Assurance Activity Report for
Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4

Version 0.5

Symantec Edge Secure Web Gateway (SWG) with SGOS v7.4
Security Target
Version 1.0

collaborative Protection Profile for Network Devices
Version 2.2e

Evaluated by:

Wing-A, Ground Floor, Beta Building, Unit No.3, i Think Techno Campus,
Kanjurmarg East, Mumbai 400 042

Prepared for:
Indian Common Criteria Certification Scheme (IC3S)

The Developer of the TOE:
Symantec Corporation

The Author of the Security Target:
Symantec Corporation

The TOE Evaluation was Sponsored by:
Symantec Corporation

Evaluation Personnel:
Varsha Shetye
Yogesh Pawar
Yogita Kore

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	01/08/2022	Initial Release
0.2	14/04/2023	Updated after peer review
0.3	09/06/2023	Updated after lead review
0.4	16/06/2023	Updated after lead review
0.5	11/08/2023	Updated after Test Report changes

Table of Contents

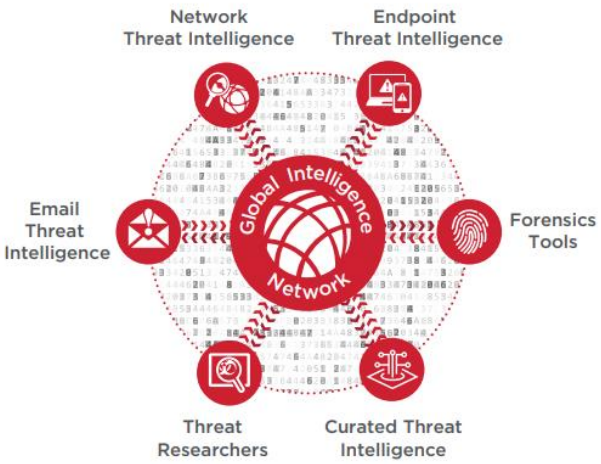
1 TOE Overview

The TOE is the Symantec Edge SWG running SGOS software version 7.4. The Symantec Edge SWG is not tied to any specific hardware. The TOE type is a network device. The purpose of the TOE is to provide a layer of security between an Internal and External Network (typically an office network and the Internet). The TOE allows administrators to create and manage configurable policies on controlled protocol traffic to and from the Internal Network users. A policy may include authentication, authorization, content filtering, and auditing.

The Edge SWG appliances from Symantec provide companies the ability to deploy a scalable proxy-based security solution to protect their organization against advanced threats. The Edge SWG acts as gateway between web users and the Internet: a single point where all web traffic can be monitored and corporate policies for web use can be enforced. This strategic position makes the Edge SWG a natural place to build in additional network security technologies that defend against a very wide range of cybercrimes, malware, and phishing.
The Edge SWG offers the following features.

- High-speed decryption and re-encryption of SSL/TLS traffic, so attackers cannot use encryption to conceal malware or command and control traffic into and out of the corporate network
- Universal Policy Enforcement (UPE) from Symantec allows organizations to enforce acceptable web use policies for employees who connect through the Edge SWG. Symantec allows you to centralize your policy creation, maintenance, and installation for simplified, unified administration.
- Out of the box protection - Recommended, strong, and maximum policies crafted by security experts.
- Immediate protection with the broadest advanced threat integrations
- Direct cloud application visibility and real-time controls
- Unmatched performance and reliability
- Logs and reports on how users connect to websites.
- Strong user authentication can be incorporated into the policies, supporting a wide variety of identity sources, including NTLM, LDAP, RADIUS, one-time passwords, and certificates
- Integration the world's largest civilian threat intelligence dataset with the Symantec Global Intelligence Network (GIN)
- When paired with other Symantec technologies, it can provide:
    - Malware detection using multiple anti-malware engines and detection methods
    - Multi-layered deep content inspection and analysis to detect spam and application-level threats in the payloads of network traffic
    - Data Loss Prevention (DLP) to identify confidential information and block it from leaving the corporate network.
    - Cloud Access Security Broker (CASB) features to monitor and control what applications users can access and how documents and files are sent to the cloud
    - Web (browser) isolation to create a safe browsing experience, prevent malware from moving from browsers onto employees' systems, and block sharing of credentials on suspicious websites

The Symantec Global Intelligence Network (GIN), which monitors more than 175 million endpoints and Edge SWGs protecting 80 million users. It uses artificial intelligence to analyze over 3.7 billion lines of telemetry to identify and categorize emerging threats and suspicious and malicious URLs and websites. Key data is continually forwarded to hardware and virtual Edge SWGs in data centers and in cloud deployments and to hosted SaaS platforms.



1.1 TOE Description

This section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

For the Symantec Edge SWG with SGOS v7.4, TOE evaluated configuration is comprised of one instance of the SGOS executing on SSP1-S410-20 hardware running ISG and a virtual appliance Dell Power Edge R440 hardware platform with ESXi 6.5.

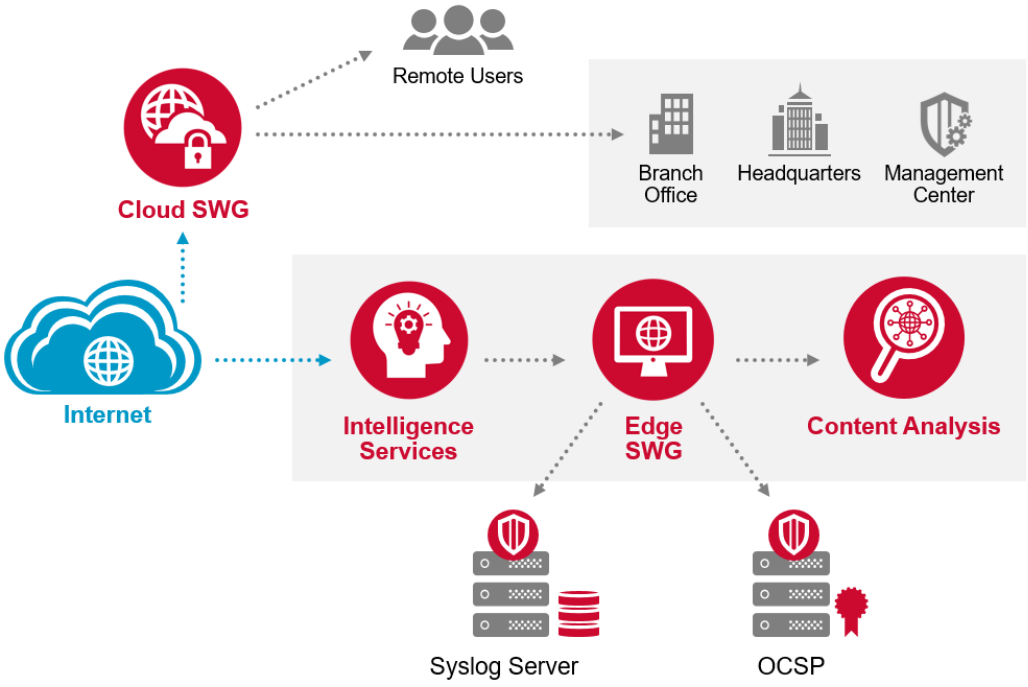


Figure 1 - Representative TOE Deployment

A brief overview of each component in the above figure is as follows:

[1] SSP – Symantec Security Platform

- **Cloud SWG** - Edge SWG running as a SaaS on Google Cloud Platform (cloud version of Edge SWG), same functionality as the TOE, just in the cloud.
- **Intelligence Services** - this is where all the data that ProxySG can use to help filter and protect based on URL reputation/categorization (is this a safe URL?)
- **Edge SWG** - the TOE
- **Content Analysis** - Can analyze the content being accessed (files, web pages) and look at them for potential viruses/malware. Edge SWG applies filters on traffic and can use the result/verdict received from Content Analysis to allow or deny traffic through the proxy.
- **Syslog server** - A syslog server is a destination for transmitting audit logs.
- **OCSP** - Online Certificate Status Protocol (OCSP) is a method used to check the revocation status of digital certificates, ensuring that they are still valid and trustworthy. This process is conducted online, providing real-time validation of certificate status.
- **Remote Users** - Users navigating for web traffic (these users generally are not aware of the Edge SWG explicitly).
- **Branch Office** - A Branch Office is a remote location that serves as a representation of the company to its customers, appearing as though they have a physical office presence.
- **Headquarters** – It is a facility similar to the Branch Office but older/bigger.
- **Management Center** - Symantec product that can be used to manage Edge SWGs. Meant to centralize management tasks.

1.1.1 Physical Boundaries

The TOE is a software solution that is comprised of the network device and its configurations described in Section 1.1. The boundaries are illustrated in Figure 2. The red rectangle represents the physical boundary of the TOE.

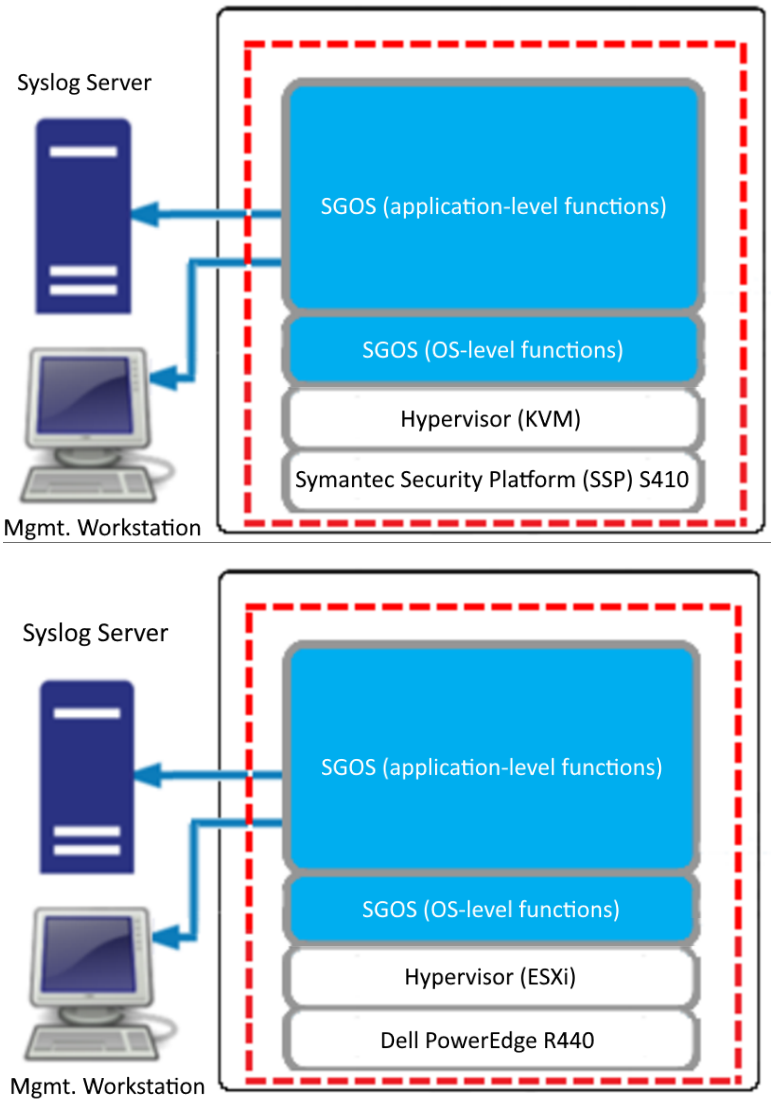


Figure 2 - TOE Boundaries

The TOE boundary includes the 'SGOS' software version 7.4. Licenses activate different features in the executable.

The TOE physical boundary also includes the following:

- VMware ESXi 6.5 Hypervisor hosted on Dell Power Edge R440, with Intel Xeon Silver 4216 Processor (Cascade Lake)
- SSP-S410-20 with ISG using Intel Xeon Silver 4210 Processor (Cascade Lake)

1.1.2 Security Functions Provided by the TOE

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

1.1.2.1 Security Audit

The Network Appliances provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include:

- Start-up of the TOE from both cold boot and reboot,
- Shutdown of the TOE (when shut down from the local CLI and Remote CLI),
- All administrative actions (both security relevant and non-security relevant) from the local CLI and remote CLI,
- Remote administrative SSH connection establishment,
- Remote administrative SSH connection closure,
- Errors during Remote administrative SSH connection establishment,
- Generation of self-signed certificates,
- Import of certificates,
- Deletion of certificates,
- Successful authentication attempts (from the local CLI and Remote CLI),
- Unsuccessful authentication attempts (from the local CLI and Remote CLI),
- All attempts to update the TOE software,
- Changes to time,
- Start of a local administrative session,
- End of a local administrative session,
- Administration session timeout (from the local CLI and Remote CLI).

The TOE is configured to transmit its audit messages to an external audit server. Communication with the audit server is protected using TLS.

The logs for all the appliances can be viewed via the CLI. The records include the date/time the event occurred, the event/type of event, the user ID associated with the event, and additional information of the event and its success and/or failure.

1.1.2.2 **Cryptographic Support**

The TOE provides cryptographic support for the following features,

- TLSv1.2 connectivity with the following entities:
    - Audit Server.
- SSH connectivity with the following entities:
    - Management SSH Client.
- Secure software update

Cryptographic Method	Use within the TOE
AES	• TLS Traffic Encryption/Decryption • SSH Traffic Encryption/Decryption
RSA	• TLS Session Establishment • SSH Session Establishment
SP800-90A	• TLS Session Establishment • SSH Session Establishment
SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
HMAC-SHS	• Used to provide TLS traffic integrity verification • Used to provide SSH traffic integrity verification
SP800-56A	• TLS Session Establishment • SSH Session Establishment
SP800-135rev1	• TLS Session Key Derivation • SSH Session Key Derivation

Table 1 - TOE Cryptography Implementation

The TOE provides cryptographic support for the services as described in sections 5.2.2.1 through 5.2.2.13 of the ST "Symantec Edge SWG with SGOS 7.4 Security Target v0.9" under FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1/DataEncryption, FCS_COP.1/SigGen, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG_EXT.1, FCS_SSHS_EXT.1 and FCS_TLSC_EXT.1, security functional requirements. Additional details are included in section 6 of the ST "Symantec Edge SWG with SGOS 7.4 Security Target v1.0".

The CAVP certificate numbers for the cryptographic algorithms are given in Table 15 of the ST "Symantec Edge SWG with SGOS 7.4 Security Target v0.9". The TOE uses SGOS 7.4 with OpenSSL v3.0 to implement protocol logic as well as all the cryptographic primitives used by the protocols.

1.1.2.3 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOE's administrator interfaces (local CLI and remote CLI). The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on any TOE administrative interface.

1.1.2.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. Management can take place over a variety of interfaces including:

- Local console command line administration;
- Remote CLI administration via SSH;

All administration functions can be accessed via remote CLI or via a direct connection to the TOE. The TOE provides the ability to securely manage the below listed functions;

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE.

1.1.2.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, the TOE software (7.4) is custom-built for the appliance.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the security appliances themselves. The TOE verifies all software updates via digital signature (2048-bit RSA/SHA-256) and requires administrative intervention prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

1.1.2.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE displays an Authorized Administrator specified banner on both the local and remote CLI management interfaces prior to allowing any administrative access to the TOE.

1.1.2.7 **Trusted Path/Channels**

The TOE supports several types of secure communications, including,

- Trusted paths with remote administrators over SSH,
- Trusted channels with remote IT environment audit servers over TLS.

2 Assurance Activities Identification

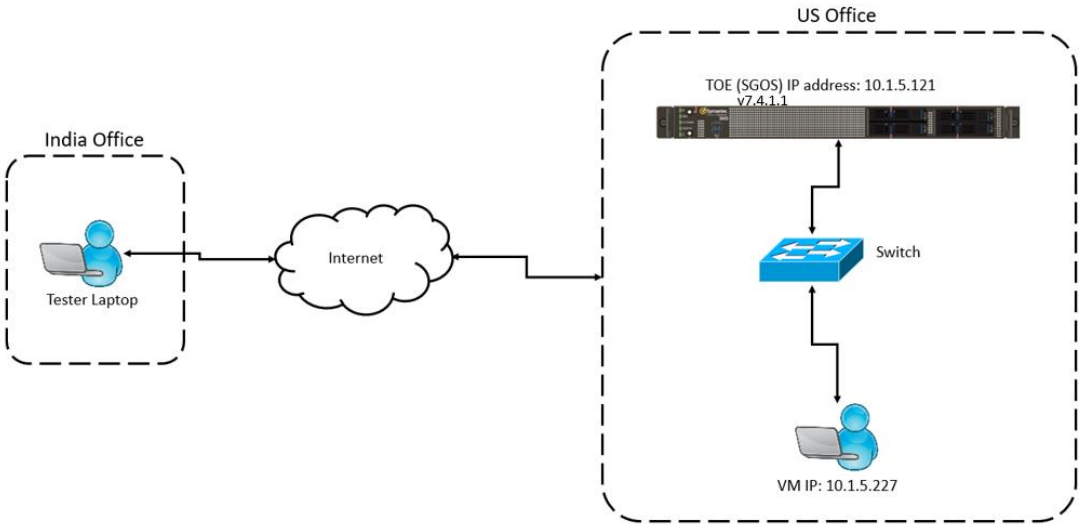
The Assurance Activities contained within this document include all those defined within the NDcPP v2.2e based upon the core SFRs and those implemented based on selections within the PP.

3 Test Equivalency Justification

NA

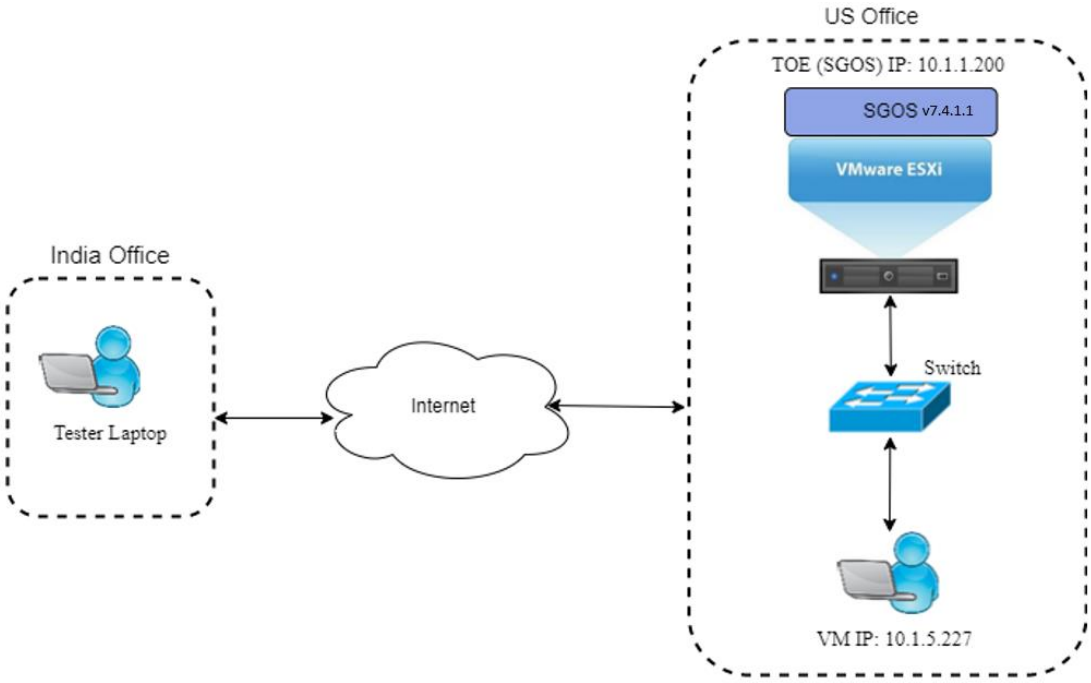
4 Test Bed Descriptions

4.1 SSP-S410-20 with ISG using Intel 4210



Testbed #1

4.2 VMware ESXi 6.5 Hypervisor hosted on Dell Power Edge R440, with Intel 4216



Testbed #2

4.3 TOE Version

```
10.1.5.121 - Edge SWG#show version
Version: SGOS 7.4.1.1 SWG Edition
Release id: 287291 64-bit, gdb, unoptimized
Serial number: 0070990142
Appliance identifier: d59dc1f242f06c59
NIC 0 MAC: 00D083D00241
System is in FIPS mode; cryptographic module algorithm version: 5.1.1
```

4.4 Test Bed Components

The following table describes the characteristics of the components within the test bed:

Name	OS	Version	Function	Protocol	Time	Tools (version)
Hardware Appliance: SSP-S410-20	ISG (Integrated Secure Gateway)	2.4.2.1	Console/SSH	SSHv2	NTP synced	NA
ESXi Server	ESXi	6.5.0 (ESXi build number:4887370)	Console	HTTPS	Manually set and verified	NA
Symantec Edge Web Gateway (SWG)	SGOS	7.4.1.1	TOE	SSHv2	NTP synced	NA
Syslog Server/OCSP server/NTP Server	Ubuntu	Ubuntu 20.04.4LTS	Audit server, OCSP server, NTP server	TLS/SSHSv2	NTP synced	OpenSSL 3.0.0 7 sep 2021, Rsyslogd 8.2001.0 acumen-tlsc-v2.2e, acumen-tlsc, chrony version 3.5
NTP server	Ubuntu	Ubuntu 20.04.4LTS	NTP server	SSHSv2	NTP synced	chrony version 3.5
Test user Laptop	Windows 10	Windows 10	Test Workstation	SSHv2	Manually set and verified	XCAv2.4.0, Wireshark v3.6.13, Firefox Browser 113.0.2 (64-bit)
Switch	NA	NA	NA	NA	NA	NA

4.5 Test Time and Location

All testing were carried at the Acucert Labs office located in Kanjurmarg East, Mumbai 400 042. Testing occurred from 12th May 2023 to 11th August 2023. The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Auditing)

5.1.1 FAU_GEN.1

5.1.1.1 FAU_GEN.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys: **The TOE generates the following types of audit logs during operation:** • **Generation of self-signed certificates,** • **Import of certificates,** • **Deletion of certificates** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.2 FAU_GEN.1 TSS 2

Objective	For distributed TOEs the evaluator shall examine the TSS to ensure that it describes which of the overall required auditable events defined in FAU_GEN.1.1 are generated and recorded by which TOE components. The evaluator shall ensure that this 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 (where applicable to the overall TOE). This includes that the evaluator shall confirm that all components defined as generating audit information for a particular SFR should also contribute to that SFR as defined in the mapping of SFRs to TOE components, and that the audit records generated by each component cover all the SFRs that it implements.
Evaluator Findings	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 1

Objective	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 examined the section titled **'Audit Record Examples'** in the AGD to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the AGD includes an example of the applicable audit events. There are no missing examples of auditable activities.

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

5.1.1.4 FAU_GEN.1 Guidance 2

Objective	The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.
Evaluator Findings	The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator first examined the entirety of AGD to determine what administrative commands are associated with each administrative activity. Upon investigation, the evaluator found that the following are applicable:

Administrative Activity	**Method (Command/GUI Configuration)**	**Section**
Audit configuration	Command Line Interface	Section titled: **"Syslog Event Monitoring"**
User Creation	Command Line Interface	Section titled: **"User Creation"**
Authentication failure configuration	Command Line Interface	Section titled: **"Subcommands"** under Section titled: **"Defining the Local User List"**
Software update	Command Line Interface	Section titled: **"Software Status and Upgrade"**
Setting time	Command Line Interface	Section titled: **"Time Settings"**
Configuring banner	Command Line Interface	Section titled: **"Configuring the Banner"**

Next, the evaluator examined each of the test cases and identified test cases which exercised the above referenced functionality. The audit record associated with the configuration was captured. The following table identifies the test cases in which audit records for those configurations can be found.

Administrative Activity	**Method (Command/GUI Configuration)**	**Test Case(s)**

	Audit configuration	CLI	FAU_STG_EXT.1_Test 2
	User Creation	CLI	FIA_PMG_EXT.1.1_Test 1
	Authentication failure configuration	CLI	FIA_AFL_EXT.1_Test 1
	Software update	CLI	FPT_TUD_EXT.1 Test #1
	Setting time	CLI	FPT_STM.1.1 Test#1
	Configuring banner	CLI	FTA_TAB.1 Test#1
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

5.1.2 FAU_GEN.2

5.1.2.1 FAU_GEN.2 TSS 1 and Guidance 1

Objective	The TSS and Guidance Documentation requirements for FAU_GEN.2 are already covered by the TSS and Guidance Documentation requirements for FAU_GEN.1.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target and section titled **'Audit Record Examples'** in the AGD to determine the verdict of this assurance activity. The evaluator also examined FAU_GEN.1 requirements (as stated above) and ensured that the existing documentation adequately meets the requirements for FAU_GEN.2 as well. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FAU_STG_EXT.1

5.1.3.1 FAU_STG_EXT.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states that: **The TOE provides the ability to securely transmit audit logs to an external audit server using Syslog over TLS.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.3.2 FAU_STG_EXT.1 TSS 2

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS 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. Upon investigation, the evaluator found that the TSS states that: **The maximum size of audit records stored by the TOE can be configured by an administrator. The upper limit on local audit storage is based on the amount of available hard drive space, but an administrator can set a lower limit if desired. For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents. However, the Authorized Administrator may do a onetime configuration that will not allow the administrator to erase logs. This command is irreversible and does not reset even if the machine is returned to factory defaults.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.3.3 FAU_STG_EXT.1 TSS 3

Objective	The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. Upon investigation, the evaluator found that the TSS states that: **The TOE provides the ability to securely transmit audit logs to an external audit server using TLS/HTTPS. The TOE is a standalone and stores logs locally. For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.3.4 FAU_STG_EXT.1 TSS 4

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS states that: **For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.3.5 FAU_STG_EXT.1 TSS 5

Objective	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 realtime or periodically. In case the TOE does not perform transmission in realtime 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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. Upon investigation, the evaluator found that the TSS states that: **the TOE provides the ability to securely transmit audit logs to an external audit server using syslog over TLS in real-time.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.6 FAU_STG_EXT.1 TSS 6

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.7 FAU_STG_EXT.1 TSS 7

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.8 FAU_STG_EXT.1 Guidance 1

Objective	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 section titled **'Syslog Event Monitoring'** in the AGD to verify that 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. Upon investigation, the evaluator found that the AGD states the description of the protocols used to communicate with the audit server (TLS, UDP or TCP) and the commands required to configure the TOE to connect to the remote audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.9 FAU_STG_EXT.1 Guidance 2

Objective	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 examined the section titled **'Syslog Event Monitoring'** in the AGD to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD states that **when configured to use an audit server the SGOS appliance transmits audit events to the audit server at the same time logs are written locally. If the connection fails, the SGOS continues to store audit records locally and will transmit any stored contents when connectivity to the syslog server is restored.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.10 FAU_STG_EXT.1 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined the section titled **'Local Storage Full'** and **'Local Storage Reset'** in the AGD to verify that it describes all possible configuration options for FAU_STG_EXT.1.3 and the

	resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the AGD states the description of the available configuration options for handling a full local audit record. Next, the evaluator compared the exhausted local audit handling description found in AGD to the description provided by the TSS of the ST. The descriptions of the behavior found in AGD and ST are consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as "Test/CAVP" activities.

5.2.1 FCS_CKM.1

5.2.1.1 FCS_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that: **The TOE can create a RSA public-private key pair with a RSA key size of 2048 and 3072bits. The RSA key pair can be used to generate a Certificate Signing Request (CSR). The TOE generates Elliptic-curve keys using NIST curves P-256, P-384, and P-521 with key sizes of 256, 384, and 521 bits respectively. Key generation via Diffie-Hellman group 14 per RFC 3526, Section 3 is also included since key establishment using Diffie-Hellman group 14 is included in FCS_CKM.2.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.2 FCS_CKM.1 Guidance 1

Objective	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 examined the section titled **'Certificate Signing Request (CSR)'** and **'Managing SSH Client Keys'** in the AGD to verify that it 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. Upon investigation, the evaluator found that the AGD states the configuration for generating SSH Keys and CSR related keys is described. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.

Evaluator Findings	CAVP Certs: #A2936 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FCS_CKM.2

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

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that: **In support of secure cryptographic protocols, the TOE supports key establishment schemes, including,** • **FFC Diffie-Hellman as specified in NIST SP 800-56A Revision 2: Used as part of SSH and TLS session establishment,** • **Elliptic Curve Diffie-Hellman as specified in NIST SP 800-56A Revision 2: used as part of SSH and TLS session establishment,** • **Diffie-Hellman group 14 per RFC 3526, Section 3: Used as part of SSH session establishment.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.2 FCS_CKM.2 Guidance 1

Objective	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 examined the section titled **Managing SSH Client Keys, Editing an SSL Device Profile** and **Certificate Signing Request (CSR)** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD describes the guidance specifically states that when TLS ciphers and certificates are configured no additional configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # A2936 Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.3 FCS_CKM.4

5.2.3.1 FCS_CKM.4 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS 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. Upon investigation, the evaluator found that the TSS states that: **The TOE stores several types of keys in volatile memory in plaintext, including,** • **Diffie-Hellman Private/Public Key Pair,** • **Elliptic Curve Diffie-Hellman Private/Public Key Pair,** • **SSH Session Encryption Key,** • **SSH Session Integrity Key,** • **TLS Session Encryption Key,** • **TLS Session Integrity Key.** **Each plaintext key stored in volatile memory is associated with a cryptographic session. In each instance, after the session closes, the key is overwritten with the value "00"** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found that the TSS states that: **After the overwrite operation is complete, the TOE performs a specific "read-verify" operation to confirm that the storage space no longer contains the key.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.2 FCS_CKM.4 TSS 2

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that 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. Upon investigation, the evaluator found that the TSS states that: **Each plaintext key stored in volatile memory is associated with a cryptographic session. In each instance, after the session closes, the key is overwritten with the value "00" After the overwrite operation is complete, the TOE performs a specific "read-verify" operation to confirm that the storage space no longer contains the key.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.3 FCS_CKM.4 TSS 3

Objective	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	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify 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. Upon investigation, the evaluator found that the TSS states that: **The TOE stores RSA key pairs used for TLS and SSH in non-volatile storage and a Master Encryption Key (MEK) is used to encrypt all the other keys stored in non-volatile storage.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.4 FCS_CKM.4 TSS 4

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS states that the TOE does not have any circumstances that may not conform to key destruction requirements. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.5 FCS_CKM.4 TSS 5

Objective	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	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. Upon investigation, the evaluator found in section titled 'Security Functional Requirements' that the selection was not selected in the ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.6 FCS_CKM.4 Guidance 1

Objective	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). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the section titled **'Zeroization'** in the AGD to verify that it 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. Upon investigation, the evaluator reviewed the TSS and AGD documentation for the TOE and found no items that did not meet conformance to the key destruction requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4 FCS_COP.1/DataEncryption

5.2.4.1 FCS_COP.1/DataEncryption TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that: **The TOE provides symmetric encryption and decryption capabilities using AES in CTR and GCM mode (128 and 256 bits for CTR and GCM) as described AES as specified in ISO 18033-3. AES is implemented in support of the following protocols: TLS, and SSH.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.2 FCS_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled **'Configuring Ciphers'** and **'Editing an SSL Device Profile'** in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD states how to configure the TOE in the evaluated configuration by selecting the ciphers. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: #A2936 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FCS_COP.1/SigGen

5.2.5.1 FCS_COP.1/SigGen TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that: **The TOE provides cryptographic signature services using following algorithms and key sizes:** • **RSA Digital Signature Algorithm with key sizes of 2048 and 3072 as specified in section 5.5 of the FIPS PUB 186-4, "Digital Signature Standard"** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5.2 FCS_COP.1/SigGen Guidance 1

Objective	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 examined the sections titled **Managing SSH Client Keys, Editing an SSL Device Profile** and **Certificate Signing Request (CSR)**in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature

	services. Upon investigation, the evaluator found that the AGD states steps to configure self-signed certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP RSA SigGen&SigVer (186-4) Certs: #A2936 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6 FCS_COP.1/Hash

5.2.6.1 FCS_COP.1/Hash TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states that: **The TOE provides cryptographic hashing services using SHS as specified in FIPS Pub 180-3 "Secure Hash Standard."** **SHS hashing is used within several services including, hashing, TLS/HTTPS (SHA1, SHA256, SHA384), and SSH (SHA1, SHA256, SHA384, SHA-512).** **The message digest sizes supported are: 160, 256, 384, and 512 bits.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.2 FCS_COP.1/Hash Guidance 1

Objective	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 examined the section titled **Hash Cryptographic Operation (Hash Algorithm)** in the AGD to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD states the TOE supports cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512 and message digest sizes 160, 256, 384, 512 bits. The TOE comes preconfigured for these sizes and no additional configuration is required. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHS Certs: # A2936 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7 FCS_COP.1/KeyedHash

5.2.7.1 FCS_COP.1/KeyedHash TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that: **The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512. The product supports the following cryptographic parameters for MACing, as specified in ISO/IEC 9797-2:2011:** • **Key length: 160, 256, 384, 512-bits** • **Hash function used: SHA-1, SHA-256, SHA-384, and SHA-512** • **Block size: 512, 1024-bits** • **Output MAC: 160, 256, 384, 512-bits** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.2 FCS_COP.1/KeyedHash Guidance 1

Objective	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 examined the section titled **'Configuring HMACs'** in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states the commands to configure the values that can be used by HMAC function. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	CAVP HMAC Certs: # A2936

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

5.2.8 FCS_RBG_EXT.1

5.2.8.1 FCS_RBG_EXT.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS 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. Upon investigation, the evaluator found that the TSS states that: **The TOE produces all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES).** **The entropy source used to seed the Deterministic Random Bit Generator is a random set of bits or bytes that are regularly supplied to the DRBG by polling four different set of software sources in threads. All entropy is continuously health tested by the DRBG as per the tests defined in section 11.3 of SP 900-90A before being used as a seed (instantiate, generate, reseed, and uninstantiate).** **Additionally, each call to the entropy source is subject to a continuous random number generator test to ensure that there are no stuck conditions. Any initialization or system errors during bring-up or processing of this system causes a reboot resulting in the DRBG being reseeded.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined the section titled **'Random Bit Generation'** in the AGD to verify that it contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that the AGD states that the TOE produces all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP DRBG Certs: # A2936 Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3 TSS and Guidance Activities (NTP)

5.3.1 FCS_NTP_EXT.1

5.3.1.1 FCS_NTP_EXT.1 TSS 1

Objective	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 **FCS_NTP_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the version of NTP supported, how it is implemented and what approach the TOE uses to ensure the timestamp it receives from an NTP timeserver (or NTP peer) is from an authenticated source and the integrity of the time has been maintained. Upon investigation, the evaluator found that the TSS states that: **The TSF supports time updates using NTPv3. The TSF authentications updates using an administrator configured symmetric key and SHA-1. The TOE rejects broadcast and multicast time updates. The TOE enforces a maximum limit of 32 NTP time sources that can be configured.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FCS_NTP_EXT.1 TSS 2

Objective	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 evaluator examined the **FCS_NTP_EXT.1** entry in section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes each method selected in the ST, including the version of NTP supported in element 1.1, the message digest algorithms used to verify the authenticity of the timestamp and/or the protocols used to ensure integrity of the timestamp. Upon investigation, the evaluator found that the TSS states that **The TSF authentications updates using an administrator configured symmetric key and SHA-1.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.3 FCS_NTP_EXT.1.1 Guidance 1

Objective	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 section titled **Synchronizing to the Network Time Protocol** in the AGD to verify that it provides the administrator instructions as how to configure the version of NTP supported, how to configure multiple NTP servers for the TOE's time source and how to configure the TOE to use the method(s) that are selected in the ST. Upon investigation, the evaluator found that the AGD states the steps to configure NTP server. The TOE allows up to 10 NTP time sources to be configured. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.4 FCS_NTP_EXT.1.2 Guidance 1

Objective	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.
Evaluator Findings	The evaluator examined the section titled **Synchronizing to the Network Time Protocol** in the AGD to verify that, for each of the secondary selections made in the ST, it instructs the administrator how to configure the TOE to use the algorithms that support the authenticity of the timestamp and/or how to configure the TOE to use the protocols that ensure the integrity of the timestamp. Upon investigation, the evaluator found that the AGD describes detailed instructions how to configure the TOE to use the algorithms that support the authenticity of the timestamp and how to configure the TOE to use the protocols that ensure the integrity of the timestamp. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.5 FCS_NTP_EXT.1.3 Guidance 1

Objective	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 section titled **Synchronizing to the Network Time Protocol** in the AGD to verify that it provides instructions as how to configure the TOE to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. Upon investigation, the evaluator found that the AGD states that **the TOE rejects broadcast and multicast time updates.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (SSH)

5.4.1 FCS_SSHS_EXT.1

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

Objective	The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with

	signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims). The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file. If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS states that: • **Only password-based authentication and public key-based authentication;** • **The TOE uses the username presented by the client as the user's identity.** • **The TOE then authorizes the connection if the presented public key matches an authorized public key for the claimed identity.** • **For public key-based authentication, use of 2048-bit RSA keys in support of SSH_RSA.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.2 FCS_SSHS_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes how "large packets" in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that: **Dropping SSH packets greater than 1522 bytes. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.3 FCS_SSHS_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that:

	Encryption algorithms aes128-ctr, aes256-ctr, aes-128-gcm@openssh.com, aes-256-gcm@openssh.com to ensure confidentiality of the session and reject all other encryption algorithms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.4 FCS_SSHS_EXT.1.4 Guidance 1

Objective	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 examined the section titled **'Configuring Ciphers'** in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that **Fewer ciphers are available when the appliance is in FIPS mode.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

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

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS states that: **For public key-based authentication, use of 2048-bit RSA keys in support of SSH_RSA.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.6 FCS_SSHS_EXT.1.5 TSS 2

Objective	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 examined the section titled '**TOE Summary Specification'** in the Security Target to verify that the TSS describes how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. Upon investigation, the evaluator found that the TSS states that • **The TOE then authorizes the connection if the presented public key matches an authorized public key for the claimed identity.** • **For public key-based authentication, use of 2048-bit RSA keys in support of SSH_RSA.**

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

5.4.1.7 FCS_SSHS_EXT.1.5 Guidance 1

Objective	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 examined the section titled **'Managing SSH Client Keys'** in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that **An RSA client key can only be created by an SSH client and then imported onto the appliance.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.8 FCS_SSHS_EXT.1.6 TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that: **Hashing algorithm hmac-sha1, hmac-sha-1-96, hmac-sha2-256, hmac-sha2-512 ensure the integrity of the session, and reject all other MAC algorithms** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.9 FCS_SSHS_EXT.1.6 Guidance 1

Objective	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 examined the section titled **'Configuring HMACs'** in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states commands required to configure the stated hmacs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.10 FCS_SSHS_EXT.1.7 TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that: **The TOE enforces diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 as the only allowed key exchange methods.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.11 FCS_SSHS_EXT.1.7 Guidance 1

Objective	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 examined the section titled **'Configuring Key Exchange Algorithm'** in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that the AGD states commands required to configure the stated key-exchange algorithms. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.12 FCS_SSHS_EXT.1.8 TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS specifies that both thresholds are checked, and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that: **The TOE forces a rekey before reaching 1 hour or 2^28 bytes (which is less than aggregate of one gigabyte of data), whichever occurs first.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.13 FCS_SSHS_EXT.1.8 Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **'Management Services (SSH Access)'** in the AGD to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD states that no additional configuration is required and The TOE forces a rekey before reaching 1 hour or 2^28 bytes (which is less than aggregate of one gigabyte of data), whichever occurs first. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (TLS)

5.5.1 FCS_TLSC_EXT.1

5.5.1.1 FCS_TLSC_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified include those listed for this component. Upon investigation, the evaluator found that the TSS states that: **The TOE operates as a TLS client for the trusted channel with the remote syslog server.** **TOE supports TLS 1.2. Connections using other version of TLS or SSL, such as, TLS 1.0 or SSL 3.0 are actively denied by the TOE.** **The following ciphersuites are supported for communications with the remote audit server:** • **TLS_DHE_RSA_WITH_AES_128_GCM_SHA256** • **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384** • **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** **All other proposed Ciphersuites are denied.** **The Ciphersuites are user-configurable.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.2 FCS_TLSC_EXT.1.1 Guidance 1

Objective	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 examined the section titled **'Editing an SSL Device Profile'** in the AGD to verify that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states the commands to configure the TLS ciphersuites. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 FCS_TLSC_EXT.1.2 TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify 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; whether IP addresses and wildcards are supported. Upon investigation, the evaluator found that the TSS states that: **The reference identifier for the remote audit server is configured by the administrator using the web GUI or CLI.** **When the TLS client receives an X.509 certificate from the server, the client will compare the reference identifier with the established Subject Alternative Names (SANs) in the certificate. If a SAN is available and does not match the reference identifier, then the verification fails and the channel is terminated. If there are no SANs of the correct type (IP address or DNS name) in the certificate, then the TOE will compare the reference identifier to the CN (IP address or DNS name) in the certificate Subject. If there is no CN, then the verification fails and the channel is terminated. If the CN exists and does not match, then the verification fails and the channel is terminated. Otherwise, the reference identifier verification passes, and additional verification actions can proceed. The TOE supports wildcards for DNS names in the CN and SAN. For both DNS Name 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.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.4 FCS_TLSC_EXT.1.2 TSS 2

Objective	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 attributes 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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.5 FCS_TLSC_EXT.1.2 TSS 3

Objective	If IP addresses are supported in the CN as reference identifiers, the evaluator shall ensure that the TSS describes the TOE's conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order. The evaluator shall also ensure that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that, if IP addresses are supported in the CN as reference identifiers, the TSS describes the TOE's conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order and whether canonical format is enforced. Upon investigation, the evaluator found that the TSS states that **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.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.6 FCS_TLSC_EXT.1.2 Guidance 1

Objective	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 examined the section titled **'Syslog Event Monitoring'** in the AGD to verify 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 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. Further the AGD also provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.7 FCS_TLSC_EXT.1.4 TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that:

	The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: P-256, P-384, and P-521. The non-TOE server can choose to negotiate the elliptic curve from this set for any of the mutually negotiable elliptic curve Ciphersuites. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.8 FCS_TLSC_EXT.1.4 Guidance 1

Objective	If the TSS indicates that the Supported Elliptic Curves/Supported Groups Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves/Supported Groups Extension.
Evaluator Findings	The evaluator examined the section titled **'SSL Device Profile'** in the AGD to verify that, if the TSS indicates that the Supported Elliptic Curves Extension must be configured to meet the requirement, it includes configuration of the Supported Elliptic Curves Extension. Upon investigation, the evaluator found that the AGD states that **the TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: P-256, P-384, and P-521.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Identification and Authentication)

5.6.1 FIA_AFL.1

5.6.1.1 FIA_AFL.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS states that: **The TOE permits administrators to set a positive integer for failed remote authentication attempts. When this limit is met, a trusted administrator must manually unlock the locked-out user before a successful authentication happens.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.2 FIA_AFL.1 TSS 2

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that: **The local console account is not subject to the lockout mechanism. This account should not be used for day-to-day administrator.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.3 FIA_AFL.1 Guidance 1

Objective	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 section titled **'Subcommands'** under section **'Defining the Local User List'** in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), 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). Upon investigation, the evaluator found that the AGD describes the configuration the administrative involvement unlocks. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.4 FIA_AFL.1 Guidance 2

Objective	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 section titled **'Defining the Local User List'** in the AGD to verify 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. Upon investigation, the evaluator found that the AGD states that **the local console account is not subject to the lockout mechanism. This account should not be used for day-to-day administrator.** Based on these findings, this assurance activity is considered satisfied.

5.6.2 FIA_PMG_EXT.1

5.6.2.1 FIA_PMG_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that: **The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", "", "+", "-", "=", ".", "/", "\", ":", ";", "<", ">", "[", "]", "_", "{", "}", "|", "~" "` .** **The minimum password length is settable by the Authorized Administrator.** **When the TOE is configured for "Common Criteria Compliance" the minimum password length is set to 8 characters and the maximum password length is 64 characters.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it: a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
Evaluator Findings	The evaluator examined the section titled **'Username and Passwords'** in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states that **a compliant password must be at least 8 characters long with the following complexity:** - **At least one uppercase letter** - **At least one lowercase letter** - **At least one numbers** - **At least one of the following special characters:** - **["!", "@", "#", "$", "%", "^", "&", "*", "(", ")", ["", "+", "-", "=", ".", "/", "\", ":", ";", "<", ">", "[", "]", "_", "{", "}", "|", "~" "`]]** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 FIA_UIA_EXT.1

5.6.3.1 FIA_UIA_EXT.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that: **The process for authentication is the same for administrative access whether administration is occurring via direct connection or remotely. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.2 FIA_UIA_EXT.1 TSS 2

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that: **No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.3 FIA_UIA_EXT.1 TSS 3

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.4 FIA_UIA_EXT.1 TSS 4

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.5 FIA_UIA_EXT.1 Guidance 1

Objective	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 section titled **'Management Services (SSH Access)** in the AGD to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in. Upon investigation, the evaluator found that the AGD states that **regardless of method of administering the TOE, the user is presented with an authentication prompt. At the authentication prompt the username of the administrator and credential (either password or SSH key) must be presented. Administration is available only after the correct username/credential combination is presented.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 FIA_UAU.7

5.6.4.1 FIA_UAU.7 Guidance 1

Objective	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 entire AGD to verify that it describes any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. Upon investigation, the evaluator found that no additional configuration is required to ensure that authentication data is not revealed during login. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 FIA_X509_EXT.1/Rev

5.6.5.1 FIA_X509_EXT.1/Rev TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that 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). Upon investigation, the evaluator found that the TSS identifies when the check of validity takes place, as follows, • **TLS client validation of server certificates;** • **When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates.** Next, the evaluator verified that the TSS describes the rule for extendedKeyUsage fields. Upon investigation, the evaluator found the following described in the TSS: **As X.509 certificates are not used for trusted updates, firmware integrity self-tests or client authentication, the code-signing and clientAuthentication purpose is NOT checked in the extendedKeyUsage for related certificates.** **A trusted CA certificate is defined as any certificate loaded into the TOE trust store that has, at a minimum, a basicConstraints extension with the CA flag set to TRUE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.2 FIA_X509_EXT.1/Rev TSS 2

Objective	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 evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that **In all scenarios, certificates are checked for several validation characteristics:** **a) If the certificate 'notAfter' date is in the past, then this is an expired certificate which is considered invalid;** **b) The certificate chain must terminate with a trusted CA certificate;** **c) Server certificates consumed by the TOE TLS client must have a 'serverAuthentication' extendedKeyUsage purpose;**

	d) OCSP certificates presented for OCSP responses must have the 'ocspSigning' extendedKeyUsage purpose. **Certificate revocation checking for the above scenarios is performed by querying with an OCSP Responder.** Next, the evaluator confirmed that as part of the description of the validation process revocation checking is described. The evaluator found the following description within the TSS. **The TOE performs X.509 certificate validation at the following points:** • **TLS client validation of server certificates;** • **When certificates are loaded into the TOE, such as when importing CAs, certificate responses and other device-level certificates.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.3 FIA_X509_EXT.1/Rev Guidance 1

Objective	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 examined the sections titled **'Managing X.509 Certificates'** and **'Configuring OCSP'** in the AGD to verify that it describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD describes when and how certificate validation takes place, describes any of the rules for extendedKeyUsage fields and describes how certificate revocation checking is performed and on which certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6 FIA_X509_EXT.2

5.6.6.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that: **The TOE has a trust store where root CA and intermediate CA certificates can be stored. The trust store is not cached: if a certificate is deleted, it is immediately untrusted. If a certificate is added to the trust store, it is immediately trusted for its given scope.**

	Revocation checking is performed on both leaf and intermediate CA certificates when a leaf certificate is presented to the TOE as part of the certificate chain during authentication. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.2 FIA_X509_EXT.2 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS 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. Upon investigation, the evaluator found that the TSS states that: **If, during the entire trust chain verification activity, any certificate under review fails a verification check, then the entire trust chain is deemed untrusted.** **As part of the verification process, OCSP is used to determine whether the certificate is revoked or not. If the OCSP response is unknown or cannot be obtained, then the TOE will use the last cached information available about certificate to accept or reject the certificate (or the TOE will treat the certificate as revoked/ as valid).** **The TOE contacts the OCSP responder hourly during an hourly check of certificates in the trust store.** **Instructions for configuring the trusted IT entities to supply appropriate X.509 certificates are captured in the guidance documents.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled **'Importing CA certificate to the Device'** in the AGD to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD describes instructions for configuring the usage of certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.4 FIA_X509_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the entire AGD to verify that, if the requirement that the administrator can specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD does not state that the administrator is able to specify the default action. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.5 FIA_X509_EXT.2 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Evaluator Findings	The evaluator examined the section titled **'CA Certificate List (CCL)'** in the AGD. Upon investigation, the evaluator found that the AGD states that the CCL referenced by the profile or service configuration is used when an SSL connection is established to that service or using that profile. A CA certificate list (CCL), which contains some of the CA Certificates available on the appliance, allows the administrator to control the set of CA certificates trusted for a particular set of SSL connections. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7 FIA_X509_EXT.3

5.6.7.1 FIA_X509_EXT.3 TSS 1

Objective	If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS contains a description of the device-specific fields used in certificate requests. Upon investigation, the evaluator found that the TSS does not select "device-specific information." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7.2 FIA_X509_EXT.3 Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **'Certificate Signing Request (CSR)'** in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD provides instructions for generating CSRs. The evaluator found that these instructions include the complete set of steps necessary to configure a fully formed CSR containing each of the fields described in FIA_X509_EXT.3. Finally, the evaluator found that AGD provides instructions for generating CSRs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7 TSS and Guidance Activities (Security Management)

5.7.1 FMT_MOF.1/ManualUpdate

5.7.1.1 FMT_MOF.1/ManualUpdate TSS 1

Objective	For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Evaluator Findings	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.2 FMT_MOF.1/ManualUpdate Guidance 1

Objective	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 section titled **'Software Status and Upgrade'** in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD describes the various commands required to perform a software update, query the currently active version and view installation status and install new software images. The evaluator examined the section titled **'Software Status and Upgrade'** 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 uses public hash to verify the integrity of the update. If the computed hash matches the published hash the image will be installed or else unsuccessful message will be delivered to the user.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.3 FMT_MOF.1/ManualUpdate Guidance 2

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FMT_FMT_MOF.1/Functions

5.7.2.1 FMT_MOF.1/Functions TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies 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). Upon investigation, the evaluator found that the TSS states that: **The TOE restricts the ability to modify (enable/disable) transmission of audit records to an external audit server to Security Administrators.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.2 FMT_MOF.1/Functions Guidance 1

Objective	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 section titled **'Syslog Event Monitoring'** in the AGD to verify that it describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings. Upon investigation, the evaluator found the AGD describes the configuration required to modify handling of local audit records and transmission of audit records to an external server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FMT_MTD.1/CoreData

5.7.3.1 FMT_MTD.1/CoreData TSS 1

Objective	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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that: **Users are required to login before being provided with access to any administrative functions.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that: **The TOE provides the ability for Security Administrators (i.e. Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds, administration of X.509 certificates and updates. Access to this data is governed by the privileges assigned to the administrative users. None of this functionality is accessible prior to the administrator logging into the TOE.** **The term "Authorized Administrator" is used in this ST to refer to any of the predefined user privilege levels.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 FMT_MTD.1/CoreData TSS 2

Objective	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	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that: **The TOE provides the ability for Security Administrators (i.e. Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds, administration of X.509 certificates and updates. Access to this data is governed by the privileges assigned to the administrative users. None of this functionality is accessible prior to the administrator logging into the TOE.** **The term "Authorized Administrator" is used in this ST to refer to any of the predefined user privilege levels.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.3.3 FMT_MTD.1/CoreData Guidance 1

Objective	The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.
Evaluator Findings	The evaluator examined the entire AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the following sections in the AGD describes the configuration available for each of the data manipulating functions available on the TOE, consistent with ST, • **Ways to Access the CLI Console** • **Accessing the TOE Using SSH** • **Changing the Administrator Account Credentials** • **Synchronizing to the Network Time Protocol** • **Logging Out** • **Management Services (SSH Access)** • **Event Logging** • **Importing CA certificate to the Device** • **Certificate Signing Request (CSR)** • **SSL Device Profile** • **Configuring OCSP** • **Software Status and Upgrade** • **Username and Passwords** • **Configuring the Banner** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.4 FMT_MTD.1/CoreData Guidance 2

Objective	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	The evaluator examined the section titled **'CA Certificate List (CCL)** in the AGD to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD states that **a CA certificate list (CCL), which contains some of the CA Certificates available on the appliance, allows the administrator to control the set of CA certificates trusted for a particular set of SSL connections. Further the AGD also states command to configure and maintain the CCL in a secure way for SSL connections.** The evaluator examined the section titled **'Importing CA certificate to the Device'** and **'CA Certificate List (CCL)'** in the AGD to verify that, if the TOE supports loading of CA certificates,

	it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD states commands to load the CA certificates into the configured trust store (CCL) and also explains that when the CA certificate is added to the CCL that is to be used in SSL connection it is identified as designated CA. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4 FMT_SMF.1

5.7.4.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the AGD states that **the Security Administrators (a.k.a Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via remote CLI over SSHv2, at the local console.** **The specific management capabilities available from the TOE include:**

Sr. No.	Management capabilities available from the TOE	Reference to Guidance Document
1	Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI	Section 2.1 "Ways to Access the Cli Console" and Section 2.2 "Accessing the TOE using SSH"
2	Ability to configure the access banner,	Section 2.18 "Configuring the Banner"
3	Ability to configure the session inactivity time before session termination or locking	Section 2.4.2 "Changing the TOE Timeout"
4	Ability to update the TOE, and to verify the updates using hash comparison capability prior to installing those updates,	Section 2.15 "Software Status and Upgrade"
5	Ability to configure the authentication failure parameters;	Section 2.17.4 "Subcommands" under Section 2.17 "User Roles"
6	Ability to configure audit behavior, in particularly, changes to the size of the audit space	Section 2.8.2 "Log Size" under Section 2.8 "Event Logging"
7	Ability to configure the cryptographic functionality	Section 2.12 "Certificate Signing Request"
8	Ability to re-enable an Administrator account	Section 2.17.4 "Subcommands" under Section 2.17 "User Roles"
9	Ability to configure NTP	Section 2.4.1 "Synchronizing to the Network Time Protocol"
10	Ability to configure the reference identifier for the peer (SAN-IP address and SAN-DNS hostname	Section 2.8.1 "Syslog Event Monitoring"

	11	Import and delete X.509v3 certificates	Section 2.10 “Importing CA Certificate to the Device”
	12	Generate and delete cryptographic keys	Section 2.12 “Certificate Signing Request”
	The evaluator examined the section titled **‘TOE Summary Specification’** in the TSS to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that: The evaluator additionally verified in the **‘TOE Summary Specification’** in the ST and the guidance documentation that administration via the local interface is described. Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

5.7.4.2 FMT_SMF.1 TSS 2

Objective	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. The evaluator shall check that the TOE behaviour observed during testing of the configured SFRs is as described in the TSS and Guidance Documentation.
Evaluator Findings	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.3 FMT_SMF.1 Guidance 1

Objective	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.
Evaluator Findings	The evaluator examined the section titled **‘Ways to Access the CLI Console’** in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD describes the local interface and the configurations required to communicate on the interface. The evaluator examined the section titled **‘Ways to Access the CLI Console’** 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 describes the steps associated with connecting to the serial port of a computer. This sufficiently ensures that the interface is a local interface. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5 FMT_SMR.2

5.7.5.1 FMT_SMR.2 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the TSS to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the AGD states that: **The TOE supports multiple administrative roles when accessing the administrative interface through the local or remote CLI. These roles define the access that is allowed per role.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.2 FMT_SMR.2 Guidance 1

Objective	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 examined the entire AGD to verify 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. Upon investigation, the evaluator found that the AGD describes instructions for administering the TOE both locally and remotely. For remote administration, the evaluator found that AGD describes all configurations necessary to connect to the TOE. Additionally, the section titled '**Accessing the TOE Using the CLI Console**' of AGD states that, **after FIPS mode has been enabled on an appliance per the instructions, you must use SSH from a server or desktop that has the proper ciphers**. Additionally, for each applicable function, the method for configuring the function via the via the CLI (local/remote) is described. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (Protection of the TSF)

5.8.1 FPT_APW_EXT.1

5.8.1.1 FPT_APW_EXT.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that:

	Passwords are stored on the TOE in a secured partition in non-plaintext. Prior to writing on disks each password is hashed (SHA-256) using the PBKDFv2 algorithm. The evaluator also examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details those 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: **During subsequent authentication attempts passwords entered are converted using the same PBKDFv2 algorithm. This is compared to the digest value for that user stored in the secured partition. Access is only granted if the values match.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2 FPT_SKP_EXT.1

5.8.2.1 FPT_SKP_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how any preshared 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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS 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. Upon investigation, the evaluator found that the TSS states that: **All keys stored on the TOE are protected from unauthorized modification and substitution.** **The TOE stores symmetric keys only in volatile memory never on persistent media. The TOE admin interface does not provide any mechanism to view sensitive data (passwords or keys) once stored. Unauthenticated operators do not have write access to modify, change, or delete keys.** **The TOE stores all asymmetric keys in a secure directory that is not readily accessible to administrators; therefore, there is no administrative interface access provided to directly manipulate the keys.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FPT_STM_EXT.1

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

Objective	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. 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	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that: **The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the NTP configuration. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time can be updated by a Security Administrator automatically by configurating NTP synchronization.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 FPT_STM_EXT.1 Guidance 1

Objective	The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication. 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 evaluator examined the section titled **'Synchronizing with the Network Time Protocol'** in the AGD to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD describes the configuration needed on the NTP client (i.e. TOE) to establish communication path between TOE and the NTP server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FPT_TST_EXT.1.1

5.8.4.1 FPT_TST_EXT.1.1 TSS 1

Objective	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). 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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS states that: **During the system bootup process (power on or reboot), the TOE performs various power-on self-test (POSTs) for the cryptographic components of the TOE.**

	During initialization and self-test execution, the module inhibits all access to the cryptographic algorithms. Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests. In the event of a power-on self-test failure, the cryptographic module will force the platform to reload and reinitialize the operating system and cryptographic components. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful. These tests include: • **AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly.** • **HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.** • **RNG/DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.** • **SHA Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly.** • **RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.** • **DH Known Answer Test – This test takes known input to the "z" calculation for Diffie-Hellman and compares the result to a known "z" value.** • **ECDH Known Answer Test – This test takes known input to the "z" calculation for Elliptic Curve Diffie-Hellman and compares the result to a known "z" value.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that: **The TOE runs a suite of self-tests during initial start-up to verify its correct operation.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 FPT_TST_EXT.1.1 TSS 2

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.3 FPT_TST_EXT.1.1 Guidance 1

Objective	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 examined the section titled **'Self-Test Errors'** in the AGD to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the evaluator found that the AGD states that **Indication of self-test failures are printed on the local console and the boot process is terminated. Any indication of power on self test failures, users should contact Symantec customer support for instructions on how to proceed.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.4 FPT_TST_EXT.1.1 Guidance 2

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5 FPT_TUD_EXT.1

5.8.5.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that: **Authorized Administrator can query the software version running on the TOE by using the 'show version' command, and can initiate updates to software images.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, if a trusted update can be installed on the TOE with a delayed

	activation, describes how and when the inactive version becomes active. Upon investigation, the evaluator found that the TSS states that: **There is no delayed activation of the software version.** **FOR EXSi TOE: When the restart upgrade command is initiated the TOE is rebooted with the freshly loaded image.** **FOR SSP TOE: When an application is created for a particular software version, and that application is started, that software image is activated.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.2 FPT_TUD_EXT.1 TSS 2

Objective	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). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes all TSF software update mechanisms for updating the system software, includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS states that: **When software updates are made available, an administrator can obtain, verify the integrity of the software by manually verifying the hash of the downloaded software with the hash published on the website, and install those updates.** **The updates can be downloaded from** https://support.broadcom.com/group/ecx/downloads?**.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to 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. Upon investigation, the evaluator found that the TSS states that: **During the execution of the image, an integrity check will be performed. Only if the hash is correct, will the image be installed. If an update is unsuccessful, a message is delivered to the user. Since the update process attempts to update a different copy than what is currently being run, the current active image remains the same and the user continues to run the same code that was being run before the upgrade attempt was made.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.5.3 FPT_TUD_EXT.1 TSS 3

Objective	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 evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, if the options 'support automatic checking for updates' or 'support automatic updates' are chosen, explains what actions are involved in automatic checking or automatic updating by the TOE. Upon investigation, the evaluator found that the TOE does not support options 'support automatic checking for updates' or 'support automatic updates' Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.4 FPT_TUD_EXT.1 TSS 4

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.5 FPT_TUD_EXT.1 TSS 5

Objective	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	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves 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. Upon investigation, the evaluator found that the TSS states that: **Authorized Administrator can query the software version running on the TOE, and can initiate updates to software images. When software updates are made available, an administrator can obtain, verify the integrity of the software by manually verifying the hash**

	of the downloaded software with the hash published on the website, and install those updates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.6 FPT_TUD_EXT.1 Guidance 1

Objective	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 examined the section titled **'Checking the Software Version'** in the AGD to verify that it describes how to query the currently active version and if a trusted update can be installed on the TOE with a delayed activation AGD provides clear guidelines on how to query the loaded but inactive version. Upon investigation, the evaluator found that the AGD describes the commands to query the currently active version. The AGD also states that there is no delayed activation of the trusted update. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.7 FPT_TUD_EXT.1 Guidance 2

Objective	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 examined the section titled **'Checking the Software Version'** in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states that **the administrator downloads the proxysg_7.4.X.X-######.bcsi file and makes note of the published hashes (SHA-256 and MD5). They then must, using a local tool of their own, compute the SHA-256 hash of the .bcsi file. Once the output from the hash tool is computed, they can then visually verify that the 2 hashes are the same. If they differ, then the downloaded file is not valid and should not be used to upgrade.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.8 FPT_TUD_EXT.1 Guidance 3

Objective	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	The evaluator examined the section titled **'Checking the Software Version'** in the AGD to verify that it describes, if a published hash is used to protect the trusted update mechanism, how the Security Administrator can obtain authentic published hash values for the updates. Upon investigation, the evaluator found that the administrator can obtain the authentic published hash from the URL given in the AGD.

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

5.8.5.9 FPT_TUD_EXT.1 Guidance 4

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.10 FPT_TUD_EXT.1 Guidance 5

Objective	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	NA, the TOE is not a distributed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.11 FPT_TUD_EXT.1 Guidance 6

Objective	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 evaluator examined the Security Target & AGD and verified that a certificate-based mechanism is not used for software update digital signature verification. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (TOE Access)

5.9.1 FTA_SSL_EXT.1

5.9.1.1 FTA_SSL_EXT.1 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies whether local administrative session locking or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that: **The TOE provides the administrative user to define inactivity time out periods for administrative sessions. The inactivity period is the same for CLI (local and remote) and are configured through the TOE administrative interfaces.** **If an administrative session remains inactive for the configured length of time, the administrative session is terminated. After termination, administrative authentication is required to access any of the administrative functionality of the TOE. This is applicable from both local and remote administrative sessions.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.1.2 FTA_SSL_EXT.1 Guidance 1

Objective	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 examined the section titled **'Changing the TOE Timeout'** in the AGD to verify that it states whether local administrative session locking, or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD states that sessions terminate after passing the configured inactivity period and that this is applicable to both local and remote sessions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FTA_SSL.3

5.9.2.1 FTA_SSL.3 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that: **The inactivity period is the same for CLI (local and remote) administrative access and are configured through the TOE administrative interfaces.** **If an administrative session remains inactive for the configured length of time, the administrative session is terminated. After termination, administrative authentication is required to access any of the administrative functionality of the TOE. This is applicable from both local and remote administrative sessions.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2.2 FTA_SSL.3 Guidance 1

Objective	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 examined the section titled **'Changing the TOE Timeout'** in the AGD to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD describes how to set the inactivity period and that the inactivity period is applicable to both remote and local sessions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3 FTA_SSL.4

5.9.3.1 FTA_SSL.4 TSS 1

Objective	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 section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that **an Authorized Administrator is able to exit out of both local and remote administrative sessions. When accessing the TOE via the CLI (both local and remote), the exit command is used.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.2 FTA_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	The evaluator examined the section titled **'Logging Out'** in the AGD to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD contains instructions for logging out of the remote or local session. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4 FTA_TAB.1

5.9.4.1 FTA_TAB.1 TSS 1

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

Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that: **For TOE administration, the CLI (SSH) and local console CLI are available. Prior to an administrative user authenticating, that user is presented with an access display banner which displays an advisory notice and consent warning message regarding unauthorized use of the TOE.** **This banner will be displayed prior to allowing Administrator access through those interfaces.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4.2 FTA_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	The evaluator examined the section titled **'Configuring the Banner'** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that the guidance describes configuration settings for login banner using both the SSH and CLI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10 TSS and Guidance Activities (Trusted Path/Channels)

5.10.1 FTP_ITC.1

5.10.1.1 FTP_ITC.1 TSS 1

Objective	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. 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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, 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. Upon investigation, the evaluator found that the TSS states that: **The TOE protects communications with authorized audit server via TLS.** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes all secure communication mechanisms in sufficient detail to

	allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that: **This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.2 FTP_ITC.1 Guidance 1

Objective	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 examined the section titled **'Syslog Event Monitoring'** in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD states that if the connection fails, the SGOS continues to store audit records locally and will transmit any stored contents when connectivity to the syslog server is restored. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2 FTP_TRP.1/Admin

5.10.2.1 FTP_TRP.1/Admin TSS 1

Objective	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. 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 examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that: **All remote administrative communications take place over a secure encrypted session. Remote CLI connections take place over an SSHv2 tunnel. The SSHv2 session is encrypted using AES encryption. The remote administrators are able to initiate SSHv2 communications with the TOE.** **The TOE rejects all insecure remote authentication attempts (e.g., telnet).** The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS protocols are consistent with those specified in the requirement. Upon investigation, the evaluator found that the TSS clearly indicates that the connection is via SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2.2 FTP_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	The evaluator examined the sections titled **'Accessing the TOE Using SSH'** and **'Management Services (SSH Access)'** in the AGD to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the evaluator found that the AGD describes all of the configuration required to establish both remote SSH connections to the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Audit

6.1.1 FAU_GEN.1 Test #1

Item	Data
Test ID	*FAU_GEN.1 Test#1*
Objective	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Expected Output	Each required audit record generated by the TOE.
Pass/Fail with Explanation	Pass. TOE generates all the audit records listed in the table. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.1.2 FAU_GEN.2 Test#1

Item	Data
Test ID	*FAU_GEN.2 Test#1*
Objective	This activity should be accomplished in conjunction with the testing of FAU_GEN.1.1.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	FAU_GEN.1 Test#1 covers this test requirement.
Pass/Fail with Explanation	Pass. TOE generates the audit records for the auditable events listed in the table. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.1.3 FAU_STG_EXT.1 Test #1

Item	Data
Test ID	*FAU_STG_EXT.1 Test#1*
Objective	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.
Note	The syslog server version is *Rsyslogd v8.2001.0*
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Confirm the name and version of the audit server. • Configure the TOE to communicate with a syslog server via TLS. • Generate the audit event and confirm that each event has been logged on the syslog server. • Verify via packet capture that syslog messages have been sent encrypted.

Test Execution Steps	• Confirm the name and version of the audit server.
	• Configuration of TLS and logging host.
	• Log into the TOE:
	  ○ admin
	  ○ password
	• Generate audit records.
	• Confirm that each event has been logged on to the syslog server.
	• Verify via packet capture that syslog messages have been sent encrypted.

Expected Output	• *Each configuration change is audited and sent to the audit server.* • *The packet capture is encrypted.*
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.
Result	Pass.
Test Clean-up	Used command '**`restore-defaults keep-console`**' to clean-up the test configuration.

6.1.4 FAU_STG_EXT.1 Test #2 (a)

Item	Data
Test ID	*FAU_STG_EXT.1 Test #2 (a)*
Test Assurance Activity	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	NA. The ST does not select the option 'drop new audit data'.

6.1.5 FAU_STG_EXT.1 Test #2 (b)

Item	Data
Test ID	*FAU_STG_EXT.1 Test#2 (b)*
Objective	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '**overwrite previous audit records**' in FAU_STG_EXT.1.3)
Note	Used command "`.event-log testfill <number>`" to fill the local storage.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Observe the last archived log date and time. • Wait for the current log to reach its limit and be archived. The TOE replaced the last archive log.
Test Execution Steps	• Observe the last archived log date and time. • Wait for the current log to reach its limit and be archived. The TOE replaced the last archive log.
Expected Output	• *The TOE overwrites the logs when it reaches the maximum size.*
Pass/Fail with Explanation	Pass. Evaluator confirmed that when the TOE's local storage space is exhausted, logs are overwritten. This meets the test requirements.
Result	Pass.
Test Clean-up	

6.1.6 FAU_STG_EXT.1 Test #2 (c)

Item	Data
Test ID	*FAU_STG_EXT.1 Test #2 (c)*
Test Assurance Activity	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 TOE behaves as specified (for the option '**other action**' in FAU_STG_EXT.1.3).
Pass/Fail with Explanation	NA. The ST does not select the option 'other action'.

6.1.7 FAU_STG_EXT.1 Test #3

Item	Data
Test ID	*FAU_STG_EXT.1 Test #3*
Test Assurance Activity	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	NA. ST does not select FAU_STG_EXT.2/LocSpace.

6.1.8 FAU_STG_EXT.1 Test #4

Item	Data
Test ID	*FAU_STG_EXT.1 Test #4*
Test Assurance Activity	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	NA. The TOE is not a distributed TOE.

6.1.9 FCS_NTP_EXT.1.1 Test#1

Item	Data
Test ID	*FCS_NTP_EXT.1.1 Test#1*
Objective	The version of NTP selected in element 1.1 and specified in the ST shall be verified by observing establishment of a connection to an external NTP server known to be using the specified version(s) of NTP. This may be combined with tests of other aspects of FCS_NTP_EXT.1 as described below.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the NTP server on the TOE. • Verify that the TOE syncs with configured NTP server via pcap and logs.
Test Execution Steps	• Configure the NTP server on the TOE. • Verify NTP syncs on TOE. • Verify the NTP version with packet capture. • Verify the successful logs on the TOE.
Expected Output	• *Evidence (e.g., screenshot or CLI output) of NTP sync.* • *Logs showing each time change.* • *Pcap showing the NTP sync packets.*
Pass/Fail with Explanation	Pass. The TOE uses the correct NTP version specified in the ST. This meets the testing requirement.
Result	Pass.
Test-Cleanup	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.1.10 FCS_NTP_EXT.1.2 Test#1

Item	Data
Test ID	*FCS_NTP_EXT.1.2 Test#1*
Objective	[Conditional] If the **message digest algorithm** is claimed in element 1.2, the evaluator will change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source. The evaluator shall use a packet sniffer to capture the network traffic between the TOE and the NTP server. The evaluator uses the captured network traffic, to verify the NTP version, to observe time change of the TOE and uses the TOE's audit log to determine that the TOE accepted the NTP server's timestamp update. The captured traffic is also used to verify that the appropriate message digest algorithm was used to authenticate the time source and/or the appropriate protocol was used to ensure integrity of the timestamp that was transmitted in the NTP packets. **[TD0639 Applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the NTP server on the TOE with correct and incorrect authentication key. • Verify via pacp and logs the action of TOE upon correct and incorrect authentication key configuration.
Test Execution Steps	• Configure the NTP authentication on the TOE. • Configure the NTP server with an unsupported message digest algorithm. • Connect the TOE to an NTP server and verify that the synchronization fails. • Verify the connection is refused via packet capture. • Configure the NTP server with a supported message digest algorithm. • Connect the TOE to an NTP server and verify that the synchronization succeeds. • Verify the connection is established via packet capture. • Verify the connection is established via logs.
Expected Output	• *Evidence (e.g., screenshot or CLI output) of NTP sync for correct authentication key.* • *Logs showing each time change.* • *Pcap showing the NTP sync packets.*
Pass/Fail with Explanation	Pass. The TOE is in sync with NTP Server when the supported Message Digest algorithm is configured on NTP Server, this satisfies the requirement.
Result	Pass.
Test-Cleanup	NA

6.1.11 FCS_NTP_EXT.1.3 Test#1

Item	Data
Test ID	*FCS_NTP_EXT.1.3 Test#1*
Objective	The evaluator shall configure NTP server(s) to support periodic time updates to broadcast and multicast addresses. The evaluator shall confirm the TOE is configured to not accept broadcast and multicast NTP packets that would result in the timestamp being updated. The evaluator shall check that the time stamp is not updated after receipt of the broadcast and multicast packets.
Note	NA
Testbed	*Testbed #1, Testbed #2*

Test Flow (Generic test steps)	• Configure the NTP server on the TOE. • Verify via pacp and logs that the TOE denies the to accept broadcast and multicast packets.
Test Execution Steps	Broadcast: • Configure an NTP server to update from a broadcast address. • Configure TOE to a future date. • Verify that the TOE does not accept broadcast updates from the NTP server with packet capture. Multicast: • Configure an NTP server to update from a multicast address. • Check the current time on the TOE. • Verify with packet capture that the TOE does not accept multicast updates from the NTP server. • Check the new time. There have been no significant changes other than the normal passage of time.
Expected Output	• *Evidence (e.g., screenshot or CLI output) of NTP sync and deny of broadcast/multicast packet.* • *Pcap showing the NTP sync and deny of broadcast/multicast packet.*
Pass/Fail with Explanation	Pass. The TOE does not sync with an NTP server that sends out broadcast updates. This meets testing requirements.
Result	Pass.
Test-Cleanup	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.1.12 FCS_NTP_EXT.1.4 Test#1

Item	Data
Test ID	*FCS_NTP_EXT.1.4 Test#1*
Objective	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 behavior prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4. **[TD0528 Applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure at least 3 NTP servers on the TOE. • Verify via pacp and logs that the TOE syncs to each NTP server.
Test Execution Steps	• Configure at least 3 NTP time sources on TOE. • Verify via logs that the TOE has synced to the NTP server with IP 10.1.3.78. • Verify via packet capture that the TOE has synced to the NTP server with IP 10.1.3.78. • Stop the previous NTP server and sync with another NTP server with IP 10.1.3.78.

	• Verify via packet capture that the TOE has synced to the NTP server with IP 10.1.3.80. • Verify via logs that the TOE has synced to the NTP server with IP 10.1.3.80. • Stop the previous NTP server and sync with another NTP server with IP 10.1.3.80. • Verify via packet capture that the TOE has synced to the NTP server with IP 10.1.5.227. • Verify via logs that the TOE has synced to the NTP server with IP 10.1.5.227.
Expected Output	• *Evidence (e.g., screenshot or CLI output) of NTP sync with each 3 NTP servers.* • *Pcap showing the NTP sync with each 3 NTP servers.*
Pass/Fail with Explanation	Pass. The TOE successfully handles the use of multiple NTP servers. This meets testing requirements.
Result	Pass.
Test-Cleanup	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.1.13 FCS_NTP_EXT.1.4 Test#2

Item	Data
Test ID	*FCS_NTP_EXT.1.4 Test#2*
Objective	Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers). The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system time. This rogue time source needs to be configured in a way (e.g., degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behavior of a correctly functioning NTP server. **[TD0528 Applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the NTP server on the TOE. • Verify via pacp and logs that the TOE syncs to NTP server. • Verify that the TOE does not accept the packets that were captured during earlier sync.
Test Execution Steps	• Verify the time on the TOE. • Configure an NTP server. • Sync the TOE with NTP server and capture those packets. • Verify with packet capture. • Configure a different NTP server to which the TOE syncs. • Replay the packets from the NTP server which were captured during earlier sync. • Verify the TOE does not sync with the NTP server.
Expected Output	• *Evidence (e.g., screenshot or CLI output) of NTP sync the NTP servers.* • *Pcap showing that the TOE rejects the replay packets.*

Pass/Fail with Explanation	Pass. The TOE only accepts NTP updates from configured NTP Servers. This meets the testing requirements.
Result	Pass.
Test-Cleanup	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.1.14 FPT_STM_EXT.1 Test #1

Item	Data
Test ID	*FPT_STM_EXT.1 Test#1*
Objective	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.
Pass/Fail with Explanation	NA. ST does not claim direct setting of the time by the Security Administrator.

6.1.15 FPT_STM_EXT.1 Test #2

Item	Data
Test ID	*FPT_STM_EXT.1 Test#2*
Test Assurance Activity	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.
Note	NA
Testbed	*Testbed #1*
Test Flow (Generic test steps)	• Configure the NTP server on the TOE. • Verify that the TOE syncs with configured NTP server via pcap and logs.
Test Execution Steps	• Configure the NTP server on the TOE. • Verify NTP syncs on TOE. • Verify the NTP version with packet capture. • Verify the successful logs on the TOE.
Expected Output	• *Evidence (e.g., screenshot or CLI output) of NTP sync.* • *Logs showing each time change.* • *Pcap showing the NTP sync packets.*
Pass/Fail with Explanation	Pass. The TOE uses the correct NTP version specified in the ST. This meets the testing requirement.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.1.16 FPT_STM_EXT.1 Test #3

Item	Data
Test ID	*FPT_STM_EXT.1 Test#3*
Test Assurance Activity	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.

Pass/Fail with Explanation	NA. ST does not claim the TOE consists of several parts with independent time information.

6.1.17 FTP_ITC.1 Test #1

Item	Data
Test ID	*FTP_ITC.1 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	FAU_STG_EXT.1 and FCS_TLSC_EXT.1 covers this test requirements.
Pass/Fail with Explanation	Pass. The TOE can be configured to successfully communicate with the external authentication server via syslog server over TLS. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.1.18 FTP_ITC.1 Test #2

Item	Data
Test ID	*FTP_ITC.1 Test #2*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	FAU_STG_EXT.1 and FCS_TLSC_EXT.1 covers this test requirements.
Pass/Fail with Explanation	Pass. The TOE can be configured to successfully communicate with the external authentication server via syslog server over TLS. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.1.19 FTP_ITC.1 Test #3

Item	Data
Test ID	*FTP_ITC.1 Test #3*
Objective	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	FAU_STG_EXT.1 and FCS_TLSC_EXT.1 covers this test requirements.
Pass/Fail with Explanation	Pass. External connections from the TOE are sent via an encrypted channel. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.1.20 FTP_ITC.1 Test #4

Item	Data
Test ID	*FTP_ITC.1 Test #4*
Objective	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations: 1. A duration that exceeds the TOE's application layer timeout setting, 2. 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE to connect with an authorized IT entity. ○ This will configure a secure channel between the TOE and the IT entity. • Initiate the connection between the TOE and the IT entity. • Perform a packet capture of the traffic between the TOE and the IT entity. • Verify that the connection is not sent plaintext. • Disconnect the remote entity from the network. • From the TOE, continue to send data. • Verify that the data sent from the TOE is not sent plaintext. • Reconnect the remote entity to the network. • From the TOE, continue to send data. • Verify that the data sent from the TOE is not sent plaintext.
Test Execution Steps	• Configure the TLS server on the TOE. 1. Interrupt the connection between the devices for a duration that exceeds the TOE's application layer timeout setting verify that connection is down. • Establish the connection between TOE and TLS server. • Verify the disconnection via TOE logs. • Continue to attempt communication and re-connect the TLS server and TOE after a short period of time. Verify communication return. 2. Interrupt the connection between the devices for a duration shorter than the application layer timeout but of sufficient length to interrupt the Network link layer and verify that connection is down. • Establish the connection between TOE and TLS server. • Verify that the traffic is encrypted when connection is restored. • Verify the connection time with TOE Logs.
Expected Output	• *Evidence (screenshot or CLI output) of TLS session configuration.* • *Logs of TLS session configuration.*

	• *Packet capture.*
Pass/Fail with Explanation	Pass. The TOE does not send plaintext traffic when disconnected from the log server. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2 Auth

6.2.1 FCS_CKM.1 RSA

Item	Data
Test ID	*FCS_CKM.1 RSA*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.2 FCS_CKM.1 ECC

Item	Data
Test ID	*FCS_CKM.1 ECC*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.

Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.3 FCS_CKM.1 FCC

Item	Data
Test ID	*FCS_CKM.1 FCC*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.4 FCS_CKM.1 Diffie-Hellman Group 14 and FFC

Item	Data
Test ID	*FCS_CKM.1 Diffie-Hellman Group 14 and FFC*
Objective	Testing for FFC Schemes using Diffie-Hellman group 14 and/or safe-prime groups is done as part of testing in CKM.2.1.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This testing was performed in conjunction with FCS_CKM.2.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_CKM.2.
Result	Pass.
Test Clean-up	NA

6.2.5 FCS_CKM.2 RSA

Item	Data
Test ID	*FCS_CKM.2 RSA*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*

Execution Output	This testing was performed in conjunction with FTP_TRP.1/Admin Test #1 and FTP_ITC.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FTP_TRP.1/Admin Test #1 and FTP_ITC.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.6 FCS_CKM.2 DH14

This test was removed by TD0580.

6.2.7 FCS_CKM.2 FCC

Item	Data
Test ID	*FCS_CKM.2 FCC*
Objective	**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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FTP_TRP.1/Admin Test#1 and FTP_ITC.1 #Test 1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.8 FCS_CKM.4

None.

6.2.9 FCS_COP.1/ Data Encryption

Item	Data
Test ID	*FCS_COP.1/ Data Encryption*
Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	CAVP AES Certs: #A2936 AES is implemented in support of the following protocols: TLS, and SSH. This testing was performed in conjunction with FCS_SSHS_EXT.1.4 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.4 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.10 FCS_COP.1/SignGen

Item	Data
Test ID	*FCS_COP.1/ SigGen*

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	CAVP AES Certs: #A2936 The TOE provides cryptographic signature services using following algorithms and key sizes: RSA Digital Signature Algorithm with key sizes of 2048 and 3072 as specified in section 5.5 of the FIPS PUB 186-4, "Digital Signature Standard". This testing was performed in conjunction with FCS_SSHS_EXT.1.2 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.2 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.11 FCS_COP.1/Hash

Item	**Data**
Test ID	*FCS_COP.1/ Hash*
Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	CAVP AES Certs: #A2936 SHS hashing is used within several services including, hashing, TLS/HTTPS (SHA1, SHA256, SHA384), and SSH (SHA1, SHA256, SHA384, SHA-512). The message digest sizes supported are: 160, 256, 384, and 512 bits. This testing was performed in conjunction with FCS_SSHS_EXT.1.6 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.6 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.12 FCS_COP.1/KeyedHash

Item	**Data**
Test ID	*FCS_COP.1/ KeyedHash*
Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	CAVP AES Certs: #A2936 The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512. This testing was performed in conjunction with FCS_SSHS_EXT.1.6 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.6 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.13 FCS_RBG_EXT.1 Test#1

Item	**Data**

Test ID	*FCS_RBG_EXT.1 Test#1*
Objective	The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	CAVP AES Certs: #A2936 The TOE produces all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES). This testing was performed in conjunction with FCS_SSHS_EXT.1.2 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_SSHS_EXT.1.2 Test#1 and FCS_TLSC_EXT.1.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.14 FIA_AFL.1 Test #1

Item	Data
Test ID	*FIA_AFL.1 Test #1*
Objective	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.**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Connect to the TOE using password-based authentication. • Set user login time out after successive unsuccessful authentication attempts. • Verify that the user is locked after the set max-failed-attempts are met.
Test Execution Steps	• Configure a maximum number of failure attempts before being locked out. • Confirm the configuration has been implemented in the config. • Authenticate and verify incorrect credentials result in a failed connection. • Verify with logs that attempts with unsuccessful credentials will be rejected. • Login with good credentials and verify that it fails. • Verify that the user account is locked. • Verify that the user account is now locked out via logs.
Expected Output	***The TOE should not allow authentication once the authentication attempt limit has been reached.***
Pass/Fail with Explanation	Pass. When the authentication attempts limit is reached, authentication attempts with valid credentials are successful.
Result	Pass.
Test Clean-up	NA

6.2.15 FIA_AFL.1 Test #2a

Item	Data
Test ID	*FIA_AFL.1 Test #2a*
Objective	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).
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Unlock the user by another admin. • Verify that the user is authenticated using password-based authentication
Test Execution Steps	• Login into the TOE using the admin administrator account. • Verify after the final attempt that the test user account is now locked out. • Verify that the user account is locked out via log. • Manually unlock the user account using the administrator account. • Verify the user was unblocked via logs. • Authenticate and verify correct credentials result in a successful connection. • Verify the connection is established via logs.
Expected Output	• *The Administrator user should be able to enable the locked user and the user should establish successful connection with correct credentials after unlocking.*
Pass/Fail with Explanation	Pass. Authentication failure disallows user from validating after configured number of failed attempts. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.16 FIA_AFL.1 Test #2b

Item	Data
Test ID	*FIA_AFL.1 Test #2b*
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 91uthorization 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 91uthorization attempt using valid credentials results in successful access.
Pass/Fail with Explanation	NA. The ST does not select time period selection in FIA_ALF.1.2

6.2.17 FIA_PMG_EXT.1 Test #1

Item	Data
Test ID	*FIA_PMG_EXT.1 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Select subsets of passwords to attempt to configure. ○ Combination of lowercase and uppercase letters: {QweRty!@#$%^789} ○ Combination of lowercase, uppercase letters, and numbers: "('Sun,456-./')&*+;" ○ Combination of lowercase, uppercase letters, numbers and special characters: ["m0on":<+?>123_`~\|] • Attempt to create users with each password.   ○ username: good1, password: {QweRty!@#$%^789}   ○ username: good2, password: "('Sun,456-./')&*+;"   ○ username: good3, password: ["m0on":<+?>123_`~|] • Verify that each attempt was accepted based on the password creation. • Verify that an audit record was generated with each attempt.
Test Execution Steps	• Set the minimum password length to 8 characters. • Verify via logs that the configuration is updated. • Configure a policy for authentication of the users. • Verify from the logs that the policy has be implemented successfully. • Create a user "good1" with a combination of lowercase, uppercase letters, numbers and special characters --- {QweRty!@#$%^789} • Verify via logs that the user has been created. • Log into the TOE using the good1 user and verify that the user was able to get the access to the TOE. • Verify via logs that the user good1 successfully logged in to the TOE. • Create a user "good2" with a combination of lowercase, uppercase letters, numbers and special characters--- "('Sun,456-./')&*+;" • Verify via logs that the user has been created. • Log into the TOE using the good2 user and verify that the user was able to get access to the TOE. • Verify via logs that the good2 user successfully logged in to the TOE. • Create a user "good3" with a combination of lowercase, uppercase letters, numbers and special characters--- ["m0on":<+?>123_`~|] • Verify via logs that the user has been created. • Log into the TOE using the good3 user and verify that the user was able to get access to the TOE. • Verify via logs that the user successfully logged in to the TOE.
Expected Output	• *Evidence (e.g., screen capture or CLI output) from each password creation attempt.* • *Logs showing the successful password creation.*

Pass/Fail with Explanation	Pass. The TOE was able to create users with good passwords. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.18 FIA_PMG_EXT.1 Test #2

Item	Data
Test ID	*FIA_PMG_EXT.1 Test #2*
Objective	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
Note	NA
Testbed	*Testbed #1, Testbed #2*

Test Flow (Generic test steps)	• Attempt to create users with each password.
	  ○ username: bad1, password: 12390Rt
	  ○ username: bad2, password: 12%$345a
	  ○ username: bad3, password: Open#Ykk
	  ○ username: bad4, password: 12345678
	  ○ username: bad5, password: abcdefgh
	  ○ username: bad6, password: Admin@123
	  ○ username: bad7, password: Water @123
	• Verify that each attempt for password creation was rejected.
	• Verify that an audit record was generated with each attempt.

Test Execution Steps	• Set the rules for password complexity and minimum password length to 8 characters. • Verify via logs that the configuration is updated. • Configure a policy for authentication of the users. • Verify from the logs that the policy has be implemented successfully. • Create a user "bad1" with 7 characters using the combination of lowercase and uppercase letters and numbers "12390Rt". • Verify that the user bad1 is created but password set action is not successful. • Create a user "bad2" with 8 characters using numbers, special characters and lowercase characters "12%$345a". • Verify that the user bad2 is created but password set action is not successful. • Create a user "bad3" with 8 characters using the combination of lowercase, uppercase letters and special characters "Open#Ykk". • Verify that the user bad3 is created but password set action is not successful. • Create a user "bad4" with 8 characters without using the combination of lowercase, uppercase letters, and special characters "12345678". • Verify that the user bad4 is created but password set action is not successful. • Create a user "bad5" with more than 8 characters without using the combination of lowercase, uppercase letters, numbers, and special characters "abcdefgh".

	• Verify that the user bad5 is created but password set action is not successful. • Create a user “bad6” with more than 8 characters with common words such as ----“Admin@123”. • Verify that the user bad6 is created but password set action is not successful. • Create a user “bad7” with more than 8 characters with a white space in between----“Water @123”. • Verify that the user bad6 is created but password set action is not successful.
Expected Output	• *Evidence (e.g., screen capture or CLI output) from each password creation attempt.* • *Logs showing the unsuccessful password creation.*
Pass/Fail with Explanation	Pass. The TOE was able to reject users with bad passwords. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command ‘`restore-defaults keep-console`’ to clean-up the test configuration.

6.2.19 FIA_UIA_EXT.1 Test #1

Item	Data
Test ID	*FIA_UIA_EXT.1 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*

Test Flow (Generic test steps)	• Configure the TOE to support authentication.
	• Attempt to login from a local connection with incorrect credentials.
	  ○ Confirm that access was denied.
	• Log into the TOE from a local connection with correct credentials.
	  ○ Confirm that access was granted.
	• Verify that an audit record was generated showing both login failure and success.
	• Repeat the above steps for any additional login method supported by TOE.

Test Execution Steps	• Configure the TOE to support authentication and show existing users. **Local Console:** • Log onto the TOE local connection with incorrect credentials. • Verify the failure via logs. • Log onto the TOE local connection with correct credentials. • Verify via logs. **SSH:** • Log onto the TOE remote SSH CLI connection with incorrect credentials. • Verify the failure via logs. • Log onto the TOE remote SSH CLI with correct credentials. • Verify via logs.

Expected Output	• *Incorrect credentials result in failed login attempt* • *Correct credentials result in successful login attempt* • *Logs reflect login attempts*
Pass/Fail with Explanation	Pass. Presenting incorrect authentication credentials results in denied access to the TOE. Presenting correct authentication credentials results in access being allowed to the TOE. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.20 FIA_UIA_EXT.1 Test #2

Item	Data
Test ID	*FIA_UIA_EXT.1 Test #2*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• At the remote authentication prompt attempt verify that the list of services available is limited to those specified in the requirement in the ST. • Verify that no other functionality is available.
Test Execution Steps	**SSH:** **Display the warning banner in accordance with FTA_TAB.1:** • Show that commands are not available prior to login and verify that the login banner is displayed. • Login into the TOE via GUI. • Verify that the services are available after login. • Verify authentication logs reflect success.
Expected Output	• *No services except displaying a banner should be available to a remote administrator attempting to login to the TOE via the SSH.*
Pass/Fail with Explanation	Pass. No system services are available to an unauthenticated user connecting remotely. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.21 FIA_UIA_EXT.1 Test #3

Item	Data
Test ID	*FIA_UIA_EXT.1 Test #3*
Objective	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.
Note	NA

Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• At the local authentication prompt attempt verify that the list of services available is limited to those specified in the requirement in the ST. • Verify that no other functionality is available.
Test Execution Steps	• Connect to the TOE via console and verify the only option presented is the username/password entry. • Attempt to connect to the TOE with correct credentials. • Verify that the configurations commands are now available. • Verify authentication logs reflect success.
Expected Output	• *No services except displaying a banner should be available to a local administrator attempting to login to the TOE via the console.*
Pass/Fail with Explanation	Pass. No system services are available to an unauthenticated user via the directly connected console. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.22 FIA_UAU.7 Test #1

Item	Data
Test ID	*FIA_UAU.7 Test #1*
Objective	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
Note	NA
Testbed	*Testbed #1, Testbed #2*

Test Flow (Generic test steps)	• At the directly connected login prompt, enter incorrect authentication credentials.
	  ○ Verify that at most obscured feedback is provided.
	• At the directly connected login prompt, enter correct authentication credentials.
	  ○ Verify that at most obscured feedback is provided.
	• At the remote login prompt, enter incorrect authentication credentials.
	  ○ Verify that at most obscured feedback is provided.
	• At the remote login prompt, enter correct authentication credentials.
	• Verify that at most obscured feedback is provide.

Test Execution Steps	**SSH:** • Connect to the TOE via SSH with correct authentication credentials and verify that no feedback is provided. • Verify authentication logs reflect success. • Connect to the TOE via SSH with incorrect authentication credentials and verify that no feedback is provided. • Verify authentication logs reflect failure. **Console:** • Connect to the TOE via console with correct authentication credentials and verify that at most obscured feedback is provided. • Log into the enable prompt.

	• Verify authentication logs reflect success. • Connect to the TOE via console with incorrect authentication credentials and verify that at most obscured feedback is provided. • Verify authentication logs reflect failure.
Expected Output	• *While entering password for authentication most obscured feedback is provided.*
Pass/Fail with Explanation	Pass. At both the directly connected and remote login prompt, the TOE does not provide anything more than obscured feedback. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.23 FMT_MOF.1/ManualUpdate Test #1

Item	Data
Test ID	*FMT_MOF.1/ManualUpdate Test #1*
Objective	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Create a read-only user on the TOE. • Login into the TOE with read-only user. • Verify that the user does not have the privilege to perform manual update on the TOE.
Test Execution Steps	• Create a read-only user on the TOE. • Verify the user was created. • Verify the user was created via logs. • Login into the TOE with read-only user. • Verify that the user does not have the privilege to perform manual update on the TOE. • Login with privileged user on the TOE and show the option to perform manual update is available.
Expected Output	• *The TOE should reject manual update option for user with no administrator (read-only) rights.*
Pass/Fail with Explanation	Pass. An unprivileged user cannot perform a software update on the TOE. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.24 FMT_MOF.1/ManualUpdate Test #2

Item	Data
Test ID	*FMT_MOF.1/ManualUpdate Test #2*
Objective	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.

Note	*FMT_MOF.1/ManualUpdate Test #2*
Testbed	*Testbed #1, Testbed #2*
Execution Output	Authenticated user can configure trusted update. This test case is covered by the test for FPT_TUD_EXT.1 Test #1. This meets the testing requirements
Pass/Fail with Explanation	Pass. Authenticated user can configure trusted update. This test case is covered by the test for FPT_TUD_EXT.1 Test #1. This meets the testing requirements
Result	Pass.
Test Clean-up	NA

6.2.25 FMT_MOF.1/Functions (1) Test #1

Item	Data
Test ID	*FMT_MOF.1/Functions (1) Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Log into the TOE as a lower privileged user. • Attempt to modify the parameters involved with the syslog server and verify the command is rejected.
Test Execution Steps	• Log into the TOE as a lower privileged user. • Make sure that the user is lower privileged user. • Attempt to modify the parameters involved with the syslog server and verify the command is rejected. • Verify the logs.
Expected Output	• *The TOE should reject attempts from an unprivileged user to modify audit data on the TOE.*
Pass/Fail with Explanation	Pass. The TOE does not allow an unauthenticated user to modify and delete the audit records.
Result	Pass.
Test Clean-up	NA

6.2.26 FMT_MOF.1/Functions (1)Test #2

Item	Data
Test ID	*FMT_MOF.1/Functions (1) Test #2*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Login to the TOE as an admin. • Attempt to modify the parameters involved with the syslog server.
Test Execution Steps	• Login to the TOE as an admin. • Make sure that "admin" is privileged user. • Attempt to modify the parameters involved with the syslog server. • Verify the logs.
Expected Output	• *The TOE should accept attempts from an Admin to modify audit data on the TOE.*
Pass/Fail with Explanation	Pass. The TOE does not allow an unauthenticated user to modify and delete the audit records.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.27 FMT_MOF.1/Functions (2) Test #1

Item	Data
Test ID	*FMT_MOF.1/Functions (2) Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow	• Log into the TOE as a lower privileged user.

(Generic test steps)	• Attempt to modify the parameters involved with the audit data and verify the command is rejected.
Test Execution Steps	• Log into the TOE as a lower-privileged user. • Make sure that the user is a lower privileged user. • Attempt to modify the parameters involved with the audit data and verify the command is rejected. • Verify the failure logs.
Expected Output	• *The TOE should reject attempts from an unprivileged user to modify audit data parameters on the TOE.*
Pass/Fail with Explanation	Pass. The TOE does not allow a lower privileged user to authenticate successfully and modify the parameters for audit records.
Result	Pass.
Test Clean-up	NA

6.2.28 FMT_MOF.1/Functions (2) Test #2

Item	Data
Test ID	*FMT_MOF.1/Functions (2) Test #2*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Log into the TOE as a higher privileged user. • Attempt to modify the parameters involved with the audit data and verify the command is accepted.
Test Execution Steps	• Log into the TOE as an administrator user. • Make sure that "admin" is a higher privileged user. • Attempt to modify the parameters involved with the audit data and verify the command is accepted. • Verify the successful logs.
Expected Output	• *The TOE should accept attempts from a privileged user to modify audit data parameters on the TOE.*
Pass/Fail with Explanation	Pass. The TOE allows a security administrator to authenticate successfully and modify the parameters for audit records.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.29 FMT_MOF.1/Functions (3) Test #1

Item	Data
Test ID	*FMT_MOF.1/Functions (3) Test #1*
Objective	(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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Log into the TOE as a lower-privileged user. • Attempt to modify the behavior when the local audit storage is full and verify the command is rejected.
Test Execution Steps	• Log into the TOE as a lower-privileged user. • Make sure that user is a lower privileged user. • Attempt to modify the behavior when the local audit storage is full and verify the command is rejected. • Verify the authentication via logs.
Expected Output	• *The TOE should reject attempts from an unprivileged user to modify local audit storage parameters on the TOE.*
Pass/Fail with Explanation	Pass. The TOE does not allow a lower-privileged user to authenticate successfully and modify the parameters when the local audit storage is full.
Result	Pass.
Test Clean-up	

6.2.30 FMT_MOF.1/Functions (3) Test #2

Item	Data
Test ID	*FMT_MOF.1/Functions (3) Test #2*
Objective	(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
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Log into the TOE as a lower-privileged user. • Attempt to modify the behavior when the local audit storage is full and verify the command is accepted.

Test Execution Steps	• Log into the TOE as an administrator user. • Make sure that “admin” is a higher privileged user. • Attempt to modify the behavior when the local audit storage is full and verify the command is accepted. • Verify the logs generated after reset.
Expected Output	• *The TOE should accept attempts from a privileged user to modify local audit storage parameters on the TOE.*
Pass/Fail with Explanation	Pass. The TOE allows a security administrator to authenticate successfully and modify the parameters when the local audit storage is full.
Result	Pass.
Test Clean-up	Used command ‘`restore-defaults keep-console`’ to clean-up the test configuration.

6.2.31 FMT_MOF.1/Functions Test #3

Item	Data
Test ID	*FMT_MOF.1/Functions (3) Test #3*
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	NA. The ST does not select 'determine the behaviour of' in the first selection.

6.2.32 FMT_MOF.1/Functions Test #4

Item	Data
Test ID	*FMT_MOF.1/Functions (3) Test #4*
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 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	NA. The ST does not select 'determine the behaviour of' in the first selection.

6.2.33 FMT_MTD.1/CryptoKeys Test #1

Item	Data
Test ID	*FMT_MTD.1/CryptoKeys Test #1*
Objective	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Login into the TOE with unprivileged user. • Verify the generation of CSR fails for unprivileged user.
Test Execution Steps	Crypto Key Generation using CSR: • Login into the TOE with unprivileged user. • Verify the generation of CSR fails for unprivileged user.
Expected Output	• *The TOE should reject attempts from an unprivileged user to manage crypto keys on the TOE.* • *Evidence (screenshot or CLI output) showing privilege level of the user.* • *Evidence (screenshot or CLI output) showing unsuccessful attempts.*
Pass/Fail with Explanation	Pass. Unprivileged user cannot perform security related configurations on the TOE. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.34 FMT_MTD.1/CryptoKeys Test #2

Item	Data
Test ID	*FMT_MTD.1/CryptoKeys Test #2*
Objective	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Login into the TOE with privileged user. • Verify the generation of CSR passes for privileged user.
Test Execution Steps	Crypto Key Generation using CSR: • Login into the TOE with privileged user. • Verify the generation of CSR passes for privileged user.
Expected Output	• *The TOE should accept attempts from a privileged user to modify, delete, generate/import crypto keys on the TOE.* • *Evidence (screenshot or CLI output) showing privilege level of the user.*

	• *Evidence (screenshot or CLI output) and log showing successful attempts.*
Pass/Fail with Explanation	Pass. Authorized user can perform security related configurations on the TOE. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.35 FMT_SMF.1 Test #1

Item	Data
Test ID	*FMT_SMF.1 Test #1*
Objective	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Note	*The TSF shall be capable of performing the following management functions:* • *Ability to administer the TOE locally and remotely;* • *Ability to configure the access banner;* • *Ability to configure the session inactivity time before session termination or locking;* • *Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates;* • *Ability to configure the authentication failure parameters for FIA_AFL.1;* • [○ *Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);* ○ *Ability to modify the behaviour of the transmission of audit data to an external IT entity;* ○ *Ability to manage the cryptographic keys;* ○ *Ability to configure the cryptographic functionality;* ○ *Ability to re-enable an Administrator account;* ○ *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;* ○ *Ability to manage the trusted public keys database;* ○ *No other capabilities*].
Testbed	*Testbed #1, Testbed #2*
Pass/Fail with Explanation	Pass. FMT_SMF.1 Specification of Management Functions requirements has been met throughout the various security functionality testing of the TOE.
Result	Pass.
Test Clean-up	NA

6.2.36 FMT_SMR.2 Test #1

Item	Data
Test ID	*FMT_SMR.2 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	As there are two interfaces where these can be tested (over the Console/SSH) management functions are tested from the Console & SSH interface. Each management function is available on the Console & SSH interface. The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces.
Pass/Fail with Explanation	Pass. As there are two interfaces where these can be tested (over the Console/SSH) management functions are tested from the Console & SSH interface. Each management function is available on the Console & SSH interface. The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces.
Result	Pass.
Test Clean-up	NA

6.2.37 FTA_SSL.3 Test #1

Item	Data
Test ID	*FTA_SSL.3 Test #1*
Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure a SSH time out period of 1 minute on administrative sessions. • Connect to the TOE from the remote CLI. • Let the SSH connection set idle for 1 minute. • Verify that the session was terminated. • Configure a SSH out period of 2 minutes on administrative sessions. • Connect to the TOE from the remote CLI. • Let the SSH connection set idle for 2 minutes. • Verify that the session was terminated.
Test Execution Steps	• Configure a SSH time out period of 1 minute on administrative sessions. • Login onto the TOE via SSH. • Let the SSH connection set idle for 1 minute. • Verify that the session was terminated. • Verify that a log was created for the configuring the timeout period. • Verify that a log was created for inactivity logout. • Configure a SSH time out period of 2 minutes on administrative sessions.

	• Login onto the TOE via SSH. • Let the SSH connection set idle for 2 minutes. • Verify that the session was terminated. • Verify that a log was created for the configuring the timeout period. • Verify that a log was created for inactivity logout.
Expected Output	• *The TOE should terminate idle remote sessions after the specified time.* • *Time of audit log indicating 'Automatic logout due to Keyboard inactivity' shows auto logout of session after TOE is idle for specified period.*
Pass/Fail with Explanation	Pass. The remote administrative time out periods can be set by the administrative user. The TOE enforces the configured inactivity period in each instance. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.2.38 FTA_SSL.4 Test #1

Item	Data
Test ID	*FTA_SSL.4 Test #1*
Objective	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Log onto the TOE through a directly connected interface. • Using the instructions provided by the user guide, log off of the TOE
Test Execution Steps	• Log into the TOE through a local administrative interface (console). • Verify the logs reflect log in. • Using the instructions provided by the user guide log off. • Verify the logs reflect the log off.
Expected Output	• *Evidence (e.g., screenshot or CLI output) from logging into the TOE locally.* • *Evidence (e.g., screenshot or CLI output) showing the log out.* • *Log showing the log in and log out.*
Pass/Fail with Explanation	Pass. The TOE allows user to terminate the directly connected administrative sessions. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.39 FTA_SSL.4 Test #2

Item	Data
Test ID	*FTA_SSL.4 Test #2*
Objective	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Note	NA

Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Log onto the TOE through remote interface. • Using the instructions provided by the user guide, log off from the TOE.
Test Execution Steps	• Login onto the TOE through SSH. • Verify via logs that the user has logged in. • Using the instructions provided by the user guide to log off. • Verify via logs that the user has logged out.
Expected Output	• *Evidence (e.g., screenshot or CLI output) from logging into the TOE remotely.* • *Evidence (e.g., screenshot or CLI output) showing the log out.* • *Log showing the log in and log out.*
Pass/Fail with Explanation	Pass. The TOE allows user to terminate the remote administrative sessions. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.40 FTA_SSL_EXT.1.1 Test #1

Item	Data
Test ID	*FTA_SSL_EXT.1.1 Test #1*
Objective	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure a local time out period of 1 minute on administrative sessions. • Connect to the TOE from the local connection. • Let the local connection set idle for 1 minute. • Verify that the session was terminated. • Configure a local time out period of 2 minutes on administrative sessions. • Connect to the TOE from the local connection. • Let the local connection set idle for 2 minutes. • Verify that the session was terminated.
Test Execution Steps	• Configure a local time out period of 1 min on administrative sessions from the local console. • Log into the TOE via local console. Let the console connection set idle for 1 minute. • Verify that the session was terminated as the user returns to the login screen. • Verify that a log was created for the configuring the timeout period. • Verify that a log was created for inactivity logout. • Configure a local time out period of 2 mins on administrative sessions from the local console. • Log into the TOE via local console. Let the console connection set idle for 2 minutes. • Verify that the session was terminated as the user returns to the login screen. • Verify that a log was created for the configuring the timeout period.

	• Verify that a log was created for inactivity logout.
Expected Output	• *The TOE should terminate idle local sessions after the specified time.* • *Time of audit log indicating 'Automatic logout due to Keyboard inactivity' shows auto logout of session after TOE is idle for specified period of time.*
Pass/Fail with Explanation	Pass. The local administrative inactivity was able to be set to multiple values. In each instance, the TOE logged the user out after the configured time. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '**`restore-defaults keep-console`**' to clean-up the test configuration.

6.2.41 FTA_TAB.1 Test #1

Item	Data
Test ID	*FTA_TAB.1 Test #1*
Objective	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure access banners on TOE. • Verify that the banner is being displayed while login.
Test Execution Steps	SSH: • Configure access banners on TOE. • Verify that the banner is being displayed in SSH while login. • Verify the logs generated for the configuration steps. Console: • Configure access banners on TOE. • Verify that the banner is being displayed while login. • Verify the logs generated for the configuration steps.
Expected Output	• *When any user accesses the TOE through the console or SSH the configured banner should be displayed prior to authenticating the TOE.*
Pass/Fail with Explanation	Pass. For both Console and SSH the banner is getting displayed. This meets the testing requirements.
Result	Pass.
Test Clean-up	Used command '**`restore-defaults keep-console`**' to clean-up the test configuration.

6.2.42 FPT_APW_EXT.1 Test#1

Item	Data
Test ID	*FPT_APW_EXT.1 Test#1*
Objective	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE

	b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs.
Note	NA
Testbed	*Testbed #1*
Execution Output	This testing was performed in conjunction with FPT_TUD_EXT.1 Test #1 to demonstrate correct operation.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FPT_TUD_EXT.1 Test #1 to demonstrate correct operation.
Result	Pass.
Test Clean-up	NA

6.2.43 FPT_SKP_EXT.1 Test#1

None.

6.2.44 FTP_TRP.1/Admin Test #1

Item	Data
Test ID	*FTP_TRP.1/Admin Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE to support remote administration. ○ This will configure a secure channel between the TOE and the remote administrator. • Initiate a remote administrative session with the TOE. • Perform a packet capture of the traffic between the TOE and the remote administrator. • Verify that the connection is not sent plaintext.
Test Execution Steps	• Start an administrative session with the device over SSH. • Capture the packets between the remote workstation and the TOE and verify that the connection is successful. • Verify via logs.
Expected Output	• *Successful communication between TOE and remote administrator via SSH. Encrypted Packets in SSH connection in packet capture confirms successful connection.*
Pass/Fail with Explanation	Pass. Remote administrative access to the TOE is over secured channels. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.2.45 FTP_TRP.1/Admin Test #2

Item	Data
Test ID	*FTP_TRP.1/Admin Test #2*
Objective	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This is covered by FTP_TRP.1/Admin Test #1 and FCS_SSH_EXT.1.1 Test#1. In those tests, the data was not sent in plaintext.
Pass/Fail with Explanation	Pass. This is covered by FTP_TRP.1/Admin Test #1 and FCS_SSH_EXT.1.1 Test#1. In those tests, the data was not sent in plaintext.
Result	Pass.
Test Clean-up	NA

6.3 SSHS

6.3.1 FCS_SSHS_EXT.1.2 Test #1

Item	Data
Test ID	*FCS_SSHS_EXT.1.2 Test #1*
Objective	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 applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE to support RSA and ECDSA based SSH authentication method. • Verify via logs and packet capture that the connection is successful, and the server supports the claimed algorithms.
Test Execution Steps	SSH-RSA: • Generate the SSH-RSA pub key. • Configure the TOE to support RSA based SSH authentication method. • Log into the TOE SSH with RSA-based authentication. • Verify authentication is successful via logs. • Verify that connection is successful via packet capture. RSA-SHA2-256: • Generate the RSA-SHA2-256 pub key. • Configure the TOE to support RSA based SSH authentication method. • Log into the TOE SSH with RSA-based authentication. • Verify authentication is successful via logs.

	• Verify that connection is successful via packet capture. RSA-SHA2-512: • Generate the RSA-SHA2-512 pub key. • Configure the TOE to support RSA based SSH authentication method. • Log into the TOE SSH with RSA-based authentication. • Verify authentication is successful via logs. • Verify that connection is successful via packet capture.
Expected Output	• *The TOE should support successful negotiations when using the claimed public key algorithm (ssh-rsa, rsa-sha2-256 and rsa-sha2-512)* • *Evidence (screenshot or CLI output) showing configuration of each algorithm.* • *Log showing successful/unsuccessful connection of each algorithm.* • *Packet capture showing successful/unsuccessful connection of each algorithm.*
Pass/Fail with Explanation	Pass. The TOE supports each supported client public-key authentication algorithm from a remote SSH client. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.2 FCS_SSHS_EXT.1.2 Test #2

Item	Data
Test ID	*FCS_SSHS_EXT.1.2 Test #2*
Objective	Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. **[TD0631 applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE to support RSA and ECDSA based SSH authentication method. • Verify via logs and packet capture that the connection is unsuccessful when the TOE is not configured to support that RSA/ECDSA keypair.
Test Execution Steps	SSH_RSA: • Configure the SSH client with a new RSA keypair for SSH without configuring the TOE and attempt to login using SSH-RSA key. • Verify authentication failure logs. • Verify authentication failure via packet capture.
Expected Output	• *The TOE should reject SSH connections when incorrect/unknown public keys are presented.* • *Evidence (screenshot or CLI output) of attempting to authenticate the TOE.* • *Packet capture of unsuccessful authentication.* • *Log showing unsuccessful authentication.*
Pass/Fail with Explanation	Pass. The TOE does not allow public key authentication if the public key of the SSH user have not uploaded to the TOE. This meets the test requirements.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.3.3 FCS_SSHS_EXT.1.2 Test #3

Item	Data
Test ID	*FCS_SSHS_EXT.1.2 Test #3*
Objective	Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication succeeds when the correct password is provided by the connecting SSH client. **[TD0631 applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Establish SSH session with password-based authentication using correct password. • Verify successful authentication logs and pcap.
Test Execution Steps	• Log into the TOE via SSH with password authentication using correct password. • Verify successful authentication logs. • Verify via capture that SSH session was established.
Expected Output	• *Evidence (screenshot or CLI output) of configuring password-based authentication.* • *Log of configuring password-based authentication.* • *Log showing successful authentication.*
Pass/Fail with Explanation	Pass. The TOE can accept password authentication from a remote SSH client. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.4 FCS_SSHS_EXT.1.2 Test #4

Item	Data
Test ID	*FCS_SSHS_EXT.1.2 Test #4*
Objective	Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client. **[TD0631 applied]**
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Establish SSH session with password-based authentication using correct password. • Verify successful authentication logs and pcap.
Test Execution Steps	• Log into the TOE via SSH with password authentication using incorrect password. • Verify authentication logs. • Verify via capture that SSH session was terminated.
Expected Output	• *Evidence (screenshot or CLI output) of configuring password-based authentication.* • *Log of configuring password-based authentication.* • *Log showing unsuccessful authentication.*

Pass/Fail with Explanation	Pass. The TOE does not establish a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.5 FCS_SSHS_EXT.1.3 Test #1

Item	Data
Test ID	*FCS_SSHS_EXT.1.3 Test #1*
Objective	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Note	Acumen-SSHS tool is used to send packets greater than 65,535 bytes to TOE.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use of Acumen-SSHS tool to send packet larger than that specified in ST. • Verify that the TOE rejects the connection. • Verify with logs and PCAP.
Test Execution Steps	• Use Acumen-SSHS tool to send packets greater than 65,535 bytes to TOE. • Verify the TOE rejects the connection attempt. • Verify authentication logs reflect failures.
Expected Output	• *The TOE should drop packets larger than the allowed range.* • *Log showing the reason for closing the connection.* • *Packet capture showing TOE closes the connection when packet sent is larger than allowed range.*
Pass/Fail with Explanation	Pass. The TOE drops large packets that are received within an SSH session. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.6 FCS_SSHS_EXT.1.4 Test #1

Item	Data
Test ID	*FCS_SSHS_EXT.1.4 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*

Test Flow (Generic test steps)	• Establish an SSH session with the configured supported encryption algorithms. • Verify that the SSH session was encrypted with the specified supported encryption algorithm.
Test Execution Steps	• Configure the TOE for SSH connection using claimed encryption algorithms. **AES128-CTR:** • Connect to the TOE using AES128-CTR. • Verify that the SSH session was encrypted via log. • Verify that the SSH session was encrypted using AES128-CTR via capture. **AES256-CTR:** • Establish an SSH session using AES256-CTR. • Verify that the SSH session was encrypted via log. • Verify that the SSH session was encrypted using AES256-CTR via capture. **AES128-GCM@OPENSSH.COM:** • Establish an SSH session using AES-128-GCM@OPENSSH.COM. • Verify that the SSH session was encrypted via log. • Verify that the SSH session was encrypted using AES-128-GCM@OPENSSH.COM via capture. **AES-256-GCM@OPENSSH.COM:** • Establish an SSH session using AES-256-GCM@OPENSSH.COM. • Verify that the SSH session was encrypted via log. • Verify that the SSH session was encrypted using AES-256-GCM@OPENSSH.COM via capture.
Expected Output	• *The TOE should support encryption using the claimed encryption algorithms.*
Pass/Fail with Explanation	Pass. The TOE can use each of the claimed symmetric algorithms for SSH connections. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.7 FCS_SSHS_EXT.1.5 Test #1

Item	Data
Test ID	*FCS_SSHS_EXT.1.5 Test #1*
Objective	Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test objective: This test case is meant to validate that the TOE server will support host public keys of the claimed algorithm types. [**TD0631 Applied.**]
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow	• Configure the TOE with the claimed host-key algorithms.

(Generic test steps)	• Verify that the connection is successful via logs and packet captures.
Test Execution Steps	• Verify the Claimed Host key algorithms by TOE. Screenshot of the TOE with Claimed Host key algorithms by TOE. **SSH-RSA:** • Established a session with the TOE using the ssh-rsa host key algorithm. • Verify through logs. • Verify through packet capture that the SSH session was encrypted using specified host key algorithm. **RSA-SHA2-256:** • Established a session with the TOE using the rsa-sha2-256 host key algorithms. • Verify through logs. • Verify through packet capture that the SSH session was encrypted using specified host key algorithm. **RSA-SHA2-512:** • Established a session with the TOE using the rsa-sha2-512 host key algorithms. • Verify through logs. • Verify through packet capture that the SSH session was encrypted using specified host key algorithm.
Expected Output	• *The TOE allows the client to connect using the supported Host public key algorithm.*
Pass/Fail with Explanation	Pass. The TOE allows client to connect using the supported Host public key algorithm. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.8 FCS_SSHS_EXT.1.5 Test #2

Item	Data
Test ID	*FCS_SSHS_EXT.1.5 Test #2*
Objective	Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected. 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. **[TD0631 Applied.]**
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Attempt to connect the TOE with the unsupported Host public key algorithm. • Verify that the connection is unsuccessful via logs and packet captures.
Test Execution Steps	• Verify the Claimed Host key algorithms by the TOE.

	• Established a session with the TOE using the non-supported host key algorithms (SSH-DSS). • Verify through logs and packet capture that the SSH session was not established.
Expected Output	• *The TOE does not allow the client to connect using the unsupported Host public key algorithm.*
Pass/Fail with Explanation	Pass. Toe rejects the connection if the session is established using a non-supported host key algorithm. This meets the testing requirement.
Result	Pass.
Test Clean-up	NA

6.3.9 FCS_SSHS_EXT.1.6 Test #1

Item	Data
Test ID	*FCS_SSHS_EXT.1.6 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Establish an SSH session with the configured supported HMAC algorithms. • Verify that the SSH session was encrypted with the specified supported HMAC algorithm.
Test Execution Steps	• Configure the TOE for SSH connection using claimed HMAC algorithms. **HMAC-SHA1:** • Establish an SSH session with HMAC-SHA1. • Verify that the SSH session was encrypted using HMAC-SHA1 via log. • Verify that the message integrity algorithm used was as configured via capture. **HMAC-SHA1-96:** • Establish an SSH session with HMAC-SHA1-96. • Verify that the SSH session was encrypted using HMAC-SHA1-96 via log. • Verify that the message integrity algorithm used was as configured via capture. **HMAC-SHA2-256:** • Establish an SSH session with HMAC-SHA2-256. • Verify that the SSH session was encrypted using HMAC-SHA2-256 via log. • Verify that the message integrity algorithm used was as configured via capture. **HMAC-SHA2-512:** • Establish an SSH session with HMAC-SHA2-512. • Verify that the SSH session was encrypted using HMAC-SHA2-512 via log. • Verify that the message integrity algorithm used was as configured via capture.

Expected Output	• *The TOE should support encryption using the claimed HMAC algorithms.*
Pass/Fail with Explanation	Pass. The TOE supports only claimed integrity algorithms. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.10 FCS_SSHS_EXT.1.6 Test #2

Item	Data
Test ID	*FCS_SSHS_EXT.1.6 Test #2*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Establish an SSH session with an unsupported HMAC algorithms. • Verify that the SSH session was terminated since unsupported HMAC algorithm was used.
Test Execution Steps	• Attempt to establish an SSH session using HMAC-MD5-96. • Verify with logs that the TOE is unable to connect. • Verify via Wireshark that the TOE rejects the connection.
Expected Output	• *The TOE should reject connection due to unsupported HMAC algorithms.*
Pass/Fail with Explanation	Pass. The SSH connection fails when the MAC algorithm used is not from ST selection. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.11 FCS_SSHS_EXT.1.7 Test #1

Item	Data
Test ID	*FCS_SSHS_EXT.1.7 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Establish an SSH session with an unsupported key exchange method. • Verify that the SSH session was terminated since unsupported key exchange method was used.
Test Execution Steps	• Attempt to establish an SSH session using Diffie-hellman-group1-sha1. • Verify that the TOE rejects the connection attempt via log. • Verify that the TOE rejects the connection attempt via PCAP.

Expected Output	• *The TOE should support reject connection when using key exchange method (Diffie-hellman-group1-sha1).* • *Evidence (screenshot or CLI output) showing configuration of each method.* • *Log showing unsuccessful connection.* • *Packet capture showing unsuccessful connection.*
Pass/Fail with Explanation	Pass. The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.12 FCS_SSHS_EXT.1.7 Test #2

Item	Data
Test ID	*FCS_SSHS_EXT.1.7 Test #2*
Objective	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Establish an SSH session with each supported key exchange method. • Verify that the SSH session was successful since supported key exchange method was used.
Test Execution Steps	• Configure the TOE for SSH connection using claimed key exchange method. **Diffie-hellman-group14-sha1:** • Attempt to establish an SSH session using diffiehellman-group14-sha1. • Verify that the TOE connects the connection attempt via log. • Verify that the TOE connects the connection attempt via PCAP. **ecdh-sha2-nistp256:** • Attempt to establish an SSH session using ecdh-sha2-nistp256. • Verify that the TOE connects the connection attempt via log. • Verify that the TOE connects the connection attempt via PCAP. **ecdh-sha2-nistp384:** • Attempt to establish an SSH session using ecdh-sha2-nistp384. • Verify that the TOE connects the connection attempt via log. • Verify that the TOE connects the connection attempt via PCAP. **ecdh-sha2-nistp521:** • Attempt to establish an SSH session using ecdh-sha2-nistp521. • Verify that the TOE connects the connection attempt via log. • Verify that the TOE connects the connection attempt via PCAP.
Expected Output	• *The TOE should support successfully connect when using claimed key exchange method.* • *Evidence (screenshot or CLI output) showing configuration for each method.* • *Log showing successful connection for each method.*

	• *Packet capture showing successful connection for each method.*
Pass/Fail with Explanation	Pass. The TOE rejects SSH connections using diffiehellman-group1-sha1 (a non-approved algorithm) for key exchange. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.13 FCS_SSHS_EXT.1.8 Test #1a

Item	Data
Test ID	*FCS_SSHS_EXT.1.8 Test #1a*
Objective	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the **time-based threshold** and the traffic-based threshold. For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. 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).
Note	Acumen-sshs tool is used to establish an SSH session with the TOE and keep it idle for 1 hour.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for SSH rekey with the time. • Verify the TOE initiates a rekey for session keys.
Test Execution Steps	• Establish an SSH session with the TOE using 'acumen-sshs' tool and keep it idle for 60 minutes (default time). • Verify the TOE initiates a rekey for session keys. • Verify the encrypted packet capture for rekey.
Expected Output	• *The TOE should issue a rekey after the specified time is reached as configured on the TOE.* • *Log showing session rekey request being sent after time-based threshold has been reached.*
Pass/Fail with Explanation	Pass. The TOE initiates a rekey after the default time of 1hour is met. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.3.14 FCS_SSHS_EXT.1.8 Test #1b

Item	Data
Test ID	*FCS_SSHS_EXT.1.8 Test #1b*
Objective	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the **traffic-based** threshold. For testing of the 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 All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.
Note	Acumen-sshs tool is used to establish an SSH session with the TOE and send 1GB of traffic.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for SSH rekey with the time. • Verify the TOE initiates a rekey for session keys.
Test Execution Steps	• Establish an SSH session with the TOE using 'acumen-sshs' tool and pass 1GB of data. • Verify the TOE initiates a rekey for session keys.
Expected Output	• *The TOE should issue a rekey after the specified amount of data is transferred as configured on the TOE.* • *Log showing session rekey request being sent after volume-based threshold has been reached.*

Pass/Fail with Explanation	Pass. The TOE initiates a rekey after the default volume of 1GB is met. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4 TLSC

6.4.1 FCS_TLSC_EXT.1.1 Test #1

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #1*
Objective	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE to connect to the TLS server. • Attempt connection with each supported ciphersuite. • Verify with logs. • Verify with PCAPs.
Test Execution Steps	• Configure the TOE to connect to the TLS server. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256: • Attempt the connection from the TOE to the TLS Server using the ciphersuite TLS_DHE_RSA_WITH_AES_128_GCM_SHA256. • Verify the with packet capture the required ciphersuite. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384: • Attempt the connection from the TOE to the TLS Server using the ciphersuite TLS_DHE_RSA_WITH_AES_256_GCM_SHA384. • Verify the with packet capture the required ciphersuite. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256: • Attempt the connection from the TOE to the TLS Server using the ciphersuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. • Verify the packet capture the required ciphersuite. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384: • Attempt the connection from the TOE to the TLS Server using the ciphersuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. • Verify the packet capture the required ciphersuite.
Expected Output	• *The TOE should establish a TLS connection using each of the ciphersuites specified by the requirement*
Pass/Fail with Explanation	Pass. TOE successfully negotiates each of the claimed cipher suites. This meets the test requirements.
Result	Pass.

Test Clean-up	NA

6.4.2 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #2*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Create and load server certificate with the Server Authentication purpose in the extendedKeyUsage field. • Verify that the connection is established. • Create and load server certificate that lacks with the Server Authentication purpose in the extendedKeyUsage field. • Verify that the connection is rejected.
Test Execution Steps	Valid Certificate: • Load the server certificate containing the Server Authentication purpose on the TLS server. • Attempt the connection from the TOE to the TLS Server. • Verify the successful connection with packet capture. Invalid Certificate: • Load the server certificate lacking the Server Authentication purpose on the TLS server. • Attempt the connection from the TOE to the TLS Server. • Verify the error with logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE shall reject connection with server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field.*
Pass/Fail with Explanation	Pass. The TOE accepted a connection with valid server certificate and denied a connection to a server using an invalid certificate.
Result	Pass.
Test Clean-up	NA

6.4.3 FCS_TLSC_EXT.1.1 Test #3

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #3*
Objective	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.

Note	Acumen-TLSC tool is used to send an RSA certificate while using ECDSA ciphersuite.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to send a server certificate that does not match the server-selected ciphersuite. • Verify that the connection is unsuccessful.
Test Execution Steps	• Start the connection using the 'Acumen-TLSC' tool to send RSA certificate and ECDSA cipher suite. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the server connection after receiving the server's Certificate handshake message.*
Pass/Fail with Explanation	Pass. The TOE denied a connection to a server using a certificate that doesn't match the cipher suite. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.4 FCS_TLSC_EXT.1.1 Test #4a

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #4a*
Objective	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Note	Acumen-TLSC tool is used to configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite. • Verify that the connection is unsuccessful.
Test Execution Steps	• Start the connection using the 'Acumen-TLS' tool with TLS_NULL_WITH_NULL NULL cipher suite. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the server connection with TLS_NULL_WITH_NULL_NULL ciphersuite.*
Pass/Fail with Explanation	Pass. The TOE does not complete the session because TLS_NULL_WITH_NULL_NULL is presented. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.5 FCS_TLSC_EXT.1.1 Test #4b

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #4b*
Objective	Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to send Server Hello using an unsupported ciphersuite. • Verify that the connection is unsuccessful.
Test Execution Steps	• Use the 'Acumen-tlsc' tool to send Server Hello using an unsupported ciphersuite. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects connection after receiving the Server Hello packet.*
Pass/Fail with Explanation	Pass. The TOE rejects the connection with wrong cipher by sending a FIN message. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.6 FCS_TLSC_EXT.1.1 Test #4c

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #4c*
Objective	[conditional]: If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension** the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to send ECDHE key with non-supported curve. • Verify that the connection is unsuccessful.
Test Execution Steps	• Use 'Acumen-tlsc' tool to send ECDHE key with non-supported curve. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects connection after receiving the server's Key Exchange handshake message.*
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.
Result	Pass.
Test Clean-up	NA

6.4.7 FCS_TLSC_EXT.1.1 Test #5a

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #5a*
Objective	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.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Attempt connection using unsupported TLSv1.0. • Verify that it is unsuccessful.
Test Execution Steps	• Attempt the connection from the TOE to the TLS Server using the unsupported TLSv1.0 and verify the connection. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects connection due to unsupported TLS version.*
Pass/Fail with Explanation	Pass. The connection fails due to unsupported TLS version. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.8 FCS_TLSC_EXT.1.1 Test #5b

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #5b*
Objective	[conditional]: If using DHE or ECDH, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to modify the signature block in the Server's Key Exchange handshake message. • Verify that the connection is unsuccessful.
Test Execution Steps	• Use 'Acumen-tlsc' tool to modify the signature block in the Server's Key Exchange handshake message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the connection, and the handshake is not finished successfully.*
Pass/Fail with Explanation	Pass. The connection fails due to the modified block in the Server Key Exchange message. This meets the test requirement.
Result	Pass.
Test Clean-up	NA

6.4.9 FCS_TLSC_EXT.1.1 Test #6a

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #6a*
Objective	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to modify a byte in the Server Finished handshake message. • Verify that the connection is unsuccessful.
Test Execution Steps	• Use the 'Acumen-tlsc' tool to modify a byte in the Server Finished handshake message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the connection, and the handshake is not finished successfully.*
Pass/Fail with Explanation	Pass. The connection is not completed when a corrupted Server Finished message is received. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.10 FCS_TLSC_EXT.1.1 Test #6b

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #6b*
Objective	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to send a garbled message from the server. • Verify that the connection is unsuccessful.
Test Execution Steps	• Use the 'Acumen-tlsc' tool to send a garbled message from the server after the server has issued the ChangeCipherSpec message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the connection, and the handshake is not finished successfully.*
Pass/Fail with Explanation	Pass. The TOE closes the connection after receiving garbled data. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.11 FCS_TLSC_EXT.1.1 Test #6c

Item	Data
Test ID	*FCS_TLSC_EXT.1.1 Test #6c*
Objective	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.
Note	
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Use the tool to modify at least one byte in the server's nonce in the Server Hello handshake message. • Verify that the connection is unsuccessful.
Test Execution Steps	• Use the 'Acumen-tlsc' tool to modify at least one byte in the server's nonce in the Server Hello handshake message. • Verify the error logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the Server Key Exchange handshake message.*
Pass/Fail with Explanation	Pass. The connection was rejected due to a modified nonce. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.12 FCS_TLSC_EXT.1.2 Test #1

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #1*
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for reference identifier as each IPv4, IPv6 and DNS name. • Create a server certificate showing no SAN and a CN that does not match the set reference identifier on the TOE. • Verify that the connection fails via logs and packet captures.

	• Repeat the 2 above steps for IPv6 and DNS name.
Test Execution Steps	CN as IPv4: • Configure the TOE for reference identifier name as IPv4. • Configure the Server certificate showing CN that does not match the reference identifier and with no SAN extension. • Load the certificate with incorrect CN and no SAN on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection fails. • Verify the device's connection failure logs which state that CN does not match the peer certificate. • Verify the unsuccessful connection due to incorrect CN in the packet capture. CN as IPv6: • Configure the TOE for reference identifier name as IPv6. • Configure the Server certificate showing CN that does not match the reference identifier and with no SAN extension. • Load the certificate with incorrect CN and no SAN on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection fails. • Verify the connection failure logs on the device which state that CN does not match the peer certificate. • Verify the unsuccessful connection due to incorrect CN in packet capture. CN as DNS name: • Configure the TOE for reference identifier name as DNS name. • Configure the Server certificate showing CN that does not match reference identifier and with no SAN extension. • Load the certificate with incorrect CN and no SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection fails. • Verify the connection failure logs on the device which states that CN does not match in peer certificate. • Verify the unsuccessful connection due to incorrect CN in packet capture.
Expected Output	• *The TOE should reject the connection for the reason of CN mismatch or missing SAN extension.*
Pass/Fail with Explanation	Pass. The TOE rejects certificates with a bad CN and No SAN. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.13 FCS_TLSC_EXT.1.2 Test #2

Item	**Data**
Test ID	*FCS_TLSC_EXT.1.2 Test #2*
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for reference identifier as each IPv4, IPv6 and DNS name. • Create a server certificate showing CN that match the set reference identifier on the TOE, but SAN does not match the reference identifier. • Verify that the connection fails via logs and packet captures. • Repeat the above 2 steps for IPv6 and DNS name.
Test Execution Steps	CN as IPv4: • Configure the TOE for reference identifier name as IPv4. • Configure the Server certificate showing CN that matches the reference identifier and with SAN extension that does not match the reference identifier. • Load the certificate with the correct CN and incorrect SAN the on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection fails. • Verify the connection failure logs on the device. • Verify the unsuccessful connection due to incorrect SAN in packet capture. CN as IPv6: • Configure the TOE for reference identifier name as IPv6. • Configure the Server certificate showing CN that match reference identifier and with SAN extension that does not match the reference identifier. • Load the certificate with correct CN and incorrect SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection fails. • Verify the connection failure logs on the device. • Verify the unsuccessful connection due to incorrect SAN in packet capture. CN as DNS name: • Configure the TOE for reference identifier name as DNS name. • Configure the Server certificate showing CN that match reference identifier and with SAN extension that does not match the reference identifier. • Load the certificate with correct CN and incorrect SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection fails. • Verify the connection failure logs on the device. • Verify the unsuccessful connection due to incorrect SAN in packet capture.
Expected Output	• *The TOE should reject connection for the reason of SAN mismatch.*
Pass/Fail with Explanation	Pass. The TOE rejects certificates with a good CN but bad SAN. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.14 FCS_TLSC_EXT.1.2 Test #3

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #3*
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for reference identifiers as each IPv4 and IPv6. • Create a server certificate showing no SAN and a CN that match the set reference identifier on the TOE. • Verify that the connection succeeds via logs and packet captures. • Repeat the above 2 steps for IPv6.
Test Execution Steps	CN as IPv4: • Configure the TOE for reference identifier name as IPv4. • Configure the Server certificate showing no SAN and a CN that match the set reference identifier on the TOE. • Load the certificate with correct CN and no SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection is successful. • Verify the connection logs on the device. • Verify the successful connection due to correct CN in packet capture. CN as IPv6: • Configure the TOE for reference identifier name as IPv6. • Configure the Server certificate showing no SAN and a CN that match the set reference identifier on the TOE. • Load the certificate with correct CN and no SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection is successful. • Verify the connection logs on the device. • Verify the successful connection due to correct CN in packet capture. CN as DNS name: • Configure the TOE for reference identifier name as DNS name. • Configure the Server certificate showing no SAN and a CN that match the set reference identifier on the TOE. • Load the certificate with correct CN and no SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection is successful. • Verify the connection logs on the device. • Verify the successful connection due to correct CN in packet capture.

Expected Output	• *The TOE should accept connection due to CN match.*
Pass/Fail with Explanation	Pass. A connection was established when TOE is presented with a server certificate which contains a CN that matches the reference identifier and does not contain the SAN extension. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.15 FCS_TLSC_EXT.1.2 Test #4

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #4*
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** 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).
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for reference identifier as each IPv4, IPv6 and DNS name. • Create a server certificate showing a CN that does not match the set reference identifier on the TOE but SAN that matches the set reference identifier. • Verify that the connection succeeds via logs and packet captures. • Repeat the above 2 steps for IPv6 and DNS name.
Test Execution Steps	CN as IPv4: • Configure the TOE for reference identifier name as IPv4. • Configure the Server certificate showing a CN that does not match the set reference identifier on the TOE but SAN that matches the set reference identifier. • Load the certificate with incorrect CN and correct SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection is successful. • Verify the connection logs on the device. • Verify the successful connection due to correct SAN in packet capture. CN as IPv6: • Configure the TOE for reference identifier name as IPv6. • Configure the Server certificate showing a CN that does not match the set reference identifier on the TOE but SAN that matches the set reference identifier. • Load the certificate with incorrect CN and correct SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection is successful. • Verify the connection logs on the device. • Verify the successful connection due to correct SAN in packet capture. CN as DNS name: • Configure the TOE for reference identifier name as DNS name.

	• Configure the Server certificate showing a CN that does not match the set reference identifier on the TOE but SAN that matches the set reference identifier. • Load the certificate with incorrect CN and correct SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection is successful. • Verify the connection logs on the device. • Verify the successful connection due to correct SAN in packet capture.
Expected Output	• *The TOE should accept connection due to SAN match.*
Pass/Fail with Explanation	Pass. A connection was established when TOE is presented with a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.16 FCS_TLSC_EXT.1.2 Test #5 (1)

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #5 (1)*
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: 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): 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.
Note	Wildcard not in left-most label. E.g., Foo.*.acumen.com & correct: - foo.eg.acumen.com
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for correct reference identifier. • Create a server certificate showing wildcard that is not in the left-most label. • Verify that the connection fails via logs and packet captures. • Repeat the above 2 steps for CN and SAN.
Test Execution Steps	CN: • Configure the TOE for the correct reference identifier. • Configure the server certificate showing wildcard that is not in the left-most label of CN. • Load the certificate showing wildcard that is not in the left-most label of CN on the TLS server. • Initiate the connection from the TOE to the TLS Server 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 correct reference identifier. • Configure the server certificate showing wildcard that is not in the left-most label of SAN.

	• Load the certificate showing wildcard that is not in the left-most label of SAN on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the error logs on the device due to SAN mismatch. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects connection to the server certificate containing a wildcard that is not in the left-most label of the presented identifier.*
Pass/Fail with Explanation	Pass. When configuring the reference identifier with no left-most labels on TOE the connections fail. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.17 FCS_TLSC_EXT.1.2 Test #5 (2)(a)

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #5 (2)(a)*
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: 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): 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.)
Note	Wildcard in the left most label. E.g., *.acumen.com & correct: - eg.acumen.com
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE for correct reference identifier. • Create a server certificate showing wildcard that is in the left-most label. • Verify that the connection fails via logs and packet captures. • Repeat the above 2 steps for CN and SAN.
Test Execution Steps	CN: • Configure the TOE for the reference identifier with single left-most label. • Configure the server certificate showing wildcard in the leftmost label in CN. • Load the certificate with Wildcard in leftmost label in CN on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the logs indicate successful connection. • Verify the successful connection via packet capture. SAN: • Configure the TOE for the reference identifier with single left-most label.

	• Configure the server certificate showing wildcard in the leftmost label in SAN. • Load the certificate with Wildcard in leftmost label in SAN on the TLS server. • Initiate the successful connection from the TOE to the TLS Server and verify the connection. • Verify the logs indicate successful connection. • Verify the connection via packet capture.
Expected Output	***The TOE accepts connection to the server certificate containing a wildcard that is in the left-most label of the presented identifier.***
Pass/Fail with Explanation	Pass. TOE accepts the connection when the reference identifier with single left-most labels is presented in the certificate. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.18 FCS_TLSC_EXT.1.2 Test #5 (2)(b)

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #5 (2)(b)*
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: 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): 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.)
Note	E.g., *.acumen.com & correct: - acumen.com
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE with the reference identifier without a left-most label as in the certificate. • Create a server certificate showing wildcard that is in the left-most label. • Verify that the connection fails via logs and packet captures. • Repeat the above 2 steps for CN and SAN.
Test Execution Steps	CN: • Configure the TOE for the reference identifier without a leftmost label. • Configure the server certificate showing wildcard in the leftmost label in CN. • Load the certificate with Wildcard in leftmost label in CN on the TLS server. • Initiate the connection from the TOE to the TLS Server 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 server certificate showing wildcard in the leftmost label in SAN. • Load the certificate with Wildcard in leftmost label in SAN on the TLS server. • Initiate the connection from the TOE to the TLS Server 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.
Expected Output	• *The TOE rejects connection to the server certificate containing a wildcard that is in the left-most label of the presented identifier due to SAN/CN mismatch.*
Pass/Fail with Explanation	Pass. When configuring the reference identifier with no left-most labels on TOE the connections fail. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.19 FCS_TLSC_EXT.1.2 Test #5 (2)(c)

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #5 (2)(c)*
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: 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): 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.)
Note	E.g., *.acumen.com & correct: - foo.eg.acumen.com
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE with the reference identifier with two left-most labels. • Create a server certificate containing a wildcard in the left-most label. • Verify that the connection fails via logs and packet captures. • Repeat the above 2 steps for CN and SAN.
Test Execution Steps	CN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the server certificate showing wildcard in the leftmost label in CN. • Load the certificate with leftmost label in CN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the failure logs on the TOE. • Verify the unsuccessful connection via packet capture. SAN: • Configure the TOE for the reference identifier with two leftmost labels.

	• Configure the server certificate showing wildcard in the leftmost label in SAN. • Load the certificate with leftmost label in SAN on TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the failure logs on the TOE. • Verify the unsuccessful connection via packet capture.
Expected Output	• *The TOE rejects connection to the server certificate containing a wildcard that is in the left-most label of the presented identifier due to SAN/CN mismatch.*
Pass/Fail with Explanation	Pass. When configure the reference identifier with two left-most labels on TOE the connections fail. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.4.20 FCS_TLSC_EXT.1.2 Test #6

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #6*
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT**. If IP addresses are supported, 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 an asterisk (*) (e.g. CN=192.168.1.* when connecting to 192.168.1.20, 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE with the correct reference identifier. • Create a server certificate with one of the groups replaced with an asterisk (*). • Verify that the connection fails via logs and packet captures. • Repeat the above 2 steps for IPv4 and IPv6.
Test Execution Steps	IPv4: • Configure the TOE for the correct reference identifier. • Create a server certificate with a CN that matches the reference identifier but replaces one of the groups with an *. • Load the certificate on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the 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 replaces one of the groups with an *. • Load the certificate on the TLS server. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the failure logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the connection to the server certificate with CN's reference identifier one group replaced with an asterisk*.
Pass/Fail with Explanation	Pass. TOE rejects the connection when configured server certificate that contains a CN that matches the reference identifier IP except one of the groups has been replaced with an asterisk (*). This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.4.21 FCS_TLSC_EXT.1.2 Test #7a

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #7a*
Test Assurance Activity	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): 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.
Pass/Fail with Explanation	NA. ST does not select the use of the secure channel for FPT_ITT.

6.4.22 FCS_TLSC_EXT.1.2 Test #7b

Item	Data
Test ID	*FCS_TLSC_EXT.1.2 Test #7b*
Test Assurance Activity	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): 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.
Pass/Fail with Explanation	NA. ST does not select the use of the secure channel for FPT_ITT.

6.4.23 FCS_TLSC_EXT.1.2 Test #7c

Item	**Data**
Test ID	*FCS_TLSC_EXT.1.2 Test #7c*
Test Assurance Activity	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): 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.
Pass/Fail with Explanation	NA. ST does not select the use of the secure channel for FPT_ITT.

6.4.24 FCS_TLSC_EXT.1.2 Test #7d

Item	**Data**
Test ID	*FCS_TLSC_EXT.1.2 Test #7d*
Test Assurance Activity	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): 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.)
Pass/Fail with Explanation	NA. ST does not select the use of the secure channel for FPT_ITT.

6.4.25 FCS_TLSC_EXT.1.3 Test #1

Item	**Data**
Test ID	*FCS_TLSC_EXT.1.3 Test #1*
Objective	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.

Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	This test is satisfied by FIA_X509_EXT.1.1/ Rev Test #1a. The TOE accepts the certificate when it has the full CA chain.
Pass/Fail with Explanation	Pass. This test is satisfied by FIA_X509_EXT.1.1/ Rev Test #1a. The TOE accepts the certificate when it has the full CA chain.
Result	Pass.
Test Clean-up	NA

6.4.26 FCS_TLSC_EXT.1.3 Test #2

Item	**Data**
Test ID	*FCS_TLSC_EXT.1.3 Test #2*
Objective	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	A connection was failed when presented 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 requirements of this test case are exercised in in FCS_TLSC_EXT.1.2 Test #1 and Test #2, FIA_X509_EXT.1.1 Test #1b, FIA_X509_EXT.1.1 Test #2 and Test #3.
Pass/Fail with Explanation	Pass. A connection was failed when presented 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 requirements of this test case are exercised in in FCS_TLSC_EXT.1.2 Test #1 and Test #2, FIA_X509_EXT.1.1 Test #1b, FIA_X509_EXT.1.1 Test #2 and Test #3.
Result	Pass.
Test Clean-up	NA

6.4.27 FCS_TLSC_EXT.1.3 Test #3

Item	**Data**
Test ID	*FCS_TLSC_EXT.1.3 Test #3*
Objective	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.
Expected Output	ST does not select override options for failed certificate validation.
Pass/Fail with Explanation	ST does not select override options for failed certificate validation.
Result	Pass.
Test Clean-up	NA

6.4.28 FCS_TLSC_EXT.1.4 Test #1

Item	Data
Test ID	*FCS_TLSC_EXT.1.4 Test #1*
Objective	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure the TOE to connect to the TLS server. • Attempt connection with each supported elliptic curve. • Verify with successful connection via logs. • Verify with successful connection via PCAPs.
Test Execution Steps	• Initiate the connection from the TOE to the TLS Server using the curve secp256r1 and verify the connection. • Verify with packet capture that the required curve is secp256r1. • Initiate the connection from the TOE to the TLS Server using the curve secp384r1 and verify the connection. • Verify with packet capture that the required curve is secp384r1. • Initiate the connection from the TOE to the TLS Server using the curve secp521r1 and verify the connection. • Verify with packet capture that the required curve is secp521r1.
Expected Output	• *The TOE should establish a TLS connection using each of the ciphersuites specified by the requirement.*
Pass/Fail with Explanation	Pass. The TOE accepted a connection when supported curves were introduced. This meets the test requirements.
Result	Pass
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.5 Update

6.5.1 FPT_TST_EXT.1 Test #1

Item	Data
Test ID	*FPT_TST_EXT.1 Test #1*
Objective	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this. For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	***Power on the TOE and observe the required self-tests are passed.***
Test Execution Steps	• Power on the TOE and observe the TOE Start up. • Ensure that evidence of the execution of self-tests are provided.
Expected Output	• *The TOE executes all required self-tests during bootup.*
Pass/Fail with Explanation	Pass. The TOE successfully executes self-test. This meets the testing requirement.
Result	Pass.
Test Clean-up	NA

6.5.2 FPT_TUD_EXT.1 Test #1

Item	Data
Test ID	*FPT_TUD_EXT.1 Test #1*
Objective	The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Verify the current version of the TOE. • Load the new image on the TOE and verify that the version has not changed.

	• Boot the TOE with the new image and verify that the TOE shows new version of the image.
Test Execution Steps	• Verify the current version of the TOE. • Upload the new image on the ISG. • Verify that the TOE version has not changed. • Create a new sg application for this image. • Stop the previous sg application and start the new sg application. • Attach console to new sg application. • After reboot, show the new version of the software. • Enable FIPS-mode. • Verify that the system is now in FIPS-mode. • Verify the successful update with logs.
Expected Output	• *The TOE successfully updates the current image version with the new image after verifying that the new image is authentic.* • *The logs indicate the same that the new image is verified and has then been installed.*
Pass/Fail with Explanation	Pass. The TOE can be successfully upgraded with a valid update image. This meets the testing requirement.
Result	Pass.
Test Clean-up	NA

6.5.3 FPT_TUD_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	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.
Pass/Fail with Explanation	NA. The ST does not select “the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE”.

6.5.4 FPT_TUD_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	[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: 2) 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.
Pass/Fail with Explanation	NA. The ST does not select “the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE”.

6.5.5 FPT_TUD_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	[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: 3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature) If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Pass/Fail with Explanation	NA. The ST does not select “the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE”.

6.5.6 FPT_TUD_EXT.1 Test #3 (a)

Item	Data
Test ID	*FPT_TUD_EXT.1 Test #3 (a)*
Objective	[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. 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Verify the current version on the TOE. • Modify the hash and ensure that it does not match the published hash. • Verify the failure via logs.
Test Execution Steps	• Verify the current version of the TOE. • Calculate the hash of the update and ensure that it matches the published hash. • Modify the update's hash and ensure that it does not match the published hash. • Upload the modified image to the TOE and confirm that the update installation fails. • Verify the failure via logs.
Expected output	• *The TOE should reject the hash that does not match the published hash and accept the update when the hash matches the published hash.*
Pass/Fail with Explanation	Pass. The TOE rejects the modified software update. This meets the testing requirements.
Result	Pass.

Test Clean-up	NA

6.5.7 FPT_TUD_EXT.1 Test #3 (b)

Item	Data
Test ID	*FPT_TUD_EXT.1 Test #3 (b)*
Objective	[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. 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Execution Output	The TOE itself does not verify the computed hash and the published hash.
Pass/Fail with Explanation	NA. The TOE itself does not verify the computed hash and the published hash.
Result	NA

Test Clean-up	NA

6.6 X509-Rev

6.6.1 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data
Test ID	*FIA_X509_EXT.1.1/Rev Test #1a*
Objective	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the 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).
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Configure TOE to connect to TLS server. • Create and upload full chain of certificates to validate the server certificate. • Verify the connection is successful via logs and packet capture.
Test Execution Steps	• Create a full chain of certificates to connect to the TOE. • Upload the Root CA certificate to the TOE's trust store. • Configure TOE to connect to the TLS server. • Attempt the connection from the TOE to the TLS server. • Verify the successful connection from logs on the device. • Verify the connection is successful via packet capture.
Expected Output	• *The TOE accepts connection when complete certificate validation chain is present on the TOE.*
Pass/Fail with Explanation	Pass. When a complete certificate trust chain is present, the TOE can make a successful connection. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.6.2 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test ID	*FIA_X509_EXT.1.1/Rev Test #1b*
Objective	Test 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow	• Attempt to connect to the TOE with a server certificate with an incomplete chain and verify that it fails.

(Generic test steps)	• Verify with packet capture that server certificate chain is incomplete.
Test Execution Steps	• Remove the ICA from TOE's trust store. • Attempt the connection from the TOE to the TLS server. • Verify the unsuccessful connection from logs on the device. • Verify the unsuccessful connection via packet capture.
Expected Output	• *When a complete certificate chain is not provided, the TOE fails to establish a TLS server connection.* • *The packet capture shows that this connection is not established due to an unknown CA certificate.*
Pass/Fail with Explanation	Pass. When an incomplete certificate trust chain is present, the TOE is not able to make a successful connection. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.6.3 FIA_X509_EXT.1.1/Rev Test #2

Item	**Data**
Test ID	*FIA_X509_EXT.1.1/Rev Test #2*
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Create and load an expired certificate on the server. • Verify via logs and packet capture that the connection is unsuccessful.
Test Execution Steps	Server Expired: • Create a server certificate which is expired. • Show clock on the TOE. • Attempt the connection from the TOE to the TLS server. • Verify the logs on the device. • Verify the connection is unsuccessful via packet capture. ICA Expired: • Create an ICA certificate which is expired. • Show clock on the TOE. • Attempt the connection from the TOE to the TLS server. • Verify the logs on the device. • Verify the connection is unsuccessful via packet capture.
Expected Output	• *The TOE rejects the TLS server connection because the certificate has expired.* • *The packet capture and logs confirm that the connection wasn't established and shows when the certificate has expired.*

Pass/Fail with Explanation	Pass. The TOE denied the connection because of the expired certificate. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.6.4 FIA_X509_EXT.1.1/Rev Test #3

Item	Data
Test ID	*FIA_X509_EXT.1.1/Rev Test #3*
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 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. Revocation 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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	1. Valid Certificate: • Create and load server certificate with OCSP EKU signing and URI of OCSP responder. • Configure the TOE for OCSP checking. • Verify the logs and packet capture for successful connection and responder responses. 2. Revoked End entity: • Revoke and load the server certificate on the server. • Verify the logs and packet capture for unsuccessful connection and responder responses. 3. Revoked ICA: • Revoke and load the ICA certificate on the server. • Verify the logs and packet capture for unsuccessful connection and responder responses.
Test Execution Steps	1. Valid Certificate: • Create certificates with OCSP EKU signing and configure URI of the OCSP responder. • Load the Root CA and ICA on the TOE. • Configure the TOE for OCSP checking. • Configure the TOE for syslog server. • Start OCSP responder for ICA and Server certificates. • Start the Syslog server using Server and ICA certificates. • Verify the logs on the TOE.

	• Verify the successful connection with packet capture. 2. Revoked End Entity Certificate: • Revoke the End Entity certificate. • Start OCSP responder for ICA and Server certificates. • Start the Syslog server using Server and ICA certificates. • Verify the logs on the TOE. • Verify the unsuccessful connection with packet capture. 3. Revoked Intermediate CA Certificate: • Reset the certificate chain and revoke only the intermediate CA certificate. • Start OCSP responder for ICA and Server certificates. • Start the Syslog server using Server and ICA certificates. • Verify the logs on the TOE. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects any TLS server connection when either the intermediate certificate or the server certificate has been revoked.* • *The OCSP connection also shows that the certificates have been revoked.* • *The Packet capture depicts the specific certificate that has been revoked and the logs verify that the TOE has denied connection by denoting that certificate has been revoked.*
Pass/Fail with Explanation	Pass. Connection with revoked certificates is not accepted by the TOE which meets the requirement.
Result	Pass.
Test Clean-up	NA

6.6.5 FIA_X509_EXT.1.1/Rev Test #4

Item	Data
Test ID	*FIA_X509_EXT.1.1/Rev Test #4*
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Create and load server certificate with no OCSP signing EKU. • Verify the logs and packet capture for unsuccessful connection and responder responses
Test Execution Steps	• Generate a certificate that does NOT have OCSP signing purpose. • Use this certificate in the OCSP responder.

	• Attempt the connection from the TOE to the TLS server and verify the connection being unsuccessful. • Verify the logs on the device. • Verify the packet capture.
Expected Output	• *The TOE doesn't establish a TLS server connection when the OCSP signing purpose is missing and validation fails.* • *The packet capture shows that there is a handshake failure due to the absence of OCSP Signing.* • *The logs are used to validate the fact that the connection has been rejected by OCSP due to failure in certificate verification.*
Pass/Fail with Explanation	Pass. The TOE does not connect to the TLS and OCSP servers if OCSP signing is missing.
Result	Pass.
Test Clean-up	NA

6.6.6 FIA_X509_EXT.1.1/Rev Test #5

Item	**Data**
Test ID	*FIA_X509_EXT.1.1/Rev Test #5*
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Note	Acumen-TLSC tool is used to configure the server to modify the first 8 bytes of the certificate.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Run the Acumen-TLSC tool to modify any byte within the first 8 bytes of the certificate. • Verify the logs and packet capture for unsuccessful connection.
Test Execution Steps	• Run the Acumen-TLSC tool to modify any byte within the first 8 bytes of the certificate, the connection should fail. • Verify the error with logs on the TOE. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE denies a TLS connection when it is presented with a certificate that has been modified using the 'acumen-tlsc-v2.2e tool'.* • *The tool modifies the first eight bytes of the certificate.* • *The packet capture verifies that the connection is not established due to the bad certificate.* • *The logs depict that there's an encoding error thus verifying that the connection was rejected.*
Pass/Fail with Explanation	Pass. TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the test requirements.
Result	Pass.
Test Clean-up	NA

6.6.7 FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test ID	*FIA_X509_EXT.1.1/Rev Test #6*
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the 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.)
Note	Acumen-TLSC tool is used to configure the server to modify the last byte in the signatureValue field of the certificate
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Run the Acumen-TLSC tool to modify last byte in the signatureValue field of the certificate. • Verify the logs and packet capture for unsuccessful connection.
Test Execution Steps	• Run the Acumen-TLSC tool to modify last byte in the signatureValue field of the certificate. • Verify the error with logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE fails to establish a TLS connection when the last byte in the signatureValue field of the certificate is modified using the 'acumen-tlsc-v2.2e tool'.* • *The packet capture proves that there is a decrypt error, and the logs show that there is a failure in establishing connection due to certificate signature failure.*
Pass/Fail with Explanation	Pass. The modified certificate fails to validate. This meets the testing requirement.
Result	Pass.
Test Clean-up	NA

6.6.8 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test ID	*FIA_X509_EXT.1.1/Rev Test #7*
Objective	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 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.)
Note	Acumen-TLSC tool is used to configure the server to modify the public key in the certificate.
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Run the Acumen-TLSC tool to modify any byte in the public key in the certificate. • Verify the logs and packet capture for unsuccessful connection.
Test Execution Steps	• Run the Acumen-TLSC tool to modify any byte in the public key in the certificate. • Verify the error with logs on the device. • Verify the unsuccessful connection with packet capture.

Expected Output	• *The TOE rejects a remote TLS connection that is formed using the 'acumen-tlsc-v2.2e tool'.* • *The tool modifies the certificate such that its public key is modified and uses the same certificate for establishing the TLS connection.* • *The packet capture depicts that there is a decrypt error, and the logs show a failure in establishing a connection due to certificate signature failure.*
Pass/Fail with Explanation	Pass. The TOE rejects a connection when the public key of the server is modified. This meets the testing requirement.
Result	Pass.
Test Clean-up	Used command '`restore-defaults keep-console`' to clean-up the test configuration.

6.6.9 FIA_X509_EXT.1.1/Rev Test #8a

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain. **TD0527 (12/1 Update) has been applied.**
Pass/Fail with Explanation	NA. The ST does not select "Support for EC certificate as indicated in FCS_COP.1/SigGen ".

6.6.10 FIA_X509_EXT.1.1/Rev Test #8b

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid. **TD0527 (12/1 Update) has been applied.**
Pass/Fail with Explanation	NA. The ST does not select "Support for EC certificate as indicated in FCS_COP.1/SigGen ".

6.6.11 FIA_X509_EXT.1.1/Rev Test #8c

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store. **TD0527 (12/1 Update) has been applied.**
Pass/Fail with Explanation	NA. The ST does not select "Support for EC certificate as indicated in FCS_COP.1/SigGen ".

6.6.12 FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test ID	*FIA_X509_EXT.1.2/Rev Test #1*
Objective	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).*
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Create and load a CA certificate lacking basicConstraints extension on the TLS server. • Verify the error in logs on the device and unsuccessful connection with packet capture.

Test Execution Steps	• Configure the CA certificate lacking the basicConstraints extension. • Load the certificate lacking the basicConstraints on the TLS server. • Add the modified certificate to the certificate chain. • Concatenate the CA certificates. • Attempt the connection from the TOE to the TLS Server. • Verify the error in logs on the device. • Verify the unsuccessful connection with packet capture.
Expected Output	• *The TOE rejects the connection that has been made using the 'acumen-tlsc' tool which modifies the CA certificate such that it doesn't contain the basicConstraints extension.* • *The packet capture depicts that an unknown CA has been used.* • *The logs show a failure in establishing connection as the verification of certificate failed.*
Pass/Fail with Explanation	Pass. The TOE rejects a connection when the Intermediate certificate has NO Basic Constraints. This meets the testing requirement.
Result	Pass.
Test Clean-up	NA

6.6.13 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test ID	*FIA_X509_EXT.1.2/Rev Test #2*
Objective	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 it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). 6.6.14 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; 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).
Note	NA
Testbed	*Testbed #1, Testbed #2*

Test Flow (Generic test steps)	• Create and load a CA certificate with basicConstraints extension set to FALSE on the TLS server. • Verify the error in logs on the device and unsuccessful connection with packet capture.
Test Execution Steps	• Use the 'acumen x509-mod' tool to configure the CA certificate with the flag in the basicConstraints extension set to FALSE. • Concatenate the CA certificates. • Attempt the connection from the TOE to the TLS Server. • Verify the error in logs on the device. • Verify the unsuccessful connection packet capture.
Expected Output	• *The TOE rejects the TLS server connection which uses a CA certificate that has been modified using the 'x509-mod tool' such that the CA certificate contains basicConstraints 'CA is set to false'.* • *The packet capture shows that the basicConstraints for CA is false and the logs show a failure in establishing a connection due to use of an invalid CA certificate.*
Pass/Fail with Explanation	Pass. The TOE rejects a connection when the Intermediate certificate has Basic Constraints set to FALSE. This meets the testing requirement.
Result	Pass.
Test Clean-up	NA

6.6.14 FIA_X509_EXT.2 Test #1

Item	Data
Test ID	*FIA_X509_EXT.2 Test #1*
Objective	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.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Test the connection with valid certificate, when the TOE is unable to validate the certificate from the OCSP server and with administrator configurable option. • Verify the connection with logs and pcaps.
Test Execution Steps	1. Valid Certificate: • Configure the server certificate which is valid. • Configure the server certificate showing the OCSP distribution point. • Attempt the connection from the TOE to the TLS server and show the connection being successful. • Attempt the connection from the TOE to the OCSP server and show the connection being successful. • Verify the logs on TOE. • Verify the packet capture between the TOE and the OCSP server.

	• Verify the packet capture between the TOE and the TLS server. 2. TOE is unable to validate the certificate from the OCSP server: • Configure the server certificate. • Configure the server certificate 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 the logs on TOE. • Verify the packet capture between the TOE and the TLS server. • Verify the packet capture between the TOE and the OCSP server. 3. With administrator-configurable option: In the Third part of the ICA does not have OCSPSigning EKU and the OCSP server is unreachable, and TOE is configured to ignore ocsp-signing-purpose bit in the ICA, TOE makes the successful connection with the TLS server with the server certificate when failed to validate the certificate. • Generate a certificate that does NOT have OCSP signing purpose. • Configure the server certificate showing the OCSP distribution point. • Configure the option "Ignore unknown status and ocsp signing purpose" on TOE. • Start the CA and ICA responders. • Attempt the connection from the TOE to the TLS server and show the connection being successful. • Verify the successful connection logs on TOE. • Verify the packet capture between the TOE and the TLS server. • Configure the option "Ignore request-failure" on TOE. • Manipulate the environment such that the TOE is unable to reach the OCSP responders for checking the status of certificates. • Attempt the connection from the TOE to the TLS server and show the connection being successful. • Verify the successful connection logs. • Verify the packet capture between the TOE and the TLS server.
Expected Output	• *The TOE will reject the OCSP connection as the certificate used has an incorrect URL.* • *The packet capture will depict a handshake failure while the logs should show a failure in establishing a connection.*
Pass/Fail with Explanation	Pass. The TOE rejects certificates it cannot verify via OCSP when the responder is down. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.6.15 FIA_X509_EXT.3 Test #1

Item	Data
Test ID	*FIA_X509_EXT.3 Test #1*
Objective	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
Note	NA
Testbed	*Testbed #1*

Test Flow (Generic test steps)	• Generate a CSR and examine the CSR contents to confirm that it contains the public key and other required information.

Test Execution Steps	• From the TOE, generate a CSR.
	• Examine the CSR contents. Ensure the CSR contains the following fields.
	  ○ Common Name
	  ○ Organization
	  ○ Organizational Unit
	  ○ Country
	• Examine the CSR contents on openssl server.

Expected Output	• *The TOE will successfully generate a CSR with the help of an RSA key.*
Pass/Fail with Explanation	Pass. The TOE can generate a CSR with all of the requisite information. This meets the testing requirements.
Result	Pass.
Test Clean-up	NA

6.6.16 FIA_X509_EXT.3 Test #2

Item	Data
Test ID	*FIA_X509_EXT.3 Test #2*
Objective	The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds.
Note	NA
Testbed	*Testbed #1, Testbed #2*
Test Flow (Generic test steps)	• Generate CSR on the TOE and get it signed by external CA. • Ensure that full chain is not present on TOE and attempt to upload the certificate. • Verify with logs that it is unsuccessful. • Load the full validation chain on TOE and again attempt to upload the certificate. • Verify with logs that now it is successful.
Test Execution Steps	• Generate a CSR (Certificate Signing Request) on the TOE. • Generate a signed certificate based on the generated CSR from an external CA. • Ensure that the full trust chain for the signed CA is not present on the TOE. • Attempt to load the signed certificate on the TOE. • Verify that the TOE rejects the certificate because the full trust chain of the CA is not present. • Add the intermediate certificate to the TOE certificate store to ensure that the TOE has a full certificate path. • Verify from the logs that intermediate certificate is installed. • Re-attempt to load the signed certificate on the TOE. • Verify via logs that the TOE accepts the certificate because the path validation is succeeded.
Expected Output	• *The TOE doesn't validate a signed CSR if the full trust chain is not present. When a full trust chain is present, the TOE validates the signed CSR.*

Pass/Fail with Explanation	Pass. The TOE does reject a signed certificate if a valid chain is not present. This does not meet the testing requirement.
Result	Pass.
Test Clean-up	NA

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

Objective	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.
Evaluator Findings	The evaluator examined the AGD and FSD (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 and FSD. The evaluator verified that the FSD describes the purpose and method of use for each security relevant TSFI by verifying the AGD and it satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.2 ADV_FSP.1 Activity 2

Objective	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.
Evaluator Findings	The evaluator examined the AGD and FSD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD and FSD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping in FSD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.3 ADV_FSP.1 Activity 3

Objective	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 examined the AGD and FSD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD and FSD. The evaluator verified the FSD describes the parameters for each security relevant TSFI by verifying the AGD and it satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	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 below are met by the guidance documentation. Guidance documentation shall be 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 https://commoncriteria-india.gov.in/Products-Certified. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.2 AGD_OPE.1 Activity 2

Objective	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 Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are: • VMware ESXi 6.5 Hypervisor hosted on Dell Power Edge R440, with Intel Xeon Silver 4216 Processor (Cascade Lake) • SSP-S410-20 with ISG using Intel Xeon Silver 4210 Processor (Cascade Lake) Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.3 AGD_OPE.1 Activity 3

Objective	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 Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.4 AGD_OPE.1 Activity 4

Objective	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 evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator

	ensured guidance contained the necessary instructions for configuring the cryptographic engines. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.5 AGD_OPE.1 Activity 5 **[TD0536]**

Objective	In addition, the evaluator shall ensure that the following requirements are also met. a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. b) 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: i) 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). ii) 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. c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.
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 to make it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1

7.3.1.1 AGD_PRE.1 Activity 1

Objective	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).
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 section titled **TOE Environment** of the AGD. The evaluator found that this section describe how the Operational Environment must meet:

	<table><tr><th>Component</th><th>Required</th><th>Usage/Purpose Description for TOE performance</th></tr><tr><td>Remote Management Workstation (GUI).</td><td>No</td><td>This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS and TLS protected channels.</td></tr><tr><td>Remote Management Workstation (CLI).</td><td>Yes</td><td>This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels.</td></tr><tr><td>Local Management Workstation (CLI).</td><td>Yes</td><td>This includes any IT Environment Management workstation with a local CLI support that is used by the TOE administrator to support TOE administration through a direct connection.</td></tr><tr><td>NTP Server</td><td>Yes</td><td>NTP server supporting SHA-1 integrity verification.</td></tr><tr><td>Audit Server</td><td>Yes</td><td>The audit server is used for remote storage of audit records that have been generated by and pulled from the TOE.</td></tr><tr><td>CA/OCSP Server</td><td>Yes</td><td>A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for TLS connection establishment.</td></tr></table> Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.2 AGD_PRE.1 Activity 2

Objective	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, <table><tr><th>Component</th><th>Required</th><th>Usage/Purpose Description for TOE performance</th></tr><tr><td>Remote Management Workstation (GUI).</td><td>No</td><td>This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS and TLS protected channels.</td></tr><tr><td>Remote Management Workstation (CLI).</td><td>Yes</td><td>This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels.</td></tr><tr><td>Local Management Workstation (CLI).</td><td>Yes</td><td>This includes any IT Environment Management workstation with a local CLI support that is used by the TOE administrator to support TOE administration through a direct connection.</td></tr><tr><td>NTP Server</td><td>Yes</td><td>NTP server supporting SHA-1 integrity verification.</td></tr><tr><td>Audit Server</td><td>Yes</td><td>The audit server is used for remote storage of audit records that have been generated by and pulled from the TOE.</td></tr><tr><td>CA/OCSP Server</td><td>Yes</td><td>A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for TLS connection establishment.</td></tr></table> The section titled **Supported Hardware Platforms** of AGD identifies the following supported platform:

	<table><tr><th>Model</th><th>Firmware Version</th></tr><tr><td>SSP-S410-20 with ISG using Intel Xeon Silver 4210 Processor (Cascade Lake)</td><td>7.4.1.1</td></tr><tr><td>VMware ESXi 6.5 Hypervisor hosted on Dell Power Edge R440, with Intel Xeon Silver 4216 Processor (Cascade Lake)</td><td>7.4.1.1</td></tr></table>Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.3 AGD_PRE.1 Activity 3

Objective	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 functions necessary to install and configure the TOE to work in the target operating environment, including, • Configuring Administrative Accounts and Passwords • Configuring SSH and Console Connections • Configuring TLS • Configuring the Remote Syslog Server • Configuring Audit Log Options • Configuring Event Logging • Configuring a Secure Logging Channel • Configuring Software Updates • Configuring Setting Time • Configuring Login Banners Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.4 AGD_PRE.1 Activity 4

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

7.3.1.5 AGD_PRE.1 Activity 5

Objective	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 sections titled **Accessing the TOE Using the CLI Console** and **Accessing the TOE Using SSH** were used to determine the verdict of this work unit. The AGD describes setting the default password associated with the admin account and configuring SSH for remote administration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4.

	The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

7.6.1.1 AVA_VAN.1 Activity 1 **[TD0564, Labgram #116]**

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The 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. • http://nvd.nist.gov/ • http://www.us-cert.gov • http://www.securityfocus.com/ • https://www.cvedetails.com/ • www.exploitsearch.net • www.securiteam.com • http://nessus.org/plugins/index.php?view=search • http://www.zerodayinitiative.com/advisories • https://www.exploit-db.com • https://www.rapid7.com/db/vulnerabilities The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on 09/06/2023. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include: • Blue Coat ProxySG • SGOS v7.4 • SGOS v7.4.1.1 • SGOS

	• Symantec Proxy SG Operating • ISG v2.4.2.1 • cpe:/:broadcom:symantec_proxysg • Broadcom ProxySG • Symantec ProxySG • Symantec ProxySG_firmware • Secure Gateway • Symantec Web Proxy • Symantec Blue Coat ProxySG • SSP-S410-20 • Dell Power Edge R440 • cpe:2.3:o:vmware:esxi:6.5:650-201701001:*:*:*:*:*:* • Intel 4210 • Intel 4216 • Opensslv3.0 • TLS v1.2 • SSH • TCP • UDP The evaluation lab examined each result provided from NVD and Exploit Search 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. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.2 AVA_VAN.1 Activity 2

Objective	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.
Evaluator Findings	The evaluator documented the fuzz testing results with respect to this requirement. The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

8 Conclusion

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

End of Document