Assurance Activity Report for
Ivanti Policy Secure 22.2

Ivanti Policy Secure 22.2 Security Target
Version 0.5

collaborative Protection Profile for Network Devices
Version 2.2e

AAR Version 1.1, 12/15/2023

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Ivanti, Inc.

The Author of the Security Target:
Intertek Acumen Security

The TOE Evaluation was Sponsored by:
Ivanti, Inc.

Evaluation Personnel:
Reema Nagwekar
Ruban Abinesh
Calvin Sneed
Rahul Joshi

Intertek Acumen Security

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
1.0	10/06/2023	Initial Release
1.1	12/15/2023	ECR comments addressed

CONTENTS

1 Product Overview

1.1 Product Type

Ivanti Policy Secure (IPS) is a next-generation Network Access Control (NAC) that enables visibility to understand an organization's security posture and enforce role-based access and endpoint security policies for network users. IPS allows administrators to define, implement, and enforce policy by enabling endpoint discovery, monitoring, and alerting. For a list of product features and functionality that is excluded from the evaluation, please refer to Section **Error! Reference source not found.** of ST.

1.2 TOE Usage

The TOE is classified as a network device (a generic infrastructure device that can be connected to a network) or a virtual network device (a Virtual Appliance that can be connected to a network) depending on the underlying platform. The TOE software consists of Ivanti Policy Secure (IPS) 22.2R3. The appliance's software is built on IVE OS 3.0. The TOE consists of the IPS application, IVE OS, and either the TOE hardware or the VM hypervisor, all of which are delivered with the TOE. The TOE hardware consists of either the ISA Models 6000, 8000C, or 8000F.

The TOE provides following security features that are part of the evaluated configuration:

- Secure remote administration of the TOE via HTTPS/TLS web interface
- Secure Local administration of the TOE
- Secure connectivity with remote audit servers using mutually authenticated TLS
- Identification and authentication of the administrator of the TOE
- CAVP validated cryptographic algorithms
- Self-protection mechanisms such as executing self-tests to verify correct operation
- Secure firmware updates

For a complete list of security features provided by the TOE, please refer to Section **Error! Reference source not found.** of ST.

2 Assurance Activities Identification

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

3 Test Equivalency Justification

The following equivalency analysis provides a per-category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the Supporting Documentation for the NDcPPv2.2e. Additionally, a comparison of the data presented is provided to identify a testing subset that will exercise each of the differences in TOE models.

3.1 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any TSF functionality. The hardware within the TOE differs only by configuration and performance.

Table 1 – Hardware Dependencies

Model	ISA 8000C	ISA 8000F
Processor	Intel Xeon Gold 5317 (Ice Lake)	Intel Xeon Gold 5317 (Ice Lake)
Network	2 x 10 Gigabit Ethernet copper or fiber traffic ports with link redundancy 1 x 1GbE Management port	2 x 10 Gigabit copper or fiber traffic ports with link redundancy 1 x 1GbE Management port
Platform	IVE OS 3.0	IVE OS 3.0

The TOE chassis includes varying form factors. Although the chassis may differ, it does not affect the functionality of the TOE.
Result: Both platforms are equivalent.

3.2 Additional Analysis

The following conclusions can be drawn by reviewing the “Physical Boundaries” section in ST:

- Equivalency will be performed for 2 devices - ISA 8000C and ISA 8000F.
- Both hardware model devices use a processor with the same microarchitecture.
- The only difference is that ISA 8000C supports copper ports and ISA 8000F supports fiber ports.
- The differences above do not impact the Security functionalities of the TOE.

Result: The differences above do not impact the throughput and performance.

3.3 Software/OS Dependencies

Table 2 – Software Dependencies

TOE Model	Description	Analysis
Operating System – This is the OS that runs on the platform		
ISA 8000C	The TOE software consists of Ivanti Policy Secure (IPS) 22.2R3. The appliance’s software is built on IVE OS 3.0.	All two hardware devices are running the same OS and installed using the same image. Verdict: The two hardware models are equivalent. Both hardware devices are running the same OS and are installed using the same image. The two hardware models are equivalent.
ISA 8000F	The TOE software consists of Ivanti Policy Secure (IPS) 22.2R3. The appliance’s software is built on IVE OS 3.0.	

Result: Software and OS is same for both the platforms.

3.4 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical and have the same version numbers. There are no differences between the included libraries. Note: the TOE uses the same cryptographic module to provide its cryptographic functionality. This is the same across platforms.
Result:

- There are no differences in the included libraries.
- Both models are equivalent.

3.5 TOE Management Interface Differences

The TOE is managed via either a remote CLI session or a directly connected CLI. These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.

ISA 8000C supports copper ports and ISA 8000F supports fiber ports.

Result: Even if the device ports are different, it does not impact the security functionality of the TOE.

3.6 TOE Functional Differences

Each hardware model within the TOE boundary provides identical functionality. There is no difference in the way the user interacts with each device or the services available to the user for each device. Each device runs the same IVE OS version. If there were differences in the functionality provided by the software, the actual release version would differ for each platform.

Result: Both models are equivalent.

3.7 Difference Comparison

Both platforms run the same software and perform identical functionality. Both hardware platforms use identical microarchitecture processors.

3.8 Recommendations/Conclusions

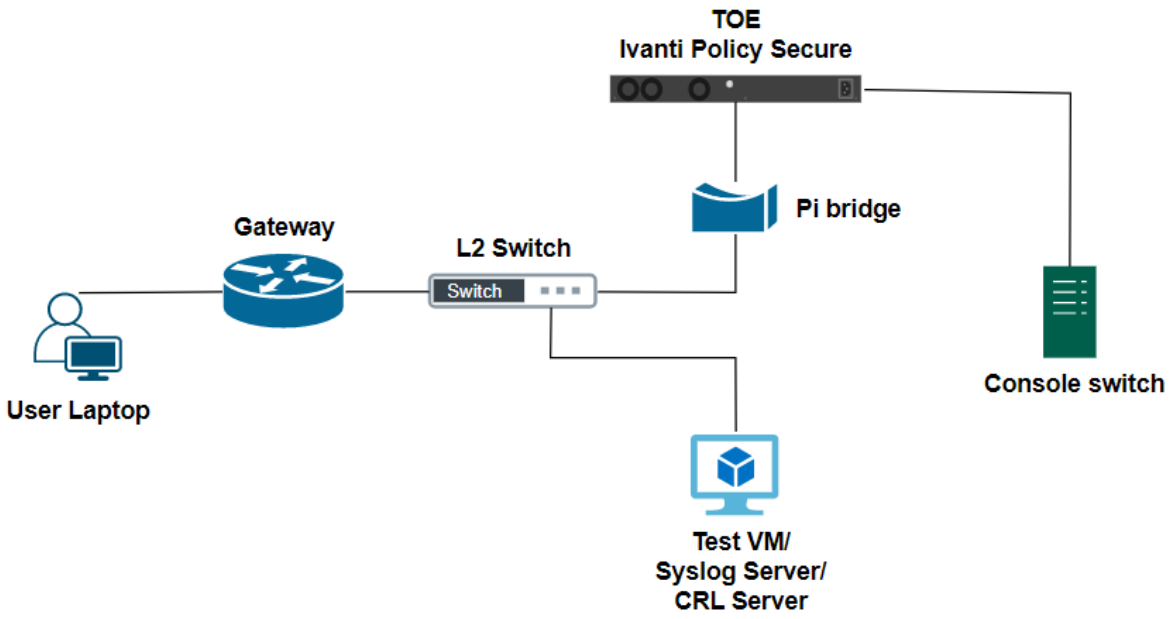
Based on the equivalency rationale listed above, testing will be performed on the following subset:

- One hardware model out of 2 will be tested.
    - ISA-8000C was selected to be tested.

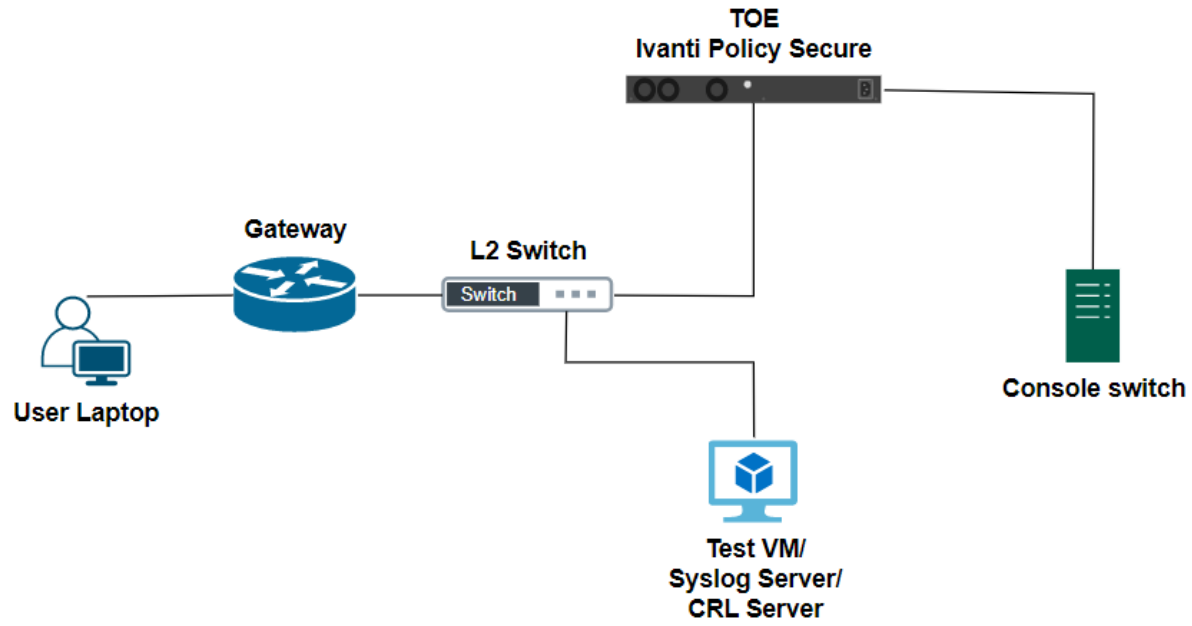
4 Test Bed Descriptions

4.1 Test Bed Diagram

4.1.1 Audit



4.1.2 Auth /TLSC-MA /TLSS /Update /X509-Rev



4.2 Configuration Information

Table 3 – Configuration Information

Name	OS	Version	Function	Protocols	Time	Tools (version)
Ivanti Policy Secure	IVE OS 3.0	22.2R3	TOE	TLS 1.2, 1.1	Manually set and verified	N/A
User Laptop	Windows 10	10	Mgt. Access/Console Access	TLS 1.2, 1.1	Manually set and verified	Chrome (Version 111.0.5563.146), Microsoft Edge (Version 111.0.1661.54), XCA (2.1.1) OpenSSL (1.1.1f) Putty (Release 0.76) MobaXterm (Version 21.3) Hex editor (Version 2.5.0.0)
Test VM/ Syslog server/ CRL server	Ubuntu Kali	Ubuntu 20.04.4/ 6.0.0-kali6-amd64	Test VM/ Syslog server/ CRL server TLS client TLS server	TLS 1.2, 1.1	Manually set and verified	OpenSSL (1.1.1f) rsyslogd 8.2210.0, acumen-tlsc-v2.2e, acumen-tlss-v2.2e, acumen-tlss, X509-mod
Console Switch	N/A	N/A	Console Access	SSH	N/A	N/A
Switch	IOS	N/A	L2 Switch	N/A	N/A	N/A
Gateway	IOS	N/A	Gateway	N/A	N/A	N/A
Pi Bridge	Linux	2021.3	Bridge	SSH	Manually set and verified	N/A

4.3 Test Time & Location

All testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from July 2022 to October 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 in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys: **Certificates are identified in the log by the Certificate DN. All generating/importing of changing or deleting of cryptographic keys relate to certificates. Public keys associated with certificates are identified by the certificate DN and the term 'public key'.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.2 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 Data Generation** 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

Table 4 – Audit data Generation

Requirement	Auditable Events	Additional Audit Record Contents	Sample logs
FAU_GEN.1	• Start-up and shut-down of the audit functions. • Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators). • Changes to TSF data related to configuration	None	AGD Section: **Audit Data Generation**

			changes (in addition to the information that a change occurred it shall be logged what has been changed). • Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). • Resetting passwords (name of related user account shall be logged).		
		FAU_GEN.2	None	None	NA
		FAU_STG.1	None	None	NA
		FAU_STG_EXT.1	None	None	NA
		FCS_CKM.1	None	None	NA
		FCS_CKM.2	None	None	NA
		FCS_CKM.4	None	None	NA
		FCS_COP.1/DataEncryption	None	None	NA
		FCS_COP.1/SigGen	None	None	NA
		FCS_COP.1/Hash	None	None	NA
		FCS_COP.1/KeyedHash	None	None	NA
		FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure	Failure to establish a HTTPS session: AGD Section **HTTPS session**
		FCS_RBG_EXT.1	None	None	NA
		FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	AGD Section: **Failure to establish a TLSC Session**
		FCS_TLSC_EXT.2	None	None	NA
		FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	AGD Section: **Failure to establish a TLSS connection**

		FCS_TLSS_EXT.2	Failure to authenticate the client	Reason for failure	NA – Not claimed
		FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address)	AGD Section: **Unsuccessful login attempts limit is met or exceeded**
		FIA_PMG_EXT.1	None	None	NA
		FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	AGD Section: **Successful and unsuccessful login attempts**
		FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	AGD Section: **Administrative login and logout**
		FIA_UAU.7	None	None	NA
		FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	AGD Session: **Failure to establish a TLSC Session** and **Unsuccessful attempt to validate a certificate**
		FIA_X509_EXT.2	None	None	NA
		FIA_X509_EXT.3	None	None	NA
		FMT_MOF.1/Functions	None	None	NA
		FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	AGD Session: **Initiation of update**
		FMT_MOF.1/Services	None	None	NA – Not Claimed
		FMT_MTD.1/CoreData	None	None	NA
		FMT_MTD.1/CryptoKeys	None	None	AGD Session: **Generating/import of, changing, or deleting of cryptographic keys**
		FMT_SMF.1	All management activities of TSF data	None	Ability to administer the TOE

					locally and remotely AGD Section: **Successful and unsuccessful login attempts** Ability to configure the access banner AGD Section: **Access banner configuration logs** Ability to configure the session inactivity time before session termination or locking AGD Section: **Session inactivity time configuration log** Ability to update the TOE, and to verify the updates using [selection: digital signature, hash comparison] capability prior to installing those updates AGD Section: **Initiation of update** Ability to configure the authentication failure parameters for FIA_AFL.1 AGD Section: **Authentication failure parameters configuration log**

					Ability to configure/ modify audit behaviour AGD Section: **Configure/ modify audit behaviour logs** Ability to manage the cryptographic keys AGD Section: **Generating/import of, changing, or deleting of cryptographic keys** Ability to set the time which is used for time-stamps AGD Section: **Changes to TSF data related to configuration changes** Ability to import/manage X.509v3 certificates to the TOE's trust store AGD Section: **Changes to TSF data related to configuration changes**
		FMT_SMR.2	None	None	NA
		FPT_SKP_EXT.1	None	None	NA
		FPT_APW_EXT.1	None	None	NA
		FPT_TST_EXT.1	None.	None.	NA
		FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process	For discontinuous changes to time: The old and new values for the	AGD Section: **Changes to TSF data related to configuration changes**

			(Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	time. Origin of the attempt to change time for success and failure (e.g., IP address).	
		FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	
		FTA_SSL.3	The termination of a remote session by the session locking mechanism	None	
		FTA_SSL.4	The termination of an interactive session	None	
		FTA_SSL_EXT.1 (if "lock the session" is selected)	Any attempts at unlocking of an interactive session	None	NA
		FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism	None	
		FTA_TAB.1	None	None	NA
		FTP_ITC.1	• Initiation of the trusted channel • Termination of the trusted channel • Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	Initiation and termination of the trusted channel AGD section: **Successful TLS session** and **Start-up and shutdown of the audit functions** Failure of the trusted channel functions AGD Section: **Failure to establish a TLSC Session**
		FTP_TRP.1/Admin	• Initiation of the trusted path	None	Initiation and termination of the trusted path

		• Termination of the trusted path. • Failure of the trusted path functions.		AGD Section: **Administrative login and logout** Failure of the trusted path functions AGD Section: **HTTPS session**
	Based on these findings, this assurance activity is considered satisfied.			
Verdict	Pass			

5.1.1.3 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:

Table 5 – Administrative Activity in AGD

Administrative Activity	Method (Command/GUI Configuration)	Section
Audit configuration	Graphical User Interface	Section Titled: **'Configuring Syslog Server and Configure Syslog Server Parameters'**
User Creation	Graphical User Interface	Section Titled: **'User Creation'**
Software update	Graphical User Interface	Section Titled: **'Software updates'**

Setting time	Graphical User Interface	Section Titled: **'Set system time'**
Configuring banner	Graphical User Interface	Section Titled: **'Administrative Banner Configuration'**
Configuring password minimum length	Graphical User Interface	Section Titled: **Password Minimum Length Configuration**
Configuring Role Mapping	Graphical User Interface	Section Titled: **Role Mapping**
Configuring NDcPP mode (inbound SSL options, FIPS mode)	Graphical User Interface	Section Titled: **Enable NDcPP mode**
Configuring Authentication Lockout	Graphical User Interface	Section Titled: **Configuring Authentication Lockout**
Import trusted client CA	Graphical User Interface	Section Titled**: Import trusted client CA**
Import trusted server CA	Graphical User Interface	Section Titled: **Import trusted server CA**
Generate RSA or ECC certificate	Graphical User Interface	Section Titled: **Generate RSA or ECC certificate**
Configuring Client Auth Certificates	Graphical User Interface	Section Titled: **Client Auth Certificates**

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.

Table 6 – Administrative Activity in Test Cases

Administrative Activity	Method (Command/GUI Configuration)	Test Case(s)
Audit configuration	Graphical User Interface	FAU_STG_EXT.1 Test #1
User Creation	Graphical User Interface	FIA_PMG_EXT.1 Test#1

	Software update	Graphical User Interface	FPT_TUD_EXT.1 Test #1
	Setting time	Graphical User Interface	FPT_STM_EXT.1 Test #1
	Configuring banner	Graphical User Interface	FTA_TAB.1 Test#1
	Configuring password minimum length	Graphical User Interface	FIA_PMG_EXT.1 Test#1
	Configuring Role Mapping	Graphical User Interface	FMT_MOF.1/Functions (1) Test #1 FMT_MOF.1/Functions (1) Test #2
	Configuring NDcPP mode (inbound SSL options, FIPS mode)	Graphical User Interface	FPT_TST_EXT.1 Test #1
	Configuring Authentication Lockout	Graphical User Interface	FIA_AFL.1 Test #1 FIA_AFL.1 Test #2b
	Import trusted client CA	Graphical User Interface	FIA_X509_EXT.1.1/Rev Test #3
	Import trusted server CA	Graphical User Interface	FIA_X509_EXT.1.1/Rev Test #1a
	Generate RSA or ECC certificate	Graphical User Interface	FIA_X509_EXT.3 Test #1
	Configuring Client Auth Certificates	Graphical User Interface	FCS_TLSC_EXT.2.1
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

5.1.2 FAU_STG.1

5.1.2.1 FAU_STG.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally and how these records are protected against unauthorized modification or

	deletion. The evaluator shall ensure that the TSS describes the conditions that must be met for authorized deletion of audit records.
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, how these records are protected against unauthorized modification or deletion, and the conditions that must be met for authorized deletion of audit records. Upon investigation, the evaluator found that the TSS states that **By default, the TSF allocates 200 MB to local audit storage; however, the administrator can configure the file size, up to 500 MB. The TSF divides the local audit storage between two audit files (active and inactive). When the current audit file reaches capacity; the TSF overwrites the inactive log file (if present). If the inactive log file is not present, then the TOE creates a new log file, switches logging to the new log file, and generates an audit log indicating that a log file reached capacity.** **The TSF protects audit data from unauthorized modification and deletion though the restrictive administrative interfaces. The filesystem of the TSF is not exposed to the administrative user over the HTTPs GUI or the local CLI. The administrative user must be positively identified and authenticated prior to being allowed to clear the local audit log or change audit settings.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.2 FAU_STG.1 Guidance

Objective	The evaluator shall examine the guidance documentation to determine that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion.
Evaluator Findings	The evaluator examined the section titled **Role Mapping** in the AGD to verify that it describes any configuration required for protection of the locally stored audit data against unauthorized modification or deletion. Upon investigation, the evaluator found that the AGD states that depending upon privilege level of users configuration modification and deletion rights are provided. 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 TSF implements Syslog over TLS using either TLS v1.1 or TLS v1.2. Logs are sent to the Syslog servers is real-time**.

	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 **By default, the TSF allocates 200 MB to local audit storage; however, the administrator can configure the file size, up to 500 MB. The TSF divides the local audit storage between two audit files (active and inactive). When the current audit file reaches capacity; the TSF overwrites the inactive log file (if present). If the inactive log file is not present, then the TOE creates a new log file, switches logging to the new log file, and generates an audit log indicating that a log file reached capacity.** **The TSF protects audit data from unauthorized modification and deletion though the restrictive administrative interfaces. The filesystem of the TSF is not exposed to the administrative user over the HTTPs GUI or the local CLI. The administrative user must be positively identified and authenticated prior to being allowed to clear the local audit log or change audit settings.** 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 is a standalone TOE. By default, the TSF allocates 200 MB to local audit storage; however, the administrator can configure the file size, up to 500 MB. The TSF divides the local audit storage between two audit files (active and inactive). When the current audit file reaches capacity; the TSF overwrites the inactive log file (if present). If the inactive log file is**

	not present, then the TOE creates a new log file, switches logging to the new log file, and generates an audit log indicating that a log file reached capacity. 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 **By default, the TSF allocates 200 MB to local audit storage; however, the administrator can configure the file size, up to 500 MB. The TSF divides the local audit storage between two audit files (active and inactive). When the current audit file reaches capacity; the TSF overwrites the inactive log file (if present). If the inactive log file is not present, then the TOE creates a new log file, switches logging to the new log file, and generates an audit log indicating that a log file reached capacity.** 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 TSF implements Syslog over TLS using either TLS v1.1 or TLS v1.2. Logs are sent to the Syslog servers is real-time**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.6 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 **Configuring Syslog Server** and **Configure Syslog Server Parameters** 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 that the AGD includes a description of the protocols used to communicate with the server and the steps required to configure the TOE to connect to the remote audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.7 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 **Configure Syslog Server Parameters** 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 Logs are sent to the syslog server in real-time, that is when an audit event is generated, it is simultaneously sent to the external server and stored locally. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.8 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 **Configure Syslog Server Parameters** 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 as described in AGD. 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 TSF supports the generation of RSA 2048 bit and 3072 bit keys for TLS client authentication, TLS server authentication, and RSA key encapsulation.** **The TSF generates ECDSA P-256 and P-384 keys for TLS client authentication, TLS server authentication, and TLS ECDHE key establishment.** 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 **Device Certificates** 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 describes the configuration for key generation and key size for the webUI. 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	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below are the key generation mechanisms supported by the TOE. RSA KeyGen (FIPS186-4) ECDSA KeyGen (FIPS186-4) CAVP Certs: # A3010. For additional details, please refer to the CAVP Mapping table in Section 8. 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 **The TSF uses both elliptic curve-based and RSA-based key establishment in support of TLS. When the TOE is configured with a server certificate with an RSA key, then RSA-based key establishment is used and the TOE acts as the sender. When the TOE is configured with a server certificate with an ECDSA key, then elliptic curve-based establishment is used and the TOE acts as the sender.** **The TOE supports the following schemes for key establishment:** • **RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1** • **Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"** **For syslog server, the TSF acts as the client and is the recipient. For these sessions, the TSF utilizes elliptic curve key agreement when an ECDHE TLS ciphersuite is negotiated and RSA based key encapsulation when any other TLS ciphersuite is negotiated.** 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 **Enable NDcPP mode** and **Device Certificates** 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 states that the guidance specifically states that when ECC 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	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below are the key establishment mechanisms supported by the TOE. RSA (RFC 3447) KAS-ECC-SSC (Sp800-56Ar3) CAVP Certs: # A3010 For additional details, please refer to the CAVP Mapping table in Section 8. The CAVP certificate covers the KAS-ECC-SSC but NO CAVP certificate exists for RSAES-PKCS1-v1_5. For the RSA, a known good implementation test was performed and document in Section 6.17 below. 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 TSF stores the following persistent keys on internal Hard Disk Drives in plaintext:** • **HTTPs/TLS Private Host Key – generated using the DRBG and FCS_CKM.1 or entered by the Security Administrator.** • **Syslog/TLS Private Client Key – generated using the DRBG and FCS_CKM.1 or entered by the Security Administrator.** **The HTTPS/TLS Private Host Key and the Syslog/TLS Private Client key are zeroized from the disk when the Security Administrator deletes the key, replaces the key, or zeroizes the entire TOE.** **The TSF zeroizes the HTTPs/TLS Private Host Key and the Syslog/TLS Private Client key on the hard disk drives by overwriting the file location with data from /dev/random three times. Each overwrite calls** **/dev/random ensuring that a different pseudo random pattern is used each time.**

	The TSF stores loads the persistent keys into RAM when they are used and the TSF also stores the following ephemeral keys in RAM: • **TLS Session keys – Established according to FCS_CKM.2 and derived using the TLS KDF** • **DRBG State – Derived from the entropy source** **HTTPS/TLS keys are zeroized from RAM when the HTTP or Syslog process terminates. The TLS Session keys are zeroized from RAM when the associated TLS session is terminated.** **The DRBG state and all ephemeral keys are zeroized when the TSF is shutdown, suffers loss of power, or restarted. The TSF zeroizes keys in RAM by writing zeros to the memory location one time and performing a read verify to ensure that the memory location was set to all zeros. If the read verify fails, the TSF repeats the zeroization process.** 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 **The above key destruction methods apply to all configurations and circumstances, except one. The only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored on the disk. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. However, all keys on the disk are protected because the TOE enables full disk encryption by default**. 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 **The HTTPS/TLS Private Host Key and the Syslog/TLS Private Client key are zeroized from the disk when the Security Administrator deletes the key, replaces the key, or zeroizes the entire TOE.** **The TSF zeroizes the HTTPs/TLS Private Host Key and the Syslog/TLS Private Client key on the hard disk drives by overwriting the file location with data from /dev/random three times. Each overwrite calls /dev/random ensuring that a different pseudo random pattern is used each time.** **The above key destruction methods apply to all configurations and circumstances, except one. The only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored on the**

	disk. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. However, all keys on the disk are protected because the TOE enables full disk encryption by default. 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 does not describe any keys stored in non-plaintext form. 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 HTTPS/TLS Private Host Key and the Syslog/TLS Private Client key are zeroized from the disk when the Security Administrator deletes the key, replaces the key, or zeroizes the entire TOE. The TSF zeroizes the HTTPs/TLS Private Host Key and the Syslog/TLS Private Client key on the hard disk drives by overwriting the file location with data from /dev/random three times. The DRBG state and all ephemeral keys are zeroized when the TSF is shutdown, suffers loss of power, or restarted. The TSF zeroizes keys in RAM by writing zeros to the memory location one time and performing a read verify to ensure that the memory location was set to all zeros. If the read verify fails, the TSF repeats the zeroization process. The above key destruction methods apply to all configurations and circumstances, except one. The only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored on the disk. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. However, all keys on the disk are protected because the TOE enables full disk encryption by default. 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 verified that ST does not specify the use of 'a value that does not contain any CSP' to overwrite keys. 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 process** 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 that the AGD states: The above key destruction methods apply to all configurations and circumstances, except one. The only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored on the disk. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. However, all keys on the disk are protected because the TOE enables full disk encryption by default. 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 AES encryption/decryption in CBC and GCM modes with 128- and 256-bit keys.** 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 **Enable NDcPP mode** and **Device Certificates** 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 that the steps to configure modes and key size. 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	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below are the implementations of encryption supported by the TOE. AES-CBC and AES-GCM CAVP AES Certs: # A3010 For additional details, please refer to the CAVP Mapping table in Section 8. 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 supports signature generation and verification with RSA (2048-. 3072-bit) with SHA-1/256/384/512 in accordance with FIPS PUB 186-4 and ECDSA with NIST curves P-256 and P-384 with SHA-1/256/384/512 in accordance with FIPS PUB 196-4.** **These signatures support TLS authentication.** 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 section titled **Enable NDcPP mode** and **Device Certificates** in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services. Upon investigation, the evaluator found that the AGD states the step to configure the TOE to use the selected cryptographic algorithm and key size. 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	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below are the implementations of signature generation and verification supported by the TOE. RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4) ECDSA SigGen (FIPS186-4) ECDSA SigVer (FIPS186-4) Certs: # A3010 For additional details, please refer to the CAVP Mapping table in Section 8. 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 for key generation using SHA-256 as specified in NIST SP 800-90 DRBG. SHA-1, SHA-256, and SHA-384 are used in support of TLS. SHA-256 is used for file integrity checking and password obfuscation. SHA-512 is used for hashing of the digital signature to verify the firmware manifest file.**

	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 Functions** 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 that the TOE supports cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512. 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	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below are the implementations of hashing supported by the TOE. SHA-1 SHA-256 SHA-384 SHA-512 CAVP SHS Certs: # A3010 For additional details, please refer to the CAVP Mapping table in Section 8. 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 implements HMAC message authentication for the following uses:**

	• **TLSv1.1 Master Secret Derivation: HMAC-SHA1, key sizes of 128 bits with ECDH P-256 or 192 bits with RSA and ECDH P-384, block size 512 bits, and output length of 160 bits;** • **TLSv1.2 Master Secret Derivation: HMAC-SHA256, key sizes of 128 bits with ECDH P-256 or 192 bits with RSA and ECDH P-384, block size 512 bits, and output length of 256 bits;** • **TLSv1.2 Master Secret Derivation: HMAC-SHA384, key sizes of 256 bits with ECDH P-256 or 384 bits with RSA and ECDH P-384, block size 1024 bits, and output length of 384 bits;** • **TLSv1.1 Key Block Derivation: HMAC-SHA1, key size of 192 bits, block size of 512 bits, and output length of 160 bits;** • **TLSv1.2 Key Block Derivation: HMAC-SHA256, key size of 384 bits, block size of 512 bits, and output length of 256 bits;** • **TLSv1.2 Key Block Derivation: HMAC-SHA384, key size of 384 bits, block size of 1024 bits, and output length of 384 bits** • **TLS Message Authentication: HMAC-SHA1, key size of 160 bits, block size 512 bits, and output length of 160 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 **Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)** in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states that the TOE supports keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and cryptographic key sizes 160-bits, 256-bits, 384- bits, and message digest sizes 160, 256, 384 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. 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

5.2.7.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below are the implementations of MACing supported by the TOE.

	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 CAVP HMAC Certs: # A3010 For additional details, please refer to the CAVP Mapping table in Section 8. 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 implements a DRBG in accordance with ISO/IEC 18031:2011 using a CTR DRBG with AES. The TSF seed the CTR_DRBG using 256-bits of data that contains at least 256 bits of entropy. The TSF gathers and pools entropy from 3 software based noise sources.** • **Device Specific randomness** • **Input layer timing randomness** • **Interrupt randomness** 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 **Enable NDcPP mode** 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 In NDcPP mode, the RNG is not configurable and there are no instances when key destruction could be delayed. 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	The evaluator examined the section titled **CAVP Algorithm Certificate Details** in the Security Target and CAVP **certificate A3010**. Upon investigation, the evaluator found that below is the implementation of SP 800-90A DRBG supported by the TOE. Counter DRBG (AES-256) CAVP DRBG Certs: # A3010 For additional details, please refer to the CAVP Mapping table in Section 8. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (HTTPS)

5.3.1 FCS_HTTPS_EXT.1

5.3.1.1 FCS_HTTPS_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS provides enough detail to explain how the implementation complies with RFC 2818. Upon investigation, the evaluator found that the TSS states that **The TSF implements the server and client sides of the HTTPs protocol according to RFC 2818 by using a TLS session to secure the HTTP session. All MUST and REQUIRED statement within RFC 2818 are followed.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FCS_HTTPS_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.
Evaluator Findings	The evaluator examined the section titled **Configuring External, Management Interfaces/Ports** and **Device Certificates** in the AGD to verify that it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server. Upon investigation, the evaluator found that the AGD states that describes the components required to login to HTTPS interface for the TOE, generating a certificate and installing the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (TLS)

5.4.1 FCS_TLSC_EXT.1

5.4.1.1 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 TSF supports and proposes the following ciphersuites and extensions in the ClientHello Message:** ○ **TLS_RSA_WITH_AES_128_CBC_SHA** ○ **TLS_RSA_WITH_AES_256_CBC_SHA** ○ **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA** ○ **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA** ○ **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA** ○ **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA** ○ **TLS_RSA_WITH_AES_128_CBC_SHA256** ○ **TLS_RSA_WITH_AES_256_CBC_SHA256** ○ **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256** ○ **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384** ○ **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** ○ **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** ○ **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** ○ **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.2 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 **Enable NDcPP mode** 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 describes the instructions on configuring TLS on TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.3 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 TSF establishes reference identifiers for the remote server as follows:** • **When the server is specified using a domain name, the TSF verifies that the domain name matches a Subject Alternative Name DNS Name field in the certificate using exact or wildcard matching specified in Section 3.1 of RFC 2818. If the certificate does not contain any Subject Alternative Name fields, the TSF matches the domain name against the Common Name in the certificate.** • **When the server is specified using an IP address, the TSF verifies that the IP address exactly matches a Subject Alterative Name IP Address field in the certificate using the rules specified in Section 3.1 of RFC 2818. If the certificate does not contain any Subject Alternative Name fields, the TSF matches the IP address against the Common Name in the certificate.** **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 as specified in RFC 3986. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name.** **The TSF does support wildcards but does not support certificate pinning and determines if the certificate is valid for the specified server based on the DNS name or IP address of the server. Wildcards are supported only at the left-most label of the identifier.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.4 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 as specified in RFC 3986. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.5 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 **Configure Syslog Server Parameters** 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 states that **The TSF establishes reference identifiers for the remote server as follows:** • **When the server is specified using a domain name, the TSF verifies that the domain name matches a Subject Alternative Name DNS Name field in the certificate using exact or wildcard matching specified in Section 3.1 of RFC 2818. If the certificate does not contain any Subject Alternative Name fields, the TSF matches the domain name against the Common Name in the certificate.** • **When the server is specified using an IP address, the TSF verifies that the IP address exactly matches a Subject Alterative Name IP Address field in the certificate using the rules specified in Section 3.1 of RFC 2818. If the certificate does not contain any Subject Alternative Name fields, the TSF matches the IP address against the Common Name in the certificate.** • **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 as specified in RFC 3986. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name.** • **The TSF does support wildcards but does not support certificate pinning and determines if the certificate is valid for the specified server based on the DNS name or IP address of the server. Wildcards are supported only at the left-most label of the identifier.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.6 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 • **Supported Elliptic Curves:** ○ **secp256r1** ○ **secp384r1** **The TOE sends the supported elliptic curves extension if an ECDHE ciphersuite is selected and does not require administrator intervention.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.7 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 **Enable NDcPP mode** and **Device Certificates, Configuring Syslog Server** 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 describes the instructions on configuring TLS on the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.2 FCS_TLSC_EXT.2

5.4.2.1 FCS_TLSC_EXT.2.1 TSS 1

Objective	The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that **When the Syslog server sends the Certificate Request message, the TSF replies with a Client Certificate message.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.2.2 FCS_TLSC_EXT.2.1 Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **Configure Secure Channel to Syslog Server** and **Import Client Auth Certificate** in the AGD to verify that it includes instructions for configuring the client-side certificates for TLS mutual authentication and the TSS indicates that mutual authentication using X.509v3 certificates is used. Upon investigation, the evaluator found that the AGD includes instructions for configuring client-side certificates for TLS mutual authentication. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3 FCS_TLSS_EXT.1

5.4.3.1 FCS_TLSS_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 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 ciphersuites supported and that the ciphersuites specified are identical to those listed for this component. Upon investigation, the evaluator found that the TSS states that **When configured with an RSA certificate, the TSF supports the following TLS ciphersuties for connections to the TOE:** • **TLS_RSA_WITH_AES_128_CBC_SHA** • **TLS_RSA_WITH_AES_256_CBC_SHA** • **TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA** • **TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA** • **TLS_RSA_WITH_AES_128_CBC_SHA256** • **TLS_RSA_WITH_AES_256_CBC_SHA256** • **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** **When configured with an ECDSA certificate, the TSF supports the following TLS ciphersuites for connections to the TOE:** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA** • **TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256** • **TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384** • **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.2 FCS_TLSS_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 (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled **Enable NDcPP mode** 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 describes the instructions on configuring TLS on TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.3 FCS_TLSS_EXT.1.2 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.
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 denial of old SSL and TLS versions. Upon investigation, the evaluator found that the TSS states that **If the TSF receives a ClientHello message that requests TLSv1.0 or earlier, the TSF sends a fatal handshake_failure message and terminates the connection.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.4 FCS_TLSS_EXT.1.2 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled **Enable NDcPP mode** in the AGD to verify that it contains any configuration necessary to meet the requirement must be contained in the AGD guidance. Upon investigation, the evaluator found that the AGD states that once NDcPP mode is selected, accept only TLS 1.1 and later is selected by default. If the TSF receives a ClientHello message that requests TLSv1.0 or earlier, the TSF sends a fatal handshake_failure message and terminates the connection. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

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

Objective	If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that, if using ECDHE or DHE ciphers, the TSS describes the key agreement parameters

	of the server Key Exchange message. Upon investigation, the evaluator found that the TSS states that **The TOE conforms to RFC 5246, section 7.4.3 for key exchange. When the TSF selects an ECDHE ciphersuite, it sends the client secp256r1 or secp384r1 key agreement parameters. The TSF prefers secp256r1 if the client indicates support for both curves in the ClientHello message.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.6 FCS_TLSS_EXT.1.3 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled **Enable NDcPP mode** in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD describes the required configuration for cipher selection. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.7 FCS_TLSS_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that **The TOE does not support session resumption based on sessionID or session tickets.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.8 FCS_TLSS_EXT.1.4 TSS 2

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS_COP.1/DataEncryption. The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that **The TOE does not support session resumption based on sessionID or session tickets.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.9 FCS_TLSS_EXT.1.4 TSS 3

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that **The TOE does not support session resumption based on sessionID or session tickets.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.3.10 FCS_TLSS_EXT.1.4 TSS 4 **[TD0569]**

Objective	If the TOE claims a (D)TLS server capable of session resumption (as a single context, or across multiple contexts), the evaluator verifies that the TSS describes how session resumption operates (i.e. what would trigger a full handshake, e.g. checking session status, checking Session ID, etc.). If multiple contexts are used the TSS describes how session resumption is coordinated across those contexts. In case session establishment and session resumption are always using a separate context, the TSS shall describe how the contexts interact with respect to session resumption (in particular regarding the session ID). It is acceptable for sessions established in one context to be resumable in another context.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target and determined that the TOE does not claim a (D)TLS server capable of session resumption. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (Identification and Authentication)

5.5.1 FIA_AFL.1

5.5.1.1 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 **An administrator can configure the number of unsuccessful attempts a remote administrator can make before a lock-out and can configure the length of time that the remote administrator is locked out. The attempts can be configured for range between 3 and 10. The length of time can be configured between 10 and 999 minutes.**

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

5.5.1.2 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 **If the user enters an incorrect password the configured number of times, the user is locked out they cannot login through any remote interface on the TOE. When the lockout time has expired, the administrator is allowed to authenticate to the TOE again.** **Lockouts are not enforced on the TOE's console interface. This ensures that authentication failures cannot lead to a situation where no administrator access is available.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 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 **Configuring authentication lockout** 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 states that the steps to configure the number of successive unsuccessful authentication and the time period (in Minutes). When the lockout time has expired, the administrator is allowed to authenticate to the TOE again. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.4 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 **Configuring authentication lockout** 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 Lockouts are not enforced on the TOE's console interface. This ensures that authentication failures cannot lead to a situation where no administrator access is available. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 FIA_PMG_EXT.1

5.5.2.1 FIA_PMG_EXT.1.1 TSS 1 **[TD0792]**

Objective	The evaluator shall check that the TSS lists the supported special character(s) for the composition of administrator passwords. The evaluator shall check the TSS to ensure that the minimum_password_length parameter is configurable by a Security Administrator. The evaluator shall check that the TSS lists the range of values supported for the minimum_password_length parameter. The listed range shall include the value of 15.
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 TSF supports administrator password composition to include any combination of upper and lower case letters, numbers, and the following special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", and the complete set of standard printable ASCII characters (values 0x20 – 0x7E)with a minimum length settable by the administrator and support 15 characters.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.2 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 **Password Minimum Length Configuration** 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 the steps to configure minimum password length and all characters which includes combination of lowercase, uppercase letters, numbers, and special characters are allowed

	while setting the password. For strong passwords the Minimum Password Length should meet. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3 FIA_UIA_EXT.1

5.5.3.1 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 TSF utilizes HTTPS to secure a remote administration web UI session. When connecting over HTTPS, the TSF presents Security Administrators with a username and password prompt; The Security Administrator using password authentication is considered authenticated if the username and the SHA-256 hash of the password matches the stored username and SHA-256 password hash. A successful authentication takes the user to the System Status page. The TSF utilizes a local serial CLI which presents Security Administrators with a username and password prompt. The Security Administrator is considered authenticated if the username and password provided match the credentials configured in the TSF. A successful login takes the user to the CLI menu.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.2 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 **Prior to successful identification and authentication, the TSF displays the TOE access banner specified in FTA_TAB.1 and responds to ICMP Echo messages with ICMP Echo Reply messages.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.3 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 **Connect Administrator Web Console, Serial Console Access Control Configuration** and **Administrative Banner Configuration** 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 a banner and then with an authentication prompt. At the authentication prompt the username of the administrator and credential (password) 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

5.5.4 FIA_UAU.7

5.5.4.1 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 section titled **Logging into the Console** in the 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 the AGD states that no preparatory steps are required to ensure that authentication data is not revealed while entering the credentials, the TOE does not provide any feedback while entering the password at both the directly connected and remote login prompt. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5 FIA_X509_EXT.1/Rev

5.5.5.1 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 states that **When a certificate is used (to identify the TSF or identify an external entity to the TSF), the TSF verifies certificates by checking the following:** **1. The current date between the "Valid from" and "Valid to" dates.** **2. The certificate is not listed on the CRL. If the TSF has a cached response that has not expired, the TSF uses the cached response in lieu of querying the CRL server.** **3. The certificate chain is valid:** **• Each certificate in the certificate chain passes the checks described in #1 and #2.** **• Each certificate (other than the first certificate) in the certificate chain has the Subject Type=CA flag set.** **• Each certificate is signed by:** **○ a certificate in the certificate chain, or** **○ a trusted root CA that has been installed in the TSF** **The TSF verifies the validity of a certificate when:** **• An HTTPS client establishes a TLS connection (HTTPs Server Certificate)** **• The TSF verifies the server certificate of the Syslog server** **• The TSF uses its client certificate authenticate to the Syslog server** **If the Security Administrator loads a certificate with a Subject Type=CA, the TSF does not validate the certificate path.** **The rules for extendedKeyUsage fields are followed in all instances; Server Authentication purpose is checked for all presented Server certificates.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5.2 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 **When a certificate is used (to identify the TSF or identify an external entity to the TSF), the TSF verifies certificates by checking the following:** **1. The current date between the "Valid from" and "Valid to" dates.** **2. The certificate is not listed on the CRL. If the TSF has a cached response that has not expired, the TSF uses the cached response in lieu of querying the CRL server.**

	3. The certificate chain is valid: • **Each certificate in the certificate chain passes the checks described in #1 and #2.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5.3 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 section titled **CRL checking configuration** in the AGD to verify that it contains describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD states that • The TOE uses a CRLs to verify whether intermediate CA certificate has been revoked when intermediate certificate is uploaded in TOE's trust store. • The TOE uses a CRLs to verify whether the leaf certificate has been revoked 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

5.5.6 FIA_X509_EXT.2

5.5.6.1 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, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator 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 TSF presents its own certificate to the Syslog server. This certificate is configured specifically for authentication to the Syslog server by the Security Administrator.** **When establishing a connection to the Syslog server, the TSF uses the certificate presented by the Syslog server to verify the server's identity.** The evaluator examined the section titled **Import Trusted Client CA, Import Trusted Server CA, Device Certificates, Configure Secure Channel to Syslog Server, Import Client Auth Certificate, CRL checking configuration** in the AGD to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.

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

5.5.6.2 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 the TSF cannot contact the CRL server or the server does not respond, the TSF logs the failure and considers the certificate valid.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6.3 FIA_X509_EXT.2 Guidance 1

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.
Evaluator Findings	The evaluator examined the section titled **Import Trusted Client CA, Import Trusted Server CA, Device Certificates, Configure Secure Channel to Syslog Server, Import Client Auth Certificate, CRL checking configuration** 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 provides instructions and warnings for configuring the operating environment so that the TOE can use the certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6.4 FIA_X509_EXT.2 Guidance 2

Objective	The guidance documentation shall also include any required configuration on the TOE to use the certificates.
Evaluator Findings	The evaluator examined the section titled **CRL checking configuration** and **Removing Cached CRL Entry of CA Chain** in the AGD to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD states that if the TSF cannot contact the CRL server or the server does not respond, the TSF logs the failure and considers the certificate valid. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6.5 FIA_X509_EXT.2 Guidance 3

Objective	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 **Import Trusted Client CA, Import Trusted Server CA, Device Certificates, Configure Secure Channel to Syslog Server, Import Client Auth Certificate, CRL checking configuration** in the AGD. Upon investigation, the evaluator found that the AGD provides instructions for the configuring the operating environment so that the TOE can use the certificates and if the TSF cannot contact the CRL server or the server does not respond, the TSF logs the failure and considers the certificate valid. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.7 FIA_X509_EXT.3

5.5.7.1 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 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 ST does not select "device-specific information". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.7.2 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 **Device Certificates** 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 states the instructions on the generation of a Certificate Request which also includes instructions for establishing all required fields "Common Name", "Organization", "Organizational Unit", or "Country", before creating the Certificate Request. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Security Management)

5.6.1 FMT_MOF.1/ManualUpdate

5.6.1.1 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 updates** in the AGD to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD states that describes the steps to follow while performing the update. The evaluator examined the section titled **Software updates** 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 if the signature check detects tampering with the update and/or signature, the TSF presents the user with an error message and discards the update. It also states that the administrator Console (Web UI) will be unavailable while the system reboots. The Serial console will be available to check the logs/messages. When the system reboot is completed administrator console (Web UI) will be available for use. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2 FMT_MOF.1/Functions

5.6.2.1 FMT_MOF.1/Functions TSS 2

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 TSF implements the Security Administrator role to authorized administrators of the TOE. The TSF allows the Security Administrators to administer the TSF via CLI through a serial cabled connected to the TOE and a web UI over a remote HTTPS channel. The TSF permissions restrict access to these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role. The web UI and local console allow the Security Administrator to perform the following TSF management functions:** • **Verify/Install Firmware Updates** • **View/Edit settings for sending audit data to the Syslog Server** • **View/Edit the amount of space allocated Local Audit storage** • **Clear/Delete Local Audit records** • **View/Edit enabled TLS versions** • **View/Edit enabled TLS ciphersuties** • **View/Edit X.509 Certificates**

	• **Generate and configure cryptographic keys used to identify the TOE** • **Configure cryptographic keys used to authenticate users** • **View/Edit the TOE access banner** • **View/Edit the session inactivity timeout** • **View/Edit authentication failure parameters** • **Set user account passwords** • **Modify system time** **The administrative interfaces provided by the TSF do not allow any of these functions to be accessed by unauthenticated or unauthorized users.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 FMT_MOF.1/Functions Guidance 2

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 **Role Mapping**, **Configuring Syslog Server** and **Configure Syslog Server Parameters** 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 that the AGD states that describes all steps through which administrator determines or modifies the behaviour of audit data. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 FMT_MTD.1/CoreData

5.6.3.1 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

	The only functions accessible prior to authentication are the display of the configurable warning and consent banner and the automated response to ICMP echo messages with ICMP echo reply messages. 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 administrative interfaces provided by the TSF do not allow any of the functions to be accessed by unauthenticated or unauthorized users.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.2 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 a trust store to store certificates. The permissions on the trust store restrict access so that only Security Administrators can import or delete certificates from the trust store. Security Administrators can also view the certificates stored in the trust store. No other access to the trust store is allowed**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.3 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 following sections in the 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 AGD includes configuration of the following in the respective sections: • **Audit Configuration:** Section titled **Configuring Syslog Server** and **Configure Syslog Server Parameters** • **TOE Banner:** Section titled **Administrative Banner Configuration** • **Session time-out:** Section titled **Configure Inactivity Timeout Period** • **TOE updates:** Section titled **Software updates**

	• **X.509 Certificates:** Section titled **Import Trusted Client CA, Import Trusted Server CA, Device Certificates, Import Client Auth Certificate** • **Basic Startup Configuration:** Section titled **Commissioning the Appliances** • **User account settings:** Section titled **Password Minimum Length Configuration, User Creation, configuring authentication lockout, Configure Inactivity Timeout Period** In addition, section '**Role Mapping**' in the guidance document specifies all the security functions are restricted to authorized security administrators. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.4 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 **Role Mapping** 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 only the administrator or the user with all permissions can configure and maintain trust store. The evaluator examined the section titled **Import Trusted Client CA, Import Trusted Server CA, Device Certificates and Import Client Auth Certificate** 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 the steps to upload EC and RSA signatures self-signed certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 FMT_MTD.1/CryptoKeys

5.6.4.1 FMT_MTD.1/CryptoKeys TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states that

	The TOE restricts the ability to manage TLS (session keys), and any configured X.509 certificates (public and private key pairs) to security administrators via GUI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4.2 FMT_MTD.1/CryptoKeys Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the section titled **Device Certificates** in the AGD to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD states that states steps to generate and import certificate signing request. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 FMT_SMF.1

5.6.5.1 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).
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the ST states that **The TSF allows the Security Administrators to administer the TSF via CLI through a serial cable connected to the TOE and a web UI over a remote HTTPS channel.** The evaluator examined the section titled **Initial Setup Through Serial Console** in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that the local CLI accessed via the physical serial port on the TOE using the provided null modem crossover cable to link your console terminal or laptop to the device's serial port. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.2 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 **Initial Setup Through Serial Console** in the AGD to verify that it describes the local administrative interface and It includes appropriate warnings

	for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD describes the local CLI accessed via the physical serial port on the TOE using the provided null modem crossover cable to link your console terminal or laptop to the device's serial port. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6 FMT_SMR.2

5.6.6.1 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 following user roles are supported by the TOE:** **• System Administrator : Who have full read and write access to Admin UI pages.** **• Read-only-Administrators : System Administrator can enable these roles whose write access is restricted and can only read admin UI** **• Delegate Administrators : System administrator can create role with some endpoints read or write access.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.2 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 section titled **Initial Setup Through Serial Console, Connect Administrator Web Console** and **Serial Console Access Control Configuration** in the 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 all steps for administering the TOE both locally and remotely. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7 TSS and Guidance Activities (Protection of the TSF)

5.7.1 FPT_APW_EXT.1

5.7.1.1 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 **The TSF does not store plaintext password. The TSF stores the SHA-256 hash of each users' password.** The evaluator also examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that **the TSF does not provide a user interface to view the password hashes.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FPT_SKP_EXT.1

5.7.2.1 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 **The TSF stores pre-shared keys, symmetric keys, and private keys in plaintext on the hard disk; however, it does not provide an interface to allow any user to view any of these values.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FPT_STM_EXT.1

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

Objective	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 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 ST does not select “obtain time from the underlying virtualization system”. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 FPT_STM_EXT.1 Guidance 1 **[TD0632]**

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 **Set System time** in the AGD to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD describes steps to set system date and time. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4 FPT_TST_EXT.1.1

5.7.4.1 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
	
	The TSF performs the following hardware self-tests at power-on:
	
	• **BIOS checks at power-on (on hardware platforms only)**
	  ○ **Verify boot block checksum. System will hang here if checksum is bad.**
	  ○ **Verify main BIOS checksum.**
	  ○ **Check CMOS diagnostic byte to determine if battery power is OK and CMOS checksum is OK.**

	○ **Verify CMOS checksum manually by reading storage area. If the CMOS checksum is bad, update CMOS with power-on default values and clear passwords.** • **Cryptographic library tests:** ○ **HMAC-SHA-256 integrity check of the library** ○ **HMAC-SHA-1 KAT** ○ **HMAC-SHA-256 KAT** ○ **HMAC-SHA-384 KAT** ○ **AES 128 ECB Encrypt and Decrypt KAT** ○ **AES 256 GCM Encrypt and Decrypt KAT** ○ **RSA 2048 SHA-256 Sign and Verify KAT** ○ **ECDSA P-224 SHA-512 Sign and Verify PCT** ○ **DRBG AES-CTR-256 KAT (invoking the instantiate, reseed, and generate functions)** • **Firmware checks:** ○ **RSA 2048 SHA-512 digital signature verification of the manifest file. This file contains a list of all executables that are part of the TSF** ○ **SHA-256 integrity check of each executable file in the TSF using the pre-calculated hashes from the manifest file.** 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 Cryptographic library test and the Firmware checks provide a high level of assurance that the firmware has not been tampered with and that the cryptographic algorithms are working properly.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.2 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** 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 • If BIOS checks at power-on fails, the TOE does not power up. • If software integrity check fails, the TOE generates a log entry. • If cryptographic library tests fail, the TSF will not start up, and an error log entry is generated.

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

5.7.5 FPT_TUD_EXT.1

5.7.5.1 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 **The TSF allows the Security Administrator to view the currently running version of firmware from the System Maintenance > Platform page of the web UI.** 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 trusted update cannot be installed on the TOE with a delayed activation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.2 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 **The TSF allows the Security Administrator to install firmware updates. The Security Administrator obtains candidate updates by downloading them from the Ivanti Secure website. When the Security Administrator uploads a firmware update, the TSF performs an RSA 2048 SHA-256 digital signature verification of the update using the Ivanti Secure firmware update public key. Ivanti Secure retains control over the private key used to sign firmware updates. If the signature check is successful, the TSF installs the update. If the**

	signature check detects tampering with the update and/or signature, the TSF presents the user with an error message and discards the update. 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 **When the Security Administrator uploads a firmware update, the TSF performs an RSA 2048 SHA-256 digital signature verification of the update using the Ivanti Secure firmware update public key. The public key is distributed as part of the firmware package. Ivanti Secure retains control over the private key used to sign firmware updates. If the signature check is successful, the TSF installs the update. If the signature check detects tampering with the update and/or signature, the TSF presents the user with an error message and discards the update.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.3 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 Security Target and found that the options 'support automatic checking for updates' or 'support automatic updates' are not selected from the selection in FPT_TUD_EXT.1.2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.4 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 Security Target and found that the published hash is not used to protect the trusted update mechanism. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.5 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 **Software Version Verification** 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, the loaded but inactive version. Upon investigation, the evaluator found that the AGD includes the steps required to show the software version and a trusted update cannot be installed on the TOE with a delayed activation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.6 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 **Software updates** 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 when the Security Administrator uploads a firmware update, the TSF performs an RSA 2048 SHA-256 digital signature verification of the update using the Ivanti Secure firmware update public key. Ivanti Secure retains control over the private key used to sign firmware updates. If the signature check is successful, the TSF installs the update. If the signature check detects tampering with the update and/or signature, the TSF presents the user with an error message and discards the update. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.7 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 Security Target & AGD and verified that published hash is not used to protect the trusted update mechanism. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.8 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 the certificate-based mechanism is not used for software update digital signature verification. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (TOE Access)

5.8.1 FTA_SSL_EXT.1

5.8.1.1 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 **User sessions can be terminated by users. The Security Administrator can set the TOE so that local and remote sessions are terminated after a Security Administrator-configured period of inactivity.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.1.2 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 **Terminating a Local Console Session** and **Configure Inactivity Timeout Period** 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 local sessions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2 FTA_SSL.3

5.8.2.1 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

	User sessions can be terminated by users. The Security Administrator can set the TOE so that local and remote sessions are terminated after a Security Administrator-configured period of inactivity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.2 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 **Configure Inactivity Timeout Period** 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 the instructions for configuring the inactivity time period for remote administrative session termination. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FTA_SSL.4

5.8.3.1 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 **User sessions can be terminated by users. The Security Administrator can set the TOE so that local and remote sessions are terminated after a Security Administrator-configured period of inactivity.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 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 **Terminating a GUI Session** and **Terminating a Local Console Session** 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 web GUI (remote) or CLI (local). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FTA_TAB.1

5.8.4.1 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 **The TSF enables Security Administrators to configure an access banner provided with the authentication prompt. The banner can provide warnings against unauthorized access to the TOE as well as any other information that the Security Administrator wishes to communicate. The TSF presents the access banner prior to authentication when a user connects to the remote web UI or local console CLI described in the FIA_UIA_EXT.1, FIA_UAU_EXT.2 description.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 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 **Administrative Banner Configuration** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that describes how to configure the banner message for both local and web GUI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (Trusted Path/Channels)

5.9.1 FTP_ITC.1

5.9.1.1 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 TSF communicates with the external syslog server using Syslog over TLS with Authentication as described in the descriptions of FAU_STG_EXT.1 and FCS_TLSC_EXT.2.** 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 clearly indicates that the connection is via TLS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.1.2 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 **Configuring Syslog Server** and **Configure Syslog Server Parameters** 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 describes instructions for establishing the allowed protocols with each authorized IT entity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FTP_TRP.1/Admin

5.9.2.1 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 **The TSF provides a trusted path for remote administration using HTTPs/TLS** Next, the evaluator compared the protocols identified in the TSS to the definition of the SFR. The evaluator found that the protocols listed in the TSS are consistent with the protocols listed in the definition of the SFR.

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

5.9.2.2 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 section titled **Initial Setup Through Serial Console, Connect Administrator Web Console** and **Serial Console Access Control Configuration** 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 the instructions for establishing the remote administrative sessions for each supported method. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 FAU_GEN.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Test Steps	• Trigger each auditable event on the TOE. • Verify that each audit record is generated and contains the required information.
Expected Test Results	• The TOE accurately generates audit records for all the required auditable events. • Screenshot evidence of the audit records generated on TOE for all the required auditable events.
Pass/Fail with Explanation	Pass. The audit records associated with each test case are recorded with each test case. A comparison of required audit records to the presented audit records was additionally performed. This analysis shows that each required audit record is generated by the TOE. This meets the testing requirements.

6.2 FAU_STG_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
Test Steps	• Configure the TOE to send logs to a syslog server. • Configure syslog server with port and certificates. • Restart the Syslog service. • Verify the Syslog version on VM. • Verify the logs generated on the TOE. • Verify the logs seen on the remote Syslog server are the same. • Verify that the logs are encrypted with packet capture.

Expected Test Results	• The TOE supports transferring of audit data without admin intervention. • The communication between the TOE and the Syslog server is encrypted. • Screenshot evidence of the packet capture showing no data is sent in clear text.
Pass/Fail with Explanation	Pass. The TOE passes all audit traffic to the remote audit server through a secure channel without admin interference. This meets the testing requirements.

6.3 FAU_STG_EXT.1 Test #2 (a)

Item	Data
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 '**drop new audit data**'.

6.4 FAU_STG_EXT.1 Test #2 (b)

Item	Data
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 existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '**overwrite previous audit records**' in FAU_STG_EXT.1.3)
Test Steps	• Configure the smallest possible logging space. • Generate logs and full the log buffer. • Once logs are full take a system snapshot and get it decrypted. • Verify the oldest log file is overwritten by the new log file once the buffer is full.
Expected Test Results	• The TOE should successfully allow the overwriting of old logs by new ones (the oldest log file is overwritten by the new log file). • Screenshot evidence of the log file showing the oldest log file is overwritten by the new log file.
Pass/Fail with Explanation	Pass. The device passed because once the limit was reached the oldest audit record was overwritten (the oldest log file is overwritten by the new log file). This meets the testing requirements.

6.5 FAU_STG_EXT.1 Test #2 (c)

Item	Data
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 '**other action**'.

6.6 FAU_STG_EXT.1 Test #3

Item	Data
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, the ST does not select FAU_STG_EXT.2/LocSpace.

6.7 FPT_STM_EXT.1 Test #1

Item	Data
Test Assurance Activity	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.
Test Steps	• Confirm current time. • Set new time. • Verify the time on the TOE was updated. • Verify the logs generated for time change.
Expected Test Results	• The TOE should support setting of time by the security administrator. • Screenshot evidence of the TOE's ability to set new time by the Security Administrator. • Screenshot evidence of the logs on the TOE showing successful modification of time.
Pass/Fail with Explanation	Pass. The security administrator was able to manually set the time. This meets the testing requirements.

6.8 FPT_STM_EXT.1 Test #2 (TD0632)

Item	Data
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.
Pass/Fail with Explanation	NA, as the TOE does not support use of an NTP server.

6.9 FPT_STM_EXT.1 Test #3

Item	Data
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	N/A. TOE does not obtain time from the underlying VS.

6.10 FTP_ITC.1 Test #1 (TD0572)

Item	Data
Test Assurance Activity	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.
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FAU_STG_EXT.1 Test #1 and FCS_TLSC_EXT.1. TOE successfully communicates to syslog and auth server with encrypted channel. The connection can be initiated by the TOE. This meets the testing requirements.

6.11 FTP_ITC.1 Test #2 (TD0572)

Item	Data
Test Assurance Activity	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.
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FAU_STG_EXT.1 Test #1 and FCS_TLSC_EXT.1. The TOE can be configured to successfully communicate with the external syslog server over TLS. This meets the testing requirements.

6.12 FTP_ITC.1 Test #3 (TD0572)

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FAU_STG_EXT.1 Test #1 and FCS_TLSC_EXT.1. The test showed all communication with an external syslog server is protected by TLS encryption. This meets the testing requirements.

6.13 FTP_ITC.1 Test #4 (TD0572)

Item	Data
Test Assurance Activity	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations: i. A duration that exceeds the TOE's application layer timeout setting, ii. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer. The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext. In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.
Test Steps	**Longer duration:** • Start a secure connection between TOE and peer. • Verify the logs on the TOE that the peer is successfully connected. • Physically interrupt the connection for 15 minutes and verify the logs on the TOE that the peer is disconnected. • Ensure that the TOE re-initiates the connection once the physical connection is reconnected after 15 minutes. • Verify the logs on the TOE that the peer is successfully reconnected. • Verify the packet capture and ensure no data was going through during the physical interruption. • Verify the packet capture that the TOE re-initiates connection with the peer and does not send any data in plain text after physical interruption. **Shorter duration:** • Start a secure connection between TOE and peer. • Verify the logs on the TOE that the peer is successfully connected. • Physically interrupt the connection for 2 minutes and ensure with the packet capture that no data was sent. • Verify the packet capture that the TOE does not send any data in plain text after physical interruption.
Expected Test Results	• The TOE should ensure that the traffic sent between itself and the remote endpoint should remain secure at all times, before and after any interruption as well. • Screenshot evidence of the packet capture showing retransmission packets during the disconnection. • Screenshot evidence of the packet capture showing that the TOE re-initiates the TLS connection after the disconnection for longer duration.
Pass/Fail with Explanation	Pass. Despite the physical interruptions, the connection remained secure when connections were re-established. This meets the testing requirements.

6.14 FAU_STG.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall access the audit trail without authentication as Security Administrator (either by authentication as a nonadministrative user, if supported, or without authentication at all) and attempt to modify and delete the audit records. The evaluator shall verify that these attempts 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 access the audit trail can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Attempt to log into the device without authentication as Security Administrator. • Verify the logs on the TOE to ensure “test” user is logged in with Read-Only permission. • Attempt to modify and delete audit records. As this is not a Security Administrator account, such options are unavailable.
Expected Test Results	• Attempt to modify and delete audit records without authentication as Security Administrator should fail as no such options are available.
Pass/Fail with Explanation	Pass. Users without Security Administrator privileges cannot modify or delete audit logs. This meets the testing requirements.

6.15 FAU_STG.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall access the audit trail as an authorized administrator and attempt to delete the audit records. The evaluator shall verify that these attempts succeed. The evaluator shall verify that only the records authorized for deletion are deleted.
Test Steps	• Login as Security Administrator. • Verify the logs on the TOE to ensure “admin” user is logged in with Administrators permission. • Attempt to delete audit records. This will succeed. • Confirm audit record deletion via TOE logs.
Expected Test Results	• Attempt to modify and delete audit records with authentication as Security Administrator is passed. • TOE logs should show audit logs deletion.
Pass/Fail with Explanation	Pass. The TOE allows an authorized administrator to modify and delete the audit records. This meets the testing requirements.

6.16 FCS_HTTPS_EXT.1 Test #1

Item	Data
Test Assurance Activity	This test is now performed as part of FIA_X509_EXT.1/Rev testing. Tests are performed in conjunction with the TLS evaluation activities.

	If the TOE is an HTTPS client or an HTTPS server utilizing X.509 client authentication, then the certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1.
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FIA_X509_EXT.1.

6.17 FCS_CKM.2 RSA

Item	Data
Test Assurance Activity	**Key Establishment Schemes** 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. **TD0580 applied**
Pass/Fail with Explanation	Pass. This test was performed in conjunction with FTP_TRP.1/Admin Test#1, FTP_TRP.1/Admin Test#2 and FTP_ITC.1 Test #1, FTP_ITC.1 Test #2, FTP_ITC.1 Test #3 to demonstrate correct operation.

6.18 FIA_AFL.1 Test #1 (TD0570)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Test Steps	• Set admin lock out options for three attempts, locking out the admin user for 10 minutes. • Verify the logs on the TOE and ensure that the lock out options has been updated. • Attempt to log in unsuccessfully three times, triggering the lock out. • Attempt to log in a fourth time using correct credentials. This will fail. • Verify the logs on TOE showing an account is locked out.
Expected Test Results	• The TOE should support admin lockout after configured number of unsuccessful attempts of login and locking out time. • TOE should show account locked out logs.
Pass/Fail with Explanation	Pass. The TOE successfully locks out a user after a configured number of failed logins attempts also once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful. This meets the testing requirements.

6.19 FIA_AFL.1 Test #2a (TD0570)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: If the **administrator action** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).
Pass/Fail with Explanation	N/A. administrator action is not selected

6.20 FIA_AFL.1 Test #2b (TD0570)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: If the **time period** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorisation attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorisation attempt using valid credentials results in successful access.
Test Steps	• Attempt to log in unsuccessfully three times, triggering the lock out. • Check logs on the TOE showing unsuccessful login attempts. • Wait for 9 minutes after user lockout then attempt to login again. This will fail. • Check logs on TOE at 9 minutes, showing account is locked out. • Wait for the full 10 minutes of lockout, then attempt to login. This will succeed. • Check logs on TOE at 10 minutes, showing successful login.
Expected Test Results	• The TOE should allow a locked-out user to log in again after lockout time expires. • TOE should show account locked out logs and successful authentication logs once locked out time is completed.
Pass/Fail with Explanation	Pass. The TOE successfully rejects log in with valid credentials till lockout period and allows a locked-out user to log in again after lockout time expires. This meets the testing requirements.

6.21 FIA_PMG_EXT.1 Test #1 (TD0571)

Item	Data
Test Assurance Activity	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.

Test Steps	• Set the minimum password requirements.
	  • Minimum 15-character length
	  • Minimum 1 upper case
	  • Minimum 1 lower case
	  • Minimum 1 digit
	  • Minimum 1 special character
	• Attempt to create 15 characters password with username: good & password: AB1CD7E!a@bc1de.
	• Attempt to create 15 characters password with username: good1 & password: FG2HI8J#f$gh2ij.
	• Attempt to create 15 characters password with username: good2 & password: KL3MN9O%k^lm3no.
	• Attempt to create 15 characters password with username: good3 & password: PQ4RS0T&p*qr4st.
	• Attempt to create 15 characters password with username: good4 & password: UV5WX1Y(u)vw5xy.
	• Attempt to create 15 characters password with username: good5 & password: ZA6BC2D!z@ab6cd.
	• Verify all the usernames with correct password requirements are created.

Expected Test Results	• The TOE should correctly support passwords which match requirements. • Screenshot evidence of the TOE's ability to correctly support passwords which match requirements. • TOE logs showing successful creation of usernames with correct password requirements are created.
Pass/Fail with Explanation	Pass. The TOE successfully creates user accounts with strong passwords. This meets the testing requirements.

6.22 FIA_PMG_EXT.1 Test #2 (TD0571)

Item	Data
Test Assurance Activity	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.
Test Steps	• Attempt to create user with missing upper case character in password with username: bad & password: ab1cd7e!a@bc1de. • Verify that the user could not be created. • Attempt to create user with missing lowing case character in password with username: bad1 & password: FG2HI8J#F$GH2IJ. • Verify that the user could not be created. • Attempt to create user with missing digits in password with username: bad2 & password: KLmMNra%k^lmsno.

	• Verify that the user could not be created. • Attempt to create user with missing special character in password with username: bad3 & password: PQ4RS0T2prqr4st. • Verify that the user could not be created. • Attempt to create user with less than 15 characters in password username: bad4 & password: UV5WX1Y(u)vw. • Verify that the user could not be created.
Expected Output	• TOE generates error on addition of users with incorrect password combinations result in failure due to Invalid Password. • Screenshot evidence of the TOE generating error for incorrect password combinations.
Pass/Fail with Explanation	Pass. The TOE rejected passwords that do not meet requirements. This meets the testing requirements.

6.23 FIA_UIA_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
Test Steps	GUI • Attempt to log into the device with incorrect credentials. Login will fail. • Verify the login attempt failure logs on TOE. • Attempt to log into the device with correct credentials. This will succeed. • Verify the successful authentication logs on TOE. Console • Attempt to log into the device with incorrect credentials. Login will fail. • Verify the login attempt failure logs on TOE. • Attempt to log into the device with correct credentials. This will succeed. • Verify the successful authentication logs on TOE.
Expected Test Results	• The TOE should allow the user with correct credentials and reject the user with incorrect credentials. • TOE should generate logs for successful and unsuccessful login attempt.
Pass/Fail with Explanation	Pass. The TOE successfully authenticates users with correct credentials and login fails when incorrect credentials are used. This meets the testing requirements.

6.24 FIA_UIA_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
Test Steps	• Verify prior to log in, only a banner is available. • Verify that after clicking 'Proceed' icon, the page will be displayed asking for login credentials and no other system services can be accessed. • Login into the TOE with valid credentials. • Verify that the services are available after the login. • Verify successful login via TOE logs.
Expected Test Results	• The TOE should not expose services to an unauthenticated remote entity, and it should only display banner.
Pass/Fail with Explanation	Pass. The TOE allows only banner to be visible prior to log in. This meets the testing requirements.

6.25 FIA_UIA_EXT.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
Test Steps	• Connect to the TOE via console and verify the only option presented is the username/password entry. • Verify successful login via TOE logs.
Expected Test Results	• The TOE does not expose any services other than the ones meant to be exposed.
Pass/Fail with Explanation	Pass. No system services are available to an unauthenticated user via the directly connected console. This meets the testing requirements.

6.26 FIA_UAU.7 Test #1

Item	Data
Test Assurance Activity	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.
Test Steps	• Log into the TOE via console. Verify that authentication information, such as the password is obscured.

	• Log into the TOE via GUI. Verify that authentication information, such as the password is obscured.
Expected Test Results	• The TOE supports obscuring of passwords.
Pass/Fail with Explanation	Pass. No feedback is shown for the password. This meets the testing requirements.

6.27 FMT_MOF.1/ManualUpdate Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Steps	• Log into TOE as a user that does not have Security Administrator privileges. • Verify the logs on the TOE to ensure "test" user is logged in with Read-Only permission. • Attempt to run a system update. As this is not a Security Administrator account, such options are unavailable.
Expected Test Results	• The TOE should block update attempts without prior authentication as Security Administrator.
Pass/Fail with Explanation	Pass. The TOE does not allow a user without administrator privileges to update the image. This meets the testing requirements.

6.28 FMT_MOF.1/ManualUpdate Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Pass/Fail with Explanation	Pass. This test has been completed as part of the requirements specified in FPT_TUD_EXT.1 Test#1.

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

Item	Data
Test Assurance Activity	Test 1 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can

	be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Login as user without Security Administrator privileges. • Verify the logs on the TOE to ensure “test” user is logged in with Read-Only permission. • Attempt to modify transmission protocol of audit data. This will fail as the options are unavailable.
Expected Test Results	• The TOE should not allow non – admin users without authentication to perform high privilege operations.
Pass/Fail with Explanation	Pass. Unauthorized users are unable to modify security related parameters for transmission protocol. This meets the testing requirements.

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

Item	Data
Test Assurance Activity	Test 2 (if **‘transmission of audit data to external IT entity’** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.
Test Steps	• Login as a user with Security Administrator privileges. • Verify the logs on the TOE to ensure “admin” user is logged in with Administrators permission. • Attempt to modify transmission protocols of audit data. This will succeed. • Verify the logs of transmission protocol modification.
Expected Test Results	• The TOE should allow a high privilege user to perform high privilege operations. • TOE should generate logs for transmission protocol modification.
Pass/Fail with Explanation	Pass. Authorized users can modify audit record transmission protocols. This meets the testing requirements.

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

Item	Data
Test Assurance Activity	Test 1 (if **'handling of audit data'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as

	Security Administrator. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.
Test Steps	• Log into TOE as a user without Security Administrator privileges. • Verify the logs on the TOE to ensure "test" user is logged in with Read-Only permission. • Attempt to modify handling of audit data. This will fail as there are no available options.
Expected Test Results	• The TOE should not allow non–admin users without authentication to perform modification of handling of audit data.
Pass/Fail with Explanation	Pass. Users without admin access cannot modify security-related parameters of audit data. This meets the testing requirement.

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

Item	Data
Test Assurance Activity	Test 2 (if **'handling of audit data'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the handling of audit data with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The term 'handling of audit data' refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace. The evaluator does not necessarily have to test all possible values of the security related parameters for configuration of the handling of audit data but at least one allowed value per parameter.
Test Steps	• Login as a user with Security Administrator privileges. • Attempt to modify the amount of space allocated for Local Audit storage. This will succeed. • Verify the logs generated for modification of handling of audit data.
Expected Test Results	• The TOE should allow admin users to perform modification of handling of audit data. • TOE should generate logs for modification of handling of audit data.
Pass/Fail with Explanation	Pass. Authorized users can modify handling of audit record data. This meets the testing requirements.

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

Item	Data
Test Assurance Activity	(if **'audit functionality when Local Audit Storage Space is full**' is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This attempt should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it

	shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Pass/Fail with Explanation	NA, the ST does not select **'audit functionality when Local Audit Storage Space is full**'.

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

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

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

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Attempt to log into TOE that does not have Security Administrator privileges. • Verify the logs on the TOE to ensure “test” user is logged in with Read-Only permission. • Attempt to determine the behavior for external transmission of audit data. This will fail as there are no ways to modify audit data behavior.
Expected Test Results	• The TOE should not allow non–admin users without authentication to determine the behavior of external transmission of audit data.
Pass/Fail with Explanation	Pass. Unauthorized users cannot determine the behavior for external transmission of audit data. This meets the testing requirements.

6.36 FMT_MOF.1/Functions (3) Test #4

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all

	options chosen from the second selection 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.
Test Steps	• Attempt to log into TOE with Security Administrator privileges. • Verify the logs on the TOE to ensure "admin" user is logged in with Administrators permission. • Attempt to determine the behavior of external transmission of audit data. This will pass. • Verify the logs generated by TOE.
Expected Test Results	• The TOE should allow admin users to determine the behavior of external transmission of audit data.
Pass/Fail with Explanation	Pass. Authorized users can determine the behavior of external transmission of audit data. This meets the testing requirements.

6.37 FMT_MTD.1/CryptoKeys Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Attempt to log in as user without Security Administrator privileges. • Verify the logs on the TOE to ensure "test" user is logged in with Read-Only permission. • Attempt to modify cryptographic keys. This will fail as all such options are unavailable.
Expected Test Results	• The TOE should not allow the unprivileged user to generate keys. All options are unavailable.
Pass/Fail with Explanation	Pass. Unauthorized user cannot perform security related configurations on the TOE. This meets the testing requirements.

6.38 FMT_MTD.1/CryptoKeys Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Test Steps	• Attempt to log into the TOE as a user with Security Administrator privileges. • Attempt to modify/delete cryptographic keys. This will succeed. • Verify the logs generated for deletion of device certificate.

Expected Test Results	• The TOE allows the admin user to generate/delete the crypto key. • TOE should generate logs for generation/deletion of the crypto key.
Pass/Fail with Explanation	Pass. Authorized users can modify and delete cryptographic keys. This meets the testing requirement.

6.39 FMT_SMF.1 Test #1

Item	Data
Test Assurance Activity	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Test Steps	**This test is completed throughout the process of testing the following SFRs:** **Table 7 – Management Functions exercised SFRs**

Management Functions	Test cases
Ability to administer the TOE locally and remotely	FIA_UIA_EXT.1
Ability to configure the access banner	FTA_TAB.1
Ability to configure the session inactivity time before session termination or locking	FTA_SSL_EXT.1, FTA_SSL.3
Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates	FPT_TUD_EXT.1, FMT_MOF.1/ManualUpdate
Ability to configure the authentication failure parameters for FIA_AFL.1	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);	FMT_MOF.1/Functions Test #4
Ability to modify the behaviour of the transmission of audit data to an external IT entity	FMT_MOF.1/Functions (1) Test#1, FMT_MOF.1/Functions (1) Test#2
Ability to manage the cryptographic keys	FMT_MTD.1/CryptoKeys Test #1, FMT_MTD.1/CryptoKeys Test #2
Ability to configure the cryptographic functionality	FPT_TST_EXT.1
Ability to import X.509v3 certificates to the TOE's trust store	FIA_X509_EXT.1/ Rev
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors	FIA_X509_EXT.1/ Rev
Ability to set the time which is used for timestamps	FPT_STM_EXT.1

Pass/Fail with Explanation	Pass. Throughout the various security functionality testing of the TOE, FMT_SMF.1 Specification of Management Functions requirements have been met. Therefore, this test passed.

6.40 FMT_SMR.2 Test #1

Item	Data
Test Assurance Activity	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
Pass/Fail with Explanation	Pass. As there are two interfaces where these can be tested (over the GUI/Console) management functions are tested from the GUI interface. Each management function is not available on the Console interface. The evaluator has met this requirement through the execution of the entirety of this test report for the TOE interfaces.

6.41 FTA_SSL.3 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Steps	• Configure the TOE with a maximum inactivity time period of five minutes. • Verify the logs for the updated session timeout. • Log into the TOE via remote connection. • Allow the session to time out. • Verify the logs for session timeout. • Configure the TOE with a maximum inactivity time period of seven minutes. • Verify the logs for the updated session timeout. • Log into the TOE via remote connection. • Allow the session to time out. • Verify the logs for session timeout. • Configure the TOE with a maximum inactivity time period of ten minutes. • Verify the logs for the updated session timeout. • Log into the TOE via remote connection. • Allow the session to time out. • Verify the logs for session timeout.
Expected Test Results	• The TOE should support and successfully terminate session after the timeout period. • TOE should generate logs for session timeout.
Pass/Fail with Explanation	Pass. The TOE disconnects users from web GUI after meeting inactivity time limit. This meets the testing requirements.

6.42 FTA_SSL.4 Test #1

Item	Data
Test Assurance Activity	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	• Log in to TOE via local console connection. • Log off from TOE. • Verify the logs for log off.
Expected Test Results	• The TOE should terminate the local session after the user logs off. • TOE should generate logs for log off.
Pass/Fail with Explanation	Pass. The TOE allows the user to terminate the directly connected administrative session. This meets the testing requirements.

6.43 FTA_SSL.4 Test #2

Item	Data
Test Assurance Activity	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	• Log into the TOE via remote session. • Log out of device. • Verify the logs for logout.
Expected Test Results	• The TOE should terminate the remote session after the user logs off. • TOE should generate logs for logout.
Pass/Fail with Explanation	Pass. The TOE allows the user to terminate the remote administrative session. This meets the testing requirements.

6.44 FTA_SSL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Test Steps	• Set local timeout period to 5 mins. • Verify the logs for the updated session timeout. • Start a fresh session. • After 5 mins, the connection is terminated. • Check logs for session termination.

	• Set local timeout period to 7 mins. • Verify the logs for the updated session timeout. • Start a fresh session. • After 7 mins, the connection is terminated. • Check logs for session termination.
Expected Test Results	• The TOE should terminate the session after the configured time period. • The TOE should generate logs for session termination.
Pass/Fail with Explanation	Pass. The TOE ends user session on local console after inactivity time limit is reached. This meets the testing requirements.

6.45 FTA_TAB.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Steps	• Navigate to Authentication -> Signing In -> Sign-in Notifications. • Create a notice and consent warning message for login into the TOE. • Navigate to Authentication -> Signing In -> Sign-In Policies and click on admin URL */admin/. • In the Configure SignIn Notifications section, select the check box Pre-Auth Sign-in Notification. • Attempt to log into the TOE via GUI and confirm the presence of banner. • Attempt to log into the TOE via console and confirm the presence of banner.
Expected Test Results	• The TOE should support the display of banners.
Pass/Fail with Explanation	Pass. An access banner can be set for all the methods that can be used to access the device. This meets the testing requirements.

6.46 FTP_TRP.1/Admin Test #1

Item	Data
Test Assurance Activity	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.
Test Steps	• Log into the TOE via HTTPS. • Verify audit logs that user is successfully log in to the TOE. • Verify that the session was established, and data is encrypted via packet capture.
Expected Test Results	• The TOE encrypts the management traffic successfully. • TOE logs showing successful login.

	• Screenshot evidence of the packet capture showing that the data is encrypted.
Pass/Fail with Explanation	Pass. User is successfully able to access the TOE via TLS connection. This meets the testing requirements.

6.47 FTP_TRP.1/Admin Test #2

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Pass/Fail with Explanation	Pass. Refer to FTP_TRP.1/Admin Test #1 for encrypted channel data.

6.48 FCS_TLSC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	• Configure the TOE to connect to the TLS server. • Establish a connection with the TOE over TLS using the ciphersuite using the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_256_CBC_SHA. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection.

	• Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA256. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_256_CBC_ SHA256. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. • Verify the with packet capture the required ciphersuite. • Verify TOE logs for successful connection.
Expected Test Results	• TOE logs show the successful establishment of TLS connection. • Packet Captures show the successful establishment of TLS connection with configured ciphersuites.

Pass/Fail with Explanation	Pass. TOE successfully negotiates each of the claimed cipher suites. This meets the test requirements.

6.49 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Steps	Valid Certificate: • Load the server certificate containing the Server Authentication purpose on the TLS server. • Establish a connection with the TOE over TLS. • Verify the successful connection with packet capture. • Verify TOE logs for successful connection. Invalid Certificate: • Load the server certificate lacking the Server Authentication purpose on the TLS server. • Establish a connection with the TOE over TLS. • Verify the error with logs on the device showing connection is rejected due to invalid extension in certificate. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• TOE should establish a connection with a server with authorized server certificate, packet capture and TOE logs should show successful connection. • TOE should reject the connection when certificate lacking the Server Authentication purpose in the extendedKeyUsage field is used, packet capture and TOE logs shows the connection failure due to invalid certificate extensions.
Pass/Fail with Explanation	Pass. The TOE makes a successful connection when a valid certificate is provided and does not make the connection when the Server Authentication is not present in the extendedKeyUsage field. This meets the testing requirements.

6.50 FCS_TLSC_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall send a server certificate in the TLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite). The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool with a certificate that does not match the server-selected ciphersuite (an RSA certificate and ECDSA cipher suite), verify that it fails. • Verify the error logs on the device showing wrong certificate type.

	• Verify the unsuccessful connection with packet capture.
Expected Test Results	• The TOE should be unable to establish a connection with server certificate that does not match the server-selected ciphersuite. • TOE logs and packet capture should show connection failure due to server certificate that does not match the server-selected ciphersuite.
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.

6.51 FCS_TLSC_EXT.1.1 Test #4a

Item	Data
Test Assurance Activity	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' and send a server hello selecting TLS_NULL_WITH_NULL NULL cipher suite with MA and verify the output. Tool syntax: ./acumen-tlsc-v2.2e <ip> <port> --cert=<cert> --key=<key> -t=<test> [--ma] • Verify the error logs on the device showing failure due to unknown cipher. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• The TOE should reject a connection when server selects non-supported algorithm. • TOE logs should show connection failure due to unknown cipher. • Packet capture should show fatal error is generated by TOE as server presents 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.

6.52 FCS_TLSC_EXT.1.1 Test #4b

Item	Data
Test Assurance Activity	Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool and verify the connection with an unsupported ciphersuite. • Verify the error logs on the device showing connection failure due to wrong cipher. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• Client should reject the connection when server modifies a ciphersuite. • TOE logs should show connection failure due to wrong cipher. • Packet capture should show fatal error is generated by TOE after receiving the server hello as wrong cipher is presented by server.
Pass/Fail with Explanation	Pass. The TOE rejects the connection with unsupported ciphersuite by sending a Fatal Alert. This meets the testing requirements.

6.53 FCS_TLSC_EXT.1.1 Test #4c

Item	Data
Test Assurance Activity	[conditional]: If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension** the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool and verify the connection with an unsupported elliptical curve. • Verify the error logs on the device showing connection due to wrong curve. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• TOE should reject the connection if an unsupported curve is provided. • TOE logs should show connection failure due to wrong curve. • Packet capture should show fatal error generated by TOE 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 testing requirements.

6.54 FCS_TLSC_EXT.1.1 Test #5a

Item	Data
Test Assurance Activity	Change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool and send a server hello using an unsupported TLS version and verify that the TOE rejects the connection. • Verify the connection fails with packet capture. • Verify connection failure logs due to unsupported protocol.
Expected Test Results	• TOE should reject the connection when server sends a message with non-supported TLS version. • TOE logs should show connection failure due to unsupported protocol. • Packet capture should show fatal error is generated by TOE as server hello using an unsupported TLS version is sent.
Pass/Fail with Explanation	Pass. The connection fails due to unsupported TLS version. This meets the test requirements.

6.55 FCS_TLSC_EXT.1.1 Test #5b

Item	Data
Test Assurance Activity	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool and verify the connection when a byte is modified in the Server's Key Exchange handshake message. • Verify the error logs on the device showing connection failure due to bad signature.

	• Verify the unsuccessful connection with packet capture.
Expected Test Results	• The connection establishment should fail when the signature block in server's key exchange handshake message is modified. • TOE logs should show connection failure due to bad signature. • Packet capture should show fatal error is generated by TOE and handshake does not finish 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.

6.56 FCS_TLSC_EXT.1.1 Test #6a

Item	Data
Test Assurance Activity	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool and verify the connection when a byte is modified in the server finished handshake. • Verify the error logs on the device showing digest check failed. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• TOE should reject a connection when tool modifies server finished handshake message. • TOE logs should show connection failure due to digest check failure. • Packet capture should show encrypted alert generated by TOE and handshake does not finish successfully.
Pass/Fail with Explanation	Pass. The connection is not completed when a corrupted Server Finished message is received. This meets the test requirements.

6.57 FCS_TLSC_EXT.1.1 Test #6b

Item	Data
Test Assurance Activity	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Start the server using the 'acumen-tlsc-v2.2e' tool and verify the connection when garbled message is sent after the ChangeCipherSpec message. • Verify the error logs on the device showing data received between CCS and finished. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• Handshake should not happen when TOE receives garbled message. • TOE logs should show connection failure due to data received between CCS and finished. • Packet capture should show encrypted alert is generated by TOE as garbled message is sent after the ChangeCipherSpec message.
Pass/Fail with Explanation	Pass. The TOE closes the connection after receiving garbled data. This meets the test requirements.

6.58 FCS_TLSC_EXT.1.1 Test #6c

Item	Data

Test Assurance Activity	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.
Test Steps	• Start the server using the 'acumen-tls-v2.2e' tool and verify the connection when a byte is modified in the server's nonce in the Server Hello handshake message. • Verify the error logs showing handshake failure due to bad signature. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• Client should reject the handshake message when nonce in the server hello handshake is changed. • TOE logs should show handshake failure due to bad signature. • Packet capture should show fatal error is generated by TOE after receiving Server Key Exchange handshake message as bytes are modified in server nonce.
Pass/Fail with Explanation	Pass. The connection was rejected due to a modified nonce. This meets the test requirements.

6.59 FCS_TLSC_EXT.1.2 Test #1

Item	Data
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.** 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.
Test Steps	CN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing bad CN. • Configure the Server certificate showing no SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify the connection failure logs on the device which states that CN does not match in peer certificate. • Verify the unsuccessful connection due to bad CN in packet capture. CN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing bad CN. • Configure the Server certificate showing no SAN extension.

	• Establish a connection with the TOE over TLS and verify the connection. • Verify the connection failure logs on the device which states that CN does not match in peer certificate. • Verify the unsuccessful connection due to bad CN in a packet capture.
Expected Test Results	• The TOE rejects certificates with a bad CN and No SAN. • TOE logs should show connection failure due to bad CN and No SAN. • Packet capture should show bad CN and no SAN is configured in the certificate and FIN message is generated by TOE.
Pass/Fail with Explanation	Pass. The TOE rejects certificates with contains a CN that does not match the reference identifier and does not contain the SAN extension. This meets the testing requirements.

6.60 FCS_TLSC_EXT.1.2 Test #2

Item	Data
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.** 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.
Test Steps	CN and SAN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing good CN. • Configure the Server certificate showing bad SAN. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which state that SAN does not match in peer certificate. • Verify the unsuccessful connection due to bad SAN but the CN matches with reference identifier in packet capture. CN and SAN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing good CN. • Configure the Server certificate showing bad SAN. • Initiate the connection from the TOE to the TLS Server and verify the connection. • Verify the connection failure logs on the device which states that SAN does not match in peer certificate. • Verify the unsuccessful connection due to bad SAN but the CN matches with reference identifier in packet capture.
Expected Test Results	• The TOE rejects certificates with a good CN but bad SAN. • TOE logs should show connection failure due SAN mismatch. • Packet capture should show good CN and bad SAN in configured in the certificate and FIN message is generated by TOE.

Pass/Fail with Explanation	Pass. The TOE rejects certificates with CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. This meets the testing requirements.

6.61 FCS_TLSC_EXT.1.2 Test #3

Item	Data
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.** If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
Test Steps	CN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing good CN. • Configure the Server certificate showing no SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify the successful connection due to CN matches the reference identifier on the TOE but no SAN present in the certificate. • Verify the successful connection due to CN matches the reference identifier on the TOE but no SAN present in the certificate in packet capture. CN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing good CN. • Configure the Server certificate showing no SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify the successful connection due to CN matches the reference identifier on the TOE but no SAN present in the certificate. • Verify the successful connection due to CN matches the reference identifier on the TOE but no SAN present in the certificate in packet capture.
Expected Test Results	• The TOE accepts the connection when the certificate with a good CN and No SAN is presented. • TOE logs and packet capture should show successful connection with good CN.
Pass/Fail with Explanation	Pass. The TOE successfully accepts the connection when a server certificate contains a CN that matches the reference identifier and does not contain the SAN extension. This meets the testing requirements.

6.62 FCS_TLSC_EXT.1.2 Test #4

Item	Data

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.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).
Test Steps	CN and SAN as IPV4: • Configure the TOE for reference identifier name as IPV4. • Configure the Server certificate showing bad CN. • Configure the Server certificate showing good SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify successful connection logs on TOE. • Verify the successful connection due to SAN matches the reference identifier on the TOE but a bad CN in packet capture. CN and SAN as FQDN: • Configure the TOE for reference identifier name as FQDN. • Configure the Server certificate showing bad CN. • Configure the Server certificate showing good SAN extension. • Establish a connection with the TOE over TLS and verify the connection. • Verify successful connection logs on TOE. • Verify the successful connection due to SAN matching the reference identifier on the TOE but a bad CN in the packet capture.
Expected Test Results	• The TOE accepts the connection when the certificate with a bad CN and good SAN is presented. • TOE logs and packet capture should show a successful connection when the certificate with a bad CN and good SAN is presented.
Pass/Fail with Explanation	Pass. The TOE successfully accepts the connection when a server certificate 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.

6.63 FCS_TLSC_EXT.1.2 Test #5 (1)

Item	Data
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.
Test Steps	CN: • Configure the TOE for the correct reference identifier.

	• Configure the node certificate showing wildcard that is not in the left-most label of CN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device due to CN mismatch. • Verify the unsuccessful connection with packet capture. SAN: • Configure the TOE for the correct reference identifier. • Configure the node certificate showing wildcard that is not in the left-most label of SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device due to SAN mismatch. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• TOE rejects the connection when the reference identifier does not match the presented wildcard which is not in the leftmost label. • TOE logs should show connection failure due to CN/SAN mismatch. • Packet capture should show FIN message is generated by TOE due to mismatched parameters.
Pass/Fail with Explanation	Pass. TOE rejects the connection when the reference identifier does not match the presented wildcard which is not in the leftmost label. This meets the testing requirements.

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

Item	Data
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.)
Test Steps	CN: • Configure the TOE for the reference identifier with single left-most label. • Configure the node certificate showing wildcard in the leftmost label in CN. • Establish a connection with the TOE over TLS and verify the successful connection. • Verify the successful connection logs on device. • Verify the successful connection via packet capture. SAN: • Configure the TOE for the reference identifier with single left-most label.

	• Configure the node certificate showing wildcard in the leftmost label in SAN. • Establish a connection with the TOE over TLS and verify the successful connection. • Verify the successful connection logs on the device. • Verify the successful connection via packet capture.
Expected Test Results	• TOE accepts the connection when the reference identifier with single left-most labels is presented in the certificate. • TOE logs and packet capture should show successful connection.

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.

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

Item	Data
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.)
Test Steps	CN: • Configure the TOE for the reference identifier without a leftmost label. • Configure the node certificate showing wildcard in the leftmost label in CN. • Load the certificate with Wildcard in leftmost label in CN on the TLS server. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device due to CN mismatch. • Verify the unsuccessful connection with packet capture. SAN: • Configure the TOE for the reference identifier without a leftmost label. • Configure the node certificate showing wildcard in the leftmost label in SAN. • Load the certificate with Wildcard in leftmost label in SAN on the TLS server. • Establish a connection with the TOE over TLS and verify the connection. • Verify the error logs on the device due to SAN and reference identifier mismatch. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• When configuring the reference identifier with no left-most labels on TOE the connections fail. • TOE logs should show connection failure due to CN/SAN mismatch. • Packet capture should show FIN message is generated by TOE due to mismatched parameters.
Pass/Fail with Explanation	Pass. When configuring the reference identifier with no left-most labels on the TOE and presented a server certificate containing a wildcard in the left-most label the connections fail. This meets the testing requirements.

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

Item	Data

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.)
Test Steps	CN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the node certificate showing wildcard in the leftmost label in CN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the TOE, showing CN mismatched. • Verify the unsuccessful connection via packet capture. SAN: • Configure the TOE for the reference identifier with two leftmost labels. • Configure the node certificate showing wildcard in the leftmost label in SAN. • Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the TOE, showing SAN mismatched. • Verify the unsuccessful connection via packet capture.
Expected Test Results	• When configuring the reference identifier with two left-most labels on the TOE and a wildcard in server certificate the connections fail. • TOE logs should show connection failure due to CN/SAN mismatch. • Packet capture should show FIN message is generated by TOE due to mismatched parameters.
Pass/Fail with Explanation	Pass. When configuring the reference identifier with two left-most labels on the TOE and a server certificate with a wildcard is presented, the connections fail. This meets the testing requirements.

6.67 FCS_TLSC_EXT.1.2 Test #6

Item	Data
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**. 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.
Test Steps	IPv4: • Configure the TOE for the correct reference identifier. • Create a server certificate with a CN that matches the reference identifier but replace one of the groups with an *. • Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the device, showing validation failure due to CN mismatch. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• 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 (*) and TOE generates failure logs for CN mismatch. • Generate log on the TOE showing validation failure due to CN mismatch. • Packet capture showing unsuccessful connection due to CN mismatch.
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.

6.68 FCS_TLSC_EXT.1.2 Test #7a

Item	Data
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, the ST does not select **the secure channel is used for FPT_ITT, and RFC 5280.**

6.69 FCS_TLSC_EXT.1.2 Test #7b

Item	Data
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, the ST does not select **the secure channel is used for FPT_ITT, and RFC 5280.**

6.70 FCS_TLSC_EXT.1.2 Test #7c

Item	Data
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, the ST does not select **the secure channel is used for FPT_ITT, and RFC 5280.**

6.71 FCS_TLSC_EXT.1.2 Test #7d

Item	Data
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, the ST does not select **the secure channel is used for FPT_ITT, and RFC 5280.**

6.72 FCS_TLSC_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Test Steps	• Configure TOE to connect to the TLS server. • Create a full chain of certificates to connect to the TOE. • Upload CA and ICA to the TOE. • Attempt the connection from the TOE to the TLS server and verify the connection (complete certificate chain present). • Verify the successful connection with packet capture. • Verify TOE logs for successful connection.
Expected Test Results	• When a complete certificate trust chain is present, the TOE can make a successful connection and logs are generated for a successful connection.
Pass/Fail with Explanation	Pass. When a complete certificate trust chain is present, the TOE can make a successful connection. This meets the test requirements.

6.73 FCS_TLSC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
Test Steps	Failed matching of the reference Identifier: • The requirements of this test case are exercised in FCS_TLSC_EXT.1.2 Test #1 and Test #2. Failed validation of the Certificate Path: • Remove the ICA from a chain on the TOE. • Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the device, showing untrusted certificate is used. • Verify the unsuccessful connection with packet capture. Failed validation of the Expired Certificate: • Create a server certificate which is expired. • Show clock on the TOE.

	• Establish a connection with the TOE over TLS and verify the connection. • Verify the failure logs on the device, showing connection is not established due expired certificate. • Verify the unsuccessful connection with packet capture. Failed determination of the revocation status: • The requirements of this test case are exercised in FIA_X509_EXT.2 Test #1.
Expected Test Results	• The TOE rejects the Invalid certificates. • TOE logs showing connection failure due to invalid certificates. • Packet capture showing unsuccessful connection due to invalid certificates.
Pass/Fail with Explanation	Pass. The TOE rejects the Invalid certificates. This meets the test requirements.

6.74 FCS_TLSC_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. **If any override mechanism is defined for failed certificate validation**, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
Pass/Fail with Explanation	NA, this test is not applicable as TOE does not implement any administrator override mechanism as per ST.

6.75 FCS_TLSC_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.
Test Steps	• Initiate the connection from the TOE to the TLS Server using the curve secp256r1 and verify the connection. • Verify with packet capture that the required curve is secp256r1. • Verify TOE logs for successful connection. • 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. • Verify TOE logs for successful connection.
Expected Test Results	• The TOE accepted a connection when supported curves were introduced, packet capture and TOE logs show a successful connection.

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

6.76 FCS_TLSC_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall establish a connection to a peer server that is configured for mutual authentication (i.e. sends a server Certificate Request (type 13) message). The evaluator observes that the TOE DTLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages during its negotiation of a DTLS channel and that Application Data is sent. In addition, all other testing in FCS_DTLSC_EXT.1 and FIA_X509_EXT.* must be performed as per the requirements. **TD0670 applied.**
Test Steps	• Initiate successful connection with the TOE over TLS. • Verify TOE logs for successful connection. • Verify with packet capture for server Certificate Request (type 13) message and client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages.
Expected Test Results	• The TOE establishes a connection to a peer server that is configured for mutual authentication. • Packet capture showing type 13, type 11, and type 15 messages.
Pass/Fail with Explanation	Pass. The TOE establishes connection to a peer server that is configured for mutual authentication. This meets the test requirements.

6.77 FCS_TLSS_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	• Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_256_CBC_SHA • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • Verify the required ciphersuite with packet capture.

	• Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA256 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_RSA_WITH_AES_256_CBC_ SHA256 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Verify the required ciphersuite with packet capture. • Establish a connection with the TOE over TLS using the ciphersuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • Verify the required ciphersuite with packet capture.
Expected Test Results	• Connection should be established when supported ciphersuite is present. • Packet capture showing successful negotiation with supported ciphersuites.
Pass/Fail with Explanation	Pass. The TOE was able to make each connection via the supported ciphersuites. This meets the testing requirements.

6.78 FCS_TLSS_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
Test Steps	• Attempt to establish a TLS connection to the TOE using an unsupported ciphersuite in the Client Hello: - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256. • Verify the connection fails via packet capture.

	• Verify the failure logs on TOE showing failure due to no shared cipher. • Using acumen-tlss-v2.2e as client, verify the connection to the TOE fails with an unsupported ciphersuite: TLS_NULL_WITH_NULL_NULL. • Verify the connection fails via packet capture. • Verify the failure logs on TOE showing failure due to no shared cipher. .
Expected Test Results	• Connection should be rejected when the unsupported ciphersuite is present. • Packet capture shows handshake failure with unsupported ciphersuites. • Failure logs on TOE showing failure due to no shared cipher.
Pass/Fail with Explanation	Pass. The TOE rejects TLS connections with the unsupported ciphersuites. This meets the testing requirement.

6.79 FCS_TLSS_EXT.1.1 Test #3a

Item	Data
Test Assurance Activity	Modify a byte in the Client Finished handshake message, and verify that the server rejects the connection and does not send any application data.
Test Steps	• Run the Acumen-tlss-v2.2e tool as a client with a modified client finished message and wait for the connection, the connection should fail. • Verify the failure logs on the device showing failure due to digest check failed. • Verify the unsuccessful connection via packet capture.
Expected Test Results	• TOE should reject a connection when byte in client finished handshake message is modified. • Packet capture should show connection failure when message is modified. • TOE logs show digest check error during handshake.
Pass/Fail with Explanation	Pass. The TOE rejects the connection after receiving the modified Client Handshake message. This meets the test requirements

6.80 FCS_TLSS_EXT.1.1 Test #3b

Item	Data
Test Assurance Activity	(Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.) The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent. The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does

	not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.
Test Steps	• Initiate a connection to the TOE via Acumen-tlss from the evaluator machine. • Verify that no Alert with alert level Fatal (2) messages were sent. • Verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. • Examine the Finished message and confirm that it does not contain unencrypted data by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages.
Expected Test Results	• TOE should reject a connection when text is not encrypted otherwise it should succeed. • Evidence (Packet capture) showing message is encrypted hence the connection is successful.
Pass/Fail with Explanation	Pass. The Finished message contains Hexadecimal 16 and is sent immediately after Hexadecimal 14 in the ChangeCipherSpec message. The first byte of the encrypted Finished message does not equal hexadecimal 14. This meets the testing requirement.

6.81 FCS_TLSS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.
Test Steps	• Use the acumen-tlss tool to initiate a connection to the TOE and verify the connections fails for all the unsupported SSL and TLS versions. • Verify the connection fails with SSLv2.0. • Verify connection failure due to an unknown protocol via logs. • Verify failure using packet capture. • Verify the connection fails with SSLv3.0. • Verify connection failure due to an unknown protocol via logs. • Verify failure using packet capture. • Verify the connection fails with TLSv1.0. • Verify connection failure due to an unknown protocol via logs. • Verify failure using packet capture.

Expected Test Results	• Server should reject a connection when a client requests a connection with unsupported TLS/SSL versions. • TOE logs should show connection failure due to an unknown protocol. • Packet capture should show connection reset for unsupported TLS/SSL versions.
Pass/Fail with Explanation	Pass. The TOE rejects all SSLv2, SSLv3, and TLS v1.0 connection attempts. This meets the testing requirement.

6.82 FCS_TLSS_EXT.1.3 Test #1a

Item	Data
Test Assurance Activity	If **ECDHE ciphersuites** are supported: The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.
Test Steps	• Initiate a connection with the TOE over TLS using the curve secp256r1 and verify the connection is successful. • Verify the packet capture showing the curve secp256r1. • Initiate a connection with the TOE over TLS using the curve secp384r1 and verify the connection is successful. • Verify the packet capture showing the curve secp384r1.
Expected Test Results	• The connection should be successful when a supported ECDHE cipher and elliptic curve are configured. • Evidence (Packet capture) showing supported elliptic curve.
Pass/Fail with Explanation	Pass. The TOE was able to make connection using each supported elliptic curve. This meets the test requirements.

6.83 FCS_TLSS_EXT.1.3 Test #1b

Item	Data
Test Assurance Activity	If **ECDHE ciphersuites** are supported: The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.
Test Steps	• Initiate a connection with the TOE over TLS using the supported ciphersuite and unsupported elliptical curve and verify the connection fails. • Verify the packet capture showing connection failure. • Verify logs on the device showing connection failure.
Expected Test Results	• Connection should be rejected when supported cipher and the unsupported elliptic curve is configured.

	• Evidence (Packet capture) showing connection failure with the unsupported elliptic curve.
Pass/Fail with Explanation	Pass. The TOE rejects a connection with unsupported elliptic curves. This meets the testing requirements.

6.84 FCS_TLSS_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	If **DHE ciphersuites** are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).
Pass/Fail with Explanation	N/A. DHE ciphersuites are not claimed in ST.

6.85 FCS_TLSS_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	If **RSA key establishment ciphersuites** are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.
Test Steps	• Import the node certificate to the TOE with a key size of 2048 and use RSA for key establishment. • Assign Management Port to the node certificate for establishing TLS connection from the client. • Connect to the TOE using RSA 2048 bit key and verify that it is successful. • Verify with packet capture. • Import the node certificate to the TOE with a key size of 3072 and use RSA for key establishment. • Assign Management Port to the node certificate for establishing TLS connection from the client. • Connect to the TOE using RSA 3072 bit key and verify that it is successful. • Verify with packet capture.
Expected Test Results	• The RSA key size used should match with the configured size and the connection should be established successfully. • Evidence (Packet capture) showing RSA key size in modulus format.
Pass/Fail with Explanation	Pass. The TOE was able to establish the connection using each supported RSA key size. This meets the testing requirement.

6.86 FCS_TLSS_EXT.1.4 Test #1 (TD0569)

Item	Data
Test Assurance Activity	If the **TOE does not support session resumption based on session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2) or session tickets according to RFC5077**, the evaluator shall perform the following test: a) The client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket. b) The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake). c) The client verifies the Server Hello message contains a zero-length session identifier or passes the following steps: Note: The following steps are only performed if the ServerHello message contains a non-zero length SessionID. d) The client completes the TLS handshake and captures the SessionID from the ServerHello. e) The client sends a ClientHello containing the SessionID captured in step d). This can be done by keeping the TLS session in step d) open or start a new TLS session using the SessionID captured in step d). f) The client verifies the TOE: 1. implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or 2. terminates the connection in some way that prevents the flow of application data.
Test Steps	• Connect the TOE using the Acumen-tlss tool. • Verify that the client sends a Client Hello with a zero-length session identifier and with a SessionTicket extension containing a zero-length ticket. • The client verifies the server does not send a NewSessionTicket handshake message (at any point in the handshake). • Verify that the server hello message contains a zero-length session identifier.
Expected Test Results	• TOE should verify that server contains a zero-length session identifier. • Evidence (Packet capture) showing session ID length.
Pass/Fail with Explanation	Pass. The TOE does not send a New Session ticket and the client sends a Client Hello with a zero-length session identifier and the server hello message contains a zero-length session identifier. This meets the testing requirement.

6.87 FCS_TLSS_EXT.1.4 Test #2a (TD0569)

Item	Data
Test Assurance Activity	If the **TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):

	The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages (as shown in Figure 2 of RFC 4346 or RFC 5246).
Pass/Fail with Explanation	NA, as the TOE does not support session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2).

6.88 FCS_TLSS_EXT.1.4 Test #2b (TD0569)

Item	Data
Test Assurance Activity	If the **TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its ChangeCipherSpec message thereby disrupting the handshake. The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.
Pass/Fail with Explanation	NA, as the TOE does not support session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2).

6.89 FCS_TLSS_EXT.1.4 Test #3a (TD0569)

Item	Data
Test Assurance Activity	If the **TOE supports session tickets according to RFC5077**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator shall then attempt to correctly reuse the previous session by sending the session ticket in the ClientHello. The evaluator shall confirm that the TOE responds with an abbreviated handshake described in section 3.1 of RFC 5077 and illustrated with an example in figure 2. Of particular note: if the server successfully verifies the client's ticket, then it may renew the ticket by including a NewSessionTicket handshake message after the ServerHello in the abbreviated handshake (which is shown in figure 2). This is not required, however as further clarified in section 3.3 of RFC 5077. **TD0556 has been applied.**
Pass/Fail with Explanation	NA, as the TOE does not support session tickets according to RFC5077.

6.90 FCS_TLSS_EXT.1.4 Test #3b (TD0569)

Item	Data
Test Assurance Activity	If the **TOE supports session tickets according to RFC5077**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator will then modify the session ticket and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.
Pass/Fail with Explanation	NA, as the TOE does not support session tickets according to RFC5077.

6.91 FPT_TST_EXT.1 Test #1

Item	Data
Test Assurance Activity	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. 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.
Test Steps	• Reboot the TOE. • Observe self-tests are completed. • Verify logs on the TOE.
Expected Test Results	• The TOE should execute all claimed self-tests during bootup. • Evidence (screenshot or CLI output) showing successful self-tests. • Log showing the execution of self-tests.
Pass/Fail with Explanation	Pass. The TOE successfully executes self-test. This meets the testing requirement.

6.92 FPT_TUD_EXT.1 Test #1

Item	Data
Test Assurance Activity	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.
Test Steps	• Show current version. • Upload new software package. • Check upload status. • Install new version. • Show new version.
Expected Test Results	• The TOE should successfully update the current version with the new version after verifying that the integrity of the new image. • Screenshot evidence of the TOE successfully updated with the new version.
Pass/Fail with Explanation	Pass. The TOE can be successfully updated. This meets the testing requirements.

6.93 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
Test Steps	• Using a Hex editor modify an otherwise good firmware image. • Copy the corrupt image on the TOE. • Attempt to install this update. This will fail. • Verify software upgrade failed logs generated on TOE.
Expected Test Results	• The TOE should detect and reject the modified image for a software update. • Software upgrade failed logs generated on TOE.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image was corrupted and rejected the image. This meets the testing requirements.

6.94 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
Test Steps	• Show the current version. • Upload an update that has not been signed. • Attempt to install the update. This will fail. • Verify software upgrade failed logs generated on TOE.
Expected Test Results	• The TOE should detect and reject the image without signature for software update. • Software upgrade failed logs generated on TOE.
Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image was not signed and rejected the image. This meets the testing requirements.

6.95 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)
Test Steps	• Show the current version. • Upload an image with an invalid signature. • Attempt to install this image. This will fail. • Verify software upgrade failed logs generated on TOE.
Expected Test Results	• The TOE should detect and reject the image with an invalid signature for a software update. • Software upgrade failed logs generated on TOE.

Pass/Fail with Explanation	Pass. The TOE software was able to detect when an image had an invalid signature and rejected the image. This meets the testing requirements.

6.96 FPT_TUD_EXT.1 Test #2 (d)

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: 4) If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Pass/Fail with Explanation	NA, the TOE does not allow delayed activation of updates.

6.97 FPT_TUD_EXT.1 Test #3 (a)

Item	Data
Test Assurance Activity	[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.

Pass/Fail with Explanation	NA, as the TOE itself does not verify a hash value over an image against a published hash value that has been imported to the TOE from outside.

6.98 FPT_TUD_EXT.1 Test #3 (b)

Item	Data
Test Assurance Activity	[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.
Pass/Fail with Explanation	NA, as the TOE itself does not verify a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside

6.99 FPT_TUD_EXT.1 Test #3 (c)

Item	Data
Test Assurance Activity	[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 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.
Pass/Fail with Explanation	NA, as the TOE itself does not verify a hash value over an image against a published hash value (i.e. reference value) that has been imported to the TOE from outside.

6.100 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data
Test Assurance Activity	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).
Test Steps	• Configure TOE to connect to the TLS server. • Create a full chain of certificates to connect to the TOE. • Upload the CA and ICA certificate to the TOE. • Attempt the connection from the TOE to the TLS server and verify the connection (complete certificate chain present). • Verify TOE logs for successful connection. • Verify the successful connection with packet capture.
Expected Test Results	• When a complete certificate chain is present, the TOE should establish a successful TLS connection. • Screenshot evidence of the packet capture showing successful TLS connection.
Pass/Fail with Explanation	Pass. The TOE can make a successful connection when a complete certificate trust chain is present. This meets the test requirements.

6.101 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test Assurance Activity	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.
Test Steps	• Remove the ICA from chain on the TOE. • Attempt the connection to the TOE using openssl. • Verify the failure logs on the device, showing untrusted certificate is used. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• The TOE rejects the connection when an incomplete certificate trust chain is present. • Screenshot evidence of the packet capture showing unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The TOE rejects the connection when an incomplete certificate trust chain is present. This meets the test requirements.

6.102 FIA_X509_EXT.1.1/Rev Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps	• Create a server certificate which is expired. • Show clock on the TOE. • Attempt to connect to the TOE with a server certificate with an incomplete chain and verify that it fails. • Verify the failure logs on the device, showing connection is not established due expired certificate. • Verify the connection is unsuccessful via packet capture.
Expected Test Results	• The TOE should deny connection when the certificate is expired. • Screenshot evidence of the packet capture showing unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. A connection including an expired certificate was rejected. This meets the test requirements.

6.103 FIA_X509_EXT.1.1/Rev Test #3

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. 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.
Test Steps	1. Valid Certificate: • Using the XCA tool to generate a 3-length certificate chain and CRL. • Load the root CA on the TOE. • Configure the TOE for CRL checking. • Configure the TOE for the Syslog server. • Start the Syslog server using Server and ICA certificates using OpenSSL.

	• Verify on the CRL server that the TOE tries to fetch the CRL's. • Verify the successful connection logs on the TOE. • Verify the successful connection with packet capture. 2. Invalid End Entity Certificate: • Using the XCA tool to generate a 3-length certificate chain and CRL. • Load the root CA on the TOE. • Configure the TOE for CRL checking. • Revoke the End Entity certificate. • Start the Syslog server using Server and ICA certificates using OpenSSL. • Verify on the CRL server that the TOE tries to fetch the CRL's. • Verify the failure logs on the TOE. • Verify the unsuccessful connection with packet capture. 3. Invalid Intermediate CA Certificate: • Using the XCA tool to generate a 3-length certificate chain and CRL. • Revoke the ICA certificate. • Load the root CA and ICA on the TOE. • Verify the failure logs on the TOE. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• The TOE should deny connection when the certificate is revoked. • Packet capture showing successful TLS connection when used valid certificates and unsuccessful TLS connection when used revoked certificates. • Logs showing successful TLS connection when used valid certificates and unsuccessful TLS connection when used revoked certificates.
Pass/Fail with Explanation	Pass. Connection with revoked certificates is not accepted by the TOE. This meets the testing requirement.

6.104 FIA_X509_EXT.1.1/Rev Test #4

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.
Test Steps	• The evaluator used the XCA tool to create a 3-length chain certificates where the intermediate certificate ICA-root-CRL5 does not have the CRLsign key usage bit set. • Load this certificate chain onto the TOE. • Attempt connection to TOE using openssl. • Verify on the CRL server that the TOE tries to fetch the CRL's. • Verify via logs that connection is failed. • Verify the unsuccessful TLS connection with the help of packet capture.

Expected Test Results	• The validation of the CRL should fail and the TOE should deny the TLS connection when CRLsign key usage bit is not set in any of the CA certificates. • Screenshot evidence of the packet capture showing unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The TOE does not connect to the TLS server if the cRLsign key usage bit set is not set in CA certificate. This meets the testing requirement.

6.105 FIA_X509_EXT.1.1/Rev Test #5

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps	• Run the acumen-tlsc-v2.2e tool with modified byte within the first 8 bytes of the certificate, the connection should fail. • Verify the error with logs on the TOE showing failure due to wrong tag. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• TOE rejects connections when the first 8 bytes of the certificate are modified. • Screenshot evidence of the packet capture showing unsuccessful TLS connection. • Logs showing unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the test requirements.

6.106 FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• Run the acumen-tlsc-v2.2e tool with modified byte in the signatureValue field of the cert. • Verify the error with logs on the device showing certificate verification failed. • Verify the unsuccessful connection with packet capture.
Expected Test Results	• TOE rejects connections when the last byte of the certificate is modified. • Screenshot evidence of the packet capture showing unsuccessful TLS connection.

Pass/Fail with Explanation	Pass. The TOE rejects connections when any byte in the certificate signatureValue field of the certificate is modified. This meets the test requirements.

6.107 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. 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.)
Test Steps	• Run the acumen-tlsc-v2.2e tool with modified public key in the certificate. • Verify the error with logs on the device failure due to invalid public key**.** • Verify the unsuccessful connection with packet capture.
Expected Test Results	• The TOE rejects connections when the public key of the certificate is modified. • Screenshot evidence of the packet capture showing unsuccessful TLS connection. • Failure logs on the TOE due to invalid public key.
Pass/Fail with Explanation	Pass. The TOE rejects connections when any byte in the public key of the certificate is modified. This meets the test requirements.

6.108 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.**
Test Steps	• Configure the EC root CA certificate. • Configure the EC intermediate CA certificate. • Configure the EC node certificate. • Configure the TOE for the root certificate as a trust anchor. • Concatenate the CA certificates. • Attempt the connection from the TOE to the TLS server. • Verify the successful connection via TOE logs. • Verify the successful connection with packet capture.
Expected Test Results	• Connection using a trusted chain of the EC leaf certificate, EC intermediate certificate, and EC root certificate should be successful.

	• Screenshot evidence of the packet capture showing successful TLS connection.
Pass/Fail with Explanation	Pass. The evaluator verified the trusted chain of the EC leaf certificate, EC intermediate certificate and EC root certificate and observed that the connection was successful. This meets the test requirements.

6.109 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.**
Test Steps	• In the Second part of the test Intermediate certificate is modified with a named curve with an explicit format in the public key information field and is loaded on the TLS server. • Concatenate the CA certificates. • Configure the TOE for the root certificate as a trust anchor. • Attempt the connection from the TOE to the TLS Server. • Verify the failure logs on the device. • Verify the unsuccessful connection via packet capture.
Expected Test Results	• When the ICA uses an explicit format version of the Elliptic Curve parameters in the public key information field on the TLS server, TOE is unable to make a successful connection. • Screenshot evidence of the packet capture showing unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The evaluator verified that when the uses an explicit format version of the Elliptic Curve parameters in the public key information field on the TLS server, TOE is unable to make the successful connection. This meets the test requirements.

6.110 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.**

Test Steps	• In the Third part of the test Intermediate certificate is modified with a named curve with an explicit format in the public key information field and is loaded on the TOE. • Attempt to add the modified Intermediate certificate on the TOE. • Verify that the TOE discards the certificate. • Verify the failure logs on the device.
Expected Test Results	• When the ICA uses an explicit format version of the Elliptic Curve parameters in the public key information field on the TLS server and is loaded to the TOE's trust store, TOE does not accept such a certificate. • Failure logs on the TOE showing it discards the certificate.
Pass/Fail with Explanation	Pass. The evaluator verified that when the ICA uses an explicit format version of the Elliptic Curve parameters in the public key information field on the TLS server and is loaded to the TOE's trust store, TOE does not accept such certificate. This meets the testing requirements.

6.111 FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test Assurance Activity	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).*
Test Steps	• Create an ICA with no basicConstraint. • Upload ICA to TOE. • Verify that the TOE discards the certificate. • Verify the failure logs on the device.
Expected Test Results	• The TOE should reject certificates signed by CA that does not contain the BasicConstraints Extension.

	• Failure logs on the TOE showing it discards the certificate.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that do not contain the basicConstraints extension. This meets the test requirements.

6.112 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test Assurance Activity	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). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: i. As part of the validation of the leaf certificate belonging to this chain; ii. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).
Test Steps	• Configure the CA certificate with the flag in the basicConstraints extension set to FALSE using x509-mod tool. • Attempt to load the cert onto the TOE. • Verify that the TOE discards the certificate. • Verify the failure logs on the device.
Expected Test Results	• The TOE should reject certificates signed by CA that has CA flag set to FALSE. • Failure logs on the TOE showing it discards the certificate.
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that has the CA flag in the basicConstraints extension set to FALSE. This meets the test requirements.

6.113 FIA_X509_EXT.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity.

	The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps	• Configure Root and ICA trust points with CRL checking required. • Shutoff the CRL server. • Attempt to connect to the TOE with OpenSSL. TOE cannot verify the validity of the peer certificate and that the connection proceeds. • Check logs for CRL checking failure and successful connection logs. • Verify the successful connection with packet capture.
Expected Test Results	• The TOE should accept the certificate when validation checking of the certificate is not available. • Screenshot evidence of the packet capture showing successful TLS connection. • Logs generated on the TOE for CRL checking failure and successful TLS connection.
Pass/Fail with Explanation	Pass. The TOE accepts the connection despite loss of CRL server availability. This meets the testing requirements.

6.114 FIA_X509_EXT.3 Test #1

Item	Data
Test Assurance Activity	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.
Test Steps	• On the TOE, generate a CSR. • Examine the CSR contents on Openssl server.
Expected Test Results	• The TOE should generate CSR containing the required fields selected in the SFR. • Screenshot evidence of the Openssl output showing CSR contents.
Pass/Fail with Explanation	Pass. The TOE can generate a CSR with all the requisite information. This meets the testing requirements.

6.115 FIA_X509_EXT.3 Test #2

Item	Data
Test Assurance Activity	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.
Test 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. • Add the intermediate certificate to the TOE certificate store to ensure that the TOE has a full certificate path. • Verify from the logs that the intermediate certificate is installed. • Verify that the TOE installs a CSR response with a full trust path. • Verify that the certificate is installed via logs.
Expected Test Results	• The TOE should not validate a signed CSR if the full trust chain is not present. When a full trust chain is present, the TOE should validate the signed CSR. • TOE should generate logs for certificate installation.
Pass/Fail with Explanation	Pass. The TOE does not install CSR responses signed by a CA without a full trust path. The TOE installs a CSR response signed by a CA with a full trust path. This meets the testing requirements.

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 (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all 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 (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. 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. 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 (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. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD 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 www.niap-ccevs.org. 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: • Virtual appliance hardware Platform (ISA-V) • ISA appliances - ISA-6000, ISA-8000C, ISA-8000F 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 entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled **Operational Environment** specifies features that are not assessed and tested by the EAs. The evaluator ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.

	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 makes 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 sections titled **Operational Environment** of the AGD. The evaluator found that these sections describe how the Operational Environment must meet: • Management laptop with web browser • Syslog server • CRL Server

	• DNS Server 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 and the section titled **Operational Environment** of AGD identifies the following supported platform: **Table 8 – Component Usage** Component / Usage/Purpose Description Management laptop / Provides local console access to the TOE Workstation providing a browser to connected to the Web User Interface (WUI) over TLSv1.2 or TLSv1.1 Syslog server / The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE CRL Server / Verify client certificates DNS Server / The DNS Server is used for resolving hostnames 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 GUI and Console Connections • Configuring the Remote Syslog Server • Configuring Audit Log Options • Configuring a Secure Logging Channel • Configuring time and date • Generating CSR

	• Configuring certificates • Configuring Idle session 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 **Password Minimum Length Configuration** and **Reset Password** were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account. 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. • https://nvd.nist.gov/view/vuln.search • https://www.ivanti.com/ • https://docs.vmware.com/en/VMware-vSphere/6.7/rn/esxi670-202011002.html • https://forums.ivanti.com/s/article/SA45520?language=en_US The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on October 06, 2023. • Ivanti • Ivanti Policy Secure • Ivanti Policy Secure 22.2R3 • ISA 6000 • ISA 8000C • ISA 8000F • ISA-V • Intel(R) Xeon(R) Gold 6252 CPU • Dell PowerEdge R640 • IVE OS 3.0 • VMware ESXi 6.7 • Intel Core i3 10100E 10th gen • Intel Xeon Gold 5317 • Ivanti Secure Cryptographic Module • TLS 1.2 • TCP 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 CAVP Mapping

This section provides a table that lists all SFRs for which a CAVP certificate is claimed, the CAVP algorithm list name and the CAVP Certificate number.

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	Ivanti Secure Cryptographic Module v1.0	RSA KeyGen (FIPS186-4)	#A3010
	ECC schemes using "NIST curves" [P-256, P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	Ivanti Secure Cryptographic Module v1.0	ECDSA KeyGen (FIPS186-4)	#A3010
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"	Ivanti Secure Cryptographic Module v1.0	NA	No NIST CAVP, CCTL performed all assurance/evaluation activities as defined by the NDcPP v2.2E SD for this SFR.
	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	Ivanti Secure Cryptographic Module v1.0	KAS-ECC-SSC Sp800-56Ar3	#A3010
FCS_COP.1/ DataEncryption	The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [CBC, GCM] mode and cryptographic key sizes [128 bits, 256 bits] that meet the following: AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772].	Ivanti Secure Cryptographic Module v1.0	AES-CBC/ AES-GCM	#A3010

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Ivanti Secure Cryptographic Module v1.0	RSA SigGen (FIPS186-4)/ RSA SigVer (FIPS186-4)	#A3010
	For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [**P-256, P-384**]; ISO/IEC 14888-3, Section 6.4	Ivanti Secure Cryptographic Module v1.0	ECDSA SigGen (FIPS186-4)/ ECDSA SigVer (FIPS186-4)	#A3010
FCS_COP.1/ Hash	The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: ISO/IEC 10118-3:2004	Ivanti Secure Cryptographic Module v1.0	SHA-1, SHA-256, SHA-384, SHA-512	#A3010
FCS_COP.1/ KeyedHash	The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [160 bits, 256 bits, 384 bits used in HMAC] and message digest sizes [160, 256, 384] bits that meet the following: ISO/IEC 9797- 2:2011, Section 7 “MAC Algorithm 2”.	Ivanti Secure Cryptographic Module v1.0	HMAC-SHA-1, HMAC-SHA2-256, HMACSHA-384	#A3010
FCS_RBG_EXT.1	The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].	Ivanti Secure Cryptographic Module v1.0	Counter DRBG	#A3010

9 Conclusion

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

End of Document