test #1 and FCS_TLSC_EXT.1 Test #1 cover this test requirement. The TOE is not distributed so there are no additional components to test.
Pass/Fail with Explanation	Pass. TOE successfully communicates to an Update and Syslog server with an encrypted channel. The connection can be initiated by the TOE. This meets the testing requirements.

6.2.21 FTP_ITC.1 TEST #3

Item	Data
Test Assurance Activity	The developer 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. The evaluator shall perform the following tests: Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext. For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Notes	The NiT has issued a technical decision (TD0572) for Restricting FTP_ITC.1 to only IP address identifiers.

	DNS resolution is not mandatory to support FTP_ITC.1. There are no resolution mandates or requirements in RFC 6125. The use of the dnsName identifiers in X.509 certificates must be supported by TOEs that claim FCS_DTLSC_EXT or FCS_TLSC_EXT when associated with FTP_ITC.1. Inability to parse dnsName identifiers shall be considered a failure to meet these requirements.
Test Steps	FCS_SSHC_EXT.1.2 TEST #1, FAU_STG_EXT.1 Test #1 and FCS_TLSC_EXT.1 Test #1 cover this test requirement. The TOE is not distributed so there are no additional components to test.
Pass/Fail with Explanation	Pass. TOE successfully communicates to an Update and Syslog server with an encrypted channel. The connection can be initiated by the TOE. This meets the testing requirements.

6.2.22 FTP_ITC.1 TEST #4

Item	Data
Test Assurance Activity	The developer 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. The evaluator shall perform the following tests: Test 4: 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 network link 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. For distributed TOEs the evaluator shall perform tests on all TOE components according to the mapping of external secure channels to TOE components in the Security Target.
Notes	The NiT has issued a technical decision (TD0572) for Restricting FTP_ITC.1 to only IP address identifiers. DNS resolution is not mandatory to support FTP_ITC.1. There are no resolution mandates or requirements in RFC 6125. The use of the dnsName identifiers in X.509 certificates must be supported by TOEs that claim FCS_DTLSC_EXT or FCS_TLSC_EXT when associated with FTP_ITC.1. Inability to parse dnsName identifiers shall be considered a failure to meet these requirements.
Test Steps	Syslog server (TLS): Short duration (duration shorter than the application layer timeout) • Establish a connection from the TOE to the Syslog server to verify the successful connection. • Physically disrupt the connection for a short time (duration shorter than the application layer timeout), then test the connection. No data will go through, when connectivity is restored, the connection remains encrypted. Long duration (duration exceeds application layer timeout) • Establish a connection from the TOE to the Syslog server to verify the successful connection. • Physically disrupt the connection for a long time (duration exceeds application layer timeout), then test the connection. No data will go through. Update Server (SSH): Short duration (duration shorter than the application layer timeout) • Authenticate to the TOE via the CLI using SSH on debug TCP port 28888.

	• Establish a connection from the TOE to the update server by entering the following details UserId, Password, IP Address of the server and SFTP Port number. • Physically disrupt the connection for a short time (duration shorter than the application layer timeout), then test the connection. No data will go through, when connectivity is restored, the connection remains encrypted. Note: The TOE was initially connected to the update server; the SSH connection was physically interrupted for less than the application layer timeout. After reconnecting, the traffic can still be seen in encrypted format over the same SSH connection. Long duration (duration exceeds application layer timeout) • Establish a connection from the TOE to the update server by entering the following details UserId, Password, IP Address of the update server and SFTP Port number. • Verify that the connection has been dropped to the server due to application layer timeout. • Re-Establish a connection from the TOE to the update server and verify successful connection. • Verify via PCAPs that the SSH session was re-established, and that all data is encrypted. The existing SSH connection was dropped, and a new connection was established before any user data was transmitted. • Note: The connection of update server with the TOE was broken for more than the application layer timeout and a new session was initiated between the update server and the TOE. The traffic continues to be in an encrypted format despite the physical connection interruption between the two devices.
Pass/Fail with Explanation	Pass. The SSH and TLS connections were maintained or re-established as necessary, and all data sent between the system was encrypted. This meets the testing requirements.

6.3 CRYPTO

6.3.1 FCS_CKM.1 RSA

Item	Data
Test Assurance Activity	Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported). **Key Generation for FIPS PUB 186-4 RSA Schemes** The evaluator shall verify the implementation of RSA Key Generation by the TOE using the Key Generation test. This test verifies the ability of the TSF to correctly produce values for the key components including the public verification exponent *e*, the private prime factors *p* and *q*, the public modulus *n* and the calculation of the private signature exponent d. Key Pair generation specifies 5 ways (or methods) to generate the primes p and q. These include: a) Random Primes: • Provable primes • Probable primes b) Primes with Conditions: • Primes p1, p2, q1, q2, p and q shall all be provable primes • Primes p1, p2, q1, and q2 shall be provable primes and p and q shall be probable primes • Primes p1, p2, q1, q2, p and q shall all be probable primes

	To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation.
Pass/Fail with Explanation	Algorithm: RSA KeyGen (FIPS186-4) Key size / Modulus: 2048 CAVP #: A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.2 FCS_CKM.1 ECC

Item	Data
Test Assurance Activity	Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported). **Key Generation for Elliptic Curve Cryptography (ECC)**

	FIPS 186-4 ECC Key Generation Test For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall require the implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator shall submit the generated key pairs to the public key verification (PKV) function of a known good implementation. *FIPS 186-4 Public Key Verification (PKV) Test* For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator shall obtain in response a set of 10 PASS/FAIL values.
Pass/Fail with Explanation	Algorithm: ECDSA KeyGen (FIPS186-4) Curves: P-256, P-384, P-521 CAVP #: A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.3 FCS_CKM.1 FFC – FIPS PUB 186-4

Item	Data
Test Assurance Activity	Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported). **Key Generation for Finite-Field Cryptography (FFC)** The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p, the cryptographic prime q (dividing p-1), the cryptographic group generator g, and the calculation of the private key x and public key y. The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime q and the field prime p: • Primes q and p shall both be provable primes • Primes q and field prime p shall both be probable primes and two ways to generate the cryptographic group generator g: • Generator g constructed through a verifiable process • Generator g constructed through an unverifiable process. The Key generation specifies 2 ways to generate the private key x: • len(q) bit output of RBG where 1 <=x <= q-1

	• len(q) + 64 bit output of RBG, followed by a mod q-1 operation and a +1 operation, where 1<= x<=q-1. The security strength of the RBG must be at least that of the security offered by the FFC parameter set. To test the cryptographic and field prime generation method for the provable primes method and/or the group generator g for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set. For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm • g != 0,1 • q divides p-1 • g^q mod p = 1 • g^x mod p = y for each FFC parameter set and key pair.
Pass/Fail with Explanation	N/A. Not claimed in the ST.

6.3.4 FCS_CKM.1 FFC – "SAFE-PRIME" GROUPS **[TD0580]**

Item	Data
Test Assurance Activity	Note: The following tests require the developer to provide access to a test platform that provides the evaluator with tools that are typically not found on factory products. Generation of long-term cryptographic keys (i.e. keys that are not ephemeral keys/session keys) might be performed automatically (e.g. during initial start-up). Testing of key generation must cover not only administrator invoked key generation but also automated key generation (if supported). **FFC Schemes using "safe-prime" groups** Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1. **TD0580 has been applied.**
Pass/Fail with Explanation	N/A. Not claimed in the ST.

6.3.5 FCS_CKM.2 RSA

Item	Data
Test Assurance Activity	**RSA-based key establishment** The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5.
Pass/Fail with Explanation	N/A. Not claimed in the ST.

6.3.6 FCS_CKM.2 SP800-56A - ECC

Item	Data
Test Assurance Activity	**Key Establishment Schemes** The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE using the applicable tests below. **SP800-56A Key Establishment Schemes** The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value Z) and the calculation of the

	derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag. *Function Test* The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested. The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information field OI and TOE id fields. If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret. The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values.

	If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm. *Validity Test* The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the other info and TOE id fields. The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).i The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.
Pass/Fail with Explanation	Algorithm: KAS-ECC-SSC Sp800-56Ar3 CAVP #: A5421

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

6.3.7 FCS_CKM.2 SP800-56A - FFC

Item	Data
Test Assurance Activity	**Key Establishment Schemes** The evaluator shall verify the implementation of the key establishment schemes of the supported by the TOE using the applicable tests below. **SP800-56A Key Establishment Schemes** The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value Z) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag. *Function Test* The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported

	schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested. The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information field OI and TOE id fields. If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret. The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values. If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm. *Validity Test* The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data

	sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the other info and TOE id fields. The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass).i The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.
Pass/Fail with Explanation	N/A. Not claimed in the ST.

6.3.8 FCS_CKM.2 DH14 **[TD0580]**

Item	**Data**
Test Assurance Activity	**Diffie-Hellman Group 14** This test assurance activity was removed by TD0580.

	TD0580 has been applied.
Pass/Fail with Explanation	N/A. This test assurance activity was removed by TD0580. Based on these findings, this assurance activity is considered satisfied.

6.3.9 FCS_CKM.2 FCC SAFE-PRIME

Item	Data
Test Assurance Activity	**FFC Schemes using "safe-prime" groups** The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.
Pass/Fail with Explanation	N/A. Not claimed in the ST.

6.3.10 FCS_CKM.4

Item	Data
Test Assurance Activity	There are no test assurance activities.
Notes	**NIT Technical Decision (TD0639) for Clarification for NTP MAC Keys.** The SFRs FAU_GEN.1, FCS_CKM.4 and FPT_SKP_EXT.1 shall be applied to all cryptographic keys that are related to secure communication (i.e. related to FTP_TRP.1, FTP_ITC.1, FPT_ITT.1). The NTP requirements have been introduced in NDcPP V2.1 as a rather 'standalone' set of requirements with 'no audit requirements' specified in the ECD section for FCS_NTP_EXT.1 and no dependencies on FCS_CKM - in contrast to the corresponding sections for secure communication protocols like TLS. As NTP keys are not intended to be used for encryption of sensitive information, the level of protection is different compared to other pre-shared keys. It has therefore not been intended that NTP keys are treated as other pre-shared keys in the context of NDcPP.
Pass/Fail with Explanation	N/A. There are no test assurance activities for this SFR.

6.3.11 FCS_COP.1/DATAENCRYPTION AES-CBC

Item	Data
Test Assurance Activity	**AES-CBC Known Answer Tests** There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation. **KAT-1.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption. **KAT-2.** To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AESCBC decryption.

KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N].

To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of keys and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.i

KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256- bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128].

To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.

AES-CBC Multi-Block Message Test

The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be

tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.

The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.

AES-CBC Monte Carlo Tests

The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:

```
# Input: PT, IV, Key
for i = 1 to 1000:
        if i == 1:
                CT[1] = AES-CBC-Encrypt(Key, IV, PT)
                PT = IV
        else:
                CT[i] = AES-CBC-Encrypt(Key, PT)
```

	PT = CT[i-1] The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation. The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AESCBC-Decrypt.
Pass/Fail with Explanation	Algorithm: AES CBC Key size: 128, 256 CAVP #:A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.12 FCS_COP.1/DATAENCRYPTION AES-GCM

Item	Data
Test Assurance Activity	**AES-GCM Test** The evaluator shall test the authenticated encrypt functionality of AES-GCM for each combination of the following input parameter lengths:

	128 bit and 256 bit keys a) **Two plaintext lengths.** One of the plaintext lengths shall be a nonzero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported. a) **Three AAD lengths.** One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported. b) **Two IV lengths.** If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested. The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known. The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.
Pass/Fail with Explanation	Algorithm: AES GCM Key size: 128, 256

	CAVP #:A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.13 FCS_COP.1/DATAENCRYPTION AES-CTR

Item	Data
Test Assurance Activity	**AES-CTR Known Answer Tests** The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. Since the Counter Mode does not specify the counter that is used, it is not possible to implement an automated test for this mode. The generation and management of the counter is tested through FCS_SSH*_EXT.1.4. If CBC and/or GCM are selected in FCS_COP.1/DataEncryption, the test activities for those modes sufficiently demonstrate the correctness of the AES algorithm. If CTR is the only selection in FCS_COP.1/DataEncryption, the AES-CBC Known Answer Test, AESGCM Known Answer Test, or the following test shall be performed (all of these tests demonstrate the correctness of the AES algorithm): There are four Known Answer Tests (KATs) described below to test a basic AES encryption operation (AES-ECB mode). For all KATs, the plaintext, IV, and ciphertext values shall be 128-bit blocks. The results from each test may either be obtained by the validator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

	KAT-1 To test the encrypt functionality, the evaluator shall supply a set of 5 plaintext values for each selected keysize and obtain the ciphertext value that results from encryption of the given plaintext using a key value of all zeros. KAT-2 To test the encrypt functionality, the evaluator shall supply a set of 5 key values for each selected keysize and obtain the ciphertext value that results from encryption of an all zeros plaintext using the given key value. KAT-3 To test the encrypt functionality, the evaluator shall supply a set of key values for each selected keysize as described below and obtain the ciphertext values that result from AES encryption of an all zeros plaintext using the given key values. A set of 128 128-bit keys, a set of 192 192-bit keys, and/or a set of 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1, N]. KAT-4 To test the encrypt functionality, the evaluator shall supply the set of 128 plaintext values described below and obtain the ciphertext values that result from encryption of the given plaintext using each selected keysize with a key value of all zeros (e.g. 256 ciphertext values will be generated if 128 bits and 256 bits are selected and 384 ciphertext values will be generated if all keysizes are selected). Plaintext value i in each set shall have the leftmost bits be ones and the rightmost 128-i bits be zeros, for i in [1, 128].t **AES-CTR Multi-Block Message Test** The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 less-than i less-than-or-equal to 10 (test shall be performed using AES-ECB mode). For each i the evaluator shall choose a key and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key using a known good implementation. The evaluator shall perform this test using each selected keysize.

	AES-CTR Monte-Carlo Test The evaluator shall test the encrypt functionality using 100 plaintext/key pairs. The plaintext values shall be 128-bit blocks. For each pair, 1000 iterations shall be run as follows: # Input: PT, Key for i = 1 to 1000: CT[i] = AES-ECB-Encrypt(Key, PT) PT = CT[i] The ciphertext computed in the 1000th iteration is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation. The evaluator shall perform this test using each selected keysize. There is no need to test the decryption engine.
Pass/Fail with Explanation	Algorithm: AES CTR Key size: 128, 256 CAVP #: A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.14 FCS_COP.1/SIGGEN ECDSA

Item	Data
Test Assurance Activity	**ECDSA Algorithm Tests** **ECDSA FIPS 186-4 Signature Generation Test** For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values R and S. To determine correctness, the evaluator shall use the signature verification function of a known good implementation. **ECDSA FIPS 186-4 Signature Verification Test** For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values.
Pass/Fail with Explanation	Algorithm: ECDSA SigGen Curve: P-256 , P-384 , P-521 CAVP #: A5421 Algorithm: ECDSA SigVer Curve: P-256 , P-384 , P-521 CAVP #: A5421

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

6.3.15 FCS_COP.1/SIGGEN RSA

Item	Data
Test Assurance Activity	**RSA Signature Algorithm Tests** **Signature Generation Test** The evaluator generates or obtains 10 messages for each modulus size/SHA combination supported by the TOE. The TOE generates and returns the corresponding signatures. The evaluator shall verify the correctness of the TOE's signature using a trusted reference implementation of the signature verification algorithm and the associated public keys to verify the signatures. **Signature Verification Test** For each modulus size/hash algorithm selected, the evaluator generates a modulus and three associated key pairs, (d, e). Each private key d is used to sign six pseudorandom messages each of 1024 bits using a trusted reference implementation of the signature generation algorithm. Some of the public keys, e, messages, or signatures are altered so that signature verification should fail. For both the set of original messages and the set of altered messages: the modulus, hash algorithm, public key e values, messages, and signatures are forwarded to the TOE, which then attempts to verify the signatures and returns the verification results.

	The evaluator verifies that the TOE confirms correct signatures on the original messages and detects the errors introduced in the altered messages.
Pass/Fail with Explanation	Algorithm: RSA SigGen Key size / Modulus: 2048 CAVP #: A5421 Algorithm: RSA SigVer Key size / Modulus: 2048 CAVP #: A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.16 FCS_COP.1/HASH

Item	Data
Test Assurance Activity	The TSF hashing functions can be implemented in one of two modes. The first mode is the byte-oriented mode. In this mode the TSF only hashes messages that are an integral number of bytes in length; i.e., the length (in bits) of the message to be hashed is divisible by 8. The second mode is the bit-oriented mode. In this mode the TSF hashes

	messages of arbitrary length. As there are different tests for each mode, an indication is given in the following sections for the bit-oriented vs. the byte-oriented testmacs. The evaluator shall perform all of the following tests for each hash algorithm implemented by the TSF and used to satisfy the requirements of this PP. **Short Messages Test - Bit-oriented Mode** The evaluators devise an input set consisting of m+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m bits. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. **Short Messages Test - Byte-oriented Mode** The evaluators devise an input set consisting of m/8+1 messages, where m is the block length of the hash algorithm. The length of the messages range sequentially from 0 to m/8 bytes, with each message being an integral number of bytes. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. **Selected Long Messages Test - Bit-oriented Mode** The evaluators devise an input set consisting of m messages, where m is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the ith message is m + 99*i, where 1 ≤ i ≤ m. The message text shall be

	pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. **Selected Long Messages Test - Byte-oriented Mode** The evaluators devise an input set consisting of m/8 messages, where m is the block length of the hash algorithm (e.g. 512 bits for SHA-256). The length of the ith message is m + 8*99*i, where 1 ≤ i ≤ m/8. The message text shall be pseudorandomly generated. The evaluators compute the message digest for each of the messages and ensure that the correct result is produced when the messages are provided to the TSF. **Pseudorandomly Generated Messages Test** This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.
Pass/Fail with Explanation	Algorithm: SHA-256, SHA-384, SHA-512 CAVP #:A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.17 FCS_COP.1/KEYEDHASH

Item	Data
Test Assurance Activity	For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key and message data using a known good implementation.
Pass/Fail with Explanation	Algorithm: HMAC (SHA-256, SHA-384) CAVP #:A5421 Pass. Based on these findings, this assurance activity is considered satisfied.

6.3.18 FCS_RBG_EXT.1

Item	Data
Test Assurance Activity	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).d 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.i 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.
Pass/Fail with Explanation	Algorithm: Counter DRBG Mode: AES 256 CAVP #: A5421

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

6.4 SSHS

6.4.1 FCS_SSHS_EXT.1.2 TEST #1 **[TD0631]**

Item	Data
Test Assurance Activity	Test objective: The purpose of these tests is to verify server supports each claimed client authentication method. 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.
Pass/Fail with Explanation	Pass. Please refer to FCS_SSHS_EXT.1.5 Test#1. The TOE is able to make SSH connections with each claimed public key algorithm i.e. rsa-sha2-256 and rsa-sha2-512. This meets the testing requirements.

6.4.2 FCS_SSHS_EXT.1.2 TEST #2 **[TD0631]**

Item	Data
Test Assurance Activity	Test objective: The purpose of these tests is to verify server supports each claimed client authentication method.

	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 Steps	• Configure the SSH client with a new RSA keypair for SSH without configuring the TOE. • Log into the TOE SSH using RSA-based authentication. • Verify via the logs that the login is unsuccessful. • Verify the packet capture that the login was unsuccessful.
Pass/Fail with Explanation	Pass. The TOE does not allow public key authentication if the public key of the SSH user has not been uploaded to the TOE. This meets the testing requirements.

6.4.3 FCS_SSHS_EXT.1.2 TEST #3 **[TD0631]**

Item	Data
Test Assurance Activity	Test objective: The purpose of these tests is to verify server supports each claimed client authentication method. 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.

Pass/Fail with Explanation	N/A, not selected in ST.

6.4.4 FCS_SSHS_EXT.1.2 TEST #4 **[TD0631]**

Item	Data
Test Assurance Activity	Test objective: The purpose of these tests is to verify server supports each claimed client authentication method. 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.
Pass/Fail with Explanation	N/A, Not selected in ST.

6.4.5 FCS_SSHS_EXT.1.3 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Steps	• Run Acumen tool to log in the TOE and then send a packet larger than 32,768 bytes. • Verify through the logs that the large packet was dropped. • Verify through the packet capture that large packet has been dropped.

Pass/Fail with Explanation	Pass, The TOE drops large packets that are received within an SSH session. This meets the testing requirements.

6.4.6 FCS_SSHS_EXT.1.4 TEST #1

Item	Data
Test Assurance Activity	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection. To verify this, the evaluator shall start session establishment for an 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.
Test Steps	• Configure the TOE to support AES128-CTR for encryption algorithm. • Establish an SSH session with the configured supported algorithms. • Verify successful establishment of connection via audit log. • Verify AES128-CTR was used via packet capture. • Verify that the TOE only supports the algorithms as mentioned in the ST via packet capture. • Configure the TOE to support AES128-CBC for encryption algorithm**.** • Establish an SSH session with the configured supported algorithms. • Verify successful establishment of connection via audit log. • Verify AES128-CBC was used via packet capture.

	• Configure the TOE to support AES256-CTR for encryption algorithm. • Establish an SSH session with the configured supported algorithms. • Verify successful establishment of connection via audit log. • Verify AES256-CTR was used via packet capture. • Configure the TOE to support AES256-CBC for encryption algorithm. • Establish an SSH session with the configured supported algorithms. • Verify successful establishment of connection via audit log. • Verify AES256-CBC was used via packet capture. • Establish an SSH session with the unclaimed algorithms. (AES256-gcm@openssh.com) • Verify the connection was not successful via audit logs. • Verify the connection was not successful via packet capture.
Pass/Fail with Explanation	Pass. The TOE can make SSH connections with each claimed algorithm and The TOE rejects SSH connections using a non-approved algorithm. This meets the testing requirements.

6.4.7 FCS_SSHS_EXT.1.5 TEST #1 **[TD0631]**

Item	Data
Test Assurance Activity	Test objective: This test case is meant to validate that the TOE server will support host public keys of the claimed algorithm types. 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.

Test Steps	• Configure the TOE to support RSA based SSH authentication method. • Generate a rsa public key on the VM. • Upload the public key onto the TOE. • Verify that it is updated on the TOE. • Established a session with the TOE using the rsa-sha2-256 host key algorithms. • Verify through packet capture that the SSH session was encrypted using host key algorithms. • Established a session with the TOE using the rsa-sha2-512 host key algorithms. • Verify through packet capture that the SSH session was encrypted using host key algorithms.
Pass/Fail with Explanation	Pass. The TOE allows a client to connect using the supported Host public key algorithm. This meets the testing requirements.

6.4.8 FCS_SSHS_EXT.1.5 TEST #2 **[TD0631]**

Item	Data
Test Assurance Activity	Test objective: This negative test case is meant to validate that the TOE server does not support host public key algorithms that are not claimed. 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 Steps	• Established a session with the TOE using the unsupported host key algorithms (SSH-DSS). • Verify through logs that the SSH session was not established. • Verify through packet capture that the SSH session was not established.

Pass/Fail with Explanation	Pass, TOE does not accept the SSH connection which is established using an unsupported host key algorithm.

6.4.9 FCS_SSHS_EXT.1.6 TEST #1

Item	Data
Test Assurance Activity	Test 1: [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.
Test Steps	• Establish an SSH session with the configured supported algorithms (HMAC-SHA2-256). • Verify that the SSH session uses HMAC-SHA2-256 via capture. • Verify that the message integrity algorithm used was as configured via log.
Pass/Fail with Explanation	Pass. TOE accepts the connection if the session is established using supported MAC algorithm. This meets the testing requirement.

6.4.10 FCS_SSHS_EXT.1.6 TEST #2

Item	Data
Test Assurance Activity	Test 2: [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.
Test Steps	• Establish an SSH session with the unsupported algorithms (HMAC-SHA2-512). • Verify that the TOE rejects the HMAC-SHA2-512 algorithm via capture and connection fails. • Verify that failed connection via log.
Pass/Fail with Explanation	Pass. The SSH connection fails when the MAC algorithm used is not from the ST selection. This meets the testing requirements.

6.4.11 FCS_SSHS_EXT.1.7 TEST #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Steps	• Attempt to establish a connection with the switch from an SSH client using Diffie-hellman-group1-sha1 as the key exchange method. • Capture the traffic between the devices and observe connection failure. • Verify that the session was not established.

Pass/Fail with Explanation	Pass. The SSH connection fails when using Diffie-hellman-group1-sha1 (a non-approved algorithm) for the key exchange. This meets the testing requirements.

6.4.12 FCS_SSHS_EXT.1.7 TEST #2

Item	Data
Test Assurance Activity	Test 2: 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.
Test Steps	• Show TOE supported key exchange i.e. ECDH-SHA2-NISTP384 and ECDH-SHA2-NISTP256. • Attempt to establish a connection with the TOE from an SSH client using : ECDH-SHA2-NISTP256 as the key exchange method. • Verify that the session was established via logs. • Verify that the session was established via packet capture. • Attempt to establish a connection with the TOE from an SSH client using : ECDH-SHA2-NISTP384 as the key exchange method. • Verify that the session was established via logs. • Verify that the session was established via packet capture.
Pass/Fail with Explanation	Pass. The TOE is able to make SSH connections with each claimed data key exchange method. This meets the testing requirements.

6.4.13 FCS_SSHS_EXT.1.8 TEST #1T

Item	Data

Test Assurance Activity	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.eeIf 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).
Test Steps	• Initiate a new SSH session. • Verify via logs that rekey takes place after the time-based threshold.
Pass/Fail with Explanation	Pass. The TOE initiates a rekey every 60 minutes. This meets the testing requirements.

6.4.14 FCS_SSHS_EXT.1.8 TEST #1B

Item	Data
Test Assurance Activity	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 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). 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: 1. An argument is present in the TSS section describing this hardware- based limitation and 2. 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.

Test Steps	• Initiate a new SSH session. • Verify via logs that rekey takes place after setting the data limit (500 MB).
Pass/Fail with Explanation	Pass. The TOE issues a rekey after 500 MB of data is sent. This meets the testing requirement.

6.5 SSHC

6.5.1 FCS_SSHC_EXT.1.2 TEST #1 **[TD0636]**

Item	Data
Test Assurance Activity	Test objective: The purpose of these tests is to check the authentication of the client to the server using each claimed authentication method. Test 1: For each claimed public-key authentication method, the evaluator shall configure the TOE 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 server to demonstrate the use of all claimed public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. **TD0636 has been applied.**
Test Steps	RSA-SHA2-256: • Generate a rsa-sha2-256 host key pair on the SSH server and note its fingerprint.

	• Upload the Public key into the TOE. • Initiate a connection from the TOE to the SSH server using the host public key and verify that the session is established. • Verify via logs that the SSH session was initiated successfully. • Verify via packet capture that the configured host key algorithm was used. RSA-SHA2-512: • Generate a rsa-sha2-512 host key pair on the SSH server and note its fingerprint. • Upload the Public key into the TOE. • Initiate a connection from the TOE to the SSH server using the host public key and verify that the session is established. • Verify via logs that the SSH session was initiated successfully. • Verify via packet capture that the configured host key algorithm was used.
Pass/Fail with Explanation	Pass. The TOE can establish a SSH session connection with the server successfully using the supported public key algorithms. This meets testing requirements.

6.5.2 FCS_SSHC_EXT.1.2 TEST #2 **[TD0636]**

Item	Data
Test Assurance Activity	Test objective: The purpose of these tests is to check the authentication of the client to the server using each claimed authentication method. Test 2: [Conditional] If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then following the guidance documentation the evaluator shall configure the TOE to perform password-based authentication with a remote SSH server to demonstrate that the TOE can successfully authenticate using a password as an authentication method. **TD0636 has been applied.**

Test Steps	• Initiate an SSH connection from the TOE to the remote SSH server through the Ciena site manager. • Verify the successful password-based authentication via logs. • Verify via packet capture that SSH session was established.
Pass/Fail with Explanation	Pass. The TOE is able to establish a successful SSH connection when the correct password is provided for password-based authentication. This meets the testing requirements.

6.5.3 FCS_SSHC_EXT.1.3 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Steps	• Use the acumen-sshc tool to send a larger packet of more than 32,768 bytes. • Connect to the TOE via SSH and verify large packets being sent to the TOE by the server. • Verify through logs that the packet was dropped. • Verify via packet capture that the packet is dropped.
Pass/Fail with Explanation	Pass. The TOE drops large packets that are received within an SSH session. This meets the testing requirements.

6.5.4 FCS_SSHC_EXT.1.4 TEST #1

Item	Data
Test Assurance Activity	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection.

	To verify this, the evaluator shall start session establishment for an SSH connection with a remote server (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.
Test Steps	• Initiate a SSH connection from the TOE to the non-TOE SSH server using all the claimed cipher. • Verify the successful SSH session was established via logs. • Verify the successful SSH session was established with only claimed ciphers via packet capture.
Pass/Fail with Explanation	Pass. The TOE is able to establish a SSH session with a non-TOE server successfully using only the claimed encryption algorithms. This meets the testing requirements.

6.5.5 FCS_SSHC_EXT.1.5 TEST #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate an SSH server to the TOE. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test objective: The purpose of this positive test is to check the authentication of the server by the client (when establishing the transport layer connection), and not for checking generation of the authentication message from the client (in the User Authentication Protocol). The evaluator shall therefore establish sufficient separate SSH connections (with an appropriately configured server) to cause the TOE to demonstrate use of all public key algorithms claimed in FCS_SSHC_EXT.1.5 in the ST.

Test Steps	RSA-SHA2-256: • Generate a rsa-sha2-256 host key pair on the SSH server and note its fingerprint. • Upload the Public key into the TOE. • Initiate a connection from the TOE to the SSH server using the host public key and verify that the session is established. • Verify via logs that the SSH session was initiated successfully. • Verify via packet capture that the configured host key algorithm was used. RSA-SHA2-512: • Generate a rsa-sha2-512 host key pair on the SSH server and note its fingerprint. • Upload the Public key into the TOE. • Initiate a connection from the TOE to the SSH server using the host public key and verify that the session is established. • Verify via logs that the SSH session was initiated successfully. • Verify via packet capture that the configured host key algorithm was used.
Pass/Fail with Explanation	Pass. The TOE supports a SSH session connection with each claimed public host-key algorithm.

6.5.6 FCS_SSHC_EXT.1.5 TEST #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall configure an SSH server to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the TOE to the SSH server and observe that the connection is rejected.

Test Steps	• Attempt to establish a SSH session from the TOE to the SSH server using the unsupported host public key algorithm. • Verify the connection is unsuccessful via logs. • Verify that the connection is refused via packet capture.
Pass/Fail with Explanation	Pass. The TOE does not support a SSH session initiation with unclaimed public host-key algorithm.

6.5.7 FCS_SSHC_EXT.1.6 TEST #1

Item	Data
Test Assurance Activity	Test 1: [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.
Test Steps	HMAC-SHA2-256 • Initiate a connection from the TOE to the SSH server . • Verify the successful ssh connection via log. • Verify via packet capture that SSH session was established.
Pass/Fail with Explanation	Pass. The TOE does support a SSH session initiation with claimed MAC algorithm. This meets the testing requirements.

6.5.8 FCS_SSHC_EXT.1.6 TEST #2

Item	Data
Test Assurance Activity	Test 2: [conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST] The evaluator shall configure an SSH server to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the TOE to the SSH server 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.
Test Steps	HMAC-SHA2-512 • Configure the SSH server for the supported MAC algorithm. • Initiate a connection from the TOE to the SSH server using HMAC-SHA2-512. • Verify the unsuccessful SSH connection via log. • Verify that the connection is refused via packet capture.
Pass/Fail with Explanation	Pass. The TOE does not support a SSH session initiation with unclaimed MAC algorithm. This meets the testing requirements.

6.5.9 FCS_SSHC_EXT.1.7 TEST #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall configure an SSH server to permit all allowed key exchange methods. The evaluator shall attempt to connect from the TOE to the SSH server using each allowed key exchange method and observe that each attempt succeeds.

Test Steps	ECDH-SHA2-NISTP256 • Establish an SSH session from the TOE to the SSH server with the supported key exchange algorithm (ecdh-sha2-nistp256). • Verify through logs that the connection was established. • Verify the successful connection via packet capture. ECDH-SHA2-NISTP384 • Establish an SSH session from the TOE to the SSH server with the supported key exchange algorithm (ecdh-sha2-nistp384) • Verify through logs that the connection was established. • Verify the successful connection via packet capture.
Pass/Fail with Explanation	Pass. The TOE is able to initiate a SSH session with the SSH server with the claimed key exchange algorithm. This meets the testing requirements.

6.5.10 FCS_SSHC_EXT.1.8 TEST #1T

Item	Data
Test Assurance Activity	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 the TOE to connect to an SSH server 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 server the TOE is connected to. 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).
Test Steps	• Authenticate to the TOE via the CLI using SSH on debug TCP port 28888. • On the TOE CLI, navigate to SFTP utilities menu. • Issue command: session_API_v2. • Issue command: 1_connect. • Input UserId, Password, IP Address and TCP Port for SSH Server. • At the moment one hour has elapsed, issue command: 4_ • Verify that a traffic based SSH rekey occurs on or before 1 hour of traffic is exchanged.
Pass/Fail with Explanation	Pass. The TOE correctly issues a rekey after the specified time period (1 hour) has been crossed. This meets the testing requirements.

6.5.11 FCS_SSHC_EXT.1.8 TEST #1B

Item	Data
Test Assurance Activity	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 traffic-based threshold the evaluator shall use the TOE to connect to an SSH server 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_SSHC_EXT.1.8).

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 server the TOE is connected to.

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:

1) An argument is present in the TSS section describing this hardware- based limitation and

	2) 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.
Test Steps	• Authenticate to the TOE via the CLI using SSH on debug TCP port 28888. • On the TOE CLI, navigate to SFTP utilities menu. • Input the remote path to file and local path to the >500 MB file. • Verify that a traffic-based SSH rekey occurs once 500 MB of traffic is exchanged.
Pass/Fail with Explanation	Pass. The TOE correctly issued a rekey once the data limit (500 MB) had exceeded the set threshold. This meets the testing requirement.

6.5.12 FCS_SSHC_EXT.1.9 TEST #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall delete all entries in the TOE's list of recognized SSH server host keys and, if selected, all entries in the TOE's list of trusted certification authorities. The evaluator shall initiate a connection from the TOE to an SSH server. The evaluator shall ensure that the TOE either rejects the connection or displays the SSH server's public key (either the key bytes themselves or a hash of the key using any allowed hash algorithm) and prompts the Security Administrator to accept or deny the key before continuing the connection.
Test Steps	• Execute the following commands to ensure host key validation is enabled and to delete all host key entries in the TOE's list of recognized SSH server host keys: DLT-SSH-HOSTKEY:::CTAG:::HOST=<IP_Address>; • Verify the TOE host key database is empty by executing the following command: RTRV-SSH-HOSTKEY:::1; • Attempt to initiate a connection from the TOE to the SSH server • Verify the connection failure via logs. • Verify that the connection is unsuccessful via packet capture

Pass/Fail with Explanation	Pass. The TOE rejects connections with external SSH servers for which server host keys are not trusted. This meets the testing requirements.

6.5.13 FCS_SSHC_EXT.1.9 TEST #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall add an entry associating a host name with a public key into the TOE's local database. The evaluator shall replace, on the corresponding SSH server, the server's host key with a different host key. If 'password-based' is selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using password-based authentication, shall ensure that the TOE rejects the connection, and shall ensure that the password was not transmitted to the SSH server (for example, by instrumenting the SSH server with a debugging capability to output received passwords). If 'password-based' is not selected for the TOE in FCS_SSHC_EXT.1.2, the evaluator shall initiate a connection from the TOE to the SSH server using public key-based authentication and shall ensure that the TOE rejects the connection.
Test Steps	• Load the SSH server hostkey into the TOE. • Verify that the ssh server hostkey is being uploaded in the TOE. • Change the SSH server hostkey pair without loading it into the TOE on the SSH server • Attempt SSH connection to the SSH server and verify the connection is refused by the TOE. • Verify the connection failure via logs and that the password was not transmitted • Verify the connection failure via packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects a connection to an SSH server when the host key does not match what was imported and password data is not transmitted to the SSH server. This meets the testing requirements.

6.6 TLSC

6.6.1 FCS_TLSC_EXT.1.1 TEST #1

Item	Data
Test Assurance Activity	Test 1: 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 Steps	• Configure the TOE to connect to the syslog server over TLS. TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ciphersuite. • Verify that the session was established with the chosen ciphersuite. TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ciphersuite. • Verify that the session was established with the chosen ciphersuite. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ciphersuite. • Verify that the session was established with the chosen ciphersuite.

	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ciphersuite. • Verify that the session was established with the chosen ciphersuite. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 ciphersuite. • Verify that the session was established with the chosen ciphersuite. TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 ciphersuite. • Verify that the session was established with the chosen ciphersuite. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ciphersuite. • Verify that the session was established with the chosen ciphersuite. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • Establish a TLS connection using the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 ciphersuite. • Verify that the session was established with the chosen ciphersuite.
Pass/Fail with Explanation	Pass: The TOE allows a connection with all claimed cipher suites. This meets testing requirements.

6.6.2 FCS_TLSC_EXT.1.1 TEST #2

Item	Data

Test Assurance Activity	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 Steps	Valid Certificate: • Create a server certificate with the Server Authentication in EKU. • Attempt a connection from the TOE to a TLS server using the certificate that contains the Server Authentication in EKU. • Verify that the TOE accepts the connection via packet capture. Invalid Certificate: • Create a server certificate that lacks the Server Authentication in EKU. • Attempt a connection from the TOE to a TLS server using the invalid certificate missing the Server Authentication in EKU. • Verify that the TOE rejects the connection via packet capture. • Verify that the TOE rejects the connection using invalid certificate via logs.
Pass/Fail with Explanation	Pass. The TOE allows a connection when the value of the extendedkeyusage field contains server authentication. The TOE does not make a connection when the value is changed to not contain server authentication. This meets the testing requirements.

6.6.3 FCS_TLSC_EXT.1.1 TEST #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall send a server certificate in the TLS connection that the 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 Steps	• Create an ECDSA server certificate. • Attempt a TLS connection from the TOE to the TLS Server using an EC certificate and RSA cipher and show the connection being unsuccessful. • Verify the unsuccessful connection with the packet capture. • Verify that a log is a generated indicating that connection was terminated.
Pass/Fail with Explanation	PASS. The TOE denies a connection when a server certificate does not match the server-selected cipher suite. This meets the testing requirements.

6.6.4 FCS_TLSC_EXT.1.1 TEST #4A

Item	Data
Test Assurance Activity	Test 4: The evaluator shall perform the following 'negative tests': a) The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Test Steps	• Attempt a connection to the server using the TLS_NULL_WITH_NULL_NULL ciphersuite using acumen-tlsc tool and verify that it fails. • Verify that the TOE denies the connection using packet capture. • Verify connection failure with logs.
Pass/Fail with Explanation	PASS. Client successfully denies the connection with TLS_NULL_WITH_NULL_NULL cipher-suite selected from the server. This meets the testing requirements.

6.6.5 FCS_TLSC_EXT.1.1 TEST #4B

Item	Data
Test Assurance Activity	Test 4: The evaluator shall perform the following 'negative tests': b) 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 Steps	• Attempt a connection from the TOE to a remote TLS server using acumen-tlsc tool to modify the server's ciphersuite to one which is not present in the Client Hello. • Verify connection failure with packet capture. • Verify connection failure with logs.
Pass/Fail with Explanation	Pass. The TOE rejects the connection with wrong cipher by sending a Fatal Alert. This meets the testing requirements.

6.6.6 FCS_TLSC_EXT.1.1 TEST #4C

Item	Data
Test Assurance Activity	Test 4: The evaluator shall perform the following 'negative tests': c) [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 Steps	• Use 'acumen-tlsc' tool to configure the server to perform a connection with an unsupported curve/group • Verify via packet capture that the TOE disconnects after receiving the server's key exchange handshake message. • Verify the connection failure with logs.

Pass/Fail with Explanation	Pass. When configured the server to perform an ECDHE key exchange in the TLS connection using a non-supported curve the connection fails. This meets the requirements.

6.6.7 FCS_TLSC_EXT.1.1 TEST #5A

Item	Data
Test Assurance Activity	Test 5: The evaluator performs the following modifications to the traffic: 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 Steps	• Using acumen-tlsc tool, attempt a connection to a remote TLS server using a non-supported TLS version and verify that the TOE rejects the connection. • Verify the connection fails with packet capture. • Verify the connection failure with logs when connecting with TLSv1.0
Pass/Fail with Explanation	Pass. The connection fails due to unsupported TLS version. This meets the test requirements.

6.6.8 FCS_TLSC_EXT.1.1 TEST #5B

Item	Data
Test Assurance Activity	Test 5: The evaluator performs the following modifications to the traffic:

	a) [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 Steps	• Attempt a connection from the TOE to a remote TLS server using acumen-tlsc tool that would allow the server's signature block to be modified. Verify that the connection fails. • Verify the connection failure with packet capture. • Verify the connection failed with logs.
Pass/Fail with Explanation	Pass. The connection fails due to the modified block in the Server Key Exchange message. This meets the test requirement.

6.6.9 FCS_TLSC_EXT.1.1 TEST #6A

Item	Data
Test Assurance Activity	Test 6: The evaluator performs the following 'scrambled message tests': a) Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Attempt a connection to a modified TLS Server using acumen-tlsc tool to modify a byte in the Server Finished handshake message. Verify that the connection fails. • Verify the failed connection via packet capture. • Verify via logs that the connection fails.
Pass/Fail with Explanation	Pass. The connection is not completed when bytes were modified in server finish message. This meets the test requirements.

6.6.10 FCS_TLSC_EXT.1.1 TEST #6B

Item	Data
Test Assurance Activity	Test 6: The evaluator performs the following 'scrambled message tests': b) 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 Steps	• Attempt a connection to a modified TLS server using acumen-tlsc that would allow sending a garbled message from the server after the server issues the ChangeCipherSpec message and verify that the TOE rejects the connection. • Verify failure with packet capture. • Verify connection failure with logs.
Pass/Fail with Explanation	Pass. The TOE closes the connection after receiving garbled data after the ChangeCipherSpec message. This meets the test requirements.

6.6.11 FCS_TLSC_EXT.1.1 TEST #6C

Item	Data
Test Assurance Activity	Test 6: The evaluator performs the following 'scrambled message tests': a) 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 ciphersuite) or that the server denies the client's Finished handshake message.
Test Steps	• Attempt a connection to a modified TLS server using acumen-tlsc that would allow sending a modified nonce from the server and verify that the TLS handshake with the TOE fails. • Verify failure with packet capture. • Verify failure with logs.

Pass/Fail with Explanation	Pass. The connection was rejected due to a modified nonce. This meets the test requirements.

6.6.12 FCS_TLSC_EXT.1.2 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 1 [conditional]: 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.
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or*

	b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable or *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	Note: When the node certificate only contains CN and missing SAN extension, The hostname should be populated with the reference identifier in syslog configuration setting of the TOE. (Applicable for IPV4/IPV6/FQDN) CN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing invalid CN and missing SAN extension. • Establish a TLS connection with the syslog server using above server certificate with acumen-tlsc tool and verify the connection failure. • Verify the connection failure logs on the device. • Verify the unsuccessful connection due to invalid CN in the packet capture. CN as IPv6:

	• Configure the TOE for reference identifier name as IPV6. • Configure the Server certificate showing invalid CN and missing SAN extension. • Establish a TLS connection with the syslog server using the above server certificate with acumen-tlsc tool and verify the connection failure. • Verify the connection failure logs on the device. • Verify the unsuccessful connection due to invalid CN in the packet capture. CN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing invalid CN. • Configure the Server certificate showing no SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify the connection failure logs on the device which state certificate verify failed. • Verify the unsuccessful connection due to invalid CN in a packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates with an invalid CN and No SAN.

6.6.13 FCS_TLSC_EXT.1.2 TEST #2

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 2 [conditional]: 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 (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.
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	CN and SAN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing valid CN but invalid SAN. • Initiate the connection from the TOE to the TLS Server and verify that the connection fails.

	• Verify the connection failure logs on the device. • Verify the unsuccessful connection due to invalid SAN but the CN matches with the reference identifier in a packet capture. CN and SAN as IPV6: • Configure the TOE for reference identifier name as IPV6 • Configure the Server certificate showing valid CN but invalid SAN. • Initiate the connection from the TOE to the TLS Server and verify that the connection fails. • Verify the connection failure logs on the device. • Verify the unsuccessful connection due to invalid SAN but the CN matches with the reference identifier in a packet capture. CN and SAN as FQDN: • Configure the TOE for reference identifier name ass FQDN. • Configure the Server certificate showing valid CN. • Configure the Server certificate showing invalid SAN. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which state certificate verify failed. • Verify the unsuccessful connection due to invalid SAN but the CN matches with the reference identifier in a packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates with a good CN and bad SAN using FQDN, IPv4 and IPv6. This meets the testing requirements

6.6.14 FCS_TLSC_EXT.1.2 TEST #3

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection:

	Test 3 [conditional]: 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.
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*

Test Steps	Note: When the node certificate only contains CN and missing SAN extension, The hostname should be populated with the reference identifier in syslog configuration setting of the TOE. (Applicable for IPV4/IPV6/FQDN) CN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing valid CN and missing SAN extension. • Establish a TLS connection with the syslog server and verify the connection. • Verify the Successful connection due to valid CN in the packet capture. CN as IPv6: • Configure the TOE for reference identifier name as IPV6. • Configure the Server certificate showing valid CN and missing SAN extension. • Establish a TLS connection with the syslog server and verify the connection. • Verify the successful connection due to valid CN in the packet capture. CN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing valid CN and missing SAN extension. • Configure the Server certificate showing no SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify the successful connection due to invalid CN in a packet capture.
Pass/Fail with Explanation	Pass. The TOE accepts the connection when the certificate with valid CN and no SAN is presented using FQDN, IPv4 and IPv6. This meets testing requirements.

6.6.15 FCS_TLSC_EXT.1.2 TEST #4

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 4 [conditional]: 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).
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.*

	IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.
Test Steps	CN and SAN as IPV4: • Configure the TOE for reference identifier as IPv4 address. • Configure the Server certificate having invalid CN but a valid SAN extension. • Establish a connection with the TOE over TLS and verify that the connection succeeds. • Verify the successful connection due to SAN matching the reference identifier on the TOE despite an invalid CN in a packet capture CN and SAN as IPV6: • Configure the TOE for reference identifier as IPv6 address. • Configure the Server certificate having invalid CN but a valid SAN extension. • Establish a connection with the TOE over TLS and verify that the connection succeeds. • Verify the successful connection due to SAN matching the reference identifier on the TOE despite an invalid CN in a packet capture CN and SAN as FQDN: • Configure the TOE for reference identifier as FQDN. • Configure the Server certificate having invalid CN but a valid SAN extension. • Establish a connection with the TOE over TLS and verify that the connection succeeds. • Verify the successful connection due to SAN matching the reference identifier on the TOE despite an invalid CN in a packet capture
Pass/Fail with Explanation	Pass. The TOE accepts the connection when the certificate with an invalid CN and valid SAN is presented using FQDN, IPv4 and IPv6. This meets testing requirements.

6.6.16 FCS_TLSC_EXT.1.2 TEST #5 (1)

Item	Data

Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): 1) 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.
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.*

	• *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	CN: • Configure the TOE for the correct reference identifier. • Configure the node certificate showing a wildcard that is not in the left-most label of CN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture. SAN: • Configure the TOE for the correct reference identifier. • Configure the node certificate showing a wildcard that is not in the left-most label of SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. TOE rejects the connection when the reference identifier does not match the presented wildcard which is not in the leftmost label. This meets the testing requirements.

6.6.17 FCS_TLSC_EXT.1.2 TEST #5 (2)(A)

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection:

	Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): 1) 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, if wildcards are supported, or fails if wildcards are not supported. (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.)
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:*

	• *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* • *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	CN: • Configure the TOE for the reference identifier with a single left-most label. • Configure the node certificate showing wildcard in the leftmost label in CN. • Establish a connection with the TOE over TLS and verify the successful connection. • Verify the error logs on the device • Verify the successful connection via packet capture. SAN: • Configure the TOE for the reference identifier with a single left-most label. • Configure the node certificate showing wildcard in the leftmost label in SAN. • Establish a connection with the TOE over TLS and verify the successful connection. • Verify the error logs on the device • Verify the successful connection via packet capture.
Pass/Fail with Explanation	PASS. TOE successfully establishes TLS when a certificate presented left-most wildcard on CN or SAN identifier. This meets the testing requirements.

6.6.18 FCS_TLSC_EXT.1.2 TEST #5 (2)(B)

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection:

	Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): 2) 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 without a left-most label as in the certificate (e.g. example.com) 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.)
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.*

	IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules: • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* • *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	CN: • Configure the TOE for the reference identifier without a leftmost label. • Configure the node certificate showing wildcard in the leftmost label in CN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device due to CN mismatch. • Verify the unsuccessful connection with packet capture. SAN: • Configure the TOE for the reference identifier without a leftmost label. • Configure the node certificate showing wildcard in the leftmost label in SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device due to SAN and reference identifier mismatch. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TLS connections are unsuccessful when presenting a server certificate containing a wildcard in the left-most label after configuring the reference identifier without a left-most label. This meets the testing requirements.

6.6.19 FCS_TLSC_EXT.1.2 TEST #5 (2)(C)

Item	Data

Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 5 [conditional]: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): 2) 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 two left-most labels (e.g. bar.foo.example.com) 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.)
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.*

	IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules: • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	CN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the node certificate showing wildcard in the leftmost label in CN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the TOE, showing CN mismatched. • Verify the unsuccessful connection via packet capture. SAN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the node certificate showing wildcard in the leftmost label in SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the TOE, showing SAN mismatched. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	PASS. TOE rejects TLS communication if server presented with a certificate which has invalid CN/SAN wildcard. This meets the testing requirements.

6.6.20 FCS_TLSC_EXT.1.2 TEST #6 **[TD0790]**

Item	Data

Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Objective: The objective of this test is to ensure the TOE is able to differentiate between IP address identifiers that are not allowed to contain wildcards and other types of identifiers that may contain wildcards. Test 6: [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). 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. **TD0790 has been applied.**
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.*

	or *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Test Steps	IPv4: • Configure the TOE for the correct reference identifier. • Create a server certificate with a CN that matches the reference identifier but replace one of the groups with an * and no SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the certificate validation failure logs on the device. • Verify the unsuccessful connection with packet capture. IPv6: • Configure the TOE for the correct reference identifier.

	• Create a server certificate with a CN that matches the reference identifier but replace one of the groups with an * and no SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the certificate validation failure logs on the device. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	PASS. TOE rejects TLS connection if server presented its certificate's CN field that contains * in its IP address group. This meets the testing requirements.

6.6.21 FCS_TLSC_EXT.1.2 TEST #7A

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 7 [conditional]: If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):i a) The evaluator shall present a server certificate that does not contain an identifier in the Subject (DN) attribute type(s) that matches the reference identifier. The evaluator shall verify that the connection fails.

Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Pass/Fail with Explanation	N/A. This is not applicable as 'the secure channel is not used for FPT_ITT, and RFC 5280' is not selected in ST.

6.6.22 FCS_TLSC_EXT.1.2 TEST #7B

Item	Data

Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 7 [conditional]: If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):i b) The evaluator shall present a server certificate that contains a valid identifier as an attribute type other than the expected attribute type (e.g. if the TOE is configured to expect id-at-serialNumber=correct_identifier, the certificate could instead include id-at-name=correct_identifier), and does not contain the SAN extension. The evaluator shall verify that the connection fails. 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 this test.
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.*

	IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules: • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Pass/Fail with Explanation	N/A. This is not applicable as 'the secure channel is not used for FPT_ITT, and RFC 5280' is not selected in ST.

6.6.23 FCS_TLSC_EXT.1.2 TEST #7C

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 7 [conditional]: If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):i

	c) The evaluator shall present a server certificate that contains a Subject attribute type that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds.
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *d) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *e) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *f) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.* *IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules:* • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Pass/Fail with Explanation	N/A, FPT_ITT is not selected in the ST.

6.6.24 FCS_TLSC_EXT.1.2 TEST #7D

Item	Data
Test Assurance Activity	The evaluator shall configure the reference identifier according to the AGD guidance and perform the following tests during a TLS connection: Test 7 [conditional]: If the secure channel is used for FPT_ITT, and RFC 5280 is selected, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier):i d) The evaluator shall confirm that all use of wildcards results in connection failure regardless of whether the wildcards are used in the left or right side of the presented identifier. (Remark: Use of wildcards is not addressed within RFC 5280.)
Notes	*Note that the following tests are marked conditional and are applicable under the following conditions:* *a) For TLS-based trusted channel communications according to FTP_ITC.1 where RFC 6125 is selected, tests 1-6 are applicable.* *or* *b) For TLS-based trusted path communications according to FTP_TRP where RFC 6125 is selected, tests 1-6 are applicable* *or* *c) For TLS-based trusted path communications according to FPT_ITT.1 where RFC 6125 is selected, tests 1-6 are applicable. Where RFC 5280 is selected, only test 7 is applicable.* *Note that for some tests additional conditions apply.*

	IP addresses are binary values that must be converted to a textual representation when presented in the CN of a certificate. When testing IP addresses in the CN, the evaluator shall follow the following formatting rules: • *IPv4: The CN contains a single address that is represented a 32-bit numeric address (IPv4) is written in decimal as four numbers that range from 0-255 separated by periods as specified in RFC 3986.* *IPv6: The CN contains a single IPv6 address that is represented as eight colon separated groups of four lowercase hexadecimal digits, each group representing 16 bits as specified in RFC 4291. Note: Shortened addresses, suppressed zeros, and embedded IPv4 addresses are not tested.*
Pass/Fail with Explanation	N/A. This is not applicable as 'the secure channel is not used for FPT_ITT, and RFC 5280' is not selected in ST.

6.6.25 FCS_TLSC_EXT.1.3 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows: Test 1: 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.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FIA_X509_EXT.1.1/Rev Test #1a to demonstrate correct operation.

6.6.26 FCS_TLSC_EXT.1.3 TEST #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows: Test 2: 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 Steps	• 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.
Pass/Fail with Explanation	Pass. The test case was performed in the following test cases: FIA_X509_EXT_1.1 Test#1b (broken chain), FIA_X509_EXT_1.1 Test#2 (expired certificate) , FCS_TLSC_EXT.1.2 (failed matching of reference identifier) and FIA_X509_EXT_1.1 Test #3 (Revoked certificate) Please refer to the test cases mentioned.

6.6.27 FCS_TLSC_EXT.1.3 TEST #3

Item	Data

Test Assurance Activity	The evaluator shall demonstrate that using an invalid certificate results in the function failing as follows: Test 3 [conditional]: The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. If any override mechanism is defined for failed certificate validation, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
Pass/Fail with Explanation	N/A, ST does not claim the implementation of any administrator override mechanism.

6.6.28 FCS_TLSC_EXT.1.4 TEST #1

Item	Data
Test Assurance Activity	Test 1 [conditional]: 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 Steps	• Initiate the connection from the TOE to the TLS Server using acumen-tlsc tool, specifying the curve secp256r1 and verify the successful connection. • Verify with packet capture that the used curve is secp256r1. • Initiate the connection from the TOE to the TLS Server using acumen-tlsc tool, specifying the curve secp384r1. Verify the successful connection. • Verify with packet capture that the used curve is secp384r1. • Initiate the connection from the TOE to the TLS Server using acumen-tlsc tool, specifying the curve secp521r1. Verify the successful connection. • Verify with packet capture that the used curve is secp521r1.

Pass/Fail with Explanation	Pass. The TOE accepted a connection when supported curves were introduced. This meets the test requirements.

6.7 UPDATE

6.7.1 FPT_TST_EXT.1 TEST #1

Item	Data
Test Assurance Activity	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. Although formal compliance is not mandated, the self-tests performed should aim for a level of confidence comparable to: a) [FIPS 140-2], chap. 4.9.1, Software/firmware integrity test for the verification of the integrity of the firmware and executable software. Note that the testing is not restricted to the cryptographic functions of the TOE. b) [FIPS 140-2], chap. 4.9.1, Cryptographic algorithm test for the verification of the correct operation of cryptographic functions. Alternatively, national requirements of any CCRA member state for the security evaluation of cryptographic functions should be considered as appropriate. 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 Steps	• Restart the TOE. • Verify the OS version of the TOE. • Verify self-tests (Cryptographic algorithm known answer tests, pair-wise consistency tests, continuous random number generator tests, SP 800-90B health tests, software integrity check) are run after the TOE restarts. • Verify the TOE's correct operation of the cryptographic functions necessary to fulfil any of the SFRs by generating an SSH Key
Pass/Fail with Explanation	Pass. The TOE successfully executes self-test. This meets the testing requirement.

6.7.2 FPT_TUD_EXT.1 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 1: 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 (for this test the TOE shall be in a state where these two versions match). 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. 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.

	The evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates). For distributed TOEs the evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all TOE components.
Test Steps	• Authenticate to the TOE via SSH. • Execute the following commands to show the current running TOE software version: RTRV-SW-VER:::CTAG; • Fetch the legitimate update by executing the following command: DLVR-RELEASE:6500A-SPAP3::CTAG::REL1560Z.PJ:MINIMAL=Y,,URL="SFTP://cienatest:Procurer1-Moustache# Prior&@10.41.79.200/home/cienatest/images",,,PID=PASSWORD1,,,,,,; • Once the update has been fully fetched, execute the following command to load it into flash memory: LOAD-UPGRD:::CTAG::REL1560Z:PJ:ALRMS=N; • Confirm the current running version did not change, but that the most recently installed TOE software version increased. • Execute the following command to install the new load on the shelf processor: INVK-UPGRD:::CTAG; • Authenticate to the TOE via SSH. • Execute the following command again to install the new load on all the line cards: INVK-UPGRD:::CTAG; • Execute the following command to commit the upgrade: CMMT-UPGRD:6500A-SPAP3::CTAG; • Execute again the following command to confirm that both the current running version and most recently installed TOE software version increased: RTRV-RELEASE:::CTAG; and RTRV-SW-VER:::CTAG; • Verify the upgradation logs on device.
Pass/Fail with Explanation	PASS. TOE successfully installed new version of software image. This meets the testing requirements.

6.7.3 FPT_TUD_EXT.1 TEST #2 (A)

Item	Data

Test Assurance Activity	The evaluator shall perform the following tests: Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). 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 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.j The evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates). For distributed TOEs the evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all TOE components.
Test Steps	• Authenticate to the TOE via SSH. • Execute the following commands to output the current running and most recently installed TOE software version: RTRV-RELEASE:::CTAG; and RTRV-SW-VER:::CTAG; • Using a Hex editor modify an otherwise good firmware image. • Fetch the illegitimate update (hex modified) by executing the following command: DLVR-RELEASE:6500A-SPAP3::CTAG::REL1560Z.OB:MINIMAL=Y,,URL="SFTP://cienatest:Procurer1-Moustache# Prior&@10.41.79.200/home/cienatest/images",,,PID=PASSWORD2,,,,,,; • Verify the corrupt file does not get uploaded. • Verify software upgrade failed logs generated on TOE. • Verify that the currently running and most recently installed TOE software version did not change.

Pass/Fail with Explanation	PASS. TOE rejects the installation of corrupted image signature. This meets the testing requirements.

6.7.4 FPT_TUD_EXT.1 TEST #2 (B)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). 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) An image that has not been signed 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.

	The evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates). For distributed TOEs the evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all TOE components.
Test Steps	• Authenticate to the TOE via SSH. • Execute the following commands to output the current running and most recently installed TOE software version: RTRV-RELEASE:::CTAG; and RTRV-SW-VER:::CTAG; • Using a Hex editor modify an otherwise good firmware image. • Fetch the illegitimate update (no signature) by executing the following command:DLVR-RELEASE:6500A-SPAP3::CTAG::REL1560Z.OC:MINIMAL=Y,,URL="SFTP://cienatest:Procurer1-Moustache#-Prior&@10.41.79.200/home/cienatest/images",,,PID=PASSWORD2,,,,,,; • Verify that the installation fails in the TOE due to missing signature file. • Verify that the currently running and most recently installed TOE software version did not change.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image was not signed and rejected the image. This meets the testing requirements.

6.7.5 FPT_TUD_EXT.1 TEST #2 (C)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). 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) 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) 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. The evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates). For distributed TOEs the evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all TOE components.
Test Steps	• Authenticate to the TOE via SSH. • Execute the following commands to output the current running and most recently installed TOE software version: RTRV-RELEASE:::CTAG; and RTRV-SW-VER:::CTAG; • Using a Hex editor modify an image signature. • Fetch the illegitimate update (invalid signature) by executing the following command: DLVR-RELEASE:6500A-SPAP3::CTAG::REL1560Z.OD:MINIMAL=Y,,URL="SFTP://cienatest:Procurer1-Moustache#-Prior&@10.41.79.200/home/cienatest/images",,,PID=PASSWORD2,,,,,,; • Verify that the installation fails in the TOE due to invalid signature. • Verify that the currently running and most recently installed TOE software version did not change.
Pass/Fail with Explanation	PASS. TOE rejects installation of new software image that has invalid signature. This meets the testing requirements.

6.7.6 FPT_TUD_EXT.1 TEST #3 (A)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 3 [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted. If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is 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. 1) The evaluator obtains or produces an illegitimate update such that the hash of the update does not match the published hash. The evaluator provides the published hash value to the TOE and calculates the hash of the update either on the TOE itself (if that functionality is provided by the TOE), or else outside the TOE. The evaluator confirms that the hash values are different, and attempts to install the update on the TOE, verifying that this fails because of the difference in hash values (and that the failure is logged). Depending on the implementation of the TOE, the TOE might not allow the Security Administrator to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE If the TOE allows 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 the attempted update is rejected, the most recently installed version might or might not be updated. 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.

	If the verification of the hash value over the update file(s) against the published hash is not performed by the TOE, Test 3 shall be skipped. The evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates). For distributed TOEs the evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all TOE components.
Pass/Fail with Explanation	N/A, The TOE does not perform the verification of the hash value over the update file(s) against the published hash.

6.7.7 FPT_TUD_EXT.1 TEST #3 (B)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests: Test 3 [conditional]: If the TOE itself verifies a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE, the following test shall be performed (otherwise the test shall be omitted. If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is 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. 2) The evaluator uses a legitimate update and tries to perform verification of the hash value without providing the published hash value to the TOE. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the verification of the hash value without providing a hash value to the TOE, e.g. if the hash value needs to be handed over to the TOE as a parameter in a command line message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the

	mechanism that prevents the execution of this check shall be tested accordingly, e.g. that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE If the TOE allows 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 the attempted update is rejected, the most recently installed version might or might not be updated. 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.a If the verification of the hash value over the update file(s) against the published hash is not performed by the TOE, Test 3 shall be skipped. The evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all methods supported (manual updates, automatic checking for updates, automatic updates). For distributed TOEs the evaluator shall perform Test 1, Test 2 and Test 3 (if applicable) for all TOE components.
Pass/Fail with Explanation	N/A, The TOE does not perform the verification of the hash value over the update file(s) against the published hash.

6.8 X509-REV

6.8.1 FIA_X509_EXT.1.1/REV TEST #1A

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hhTest 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one 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 root CA certificate in the trust store).
Test Steps	• Configure TOE to connect to the TLS server. • Create a full chain of certificates to connect to the TOE. • Upload a complete certificate validation chain to the TOE. • Establish a connection with the TOE over TLS and verify the successful connection. • Verify the successful connection with packet capture
Pass/Fail with Explanation	Pass. The TOE can make a successful connection when a complete certificate trust chain is present. This meets the test requirements.

6.8.2 FIA_X509_EXT.1.1/REV TEST #1B

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perf rm the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:rTest 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
Test Steps	• Remove the ICA certificate from the TOE's certificate chain. • Establish a connection with the TOE over TLS and verify the connection. • Verify the connection failure via logs. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects the connection when an incomplete certificate trust chain is present. This meets the test requirements.

6.8.3 FIA_X509_EXT.1.1/REV TEST #2

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hTest 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps	• Create a server certificate that is expired. • Show the clock on the TOE.

	• Attempt to connect from the TOE with an expired server certificate and verify that it fails. • Verify the failure logs on the device, showing connection is not established due to expired certificate. • Verify the connection is unsuccessful via packet capture.
Pass/Fail with Explanation	Pass. A connection including an expired certificate was rejected. This meets the test requirements.

6.8.4 FIA_X509_EXT.1.1/REV TEST #3

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hhTest 3: 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. hRevocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.
Test Steps	• Enable OCSP checking on the TOE • Create server certificate with URI of the OCSP responder. • Create a CA and ICA certificate with OCSP Signing enabled. • Import the CA certificate on the TOE.

	• Verify that all certificates are valid. • Attempt to connect with the TOE. • Verify with the OCSP responder. • Verify the successful connection logs on the TOE. • Verify the successful connection with packet capture. Revoked End Entity Certificate: • Revoke the server certificate. • Verify that the database shows that the server certificate is revoked. • Attempt a connection with the TOE and verify that it fails. • Verify with the OCSP responder that the certificate is revoked. • Verify the failure logs on the TOE showing validation failed due revoked certificate. • Verify the unsuccessful connection with packet capture. Revoked Intermediate CA Certificate: • Revoke the intermediate certificate. • Verify that the database shows that the certificate is revoked. • Attempt a connection with the TOE and verify that it fails. • Verify with the OCSP responder that the certificate is revoked. • Verify the failure logs on the TOE showing validation failed due revoked certificate. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects connections that use revoked certificates and allows connections when the certificates are valid. This meets the testing requirements.

6.8.5 FIA_X509_EXT.1.1/REV TEST #4

Item	**Data**

Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hTest 4: 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 Steps	• Generate a certificate that does NOT have OCSP signing EKU. • Use this certificate in the OCSP responder. • Verify the unsuccessful TLS connection with the help of packet capture. • Verify validation of certificate is failed as CA certificate doesn't have OCSP signing EKU via TOE logs.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the Signer certificate in OCSP is invalid and does not have a signing purpose. This meets the testing requirements.

6.8.6 FIA_X509_EXT.1.1/REV TEST #5

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hhTest 5: 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 Steps	• Start the server using the acumen-tlsc-v2.2e tool with a modified byte within the first 8 bytes of the certificate, the connection should fail. • Verify the error logs on the TOE showing failure due to the wrong tag. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the test requirements.

6.8.7 FIA_X509_EXT.1.1/REV TEST #6

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hTest 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 Steps	• Start the server using the acumen-tlsc-v2.2e tool with a modified byte in the signatureValue field of the certificate. • Verify the error with logs on the device showing certificate signature failure. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the byte in the certificate signatureValue field is modified. This meets the test requirements.

6.8.8 FIA_X509_EXT.1.1/REV TEST #7

Item	Data
Test Assurance Activity	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. 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 selftesting is selected). The evaluator shall perform the following tests for FIA_X509_EXT.1/Rev. These tests must be repeated for each distinct security function that utilizes X.509v3 certificates. For example, if the TOE implements certificate-based authentication with IPSEC and TLS, then it shall be tested with each of these protocols:hTest 7: 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 Steps	• Start the server using the acumen-tlsc-v2.2e tool with the modified public key in the certificate. • Initiate a connection to the acumen-tls server • Verify the error logs on the device showing certificate signature failure. • Verify the unsuccessful connection with packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects connections when any byte in the public key of the certificate is modified. This meets the test requirements.

6.8.9 FIA_X509_EXT.1.1/REV TEST #8A **[TD0527]**

Item	Data
Test Assurance Activity	**(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** Test 8a: 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.v **TD0527 (12/1 Update) has been applied.**
Test Steps	• Show the EC root CA certificate. • Show the EC intermediate CA certificate. • Show the EC node certificate. • Configure the TOE for the root certificate as a trust anchor. • Concatenate the CA certificates. • Establish a connection with the TOE over TLS. • Verify the successful connection with packet capture.
Pass/Fail with Explanation	Pass. The evaluator verified the trusted chain of the EC leaf certificate, EC intermediate certificate and EC root certificate and observed that the connection was successful. This meets the test requirements.

6.8.10 FIA_X509_EXT.1.1/REV TEST #8B **[TD0527]**

Item	Data
Test Assurance Activity	**(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** Test 8b: 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.f

	TD0527 (12/1 Update) has been applied.
Test Steps	• In the second part of the test, the Intermediate certificate is modified with a named curve with an explicit format in the public key information field and is loaded on the TLS server. • Concatenate the CA certificates. • Configure the TOE for the root certificate as a trust anchor. • Attempt the connection from the TOE to the TLS Server. • Verify the failure logs on the device showing certificate validation failed. • Verify the unsuccessful connection via packet capture.
Pass/Fail with Explanation	Pass. The evaluator verified that when the public key information is modified in the intermediate certificate on the TLS server, TOE is unable to make a successful connection. This meets the test requirements.

6.8.11 FIA_X509_EXT.1.1/REV TEST #8C **[TD0527]**

Item	Data
Test Assurance Activity	**(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** 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.t **TD0527 (12/1 Update) has been applied**.

Test Steps	• Show the EC intermediate CA certificate. • Attempt to add the modified Intermediate certificate on the TOE. • Verify that the TOE accepts the certificate. • In the third part of the test Intermediate certificate is modified with an explicit format in the public key information field and is loaded on the TOE. • Attempt to add the modified Intermediate certificate on the TOE. • Verify that the TOE discards the certificate. • Verify error logs on the device showing the ICA certificate has an invalid public key
Pass/Fail with Explanation	Pass. The evaluator verified when a certificate is loaded that is signed by a trusted CA and the elliptic curve parameters are specified as a named curve, the certificate is accepted. The evaluator also verified that when the public key information is modified in the intermediate certificate to use an explicit version of the elliptic curve and is loaded to the TOE's trust store, TOE does not accept such a certificate. This meets the testing requirements.

6.8.12 FIA_X509_EXT.1.2/REV TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for FIA_X509_EXT.1.2/Rev. The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where 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) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation).

	For each of the following tests the evaluator shall create a chain of at least three certificates: a self-signed root CA certificate, an intermediate CA certificate and a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). 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). The evaluator shall repeat these tests for each distinct use of certificates. Thus, for example, use of certificates for TLS connection is distinct from use of certificates for trusted updates so both of these uses would be tested. But there is no need to repeat the tests for each separate TLS channel in FTP_ITC.1 and FTP_TRP.1/Admin (unless the channels use separate implementations of TLS).
Test Steps	• Create an ICA with no basicConstraint. • Upload ICA certificate to the TOE. • Verify that the TOE discards the certificate. • Verify the error in logs on the device showing the certificate rejected due to basic constraint failure.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that do not contain the basicConstraints extension. This meets the test requirements.

6.8.13 FIA_X509_EXT.1.2/REV TEST #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for FIA_X509_EXT.1.2/Rev. The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where 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) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: a self-signed root CA certificate, an intermediate CA certificate and a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). 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). The evaluator shall repeat these tests for each distinct use of certificates. Thus, for example, use of certificates for TLS connection is distinct from use of certificates for trusted updates so both of these uses would be tested. But there is no need to repeat the tests for each separate TLS channel in FTP_ITC.1 and FTP_TRP.1/Admin (unless the channels use separate implementations of TLS).
Test Steps	• Modify the CA certificate with the flag in the basicConstraints extension set to FALSE using the x509-mod tool. • Verify that the basic constraints extension is set to FALSE. • Attempt to load the certificate onto the TOE. • Verify that the TOE discards the certificate. • Verify the error in logs on the device showing the certificate rejected due to basic constraint failure.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that has the CA flag in the basicConstraints extension set to FALSE. This meets the test requirements.

6.8.14 FIA_X509_EXT.2 TEST #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: 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.
Test Steps	• Configure the certificates showing the OCSP distribution point. • Manipulate the Environment so that TOE is unable to validate the certificate from the OCSP server. • Attempt the connection from the TOE to the TLS server and show the connection being unsuccessful. • Verify via the logs on TOE. • Verify via the packet capture.
Pass/Fail with Explanation	Pass. The TOE rejects certificates if it cannot verify via OCSP when the responder is down. There is no administrator override mechanism. This meets the testing requirements.

7 CONCLUSION

The testing shows that all test cases required for conformance have passed testing.