Assurance Activity Report for

HYCU for Enterprise Clouds

HYCU for Enterprise Clouds Security Target
Version 0.2.9

collaborative Protection Profile for Network Devices
Version 2.2e

AAR Version 0.9, January 2024

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:

HYCU for Enterprise Clouds

The Author of the Security Target:
Acumen Security, LLC.

The TOE Evaluation was Sponsored by:
HYCU for Enterprise Clouds

Evaluation Personnel:
Furukh Siddique
Shaunak Shah
Alexander Fannin
Shaina Rae

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	AUTHOR	CHANGES
0.1	05/08/2023	A. Fannin	Initial draft, testing
0.2	8/14/2023	S. Rae	First draft TSS, comments released
0.3	9/18/2023	S. Rae	First iteration of Guidance
0.4	9/25/2023	S. Rae	Final Iteration Guidance and TSS addressed updates, SARS draft
0.5	10/3/2023	F. Siddique	Add Test Activities
0.6	10/04/2023	S. Rae	QA updates
0.7	10/24/2023	S. Rae	ECR updates
0.8	12/06/2023	S. Rae	ECR updates
0.9	1/10/2024	S. Rae	ECR updates

Contents

1 TOE Overview

The TOE is the HYCU, Inc. HYCU for Enterprise Clouds. HYCU for Enterprise Clouds provides application-consistent and virtualization-native data protection, data migration and disaster recovery. HYCU for Enterprise Clouds allows administrators to protect and manage clusters of a virtualized infrastructure with one integrated interface.

HYCU for Enterprise Clouds is a software-based TOE that is installed as a virtual machine. The deployed virtual machine is accessed via a web GUI.

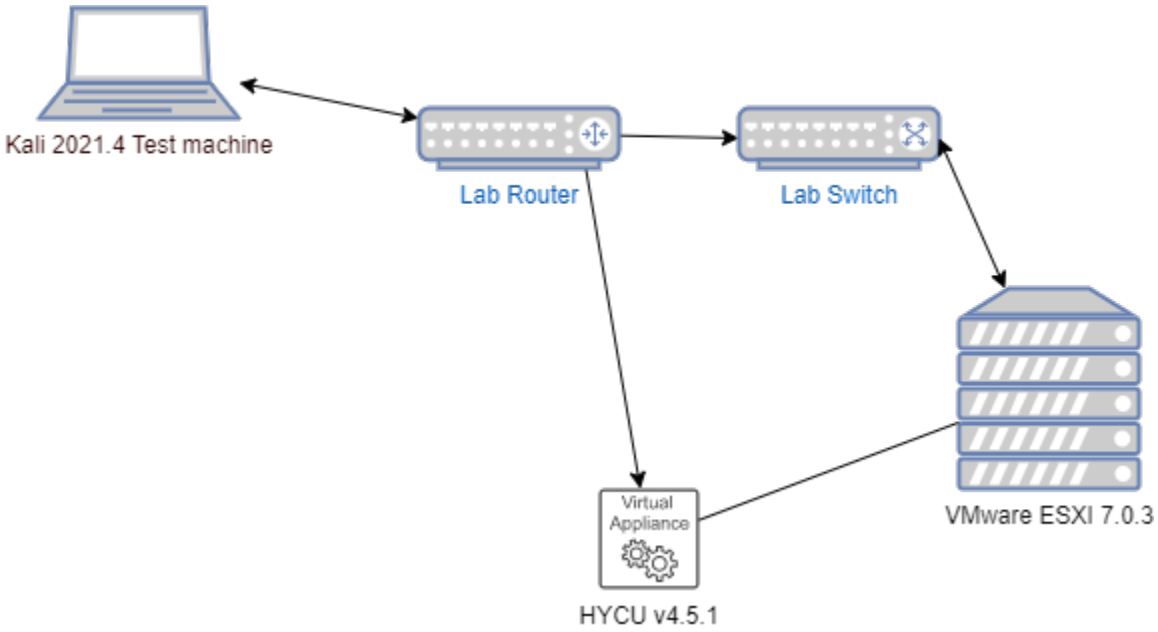
2 Assurance Activities Identification

The TOE assurance requirements are taken directly from the Collaborative Protection Profile for Network Devices v 2.2e which are derived from Common Criteria Version 3.1, Revision 5, April 2017 (Conformant).

3 Test Equivalency Justification

There are no equivalency claims for this evaluation as only a single device utilized by the TOE.

4 Test Bed Descriptions



Name	OS	Version	Credentials	Function	Protocols	IP Address	MAC Address	Time	Tools
Testing Laptop	Windows	10	NA	Testing Laptop	HTTP, HTTPS, TLS	192.x.x.x	DC:41:A9:48:12:2D	Manual	Mobaxterm, Wireshark
Testing VM	Kali	2021.4	Login / password	Testing machine	HTTP, HTTPS, TLS	10.x.x.x	00:50:56:8b:c4:10	Manual	openSSH client, openSSH server wireshark

Name	OS	Version	Credentials	Function	Protocols	IP Address	MAC Address	Time	Tools
Virtual server	VMware ESXi	7.0.3	Login / password	TOE		10.x.x.x	38:68:dd:5c:3a:a8	Manual	
HYCU virtual appliance	HYCU	v4.5.1	Login / password	TOE	HTTP, HTTPS, TLS	10.x.x.x	00:0c:29:f5:d7:23	Manual	
Syslog server	Testing tool	V1.0	NA	Audit log server	Syslog	10.x.x.x	00:50:56:8b:c4:10	NA	Acumen testing tool
Router	NA		NA	Router	NA			NA	NA
Switch	NA		NA	Switch	NA			NA	NA

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 section 6 **'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: The evaluator has found that that TOE generates audit records when specific events occur. The comprehensive list of events that generate records are located in Table 9 of the ST and have been found to correspond with selections made for this requirement as well as the information provided in the TSS. The TSS states that each recorded event includes sufficient detail to identify the user associated with the event, when the event occurred, where the event occurred, the outcome of the event, and the type of event. The key name is identified for administrative tasks of generating, changing and deleting cryptographic keys. 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 16 **'Auditable Events'** 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 states that the TOE generates a comprehensive list of audit logs. Due to the size of the list these events can be reviewed in Table 1 of the AGD. The evaluator has reviewed the list and finds that the list to contains sufficient detail of auditable events and how the record is presented. 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

<table>
<tr><td></td><td>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.</td></tr>
<tr><td>Evaluator Findings</td><td>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>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Section</th></tr>
<tr><td>Admin the TOE locally and remotely</td><td>Web GUI for Remote and Command for Local</td><td>Section 2 and 3</td></tr>
<tr><td>Configure access banner</td><td>Command</td><td>Section 8</td></tr>
<tr><td>Configure session inactivity time before session termination or locking</td><td>Command</td><td>Section 19</td></tr>
<tr><td>Update the TOE, verify update</td><td>Web GUI</td><td>Section 20</td></tr>
<tr><td>Configure authentication failure parameters</td><td>Command</td><td>Section 22</td></tr>
<tr><td>Start and stop services</td><td>• Start Services: Web Gui and Command
• Stop Services: Command</td><td>• Section 2and 3 (Start)
• Section 12 (Stop)</td></tr>
<tr><td>Modify transmission of audit data to external entity</td><td>Web GUI</td><td>Section 13</td></tr>
<tr><td>Manage cryptographic keys</td><td>Command</td><td>Section 5 and 6</td></tr>
<tr><td>Configure cryptographic functionality</td><td>Command</td><td>Section 5 and 6</td></tr>
</table></td></tr>
</table>

	Set time for time-stamps	Command	Section 9
	Manage trust store and designate x509 certificates as trust anchors	Command	Section 10
	Ability to import X509 certificates to trust store	Command	Section 21
	Based on these findings, this assurance activity is considered satisfied.		
Verdict	Pass		

5.1.2 FAU_STG_EXT.1

5.1.2.1 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 6 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 audit events are stored locally and are also sent to an external audit server as they are created. TLS is used to provide a trusted communication channel with the audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.2 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 6 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 data is stored locally in a database which also contains other system information, consequently there is no set limit on the local audit log storage. An administrator can configure the database to purge events older than a specified date. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.3 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 6 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 which is not distributed. Audit data is stored locally and is also sent to an external audit server as records are created. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.4 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 6 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 data is stored locally in a database which also contains other system information, consequently there is no set limit on the local audit log storage. An administrator can configure the database to purge events older than a specified date. The option 'overwrite previous audit record' is not selected for. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.5 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 6 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 audit events are stored locally and are also sent to an external audit server as they are created. TLS provides a trusted communication to the audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.6 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 13 titled **'Configuring the sending of audit records to an external server'** 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 administrator can reference the HYCU User Guide, Chapter 9, **'Performing Daily Tasks'** section **'Setting up webhook notifications'** for additional information. The evaluator has reviewed the pointer information and has confirmed that trusted channels are established via webhook API and that the instructions for setting up webhooks are present in Chapter 9 'Setting up webhook notifications'. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.7 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 15 titled **'System Behavior for Audit Logs'** 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 audit events are stored locally and are also sent to an external audit server as they are created. TLS is used to provide a trusted communication channel with the audit server. Only a security administrator is allowed the ability to determine the behavior of transmitting audit data to a syslog server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.8 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 11 titled **'Using a TLS Server (Syslog, AD, SMTP),** section 12 **'Prerequisites',** section 13 **'Configuring the sending of audit records to an external syslog server'** and section 15 **'System Behavior for Audit Logs'** 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 provides the information on how to configure the handling of audit logs as well as the behavior of audit logs related to TOE functionality. Local audit logs can be set up by the admin via a TLS connection to transmit data to an external server. The admin is able to disable audit log sending by clearing notification configuration if they choose. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (Communication)

There are no requirements for this category as part of the evaluation.

5.3 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.

5.3.1 FCS_CKM.1

5.3.1.1 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that the TOE supports RSA and ECC cryptographic key generation schemes which include RSA 2048-bit and ECC P-256, ECC P-384, ECC P-521s. These are detailed in FCS_CKM.1. RSA and ECC are used for TLSC and TLSS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 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 5 titled **'Enabling the CC-compliant mode'** and section 6 **'Cryptographic Requirements Enforced by the TOE in CC-mode'** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD states that there is no provisioning supported other than enabling CC-mode. Enabling CC-mode has predetermined settings for the cryptographic protocols. These include RSA key sizes of 2048, 3072 and 4096.

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

5.3.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # **A2933**

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	HYCU Java Cryptographic Library	RSA	#A2933
	ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	HYCU Java Cryptographic Library	ECDSA	#A2933

Detailed testing information can be referenced in section 6.2.1 of this document.

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

Verdict	Pass

5.3.2 FCS_CKM.2

5.3.2.1 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 section 6 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 TOE supports RSA and ECC key establishment scheme. These schemes correspond to selections made for key generation for FCS_CKM.1. Both RSA and ECC are used for TLSC AND TLSS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.2 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 5 titled **'Enabling the CC-compliant mode'** and section 6 **'Cryptographic Requirements Enforced by the TOE in CC-mode'** 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 provides information confirming that by enabling CC-mode devices are restricted to follow only pre-determined cryptographic protocols and algorithms. The RSA and ECC key establishment schemes are listed in section 6 and are synonymous with selections made for FCS_CKM.2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: # **A2933** **SFR** / **Algorithm in ST** / **Implementation name** / **CAVP Alg.** / **CAVP Cert #** FCS_CKM.2 / 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" / HYCU Java Cryptographic Library / None: CCTL tested as per the PP/SD Evaluation Activities / Lab Evaluated FCS_CKM.2 / Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography / HYCU Java Cryptographic Library / KAS-ECC-SSC / #A2933 Detailed testing information can be referenced in section 6.2.2 (RSA) and 6.2.3 (ECC) of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3 FCS_CKM.4

5.3.3.1 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS states that the TOE stores plaintext keys in volatile and non-volatile storage. Plaintext keys include private keys for TLS which are used by the HTTPS server to serve remote admin API and user interface; X.509 certificates for TLS; and password authentication to the TOE and external systems. A simplified chart of the key storage can be referenced in the ST under Table 14 'Key Storage and Zeroization' and a detailed response is outfitted below. Table 14 contained equivalent content which is further expanded upon in the TSS and is shared below: Private key is stored in non-volatile storage: • Authoritative copy is stored in a PostgreSQL database internal to the TOE (database 'cfgdb', table 'certificate'), in an encrypted form using PBKDF2 is used to derive a key, which is then encrypted using AES-CBC before stored in the database. Certificate table is stored as pages on the disk under /hycudata/opt/grizzly/data. Key destruction is handled by DELETE SQL statement. On-disk data is garbage-collected and legible for overwrite after autovacuum daemon executes the VACUUM SQL statement. • Private key is also stored on the filesystem (in /etc/pki/tls/private/hycussl-*) for use by the HTTP/S server component. Key is rendered into the file on every Java service startup. Since the TOE mandates use of HTTP/S, the private key is always present and is only deleted when switching to a different key. If multiple listeners are configured (e.g. multiple network interfaces), each listener may be configured with a separate private key. On-disk key deletion is done using `rm` system command. Private key is also stored in volatile storage: • HTTPS server loads the private key into volatile storage to accept TLS connections. Private key remains loaded in volatile storage for the duration of the mod_ssl module lifetime. When module lifetime ends (on HTTP server shutdown or reload), volatile storage is freed using standard free() call. Underlying OS ensures pages are zeroized before next use. • Java application loads the private keys into volatile storage when registering new keys into memory, and when rendering keys on the filesystem. After use, references are released, and memory reclaimed by garbage collection. On service shutdown, pages used by the java application are freed by the OS, which ensures pages are zeroized before next use. Certificates are stored in non-volatile storage:

	• Authoritative copy is stored in a PostgreSQL database internal to the TOE (database 'cfgdb', table 'certificate'), in plaintext form, since the data is public. Key destruction is handled by DELETE SQL statement. On-disk data is garbage-collected and legible for overwrite after autovacuum daemon executes the VACUUM SQL statement. • Server certificate is also stored on the filesystem (in /etc/pki/tls/certs/hycussl-*) for use by the HTTP/S server component. Certificate is rendered into the file on every Java service startup. Since the TOE mandates use of HTTP/S, the certificate is always present and is only deleted when switching to a different key. If multiple listeners are configured (e.g. multiple network interfaces), each listener may be configured with a separate private key. On-disk certificate deletion is done using `rm` system command. Certificates are also stored in volatile storage: • HTTPS server loads the certificate into volatile storage to accept TLS connections. Certificate remains loaded in volatile storage for the duration of the mod_ssl module lifetime. When module lifetime ends (on HTTP server shutdown or reload), volatile storage is freed using standard free() call. Underlying OS ensures pages are zeroized before next use. • Java application loads the certificate from database into volatile storage on startup, or when registering new or removing old certificates. These certificates are used by the TLS client to establish trusted roots during handshake. Certificates are loaded into memory in BouncyCastle's BCFKS FIPS-validated trust store. When certificates change, in-memory keystore is rebuilt, and references to old keystore are released, and memory reclaimed by automatic garbage collection. On service shutdown, pages used by the java application are freed by the OS, which ensures pages are zeroized before next use. Passwords are stored in non-volatile storage: • Authoritative copy of SMTP and Webhook password is stored in a database internal to the TOE (SMTP: database 'cfgdb', table 'smtp'; Webhook: database `grizzly`, table 'webhook`), in an encrypted form using PBKDF2 is used to derive a key, which is then encrypted using AES-CBC before being stored in the database. • Passwords are stored in volatile storage: • Passwords for Active Directory authentication (LDAP bind) are loaded from non-volatile on-demand (e.g. during login). After use, references are released, and memory reclaimed by garbage collection. Password for SMTP (if set) is loaded from non-volatile storage on service startup or SMTP configuration change and remains loaded for the duration of the service (or until SMTP configuration change). On SMTP configuration change, references are released, and memory reclaimed by garbage collection. On service shutdown, pages used by the java application are freed by the OS, which ensures pages are zeroized before next use. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.2 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 section 6 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 provides detailed information on the destruction of individual keys in non-volatile memory. After reviewing the TSS content the evaluator came to the conclusion that private keys in non-volatile storage stored in PostgreSQL databases are deleted through being handled by DELETE SQL statement. On-disk data is garbage-collected and legible for overwrite after autovacuum daemon executes the VACUUM SQL statement. In the case the private key is also stored on the filesystem then on-disk key deletion is done using 'rm' system command. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.3 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 section 6 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 there are no keys stored in non-plaintext. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.4 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 section 6 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 provides a comprehensive explanation of the varying methods of key destructions. This can be more simply reviewed in Table 14 of the ST. The evaluator has reviewed the methods of key destruction against selections made and had determine that there are no instances of non-conformance to the key destruction requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.5 FCS_CKM.4 TSS 5

Objective	Where the ST specifies the use of "a value that does not contain any CSP" to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
Evaluator Findings	The evaluator examined section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. Upon investigation, the evaluator found that the TSS does not make any claims of using CSP to overwrite keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.6 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 10 titled **'Configuring SSL certificates'** 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 found that the AGD states that public keys, private keys and passwords are stored in the PostgreSQL database and are deleted using DELETE SQL statement. On-disk data is garbage-collected and legible for overwrite after autovacuum daemon executes the VACUUM SQL statement if there is a delay or prevention on key destruction. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4 FCS_COP.1/DataEncryption

5.3.4.1 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 section 6 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 supports AES encryption and decryption conforming to CBC and GCM as specified in ISO 18033-3, ISO 10116, and ISO 19772. The AES key size supported is 128 and 256 bits. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.2 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 5 titled **'Enabling the CC-compliant** mode' and section 6 titled **'Cryptographic Requirements Enforced by the TOE in CC-mode'** 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 setting the TOE into CC-Compliant mode restricts the device to the following cryptographic protocols and algorithms. The generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start. Section 6 of the AGD confirms the pre-determined modes and key sizes used by the TOE when CC-mode is enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: # **A2933** **SFR** | **Algorithm in ST** | **Implementation name** | **CAVP Alg.** | **CAVP Cert #** FCS_COP.1/ DataEncryption | AES used in [CBC, GCM] mode and cryptographic key sizes [128 bits, 256 bits] | HYCU Java Cryptographic Library | AES | #A2933 Detailed testing information can be referenced in section 6.2.4 of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.5 FCS_COP.1/SigGen

5.3.5.1 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 section 6 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 uses RSA (2048, 3072 and 4096 bits) and ECDSA (256, 384 and 521 bits) for cryptographic signature generation. This corresponds with selections made in the SFR for this activity. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3.5.2 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 5 titled **'Enabling the CC-compliant mode'** 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 that setting the TOE into CC-Compliant mode restricts the device to the following cryptographic protocols and algorithms. The generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start. Section 6 of the AGD confirms the pre-determined cryptographic algorithms and key sizes used by the TOE when CC-mode is enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.5.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP RSA SigGen&SigVer (186-4) Certs: # **A2933** CAVP ECDSA&SigVer SigGen (186-4) Certs: # **A2933**

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	HYCU Java Cryptographic Library	RSA	#A2933
	For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4	HYCU Java Cryptographic Library	ECDSA	#A2933

Detailed testing information can be referenced in section 6.2.5 of this document.

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

5.3.6 FCS_COP.1/Hash

5.3.6.1 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 6 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 supports cryptographic hashing using TLS and HTTPS with SHA-1, SHA-256, or SHA-384 and message digest sizes of 160, 256, or 384. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.6.2 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 5 titled **'Enabling the CC-compliant mode'** 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 setting the TOE into CC-Compliant mode restricts the device to the following cryptographic protocols and algorithms. The generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start. Section 6 of the AGD confirms the pre-determined hash sizes used by the TOE when CC-mode is enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.6.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHS Certs: # **A2933** **SFR** | **Algorithm in ST** | **Implementation name** | **CAVP Alg.** | **CAVP Cert #** FCS_COP.1/ Hash | [SHA-1, SHA-256, SHA-384] and message digest sizes [160, 256, 384] bits | HYCU Java Cryptographic Library | SHS | #A2933 Detailed testing information can be referenced in section 6.2.6 of this document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.7 FCS_COP.1/KeyedHash

5.3.7.1 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 section 6 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 uses keyed-hash message authentication supporting TLS and HTTPS. TLS and HTTPS use HMAC-SHA-1, HMAC-SHA-256, or HMAC-SHA-384 with cryptographic key sizes of 160, 256, or 384 bits, message digest sizes of 160, 256, or 384 bits. The block size for HMAC-SHA-1 is 64 bytes. For HMAC-SHA-256 and HMAC-SHA-384 the block size is 128 bytes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.7.2 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 5 titled **'Enabling the CC-complaint mode'** and section 6 titled **'Cryptographic Requirements Enforced by the TOE in CC-mode'** 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 setting the TOE into CC-Compliant mode restricts the device to the following cryptographic protocols and algorithms. The generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start. Section 6 of the AGD confirms the pre-determined values used by HMAC functions which are used by the TOE when CC-mode is enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.7.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	CAVP HMAC Certs: # **A2933** **SFR** / **Algorithm in ST** / **Implementation name** / **CAVP Alg.** / **CAVP Cert #** FCS_COP.1/ KeyedHash / [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [160, 256, and 384 bits] and / HYCU Java Cryptographic Library / HMAC / #A2933

		message digest sizes [160, 256, 384] bits			

Detailed testing information can be referenced in section 6.2.7 of this document.

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

Verdict	Pass

5.3.8 FCS_RBG_EXT.1

5.3.8.1 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 section 6 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 following DRBG types are supported: • HYCU Java cryptographic library supports Hash, HMAC and CTR DRBG (AES). • HYCU Native cryptographic library supports CTR DRBG (AES) The deterministic RBG is seeded by 2 entropy sources that accumulates entropy from add_interrupt_randomness() (i.e the interrupt noise source) and add_disk_randomness() (i.e. the disk noise sources). There is a minimum of 256 bits of entropy at least equal to the greatest security strength possible according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.8.2 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 5 titled **'Enabling the CC-complaint 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 RNG is configured automatically and appropriately initialized on TOE start. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.8.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.

<table>
<tr><td>Evaluator Findings</td><td>CAVP DRBG Certs: # A2933
<table>
<tr><th>SFR</th><th>Algorithm in ST</th><th>Implementation name</th><th>CAVP Alg.</th><th>CAVP Cert #</th></tr>
<tr><td>FCS_RBG_EXT.1</td><td>Hash_DRBG (any),
HMAC_DRBG (any),
CTR_DRBG (AES)</td><td>HYCU Java Cryptographic Library</td><td>Hash DRBG
HMAC DRBG
Counter DRBG</td><td>#A2933</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

5.4 TSS and Guidance Activities (HTTPS)

5.4.1 FCS_HTTPS_EXT.1

5.4.1.1 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 section 6 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 TOE supports remote management of the TOE over an HTTPS connection using TLS. The TOE acts as a server. This protocol is used to provide an administrator with access to the TOE. The HTTPS protocol complies with RFC 2818. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.2 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 13 titled **'Configuring the sending of audit records to an external server'** 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 HYCU uses HTTPS POST webhooks to send audit data over a secure channel. The detailed procedure for configuring the use of webhooks is present in the section noted above. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (TLSC)

5.5.1 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 all supported cipher suites are listed for the TOE. There are not additional components to note. These cipher suites are: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 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 5 titled **'Enabling the CC-complaint mode'** and section 6 titled **'Cryptographic Requirements Enforced by the TOE in CC-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 states that setting the TOE into CC-Compliant mode restricts the device to the following cryptographic protocols and algorithms. The generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start.

	Section 6 of the AGD confirms the pre-determined TLS ciphers used by the TOE when CC-mode is enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3 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. The evaluator shall ensure that this description identifies if certificate pinning is supported or used by the TOE and how it is implemented.
Evaluator Findings	The evaluator examined the section 6 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; and if certificate pinning is supported or used by the TOE and how it is implemented. Upon investigation, the evaluator found that the TSS states that the TSF ensures that the presented reference identifier conforms to RFC 6125 section 6 and if FQDN in SAN matches. The TSF will not establish a trusted channel if the server certificate is invalid and there is no provision for this to be overridden. Wildcards are supported by the TOE. Certificate pinning is not supported. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.4 FCS_TLSC_EXT.1.2 TSS 3 **[TD0481]**

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 (RFC5952 for IPv6, RFC 3986 for IPv4) is enforced.
Evaluator Findings	The evaluator examined the section 2.3.1 titled **'Technical Decisions'** 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 ST provides rationale in relation to TD0634 that the TOE does not support IP addresses in the SAN or CN. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5 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 14 titled **'TLS Server Requirements'** and section 12 **'Prerequisites'** 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 TOE uses CN or SAN of the certificate and that it must match the hostname that is configured. Detailed configuration can be referenced in the following sections: • In section 11 titled 'Using a TLS Server (Syslog, AD, and SMTP)' ○ Step 5 under "Use the following to configure an AD server" ○ Step 3 under "Use the following to configure an SMTP server" Section 12 provides instructions for setting up the TLS server and what the admin must have in order to enable appropriate communications to an external server with TLS. Bullet 5 of this section states that the reference identifier is configured in the POST URL in the webhook notifications field. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that the TSF presents the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups in the client hello: secp256r1, secp384r1, and secp521r1. These curves are supported by default and do not need to be configured by an administrator. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.7 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 5 titled **'Enabling the CC-complaint mode'** and section 6 titled **'Cryptographic Requirements Enforced by the TOE in CC-mode'** in the AGD to verify that, if the TSS indicates that the Supported Elliptic Curves Extension must be configured to meet the requirement, it includes configuration of the Supported Elliptic Curves Extension. Upon investigation, the evaluator found that the AGD states that the admin can enable CC-

	compliant mode which configures the supported Elliptic Curve Extensions. The full list of these is located in section 6 of the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance (TLSS)

5.6.1 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 section 6 titled **'TOE Summary Specification'** in the Security Target and has verified 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 the supported ciphersuites are the following: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2 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 5 titled **'Enabling the CC-compliant 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 states that the TLS server must be a server that supports TCP and TLS v1.2. When checked against the TSS TLS 1.2 is the only version of TSS supported by the TOE. As the TOE utilizes a CC-compliant mode for configuring cryptographic requirements, it is verified in section 5 titled **'Enabling the CC-compliant mode'** and section 6 titled **'Cryptographic Requirements Enforced by the TOE in CC-mode'** that the listed ciphersuites are part of this functionality and conforms to the TSS list. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 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 section 6 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 the use of TSL 1.2 is mandated by the TSF and connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 are denied. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 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 section 14 titled **'TLS Server Requirements'** 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 the TLS server must be a server that supports TCP and TLS v1.2. The presented reference identifier conforms to RFC 6125 section 6 where the CN or SAN of the certificate must match the hostname configured on the TOE. Section 11 titled 'Using a TLS Server (Syslog, AD, SMTP)' provides additional instruction on configuring the differing server types. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 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 section 6 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 key establishment is performed using RSA with key sizes of 2048 bits, 3072 bits, or 4096 bits and ECDHE curves secp256r1, secp384r1, or secp521r1. ECDHE and DHE ciphers utilize standard DH parameters: - RFC 2049, section 6.2 - RFC 3526, sections 3 to 7 Parameters are selected based on authentication strength (or key size for RSA keys) configured on the server. The evaluator has determined that this is related to enabling CC-compliant mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6 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 section 5 titled **'Enabling the CC-compliant mode'** and section 6 **'Cryptographic Requirements Enforced by the TOE CC-mode'** in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD provides the instructions for enabling CC-compliant mode and that this mode holds all pre-configured settings to be compliant with TLSS requirements. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7 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 section 6 titled **'TOE Summary Specification'** in the Security Target. Upon investigation, the evaluator found that the TSS states that session resumption based on session IDs is supported conforming to RFC4346 and RFC5346. Session resumption tickets adhere to the structural format described in Section 4 of RFC 5077. Session tickets are protected according to recommendations outlined in Section 4 of RFC 5077: • encrypted with AES CBC with 128-bit key, and • MAC calculated using HMAC-SHA-256 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.8 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 section 6 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

5.7 TSS and Guidance Activities (Identification and Authentication)

5.7.1 FIA_AFL.1

5.7.1.1 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 section 6 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 maximum number of failed attempts using the CLI interface. The configurable range is between 1-15 attempts with the default being 3 attempts. When a user account has sequentially failed authentication for the configured number of times, the account will be locked for the configured period of time or until a local administrator manually unlocks the account. All failed attempts and lockouts are tracked by the TOE audit log. Additionally, there is a single console/OS account ('hycu') which is meant only for specific operations, which could include recovery from any kind of application or system failure. This is the only restore option presented in the TSS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.2 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that the TOE will always allow a user to authenticate using the local console port, even if the user account is locked. This behavior is not configurable. There is a

	single console/OS account ('hycu') which is meant only for specific operations, which could include recovery from any kind of application or system failure. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.3 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 section 22 titled **'Configuring failed login count and lock duration'** 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 provides the text-based console commands for the admin to use to set the number of failed login attempts before lockout occurs and how long the lockout time is active. Reload must be manually accomplished for setting to take effect. The default lockout is for 3 attempts and the lockout time is for 15 minutes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.4 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 22 titled **'Configuring failed login count and lock duration'** in the AGD to verify that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that the AGD states that the TOE will always allow an administrator to authenticate using the local console port, even if the account is locked. This behavior is not configurable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FIA_PMG_EXT.1

5.7.2.1 FIA_PMG_EXT.1.1 TSS 1 [TD0792]

Objective	The evaluator shall check that the TSS lists of 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that the TOE supports passwords that can be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"] Minimum password length is configurable to between [6] and [15] characters and is configurable. Based on information from FMT_MTD.1/CoreData as the only user that can manipulate functions of the TOE is the admin, the evaluator has determined that password settings are configurable only by this user. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.2 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 section 6 titled **'Cryptographic Requirements Enforced by the TOE is CC'** and section 18 **'Passwords on HYCU'**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 provides the information related to how enabling CC-mode holds much of the pre-configured cryptographic information for the security of the TOE during use. Password length can be configured by the admin via instruction provided in section 18 and all valid characters and min/max length are noted in this section of the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FIA_UIA_EXT.1

5.7.3.1 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 section 6 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 TOE supports two login methods. One is the local console and the other is the web GUI (HTTPS/TLS). For both methods users are presented with a login banner prior to login. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 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 section 6 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 without a successful login a user can only see the login banner and login screen. In order to login a user must provide a username and password. The evaluator determined that based on this evidence no actions can be performed before login by any user. Therefore, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.3 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 section 2 titled **'Logging on to HYCU Remotely'** and section 3 **'Logging on to HYCU Locally'** 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 for remote access login can be established via web browser and provides an example website link as well as the instructions for the login steps using a dedicated login credential for HYCU using a name and password. The initial default username and password should be changed after first logon. For local login access the admin can use text-based console command for entering a username and password. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.4 FIA_UAU.7

5.7.4.1 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 section 3 titled **'Logging on to HYCU Locally'** 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 authentication data is revealed while entering authentication information on this interface. The evaluator has determined that no other steps were necessary to obscure authentication information during login. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5 FIA_X509_EXT.1/Rev

5.7.5.1 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 section 6 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 validity of certificates takes place during authentication. Revocation checking is done during authentication on all certificates in the provided chain using OCSP. If the OCSP responder certificate does not contain the OCSP signing bit extendedKeyUsage, the connection will fail. All TLS certificates used to authenticate to the TOE must contain the Server Authentication extendedKeyUsage bit. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.2 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 section 6 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 revocation checking is done during authentication on all certificates in the provided chain using OCSP. The AGD provides complimentary instructions to the TSS activity in section 21 of the AGD labeled 'Managing Certificate Revocation' which is further expanded upon in the Guidance activity for FIA_X509_EXT.1/Rev. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.3 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 21 titled **'Managing Certificate Revocation'** 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 when configured in the CC-compliant mode, HYCU determines the revocation status as specified in RFC 6960 using OCSP. Certificate validation takes place on all TLS enabled connections (SMTP, syslog, LDAP/S). If the TLS endpoint uses certificate revocation, the OCSP responder must be made available to HYCU, otherwise the certificate path validation will fail. Revocation checking takes place on all certificates in the presented chain. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6 FIA_X509_EXT.2

5.7.6.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined section 6 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 TOE uses the server certificate configured by the admin. Configuration is described in the Hycu User Guide. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6.2 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 section 6 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 the TOE will not establish a trusted channel if the certificate validity check fails for any reason. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section 10 titled **'Configuring SSL certificates'** 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 a pointer to the HYCU User Guide. The section titled 'Configuring SSL certificates' provides instruction on establishing a secure and trusted connection to the environment and how to configure the SSL certificates. The admin can create a self-signing certificate or import a custom certificate. Both instructions are provided in this guide and no additional configuration of the OE is noted. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6.4 FIA_X509_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the section 10 titled **'Configuring SSL certificates'** 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 provides a pointer to the HYCU User Guide. The section titled 'Configuring SSL certificates' provides instruction on establishing a secure and trusted connection to the environment and how to configure the SSL certificates. The admin can create a self-signing certificate or import a custom certificate. Neither of these options are provided by default and requires an admin to configure.

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

5.7.6.5 FIA_X509_EXT.2 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Evaluator Findings	The evaluator examined the section 10 titled **'Configuring SSL certificates'** in the AGD. Upon investigation, the evaluator found that the AGD states that provides a pointer to the HYCU User Guide. The section titled 'Configuring SSL certificates' provides instruction on establishing a secure and trusted connection to the environment and how to configure the SSL certificates. The admin can create a self-signing certificate or import a custom certificate. Both instructions are provided in this guide and no additional configuration of the OE is noted. Section 17 'NDcPP Audit Events' presents evidence for FIA_X509_EXT.1/Rev that if a certificate cannot be validated then an audit log is generated. Section 21 further states that if a connection cannot be established for any of these TLS channels due to a failed validity check, the security administrator must ensure the certificate conforms to all requirements found in section 8. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7 FIA_X509_EXT.3

5.7.7.1 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS contains a description of the device-specific fields used in certificate requests. Upon investigation, the evaluator found that the TSS states that there is no device-specific information provided in CSR. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7.2 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 10 titled **'Configuring SSL 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 provides these instructions for configuring SSL certificates and importing a custom certificate. In the case of importing a CA-signed certificate or trust chain certificate it is included under the prerequisites that these certificates are already available prior to following the AGD guide steps. The section titled **'Importing a custom certificate'** discusses the pre-requisites for the action of importing a custom certificate and how the CA-signed certificates are imported by the admin. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (Security Management)

5.8.1 FMT_MOF.1/ManualUpdate

5.8.1.1 FMT_MOF.1/ManualUpdate TSS 1

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

5.8.1.2 FMT_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	The evaluator examined the section 20 titled 'Upgrading the HYCU Appliance' 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 to upgrade the HYCU appliance, the administrator must obtain a legitimate update file from HYCU. The administrator can determine the current TOE version from either the console or web GUI and they can install a new version using the esxi web GUI after authentication as an administrator. The evaluator examined the same section in the AGD to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD states that ff the hash verification performed by the security administrator does not pass, the TOE shall not be updated. If the hash verification performed by the security administrator succeeds, the TOE can then be updated to the new version.

	Once the update process is started, the TOE is completely unavailable to be managed or used until the update procedure is complete. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2 FMT_MOF.1/Functions

5.8.2.1 FMT_MOF.1/Functions TSS 1

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

5.8.2.2 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). Upon investigation, the evaluator found that the TSS states that the TOE restricts the ability to configure the transmission of audit records to an external audit server to the security administrator. No other users have the ability to modify the behavior of the transmission of audit data to an external IT entity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.3 FMT_MOF.1/Functions Guidance 1

Objective	For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Evaluator Findings	Upon investigation, the evaluator found that the TOE is not distributed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.4 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 13 titled **'Configuring the sending of audit records to an external server'** 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 HYCU uses HTTPS POST webhooks to send audit data over a secure channel. For details, see the HYCU User Guide, Ch. 9 "Performing daily tasks", section "Setting up webhook notifications". It is additionally noted that the admin should make sure that they are using an HTTPS webhook URL, and that they are able to establish trust with the webhook server (for example, by importing an appropriate trusted root). Section 15 'System Behavior for Audit logs' states that if local storage space is exhausted new audit records are dropped. Other than an administrator being able to clear the local audit records there is no provision to modify the records. An audit record is generated when the audit log is cleared. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FMT_MOF.1/Services

5.8.3.1 FMT_MOF.1/Services TSS 1

Objective	For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Evaluator Findings	The evaluator examined section 6 titled **'TOE Summary Specification'** in the Security Target. Upon investigation, the evaluator found that the TOE is not distributed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 FMT_MOF.1/Services TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the

	TSS states that the administrator can enable communication to an external audit server via TLS. They can also disable audit log sending by clearing the notification configuration. In addition to the audit server service, the administrator is also able to start an AD server service and an SMTP server service. They can start these services by configuring setting via the web GUI. The administrator can also stop these services by deleting their configured setting in the web GUI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.3 FMT_MOF.1/Services Guidance 1

Objective	For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Evaluator Findings	Upon investigation, the evaluator found that the TOE is not distributed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.4 FMT_MOF.1/Services Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the section 4 titled '**Admin Management'**, section 11 titled **'Using a TLS Server'**, section 12 **'Prerequisites'** and section 13 titled **'Configuring the sending of audit records to an external syslog server'** in the AGD to verify that these sections describe how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the AGD provides the information that the admin is able to start and stop services in section 4 and is expanded upon in section 11, 12, and 13. The administrator is also able to start the AD server service and the SMTP authentication server service. If a connection becomes unintentionally broken, the TOE will reattempt to connect until communication is restored securely. If the admin wants to stop any of the services mentioned above, they will have to remove the settings that have been configured. Starting the services is linked to the setup of configuration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FMT_MTD.1/CoreData

5.8.4.1 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 section 6 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 all TOE users are required to login and there is no functionality provided prior to authentication other than displaying the TOE banner on every login interface. The evaluator examined the same section 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 all abilities to manipulate TSF data are handled by an administrator and no other user accounts. This is verified in section 4 '**Admin Management**' in the AGD where all functions the admin can manipulate are listed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 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 section 6 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 restricts the ability to manage the trust store only to the administrator. No other user accounts can manage this functionality. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.3 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 section 4 titled **'Admin Management'** 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 lists the functions that the admin can manipulate. There instructions for these functions are found in the following sections: • Start and stop services – *Section 12 'Prerequisites'* • Update the TOE – *Section 20 'Upgrading the HYCU Appliance'* • Modify the behavior of the transmission of audit data to an external IT entity – *Section 13 'Configuring the sending of audit records to an external syslog server'* • Manage the cryptographic keys – Section 5 *'Enabling the CC-Compliant mode' and Section 6 'Cryptographic Requirements Enforced by the TOE in CC-mode'*

	• Configure the cryptographic functionality - *Section 5 'Enabling the CC-Compliant mode' and Section 6 'Cryptographic Requirements Enforced by the TOE in CC-mode'* • Manage the TOE's trust store and designate X509.v3 certificates as trust anchor – *Section 10 **'**Configuring SSL certificates' in the AGD which provides a pointer to the HYCU User Guide section 'Importing a custom certificate'.* The section titled **'Importing a custom certificate'** discusses the pre-requisites for the action of importing a custom certificate and how the CA-signed certificates are imported by the admin. The following management activities can be performed using the console: • Set the time which is used for time-stamps (console only) – *Section 9 'Configuring system time'* • Setting minimum password length in the console – *Section 18 'Passwords on HYCU'* • Running self-test on-demand – *Section 7 'Performing self-test'* • Configuring access banners – *Section 8 'Configuring access banners'* • Ability to configure the session inactivity time before session termination or locking – *Section 19 'Configuring session timeouts'* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.4 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 10 **'Configuring SSL certificates'** and section 21 **'Managing Certificate Revocation'** 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 instructions for the configuration of trusted roots with a CA can be found in the HYCU User Guide in the section labeled 'Configuring SSL certificates'. The evaluator examined the 'Configuring SSL certificates' in the HYCU User Guide 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 HYCU User Guide provides ample instructions on the creating of and importing of certificates and this is in alignment with trust store configuring activities. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.5 FMT_MTD.1/CryptoKeys

5.8.5.1 FMT_MTD.1/CryptoKeys TSS 1

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

5.8.5.2 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 section 6 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 generation, importing, and deletion of cryptographic keys is restricted to the security administrator.
	
	Security administrator is able to control the following cryptographic keys:
	• X.509 certificates for HTTP/S server
	  ○ Generate, import, delete
	• X.509 certificates used for trusted roots
	  ○ Import, delete
	• Passwords for access to LDAP and SMTP servers
	  ○ Create, modify, delete (by disabling LDAP/SMTP integration)
	• Passwords for local HYCU appliance users
	  ○ Create, modify, delete (by removing user)
	
	Detailed procedures for controlling these cryptographic keys are described in the guidance materials.
	
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.5.3 FMT_MTD.1/CryptoKeys Guidance 1

Objective	For distributed TOEs it is required to verify the Guidance Documentation to describe management of each TOE component. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Evaluator Findings	Upon investigation, the evaluator found that the TOE is not distributed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.4 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 5 titled **'Enabling the CC-compliant** mode', section 6 titled **'Cryptographic Requirements Enforced by the TOE in CC-mode'**, section 10 titled **'Configuring SSL Certificates',** section 11 titles **'Using a TLS Server (Syslog, AD, SMTP)'** and section 18 titled **'Passwords on HYCU'** 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 setting the TOE into CC-Compliant mode restricts the device to specific cryptographic protocols and algorithms which can be referenced in section 6 of the AGD. Section 5 states that the generation, importing, and deletion of cryptographic keys is restricted to the security administrator. RNG is configured automatically and appropriately initialized on TOE start. Instructions for configuring X.509 certificate is considered equivalent to the instructions for SSL certificates which can be found under section 10 of the AGD. Section 11 holds instructions for the configuration steps for LDAP and SMTP Passwords are created, modified, and deleted by the admin. Section 18 of the AGD holds the instructions for how these actions can be performed. Section 6 of the AGD confirms the cryptographic settings related to keys used by the TOE when CC-mode is enabled. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.6 FMT_SMF.1

5.8.6.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface).

	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.
Evaluator Findings	The evaluator examined section 6 titled **'TOE Summary Specification'** in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the TSS states that The TOE can be managed via the web GUI and local console. Management activities that can be performed though the web GUI include the following: • start and stop services • update the TOE • modify the behavior of the transmission of audit data to an external IT entity • Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full); • manage the cryptographic keys • configure the cryptographic functionality • manage the TOE's trust store and designate X509.v3 certificates as trust anchors • import X.509v3 certificates to the TOE's trust store The following management activities can be performed using the console: • set the time which is used for time-stamps (console only)) • Configuring access banners • Ability to configure the session inactivity time before session termination or locking • Ability to configure the authentication failure parameters for FIA_AFL.1 The evaluator examined the same section as noted above in the TSS to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that the local interface is the local console. This is verified in section 4 **'Admin Management'** in which the AGD states that the TOE can be manages via web GUI and local console. These activities are listed by whether the GUI or local console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.6.2 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 section 4 titled **'Admin Management'** in the AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that the TOE can be managed via local console. The evaluator examined the section 3 titled '**Logging on to the HYCU Locally'** in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD states that this interface lets the user know they are local by displaying the tty session number. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.7 FMT_SMR.2

5.8.7.1 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 section 6 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 administrator can assign users to groups and roles. These groups consist of the infrastructure group and the self-service group. In addition to the group assignment users must also be assigned a role. Access to TSF functions is limited to users assigned the administrator role.
	
	Infrastructure group administrators can manage users, create/edit/delete self-service groups, add/remove users from groups, activate/deactivate users and self-service groups, and set owners of VMs and file shares. A self-service group administrator can add/remove users from groups.
	
	Roles and Restrictions:
	• Administrator
	  ○ In user group: can administer membership.
	  ○ In "Infrastructure group": can configure appliance.
	• Backup operator – can define policies, assign them to entities and trigger backup and restore operations.
	• Restore operator – can trigger restore operations.
	• Backup and restore operator – combine privileges of both backup and restore operators
	• Viewer – can view (but not modify) entities.
	
	TSF data can only be managed by security administrators via the console or web GUI.
	
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.7.2 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 1 titled **'Deploying HYCU'** 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 provides a pointer to the HYCU User Guide for further information. Section 2 **'Deploying the HYCU Virtual appliance'** of the HYCU User Guide and provides instruction for deploying the TOE from a remote source. The evaluator has reviewed this information and has determined that the TOE deploys from the ESXI which only checks

	locally, but the connection is a remote one. Additionally, log in from both a remote or local access point is instructions in sections 2 'Logging on to the HYCU Remotely' and section 3 'Logging on to the HYCU Locally' are present in the AGD for the admin. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (Protection of the TSF)

5.9.1 FPT_APW_EXT.1

5.9.1.1 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that passwords are never displayed or stored in plaintext form. The evaluator also examined the same section 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 passwords are stored in the database in an encrypted form - PBKDF2 is used to derive a key from the password, which is then encrypted using AES-CBC before stored in the database. Passwords are only decoded on retrieval by the internal workings of the appliance, and the values are not available via any user-facing API. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FPT_SKP_EXT.1

5.9.2.1 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 section 6 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 for this activity points to the TSS for FCS_CKM.4 for information about the storage and handling of keys. Symmetric, private and pre-shared keys (including passwords needed for remote login to systems such as

	LDAPS/AD and SMTP) are stored in the database in an encrypted form. Public keys/certificates are public and hence not encrypted. There are mechanisms in place to prevent viewing key information through an interface designed specifically for that purpose. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3 FPT_STM_EXT.1

5.9.3.1 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 selection made for FPT_STM_EXT.1 in the Security Target and verified that "obtain time from underlying virtualization system" has not been selected for. The TOE provides reliable time stamps security audit functionality, administrative session inactivity, and cryptographic functions. The system time can only be changed by a security administrator. There is no possible delay because the time is not provided by the underlying virtual system. The time is manually set by the admin. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.2 FPT_STM_EXT.1 Guidance 1

Objective	The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication. If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.
Evaluator Findings	The evaluator examined the section 9 titled **'Configuring 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 states that NTP time synchronization is disabled in the CC-compliant mode. It can be manually set by the admin with instruction provided under this section of the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4 FPT_TST_EXT.1.1

5.9.4.1 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 section 6 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 TOE performs the self tests on startup and on reload. The self tests can also be initiated from the console, as described in the guidance documentation. Self-tests check the following: • the integrity of the application code, by calculating SHA256 checksum of all the application files and comparing them against checksums stored in a file created at the time of the build. • the integrity of the openssl, java and kernel operating system packages (using native RPM -v). The evaluator examined the same section 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 self-tests that run before the server is started ensures that the state of the application server and cryptographically relevant parts of the OS have not been tampered with and match the state at release time. Self-test that run before server is started ensuring that the state of the application server and cryptographically relevant parts of the OS have not been tampered with and match the state at release time. As mandated by FIPS-140-2, self-test is performed on cryptographic library initialization at first operation involving the cryptographic library. If this self-test passes, operations continue normally. If this self-test fails, the self-test failure reason is logged, and TOE startup is prevented. The native cryptographic library (OpenSSL) self-test failure prevents Apache httpd startup. Java cryptographic library (BouncyCastle) self-test failure prevents HYCU application (grizzly) startup. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4.2 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 7 titled **'Performing the self tests'** 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 possible errors during self-test are: • Checksum database file is missing or corrupted. • One or more files from the checksum database are missing on the TOE. • One or more files from the checksum database do not match their checksum on disk. Any of these situations indicate a corrupted or compromised state of the TOE. The only response is for TOE to be reinstalled or reset. For example, OS image should be replaced with the fresh image state, while retaining the existing data disk. Self-tests are run before the server is started ensuring that the state of the application server and cryptographically relevant parts of the OS have not been tampered with and match the state at release time. As mandated by FIPS-140-2, self-test is performed on cryptographic library initialization at first operation involving the cryptographic library. If this self-test passes, operations continue normally. If this self-test fails, the self-test failure reason is logged, and TOE startup is prevented. The native cryptographic library (OpenSSL) self-test failure prevents Apache httpd startup. Java cryptographic library (BouncyCastle) self-test failure prevents HYCU application (grizzly) startup. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5 FPT_TUD_EXT.1

5.9.5.1 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 section 6 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 administrator can determine the current TOE version from either the console or web GUI. The evaluator examined the same section in the Security Target to verify that the TSS, if a trusted update can be installed on the TOE with a delayed activation, describes how and when the inactive version becomes active. Upon investigation, the evaluator found that the TSS states that when an update is performed it takes effect immediately. The evaluator has determined there is no delay in activation based on this information. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.2 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 section 6 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 administrator can install a new version using the console or web GUI. The TOE uses a published has for verification. The administrator is responsible to verify the hash of the update prior to installation. The hash is made available by HYCU when the TOE update is provided. Because the hash is made available by the developer of the TOE it is considered a legitimate source. The evaluator examined the same section of the TSS 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 if the hash verification fails, the TOE will not initialize and will have to be reverted to the previous version. If the hash verification succeeds, the TOE will proceed with the update process and the version will change. . Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.3 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, if the options 'support automatic checking for updates' or 'support automatic updates' are chosen, explains what actions are involved in automatic checking or automatic updating by the TOE. Upon investigation, the evaluator found that the ST has not made the selection for 'support automatic checking for updates' and that updates are manually performed by the administrator. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.9.5.4 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. Upon investigation, the evaluator found that the TSS states that the administrator is responsible to verify the hash of the update prior to installation. The hash is made available by HYCU when the TOE update is provided. When an update is performed it takes effect immediately. None of the update procedures are automated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.5 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 20 titled **'Upgrading the HYCU Appliance'** 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 states that the administrator can determine the current TOE version from either the console or web GUI and they can install a new version using the esxi web GUI after authentication as an administrator. When an update is performed it takes effect immediately. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.6 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 section 20 titled **'Upgrading the HYCU Appliance'** in the AGD to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states that the TOE uses published

	hashes to determine the validity of the update file. Hash values can only be obtained from the HYCU website once the new update is provided. The security administrator is responsible for verifying the hash before performing any update functions. There is no hash verification done by the TOE, so it is security administrators' responsibility to verify the hash is valid. When an update is performed it takes effect immediately. None of the update procedures are automated. If the hash verification fails, the TOE will not initialize and will have to be reverted to the previous version. If the hash verification succeeds, the TOE will proceed with the update process and the version will change. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.7 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 section 20 titled **'Upgrading the HYCU Appliance'** in the AGD to verify that it describes, if a published hash is used to protect the trusted update mechanism, how the Security Administrator can obtain authentic published hash values for the updates. Upon investigation, the evaluator found that the AGD states that hash values can only be obtained from the HYCU website once the new update is provided. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5.8 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 section 20 titled **'Upgrading the HYCU Appliance'** in the AGD to verify that it, if the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, contains a description of how the certificates are contained on the device and describes how the certificates are installed/updated/selected. Upon investigation, the evaluator found that the AGD states that software updates use hash values and not a certificate-based mechanism. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10 TSS and Guidance Activities (TOE Access)

5.10.1 FTA_SSL_EXT.1

5.10.1.1 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 section 6 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 inactive remote administrator sessions and console sessions are terminated by the TOE after an administrator defined period of time. Remote administrator session timeout is configurable via /opt/grizzly/config.properties variable api.session.expiration.minutes, with default set to 15 (minutes). Console session timeout is configurable via /etc/profile.d/bash-autologout.sh, with TMOUT environment variable value by default set to 600 (seconds, or 10 minutes). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.2 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 19 titled **'Configuring session timeouts'** 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 session timeout is supported for both local and remote interfaces. Instructions for text-based console commands in order to configure session timeouts are provided in this section of the AGD. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2 FTA_SSL.3

5.10.2.1 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 section 6 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 inactive remote user and administrator sessions are terminated after an administrator configured time interval. Local and remote session timeout can be configured using the console interface. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2.2 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 19 titled **'Configuring session timeouts'** 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 states that the admin can configure the session timeout mechanism for both local and remote interfaces. Instructions for both methods are present in this section. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3 FTA_SSL.4

5.10.3.1 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 section 6 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 remote administrator sessions and local administrator sessions can be terminated by the administrator who is logged in to the session. The session is terminated by the admin executing the logout command on the Web GUI or CLI interface. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3.2 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 section 2 titled **'Logging on to HYCU Remotely'** 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 states that logout for a remote section is noted in step "c." of the instructions. Interacting with a drop down menu to logout will end the session. Section 3 titled **'Logging on to HYCU Locally'** provides instruction for the termination of local sessions in step '4' which states that the admin can log out of the interface by using the command "logout." Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.4 FTA_TAB.1

5.10.4.1 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 section 6 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 TOE provides separate login banners for the web GUI and console. The guidance documentation requires that during initial configuration of the TOE, an appropriate advisory notice and consent warning message is configured for both remote and local methods of access. The message configured is shown on both login methods. Additionally the requirement FIA_UIA_EXT.1 can be referenced for a list of administrative interfaces. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.4.2 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 8 titled **'Configuring access banners'** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD provides instructions for text-based console configuration of access banners and any additional steps the admin needs to take in order to make the changes go live. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11 TSS and Guidance Activities (Trusted Path/Channels)

5.11.1 FTP_ITC.1

5.11.1.1 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 section 6 titled **'TOE Summary Specification'** in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states that the TOE acts as a client for communication access to authorized it entities.

	The TOE uses trusted channels to protect communication with an external audit server, authentication server, and SMTP server. HTTPS POST webhooks are used for communication with an external audit server. Basic Authentication (username/password) is used for HTTPS connections via the web GUI for the TOE. Authentication via certificates is used for connections to the audit, SMTP and authentication server. LDAP/S (TLS 1.2) is used to protect communication with the authentication server. The TOE verifies that the LDAP server hostname matches the DNS entry specified in the Subject Alternative Name (SAN) extension of the LDAP server's certificate. SMTP/S (TLS 1.2) is used to protect communication with the SMTP server with the TOE acting as the client. The evaluator examined the same section as above 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 HTTPS, TLS, SMTP and an authentication server is used for secure communication mechanisms and is outlined in greater detail in the paragraph above. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.1.2 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 12 titled **'Prerequisites'** in the AGD to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD states that if a connection becomes unintentionally broken, the TOE will reattempt to connect until communication is restored securely. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.2 FTP_TRP.1/Admin

5.11.2.1 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 section 6 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 HTTPS (TLS 1.2) is used to secure remote administration. This is the only remote administration method that is available. The evaluator examined the same section of the TSS and the SFR selection in the Security Target to verify that the TSS protocols are consistent with those specified in the requirement.

	Upon investigation, the evaluator found that the TSS and SFR selection for this requirement are consistent with one another as they both claim usage of TLS and HTTPS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.2.2 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 2 titled **'Logging on to the HYCU Remotely'** 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 provides instruction for the admin to login to the TOE remotely through a web browser using a username and password. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Test Cases (Audit)

6.1.1 FAU_GEN.1 Test #1

Item	Data/Description
Test Assurance Activity	Test 1: 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.
Pass/Fail with Explanation	The TOE successfully creates audit records for both local and remote authentication.
Result	Pass

6.1.2 FAU_STG_EXT.1 Test #1

Item	Data/Description
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	• The evaluator confirms the name and version of the audit server. • The evaluator logs into the TOE. • The evaluator configures the TOE to use the syslog server. • The evaluator generates audit records. • The evaluator verifies via packet capture that syslog messages have been sent encrypted.
Expected Test Results	The TOE should allow audit records to be transmitted over the configured encrypted channel.
Pass/Fail with Explanation	The TOE successfully sends audit logs to the syslog server.

Result	Pass

6.1.3 FAU_STG_EXT.1 Test #2 (a)

Item	Data/Description
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).
Test Steps	• The evaluator configures audit log buffer size to smallest size. • The evaluator generates audit records until the log buffer is full. • The evaluator would need to free space on the file system in order for the appliance to function again. • The evaluator would need to restart the application in order for the appliance to work. • The evaluator identifies the timestamp of the oldest message in the local audit log.
Expected Test Results	The TOE should not allow any new audit data to be written once the log buffer is full.
Pass/Fail with Explanation	The TOE successfully drops new audit data when the audit log is full.
Result	Pass

6.1.4 FAU_STG_EXT.1 Test #2 (b)

Item	Data/Description
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	N/A
Expected Test Results	N/A

Pass/Fail with Explanation	N/A No mention of overwrite previous records in the Security Target.
Result	Pass

6.1.5 FAU_STG_EXT.1 Test #2 (c)

Item	Data/Description
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).
Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A The selection "drop new audit data" is selected in FAU_STG_EXT.1.3.

6.1.6 FAU_STG_EXT.1 Test #3

Item	Data/Description
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
Test Steps	Covered by FAU_STG_EXT.2/LocSpace
Expected Test Results	N/A
Pass/Fail with Explanation	N/A FAU_STG_EXT.2/LocSpace is not selected in the Security Target.

6.1.7 FAU_STG_EXT.1 Test #4

Item	Data/Description
Test Assurance Activity	Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.

Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A The TOE is not distributed.

6.1.8 FPT_STM_EXT.1 Test #1

Item	Data/Description
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	• The evaluator sets the time on the TOE. • The evaluator demonstrates time was set correctly.
Expected Test Results	The evaluator should successfully be able to set the time manually.
Pass/Fail with Explanation	Pass, The TOE successfully allowed the evaluator to configure the time

6.1.9 FPT_STM_EXT.1 Test #2

Item	Data/Description
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.
Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A The TOE doesn't support this function in the Security Target.

6.1.10 FPT_STM_EXT.1 Test #3

Item	Data/Description
Test Assurance Activity	Test 3: [conditional] If the TOE obtains time from the underlying VS, the evaluator shall record the time on the TOE, modify the time on the underlying VS, and verify the modified time is reflected by the TOE. If there is a delay between the setting the time on the VS and when the time is reflected on the TOE, the evaluator shall ensure this delay is consistent with the TSS and Guidance. [TD0632 applied]
Test Steps	N/A

Expected Test Results	N/A
Pass/Fail with Explanation	N/A The TOE doesn't support this function in the Security Target.

6.1.11 FTP_ITC.1 Test #1

Item	Data/Description
Test Assurance Activity	The evaluator shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	TLS • The evaluator authenticates to the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and syslog server. Active Directory - TLS • The evaluator authenticates to the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and AD server. SMTP • The evaluator configures SMTP on the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and SMTP server.
Expected Test Results	The TOE should successfully show encrypted traffic between the TOE and syslog, LDAP/s, and SMTP/s server.
Pass/Fail with Explanation	The TOE successfully sends encrypted audit data to the syslog server.
Result	Pass

6.1.12 FTP_ITC.1 Test #2

Item	Data/Description
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	This test was exercised in FTP_ITC.1 test 1.
Result	Pass

6.1.13 FTP_ITC.1 Test #3

Item	Data/Description

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	This test was exercised in FTP_ITC.1 test 1.
Result	Pass

6.1.14 FTP_ITC.1 Test #4

Item	Data/Description
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: 1. A duration that exceeds the TOE's application layer timeout setting, 2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer. The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext. In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g. a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g. virtual switch) and must be physical in nature.
Test Steps	Short test (5 seconds) Syslog • The evaluator authenticates to the TOE. • The evaluator displays log evidence of a successful login. • The evaluator displays packet capture data between the TOE and syslog server. Active Directory - TLS • The evaluator authenticates to the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and AD/s server. SMTP • The evaluator configures SMTP on the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and SMTP/s server. Longer test (30 seconds) Syslog

	• The evaluator authenticates to the TOE. • The evaluator displays log evidence of a successful login. • The evaluator displays packet capture data between the TOE and syslog server. Active Directory - TLS • The evaluator authenticates to the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and AD/s server. SMTP • The evaluator configures SMTP on the TOE. • The evaluator displays the most recent audit logs. • The evaluator displays packet capture data between the TOE and SMTP/s server.
Expected Test Results	The TOE should successfully send encrypted data after network interruptions for both durations.
Pass/Fail with Explanation	Pass, The TOE successfully starts encrypted data again after connectivity gets interrupted.

6.2 Test Cases (Auth and Crypto)

6.2.1 FCS_CKM.1

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

- Primes p1, p2, q1, q2, p and q shall all be probable primes

To test the key generation method for the Random Provable primes method and for all the Primes with Conditions methods, the evaluator must seed the TSF key generation routine with sufficient data to deterministically generate the RSA key pair. This includes the random seed(s), the public exponent of the RSA key, and the desired key length. For each key length supported, the evaluator shall have the TSF generate 25 key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation.

Key Generation for Elliptic Curve Cryptography (ECC)

FIPS 186-4 ECC Key Generation Test

For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall require the implementation under test (IUT) to generate 10 private/public key pairs. The private key shall be generated using an approved random bit generator (RBG). To determine correctness, the evaluator shall submit the generated key pairs to the public key verification (PKV) function of a known good implementation.

FIPS 186-4 Public Key Verification (PKV) Test

For each supported NIST curve, i.e., P-256, P-384 and P-521, the evaluator shall generate 10 private/public key pairs using the key generation function of a known good implementation and modify five of the public key values so that they are incorrect, leaving five values unchanged (i.e., correct). The evaluator shall obtain in response a set of 10 PASS/FAIL values.

Key Generation for Finite-Field Cryptography (FFC)

The evaluator shall verify the implementation of the Parameters Generation and the Key Generation for FFC by the TOE using the Parameter Generation and Key Generation test. This test verifies the ability of the TSF to correctly produce values for the field prime p, the cryptographic prime q (dividing p-1), the cryptographic group generator g, and the calculation of the private key x and public key y.

The Parameter generation specifies 2 ways (or methods) to generate the cryptographic prime q and the field prime p:

- Primes q and p shall both be provable primes
- Primes q and field prime p shall both be probable primes

and two ways to generate the cryptographic group generator g:

- Generator g constructed through a verifiable process
- Generator g constructed through an unverifiable process.

	The Key generation specifies 2 ways to generate the private key x: • len(q) bit output of RBG where 1 <=x <= q-1 • len(q) + 64 bit output of RBG, followed by a mod q-1 operation and a +1 operation, where 1<= x<=q-1. The security strength of the RBG must be at least that of the security offered by the FFC parameter set. To test the cryptographic and field prime generation method for the provable primes method and/or the group generator g for a verifiable process, the evaluator must seed the TSF parameter generation routine with sufficient data to deterministically generate the parameter set. For each key length supported, the evaluator shall have the TSF generate 25 parameter sets and key pairs. The evaluator shall verify the correctness of the TSF's implementation by comparing values generated by the TSF with those generated from a known good implementation. Verification must also confirm • g != 0,1 • q divides p-1 • g^q mod p = 1 • g^x mod p = y for each FFC parameter set and key pair. **FFC Schemes using "safe-prime" groups [TD0580 applied]** Testing for FFC Schemes using safe-prime groups is done as part of testing in CKM.2.1.
Test Output	This test is covered by CAVP certificate #A2933
Pass/Fail with Explanation	PASS. This test is covered by CAVP certificate #A2933

6.2.2 FCS_CKM.2 RSA

Item	Data/Description
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.
Expected Test Results	The evaluator tested a known good implementation for each protocol selected in FTP_ITC.1 and FTP_TRP.1/Admin
Test Output	This test is covered by other test cases: FTP_ITC.1 and FTP_TRP.1/Admin
Pass/Fail with Explanation	PASS. This test is covered by other test case: FTP_ITC.1 and FTP_TRP.1/Admin

6.2.3 FCS_CKM.2 ECC

Item	Data/Description
Test Assurance Activity	**SP800-56A Key Establishment Schemes** The evaluator shall verify a TOE's implementation of SP800-56A key agreement schemes using the following Function and Validity tests. These validation tests for each key agreement scheme verify that a TOE has implemented the components of the key agreement scheme according to the specifications in the Recommendation. These components include the calculation of the DLC primitives (the shared secret value Z) and the calculation of the derived keying material (DKM) via the Key Derivation Function (KDF). If key confirmation is supported, the evaluator shall also verify that the components of key confirmation have been implemented correctly, using the test procedures described below. This includes the parsing of the DKM, the generation of MACdata and the calculation of MACtag. *Function Test* The Function test verifies the ability of the TOE to implement the key agreement schemes correctly. To conduct this test the evaluator shall generate or obtain test vectors from a known good implementation of the TOE supported schemes. For each supported key agreement scheme-key agreement role combination, KDF type, and, if supported, key confirmation role- key confirmation type combination, the tester shall generate 10 sets of test vectors. The data set consists of one set of domain parameter values (FFC) or the NIST approved curve (ECC) per 10 sets of public keys. These keys are static, ephemeral or both depending on the scheme being tested. The evaluator shall obtain the DKM, the corresponding TOE's public keys (static and/or ephemeral), the MAC tag(s), and any inputs used in the KDF, such as the Other Information field OI and TOE id fields. If the TOE does not use a KDF defined in SP 800-56A, the evaluator shall obtain only the public keys and the hashed value of the shared secret. The evaluator shall verify the correctness of the TSF's implementation of a given scheme by using a known good implementation to calculate the shared secret value, derive the keying material DKM, and compare hashes or MAC tags generated from these values. If key confirmation is supported, the TSF shall perform the above for each implemented approved MAC algorithm. *Validity Test* The Validity test verifies the ability of the TOE to recognize another party's valid and invalid key agreement results with or without key confirmation. To conduct this test, the evaluator shall obtain a list of the supporting cryptographic functions included in the SP800-56A key agreement implementation to determine which errors the TOE should be able to recognize. The evaluator generates a set of 24 (FFC) or 30 (ECC) test vectors consisting of data sets including domain parameter values or NIST approved curves, the evaluator's public keys, the TOE's public/private key pairs, MACTag, and any inputs used in the KDF, such as the other info and TOE id fields.

	The evaluator shall inject an error in some of the test vectors to test that the TOE recognizes invalid key agreement results caused by the following fields being incorrect: the shared secret value Z, the DKM, the other information field OI, the data to be MACed, or the generated MACTag. If the TOE contains the full or partial (only ECC) public key validation, the evaluator will also individually inject errors in both parties' static public keys, both parties' ephemeral public keys and the TOE's static private key to assure the TOE detects errors in the public key validation function and/or the partial key validation function (in ECC only). At least two of the test vectors shall remain unmodified and therefore should result in valid key agreement results (they should pass). The TOE shall use these modified test vectors to emulate the key agreement scheme using the corresponding parameters. The evaluator shall compare the TOE's results with the results using a known good implementation verifying that the TOE detects these errors.
Test Output	This test is covered by CAVP certificate #A2933
Pass/Fail with Explanation	PASS. This test is covered by CAVP certificate #A2933

6.2.4 FCS_COP.1/Data Encryption

Item	Data/Description
Test Assurance Activity	**AES-CBC Known Answer Tests** There are four Known Answer Tests (KATs), described below. In all KATs, the plaintext, ciphertext, and IV values shall be 128-bit blocks. The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation. KAT-1. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 plaintext values and obtain the ciphertext value that results from AES-CBC encryption of the given plaintext using a key value of all zeros and an IV of all zeros. Five plaintext values shall be encrypted with a 128-bit all-zeros key, and the other five shall be encrypted with a 256-bit all-zeros key. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using 10 ciphertext values as input and AES-CBC decryption. KAT-2. To test the encrypt functionality of AES-CBC, the evaluator shall supply a set of 10 key values and obtain the ciphertext value that results from AES-CBC encryption of an all-zeros plaintext using the given key value and an IV of all zeros. Five of the keys shall be 128-bit keys, and the other five shall be 256-bit keys. To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using an all-zero ciphertext value as input and AES- CBC decryption. KAT-3. To test the encrypt functionality of AES-CBC, the evaluator shall supply the two sets of key values described below and obtain the ciphertext

	value that results from AES encryption of an all-zeros plaintext using the given key value and an IV of all zeros. The first set of keys shall have 128 128-bit keys, and the second set shall have 256 256-bit keys. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N].
	
	To test the decrypt functionality of AES-CBC, the evaluator shall supply the two sets of keys and ciphertext value pairs described below and obtain the plaintext value that results from AES-CBC decryption of the given ciphertext using the given key and an IV of all zeros. The first set of key/ciphertext pairs shall have 128 128-bit key/ciphertext pairs, and the second set of key/ciphertext pairs shall have 256 256-bit key/ciphertext pairs. Key i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1,N]. The ciphertext value in each pair shall be the value that results in an all-zeros plaintext when decrypted with its corresponding key.
	
	KAT-4. To test the encrypt functionality of AES-CBC, the evaluator shall supply the set of 128 plaintext values described below and obtain the two ciphertext values that result from AES-CBC encryption of the given plaintext using a 128-bit key value of all zeros with an IV of all zeros and using a 256- bit key value of all zeros with an IV of all zeros, respectively. Plaintext value i in each set shall have the leftmost i bits be ones and the rightmost 128-i bits be zeros, for i in [1,128].
	
	To test the decrypt functionality of AES-CBC, the evaluator shall perform the same test as for encrypt, using ciphertext values of the same form as the plaintext in the encrypt test as input and AES-CBC decryption.
	
	AES-CBC Multi-Block Message Test
	The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key and IV. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key and IV using a known good implementation.
	
	The evaluator shall also test the decrypt functionality for each mode by decrypting an i-block message where 1 < i <=10. The evaluator shall choose a key, an IV and a ciphertext message of length i blocks and decrypt the message, using the mode to be tested, with the chosen key and IV. The plaintext shall be compared to the result of decrypting the same ciphertext message with the same key and IV using a known good implementation.
	
	AES-CBC Monte Carlo Tests
	The evaluator shall test the encrypt functionality using a set of 200 plaintext, IV, and key 3-tuples. 100 of these shall use 128 bit keys, and 100 shall use 256 bit keys. The plaintext and IV values shall be 128-bit blocks. For each 3-tuple, 1000 iterations shall be run as follows:
	
	# Input: PT, IV, Key for i = 1 to 1000:
	if i == 1:
	CT[1] = AES-CBC-Encrypt(Key, IV, PT)
	PT = IV
	else:
	CT[i] = AES-CBC-Encrypt(Key, PT)

PT = CT[i-1]

The ciphertext computed in the 1000th iteration (i.e., CT[1000]) is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation.

The evaluator shall test the decrypt functionality using the same test as for encrypt, exchanging CT and PT and replacing AES-CBC-Encrypt with AES- CBC-Decrypt.

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

128 bit and 256 bit keys

a) **Two plaintext lengths**. One of the plaintext lengths shall be a non- zero integer multiple of 128 bits, if supported. The other plaintext length shall not be an integer multiple of 128 bits, if supported.

b) **Three AAD lengths**. One AAD length shall be 0, if supported. One AAD length shall be a non-zero integer multiple of 128 bits, if supported. One AAD length shall not be an integer multiple of 128 bits, if supported.

c) **Two IV lengths**. If 96 bit IV is supported, 96 bits shall be one of the two IV lengths tested.

The evaluator shall test the encrypt functionality using a set of 10 key, plaintext, AAD, and IV tuples for each combination of parameter lengths above and obtain the ciphertext value and tag that results from AES-GCM authenticated encrypt. Each supported tag length shall be tested at least once per set of 10. The IV value may be supplied by the evaluator or the implementation being tested, as long as it is known.

The evaluator shall test the decrypt functionality using a set of 10 key, ciphertext, tag, AAD, and IV 5-tuples for each combination of parameter lengths above and obtain a Pass/Fail result on authentication and the decrypted plaintext if Pass. The set shall include five tuples that Pass and five that Fail.

The results from each test may either be obtained by the evaluator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation.

AES-CTR Known Answer Tests
The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. Since the Counter Mode does not specify the counter that is used, it is not possible to implement an automated test for this mode. The generation and management of the counter is tested through FCS_SSH*_EXT.1.4. If CBC and/or GCM are selected in

	FCS_COP.1/DataEncryption, the test activities for those modes sufficiently demonstrate the correctness of the AES algorithm. If CTR is the only selection in FCS_COP.1/DataEncryption, the AES-CBC Known Answer Test, AES- GCM Known Answer Test, or the following test shall be performed (all of these tests demonstrate the correctness of the AES algorithm): There are four Known Answer Tests (KATs) described below to test a basic AES encryption operation (AES-ECB mode). For all KATs, the plaintext, IV, and ciphertext values shall be 128-bit blocks. The results from each test may either be obtained by the validator directly or by supplying the inputs to the implementer and receiving the results in response. To determine correctness, the evaluator shall compare the resulting values to those obtained by submitting the same inputs to a known good implementation. KAT-1 To test the encrypt functionality, the evaluator shall supply a set of 5 plaintext values for each selected keysize and obtain the ciphertext value that results from encryption of the given plaintext using a key value of all zeros. KAT-2 To test the encrypt functionality, the evaluator shall supply a set of 5 key values for each selected keysize and obtain the ciphertext value that results from encryption of an all zeros plaintext using the given key value. KAT-3 To test the encrypt functionality, the evaluator shall supply a set of key values for each selected keysize as described below and obtain the ciphertext values that result from AES encryption of an all zeros plaintext using the given key values. A set of 128 128-bit keys, a set of 192 192-bit keys, and/or a set of 256 256-bit keys. Key_i in each set shall have the leftmost i bits be ones and the rightmost N-i bits be zeros, for i in [1, N]. KAT-4 To test the encrypt functionality, the evaluator shall supply the set of 128 plaintext values described below and obtain the ciphertext values that result from encryption of the given plaintext using each selected keysize with a key value of all zeros (e.g. 256 ciphertext values will be generated if 128 bits and 256 bits are selected and 384 ciphertext values will be generated if all keysizes are selected). Plaintext value i in each set shall have the leftmost bits be ones and the rightmost 128-i bits be zeros, for i in [1, 128]. **AES-CTR Multi-Block Message Test** The evaluator shall test the encrypt functionality by encrypting an i-block message where 1 less-than i less-than-or-equal to 10 (test shall be performed using AES-ECB mode). For each i the evaluator shall choose a key and plaintext message of length i blocks and encrypt the message, using the mode to be tested, with the chosen key. The ciphertext shall be compared to the result of encrypting the same plaintext message with the same key using a known good implementation. The evaluator shall perform this test using each selected keysize. **AES-CTR Monte-Carlo Test** The evaluator shall test the encrypt functionality using 100 plaintext/key pairs. The plaintext values shall be 128-bit blocks. For each pair, 1000 iterations shall be run as follows: # Input: PT, Key

	for i = 1 to 1000: CT[i] = AES-ECB-Encrypt(Key, PT) PT = CT[i] The ciphertext computed in the 1000th iteration is the result for that trial. This result shall be compared to the result of running 1000 iterations with the same values using a known good implementation. The evaluator shall perform this test using each selected keysize. There is no need to test the decryption engine.
Test Output	This test is covered by CAVP certificate #A2933
Pass/Fail with Explanation	PASS. This test is covered by CAVP certificate #A2933

6.2.5 FCS_COP.1/SigGen

Item	Data/Description
Test Assurance Activity	**ECDSA Algorithm Tests** ***ECDSA FIPS 186-4 Signature Generation Test*** For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate 10 1024-bit long messages and obtain for each message a public key and the resulting signature values R and S. To determine correctness, the evaluator shall use the signature verification function of a known good implementation. ***ECDSA FIPS 186-4 Signature Verification Test*** For each supported NIST curve (i.e., P-256, P-384 and P-521) and SHA function pair, the evaluator shall generate a set of 10 1024-bit message, public key and signature tuples and modify one of the values (message, public key or signature) in five of the 10 tuples. The evaluator shall obtain in response a set of 10 PASS/FAIL values. **RSA Signature Algorithm Tests** ***Signature Generation Test*** The evaluator generates or obtains 10 messages for each modulus size/SHA combination supported by the TOE. The TOE generates and returns the corresponding signatures. The evaluator shall verify the correctness of the TOE's signature using a trusted reference implementation of the signature verification algorithm and the associated public keys to verify the signatures. ***Signature Verification Test*** For each modulus size/hash algorithm selected, the evaluator generates a modulus and three associated key pairs, (d, e). Each private key d is used to sign six pseudorandom messages each of 1024 bits using a trusted reference implementation of the signature generation algorithm. Some of the public keys, e, messages, or signatures are altered so that signature verification should fail. For both the set of original messages and the set of altered messages: the modulus, hash algorithm, public key e values, messages, and signatures are forwarded to the TOE, which then attempts to verify the signatures and returns the verification results.

	The evaluator verifies that the TOE confirms correct signatures on the original messages and detects the errors introduced in the altered messages.
Test Output	This test is covered by CAVP certificate #A2933
Pass/Fail with Explanation	PASS. This test is covered by CAVP certificate #A2933

6.2.6 FCS_COP.1/Hash

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

	This test is for byte-oriented implementations only. The evaluators randomly generate a seed that is n bits long, where n is the length of the message digest produced by the hash function to be tested. The evaluators then formulate a set of 100 messages and associated digests by following the algorithm provided in Figure 1 of [SHAVS]. The evaluators then ensure that the correct result is produced when the messages are provided to the TSF.
Test Output	This test is covered by CAVP certificate #A2933
Pass/Fail with Explanation	PASS. This test is covered by CAVP certificate #A2933

6.2.7 FCS_COP/1KeyedHash

Item	Data/Description
Test Assurance Activity	For each of the supported parameter sets, the evaluator shall compose 15 sets of test data. Each set shall consist of a key and message data. The evaluator shall have the TSF generate HMAC tags for these sets of test data. The resulting MAC tags shall be compared to the result of generating HMAC tags with the same key and message data using a known good implementation.
Test Output	This test is covered by CAVP certificate #A2933
Pass/Fail with Explanation	PASS. This test is covered by CAVP certificate #A2933

6.2.8 FIA_AFL.1 Test #1

Item	Data/Description
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	7 attempts • The evaluator configures the TOE to lock out the non-administrative account after 7 unsuccessful login attempts. • The evaluator attempts unsuccessful login attempts and lockout account. • The evaluator configures the TOE to re-enable locked out account after period of time. • The evaluator documents unsuccessful login attempts. 5 attempts • The evaluator configures the TOE to lock out the non-administrative account after 7 unsuccessful login attempts. • The evaluator attempts unsuccessful login attempts and lockout account.

	• The evaluator configures the TOE to re-enable locked out account after period of time. • The evaluator documents unsuccessful login attempts.
Expected Test Results	The TOE should not allow a successful login after 5 and 7 unsuccessful login attempts.
Pass/Fail with Explanation	The TOE successfully denies the evaluator access after using incorrect login information.
Result	Pass

6.2.9 FIA_AFL.1 Test #2a

Item	**Data/Description**
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).
Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A The control administrator action is not selected in the Security Target.

6.2.10 FIA_AFL.1 Test #2b

Item	Data**/Description**
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	• The evaluator defines a time period of 2 minutes for the user to be refused connection in the TOE. • The evaluator attempts to login to the TOE unsuccessfully 2 times. • The evaluator documents login attempts with log evidence.

	• The evaluator attempts to login to the TOE with valid credentials after the designated time period has elapsed. • The evaluator documents login attempts with log evidence.
Expected Test Results	The TOE should not allow a successful login after the user is locked out.
Pass/Fail with Explanation	The TOE allows a successful login after incorrect logins and the account being locked out.
Result	Pass

6.2.11 FIA_PMG_EXT.1 Test #1

Item	**Data/Description**
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	• The evaluator configures password management to be composed of the following criteria.
	  • The minimum password length shall be configurable to 15 characters.
	• The evaluator documents password management policy success with log evidence.
	• The evaluator attempts to create 3 users (good11, good22, good33) that meet the password requirements.
	  ○ Username good11 secret G00dpassword11!
	  ○ Username good22 secret G00dpassword22!
	  ○ Username: good33 secret G00dpassword33!
	• The evaluator tries to establish a TOE connection using all above 3 users that meet the password requirements.
	  ○ Connection attempt for user good11
	  ○ Connection attempt for user good22
	  ○ Connection attempt for user good33

Expected Test Results	The TOE should allow creation and successful authentication with the newly created users.
Pass/Fail with Explanation	The TOE allows successful connections by all 3 users after the evaluator configured the TOE with password restrictions.
Result	Pass

6.2.12 FIA_PMG_EXT.1 Test #2

Item	**Data/Description**

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	The evaluator attempts to create 3 users (bad4, bad5, bad6) that do not meet the password requirements. • Username bad11 secret BAD12345^&*() • Username bad22 secret 123$%^Bad • Username bad33 secret 1234567890bad
Expected Test Results	The TOE should not allow the creation of a password that does not have special characters, upper- and lower-case letters.
Pass/Fail with Explanation	The Toe does not allow new users to be created that do not meet the password requirements.
Result	Pass

6.2.13 FIA_UIA_EXT.1 Test #1

Item	**Data/Description**
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	Local • The evaluator configures local authentication. • The evaluator displays a connection attempt. • The evaluator displays an unsuccessful connection attempt. Remote • The evaluator configures remote authentication. • The evaluator displays a connection attempt. • The evaluator displays an unsuccessful connection attempt.
Expected Test Results	The TOE should allow a successful connection with correct login information. The TOE should not allow the evaluator to successfully authenticate with incorrect login information.
Pass/Fail with Explanation	The TOE allows a successful login for local authentication and remote authentication. The TOE will not allow a successful login to remote or local with incorrect credentials.

Result	Pass

6.2.14 FIA_UIA_EXT.1 Test #2

Item	Data/Description
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.
Pass/Fail with Explanation	This test is exercised in FTA_TAB.1
Result	Pass

6.2.15 FIA_UIA_EXT.1 Test #3

Item	Data/Description
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	Local • The evaluator attempts a connection showing the only option presented is a login prompt.
Expected Test Results	The TOE should always prompt for a login.
Pass/Fail with Explanation	The TOE only shows a login prompt for the evaluator for the local console and the remote interface.

Result	Pass

6.2.16 FIA_UIA_EXT.1 Test #4

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

6.2.17 FIA_UAU.7 Test #1

Item	Data/Description
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	Local • The evaluator attempts a connection to the local console. • The evaluator provides authentication logs showing the connection attempt.
Expected Test Results	The TOE should obscure the password information on the console authentication attempt.
Pass/Fail with Explanation	The TOE allows a successful local console login.
Result	Pass

6.2.18 FMT_MOF.1/ManualUpdate Test #1

Item	Data/Description
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	• The evaluator attempts a connection to the TOE. • The evaluator attempts to escalate privileges from a standard user.
Expected Test Results	The TOE should reject access to configuration mode and any update commands without the proper user privileges.
Pass/Fail with Explanation	The TOE does not allow the non-administrative user to escalate privileges.
Result	Pass

6.2.19 FMT_MOF.1/ManualUpdate Test #2

Item	Data/Description
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	This text has been exercised in FPT_TUD_EXT.1
Result	Pass

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

Item	Data/Description
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	• The evaluator attempts a connection to the TOE. • The evaluator attempts privilege escalation on the TOE. • The evaluator attempts to modify logging settings.

Expected Test Results	The TOE should not allow modification of settings without the proper permissions.
Pass/Fail with Explanation	The TOE does not allow configuration of the external audit log server as a standard user.
Result	Pass

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

Item	**Data/Description**
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	• The evaluator attempts a connection to the TOE. • The evaluator attempts privilege escalation on the TOE. • The evaluator attempts to modify logging settings. • The evaluator document evidence of the command attempts and the connection.
Expected Test Results	The modification of the logging settings to an external syslog server will be successful.
Pass/Fail with Explanation	The TOE allows a successful configuration to be created for an external audit log server.
Result	Pass

6.2.22 FMT_MOF.1/Services Test #1

Item	**Data/Description**
Test Assurance Activity	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to enable/disable this service/these services can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• The evaluator logs into the TOE as a non-administrative user. • The evaluator attempts to start a service on the TOE and verify the command is rejected.

	• The evaluator attempts to stop a service on the TOE and verify the command is rejected.
Expected Test Results	The TOE will not allow a service to start and stop without the proper permissions.
Pass/Fail with Explanation	The TOE does not successfully allow external audit logging service to be disabled.
Result	Pass

6.2.23 FMT_MOF.1/Services Test #2

Item	**Data/Description**
Test Assurance Activity	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
Test Steps	• The evaluator logs in to the TOE as an administrative user. • The evaluator attempts to start a service on the TOE and verify the command is accepted. • The evaluator attempts to stop a service on the TOE and verify the command is accepted.
Expected Test Results	The TOE should allow a service to be started since the user has the proper permissions to execute the command.
Pass/Fail with Explanation	The TOE successfully allows external audit logging to be disabled and enabled while authenticated as a Security Administrator.
Result	Pass

6.2.24 FMT_MTD.1/CryptoKeys Test #1

Item	**Data/Description**
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	• The evaluator authenticates as a non-administrative user. • The evaluator demonstrates the inability to provision cryptographic keys.

Expected Test Results	The TOE should not allow a non-administrative user to be able to provision cryptographic keys on the TOE.
Pass/Fail with Explanation	The TOE does not allow the non-administrative user to be able to provision cryptographic keys.
Result	Pass

6.2.25 FMT_MTD.1/CryptoKeys Test #2

Item	**Data/Description**
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	• The evaluator authenticates as an administrative user. • The evaluator demonstrates the ability to provision cryptographic keys.
Expected Test Results	The TOE should allow an administrative user to be able to provision cryptographic keys on the TOE.
Pass/Fail with Explanation	The TOE allows the administrative user to be able to provision cryptographic keys.
Result	Pass

6.2.26 FMT_MTD.1/CoreData

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

6.2.27 FMT_SMF.1 Test #1

Item	**Data/Description**
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 Output	• *Ability to administer the TOE locally and remotely;* *Exercised in FTA_SSL_EXT.1.1 test 1* • *Ability to configure the access banner;* Exercised in FTA_TAB.1 • *Ability to configure the session inactivity time before session termination or locking;* Exercised in FTA_SSL_EXT.1.1 test 1

	• *Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates;* *Exercised in FPT_TUD_EXT.1* • *Ability to configure the authentication failure parameters for FIA_AFL.1;* *Exercised in FIA_AFL.1 test 1 and 2b* ○ *Ability to start and stop services;* *Exercised in FMT_MOF.1/Services test 1 and 2* ○ *Ability to modify the behaviour of the transmission of audit data to an external IT entity;* ○ *Exercised in FAU_STG_EXT.1 test 1.* ○ *Ability to manage the cryptographic keys;* *Exercised in FIA_X509_EXT.1.1/Rev test 1a, 1b, and 2* ○ *Ability to configure the cryptographic functionality;* Excercised in FIA_X509_EXT.1.1/Rev test 1a and 1b ○ *Ability to set the time which is used for time-stamps;* Exercised in FPT_STM.1 ○ *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;* *Exercised in FIA_X509_EXT.1.1/Rev tests 1a, 1b and 3* ○ *Ability to import X.509v3 certificates to the TOE's trust store;* *Exercised in FIA_X509_EXT.1.1/Rev tests 8a, 8b, and 8c* ○ *Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);* *Exercised* in FAU_STG_EXT.1 test 1 ○ *No other capabilities].*
Pass/Fail with Explanation	The test was exercised in the above assurance activities.
Result	Pass

6.2.28 FMT_SMR.2 Test #1

Item	Data/Description
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	Test has been exercised in FIA_AFL.1 test 1 for local administration. Test has been exercised in FMT_MOF.1/Functions (1) test 2 for remote administration.
Result	Pass

6.2.29 FTA_SSL.3 Test #1

Item	**Data/Description**
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	1 minute • The evaluator configures a remote timeout period of 1 minute on administrative sessions from the local console. • The evaluator logs into the TOE using the web interface. • The evaluator verifies that a log was created for configuring the timeout period. • The evaluator verifies that a log was created for inactivity timeout. 3 minutes • The evaluator configures a remote timeout period of 3 minutes on administrative sessions from the local console. • The evaluator logs into the TOE using the web interface. • The evaluator verifies that a log was created for configuring the timeout period. • The evaluator verifies that a log was created for inactivity timeout.
Expected Test Results	The TOE should allow the evaluator to successfully login and them timeout the session.
Pass/Fail with Explanation	The TOE successfully allows a login to be timed out after being configured.
Result	Pass

6.2.30 FTA_SSL.4 Test #1

Item	**Data/Description**
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	• The evaluator logs in to the local interface of the TOE. • The evaluator logs out of the local interface of the TOE.
Expected Test Results	The TOE should allow a successful login and termination of the session on the local interface.

Pass/Fail with Explanation	The TOE successfully allows a termination of the session.
Result	Pass

6.2.31 FTA_SSL.4 Test #2

Item	Data/Description
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	• The evaluator logs in to the remote interface of the TOE. • The evaluator logs out of the remote interface of the TOE. • The evaluator shows packet capture evidence of the successful connection.
Expected Test Results	The TOE should allow a successful login and termination of the session on the local interface.
Pass/Fail with Explanation	The TOE allows a successful login and logout.
Result	Pass

6.2.32 FTA_SSL_EXT.1.1 Test #1

Item	Data/Description
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	Local Login (2 minutes) • The evaluator configures a local time out period of 2 minutes on administrative sessions from the local console. • The evaluator logs in to the TOE using the local interface. • The evaluator verifies that a log was created for configuring the timeout period. • The evaluator verifies that a log was created for inactivity timeout. Local Login (4 minutes) • The evaluator configures a local time out period of 2 minutes on administrative sessions from the local console. • The evaluator logs in to the TOE using the local interface. • The evaluator verifies that a log was created for configuring the timeout period. • The evaluator verifies that a log was created for inactivity timeout.
Expected Test Results	The user sessions will be successfully terminated once the TOE is configured properly.

Pass/Fail with Explanation	The TOE allows a successful login and logs out the user after the configured timeout.
Result	Pass

6.2.33 FTA_TAB.1 Test #1

Item	Data/Description
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	• The evaluator configures the access banners on the TOE. • The evaluator authenticates to the TOE using the web interface.
Expected Test Results	The TOE should react as configured displaying the newly configured login banner.
Pass/Fail with Explanation	The TOE successfully displays the login banner as configured.
Result	Pass

6.2.34 FTP_TRP.1/Admin Test #1

Item	Data/Description
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	• The evaluator attempts to establish a connection with the TOE. • The evaluator verifies that the session was established via log.
Expected Test Results	The TOE should allow a successful remote administration connection.
Pass/Fail with Explanation	The TOE successfully initiates a remote access connection.
Result	Pass

6.2.35 FTP_TRP.1/Admin Test #2

Item	Data/Description
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Test Steps	• The evaluator attempts a connection to the TOE. • The evaluator documents the connection attempt.

Expected Test Results	The TOE should allow encrypted traffic to flow.
Pass/Fail with Explanation	The TOE successfully allows encrypted traffic to be transmitted.
Result	Pass

6.2.36 FCS_HTTPS_EXT.1 Test #3

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	Test is performed as part of FIA_X509_EXT.1/Rev.
Result	Pass

6.3 Test Cases (TLSC)

6.3.1 FCS_TLSC_EXT.1.1 Test #1

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T1
Objective	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Note	FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246), ~~*TLS 1.1 (RFC 4346)*~~] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [• TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC5246

	• TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 *] and no other ciphersuites.*
Test Flow	• TLS_RSA_WITH_AES_128_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_256_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_128_CBC_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture.

	• TLS_RSA_WITH_AES_256_CBC_ SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_128_GCM_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_256_GCM_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

	• The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture.
Pass/Fail Explanation	The TOE successfully allows connection with all of the selected cipher suites. This meets testing requirements.
Result	Pass

6.3.2 FCS_TLSC_EXT.1.1 Test #2

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T2
Objective	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Flow	• The evaluator displays a successful connection. • The evaluator shows packet capture evidence. • The evaluator displays an unsuccessful connection. • The evaluator shows packet capture evidence.
Pass/Fail Explanation	The TOE successfully stops a connection with a certificate that does not have the extendedKeyUsage field but does normally allow a connection with a certificate that has the extendedKeyUsage field.
Result	Pass

6.3.3 FCS_TLSC_EXT.1.1 Test #3

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T3
Objective	The evaluator shall send a server certificate in the TLS connection that 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 Flow	• The evaluator attempts a connection with an ECDSA cipher and RSA certificate. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE does not allow traffic to pass as the cipher and the cipher in the certificate do not match.
Result	Pass

6.3.4 FCS_TLSC_EXT.1.1 Test #4a

Item	**Data/Description**

Test ID	FCS_TLSC_EXT.1.1_T4a
Objective	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Test Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE does not allow a successful handshake with a NULL cipher suite specified in the connection.
Result	Pass

6.3.5 FCS_TLSC_EXT.1.1 Test #4b

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T4b
Objective	The evaluator shall modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Test Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE does not allow an unsupported cipher suite to create a connection.
Result	Pass

6.3.6 FCS_TLSC_EXT.1.1 Test #4c

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T4c
Objective	[conditional]: If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension** the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.
Test Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE does not allow a successful connection with an unsupported EC curve group.
Result	Pass

6.3.7 FCS_TLSC_EXT.1.1 Test #5a

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5a
Objective	The evaluator shall change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE successfully denies the connection if the TLS version is unsupported.
Result	Pass

6.3.8 FCS_TLSC_EXT.1.1 Test #5b

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5b
Objective	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Flow	• The evaluator attempts a connection. • The evaluator shows the log evidence of the connection attempt. • The evaluator shows packet capture evidence of the connection attempt.
Pass/Fail Explanation	The TOE did not connect to the tool due to a modified server key exchange message.
Result	Pass

6.3.9 FCS_TLSC_EXT.1.1 Test #6a

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.1_T5b
Objective	The evaluator shall modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
Test Flow	• The evaluator uses acumen testing tool to modify a byte in the server finished handshake message. • The evaluator attempts a connection. • The evaluator shows the log evidence of the connection attempt. • The evaluator shows packet capture evidence of the connection attempt.

Pass/Fail Explanation	The TOE did not connect when there was a modification done to the server Finished Message.
Result	Pass

6.3.10 FCS_TLSC_EXT.1.1 Test #6b

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T6b
Objective	The evaluator shall send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows.
Test Flow	• Execute Acumen test tool to send garble message after the server issues the ChangeCipherSpec message. • Gather test log and capture packets using Wireshark. • Verify that TLS connection fails and packets fail to negotiate.
Pass/Fail Explanation	The TOE does not connect after receiving a garbled message after the change cipher spec message.
Result	Pass

6.3.11 FCS_TLSC_EXT.1.1 Test #6c

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.1_T6c
Objective	The evaluator shall 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 Flow	• The evaluator uses acumen testing tool to modify a byte in the server finished handshake message. • The evaluator shows the log evidence of the connection attempt. • The evaluator shows packet capture evidence of the connection attempt.
Pass/Fail Explanation	The TOE successfully declines the handshake with the modified nonce.
Result	Pass

6.3.12 FCS_TLSC_EXT.1.2 Test #1

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T1

Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.
Test Flow	• The evaluator shows the common name of the certificate. • The evaluator shows the reference identifier of the TOE. • The evaluator attempts a connection. • The evaluator shows the connection attempt with logs. • The evaluator shows the connection attempt with packet capture evidence.
Pass/Fail Explanation	The TOE did not connect due to the missing SAN extension.
Result	Pass

6.3.13 FCS_TLSC_EXT.1.2 Test #2

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T1
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.
Test Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE successfully denies the connection due to an incorrect SAN extension.
Result	Pass

6.3.14 FCS_TLSC_EXT.1.2 Test #3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T3
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
Test Flow	N/A The TOE requires the presence of the SAN extension.
Pass/Fail Explanation	N/A The TOE requires the presence of the SAN extension.
Result	N/A

6.3.15 FCS_TLSC_EXT.1.2 Test #4

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T4
Objective	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).
Test Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE successfully allows a connection with the correct SAN extension.
Result	Pass

6.3.16 FCS_TLSC_EXT.1.2 Test #5(1)

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T5(1)
Objective	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 Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt
Pass/Fail Explanation	The TOE declines the connection with the certificate that contains a wildcard that is not in the left most label of the reference identifier.
Result	Pass

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

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T5(2)(a)
Objective	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 Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.
Pass/Fail Explanation	The TOE allows a successful connection using a wildcard in the correct location in the SAN.
Result	Pass

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

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T5(2)(b)

Objective	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 Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt
Pass/Fail Explanation	The TOE does not allow a successful connection with the misconfigured reference identifier.
Result	Pass

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

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.2_T5(2)(c)
Objective	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 Flow	• The evaluator attempts a connection. • The evaluator displays the connection log of the attempt. • The evaluator displays packet capture evidence of the attempt.

Pass/Fail Explanation	The TOE does not allow a successful connection with the extra arguments in the reference identifier field.
Result	Pass

6.3.20 FCS_TLSC_EXT.1.2 Test #6

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.2_T6
Objective	Objective: The objective of this test is to ensure the TOE is able to differentiate between IP address identifiers that are not allowed to contain wildcards and other types of identifiers that may contain wildcards. Test 6:[conditional] If IP addresses identifiers are supported in the SAN or CN, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with an wildcard asterisk (*) (e.g. CN=192*.168.0.1.* when connecting to 192.168.0.1.20, 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). This negative test corresponds to the following section of the Application Note 64/105: "The exception being, the use of wildcards is not supported when using IP address as the reference identifier." **TD0790 has been applied**
Test Flow	N/A. The TOE does not support IP address identifiers in the SAN or CN field.
Pass/Fail Explanation	N/A. The TOE does not support IP address identifiers in the SAN or CN field.
Result	N/A

6.3.21 FCS_TLSC_EXT.1.2 Test #7a

Item	Data
Test ID	FCS_TLSC_EXT.1.2_T7a
Objective	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.

Test Flow	N/A RFC 6125 is claimed.
Pass/Fail with Explanation	N/A RFC 6125 is claimed.
Result	N/A

6.3.22 FCS_TLSC_EXT.1.2 Test #7b

Item	Data
Test ID	FCS_TLSC_EXT.1.2_T7b
Objective	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.
Test Flow	N/A RFC 6125 is claimed.
Pass/Fail with Explanation	N/A RFC 6125 is claimed.
Result	N/A

6.3.23 FCS_TLSC_EXT.1.2 Test #7c

Item	Data
Test ID	FCS_TLSC_EXT.1.2_T7c
Objective	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.
Test Flow	N/A RFC 6125 is claimed.
Pass/Fail with Explanation	N/A RFC 6125 is claimed.

Result	N/A

6.3.24 FCS_TLSC_EXT.1.2 Test #7d

Item	**Data**
Test ID	FCS_TLSC_EXT.1.2_T7d
Objective	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.)
Test Flow	N/A RFC 6125 is claimed.
Pass/Fail with Explanation	N/A RFC 6125 is claimed.
Result	**N/A**

6.3.25 FCS_TLSC_EXT.1.3 Test #1

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.3_T1
Objective	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Pass/Fail Explanation	This test has been exercised in FIA_X509_EXT.1.1/Rev Test 1a.
Result	Pass

6.3.26 FCS_TLSC_EXT.1.3 Test #2

Item	**Data/Description**
Test ID	FCS_TLSC_EXT.1.3_T2
Objective	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.

Test Flow	Pass, this test has been exercised in FIA_X509_EXT.1.1 tests 1a, 1b, & 2, FCS_TLSC_EXT.1.2 test 1, FCS_TLSC_EXT.1.2 test 2, and FIA_X509_EXT.2 test 1.
Pass/Fail Explanation	Pass, this test has been exercised in FIA_X509_EXT.1.1 tests 1a, 1b, & 2, FCS_TLSC_EXT.1.2 test 1, FCS_TLSC_EXT.1.2 test 2, and FIA_X509_EXT.2 test 1.
Result	Pass

6.3.27 FCS_TLSC_EXT.1.3 Test #3

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.3_T3
Objective	The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. **If any override mechanism is defined for failed certificate validation**, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
Test Flow	N/A. No override mechanisms are defined for failed certificate validation.
Pass/Fail Explanation	N/A. No override mechanisms are defined for failed certificate validation.
Result	N/A

6.3.28 FCS_TLSC_EXT.1.4 Test #1

Item	Data/Description
Test ID	FCS_TLSC_EXT.1.4_T1
Objective	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.
Test Flow	• secp256r1 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • secp384r1 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • secp521r1 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture.
Pass/Fail Explanation	The TOE successfully allows connection using all 3 specified EC extensions.

Result	Pass

6.4 Test Cases (TLSS)

6.4.1 FCS_TLSS_EXT.1.1 Test #1

Item	Data/Description
Test ID	FCS_TLSS_EXT.1.1_T1
Objective	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).
Note	**FCS_TLSS_EXT.1.1** The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites: [• TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5289 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC5289 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC5289 *] and no other ciphersuites.*
Test Flow	• TLS_RSA_WITH_AES_128_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture.

	• TLS_RSA_WITH_AES_256_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_128_CBC_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_256_CBC_ SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_128_GCM_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_RSA_WITH_AES_256_GCM_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

	• The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture. • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • The evaluator verifies the connection with logs from the TOE. • The evaluator verifies the connection with a packet capture.
Pass/Fail Explanation	The TOE successfully allows connection with all of the selected cipher suites. This meets testing requirements.
Result	Pass

6.4.2 FCS_TLSS_EXT.1.1 Test #2

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.1_T2
Objective	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 Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE.

	NULL_WITH_NULL_NULL RSA_WITH_3DES_EDE_CBC_S • The evaluator verifies that the connection fails with the non-supported ciphersuite. • The evaluator verifies using packet capture.
Pass/Fail Explanation	The TOE did not successfully connect with an unclaimed ciphersuite or a NULL ciphersuite. This meets testing requirements.
Result	Pass

6.4.3 FCS_TLSS_EXT.1.1 Test #3a

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.1_T3a
Objective	Modify a byte in the Client Finished handshake message, and verify that the server rejects the connection and does not send any application data.
Test Flow	• The evaluator executes the Acumen tool which modifies a byte in the Client Finished handshake message. • The evaluator gathers packet captures. • The evaluator verifies that the server denies TLS connection.
Pass/Fail Explanation	The TOE rejects the connection with a modified byte on Client Finished handshake message.
Result	Pass

6.4.4 FCS_TLSS_EXT.1.1 Test #3b

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.1_T3b
Objective	(Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.) The evaluator shall use one of the claimed 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 Flow	• The evaluator executes the Acumen test tool to establish TLS connection with a supported cipher-suite. • The evaluator verifies TLS connection successfully established. • The evaluator captures packets to verify finished message is encrypted.
Pass/Fail Explanation	The TOE displays a number other than 14 in the Finished message, signifying that the traffic is encrypted.
Result	Pass

6.4.5 FCS_TLSS_EXT.1.2 Test #1

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.2_T1
Objective	The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.
Test Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE and verify the connections fail for non-supported TLS versions. • The evaluator verifies the connection fails with SSL v2.0. • The evaluator verifies the connection with packet capture. • The evaluator verifies the connection fails with SSL v3.0. • The evaluator verifies the connection with packet capture. • The evaluator verifies the connection fails with TLS v1.0. • The evaluator verifies the connection with packet capture. • The evaluator verifies the connection fails with TLS v1.1. • The evaluator verifies the connection with packet capture.
Pass/Fail Explanation	The TOE does not establish a connection when non-supported protocol versions are used. This meets testing requirements.
Result	Pass

6.4.6 FCS_TLSS_EXT.1.3 Test #1a

Item	Data/Description
Test ID	FCS_TLSS_EXT.1.3_T1a
Objective	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 Flow	• The evaluator executes the Acumen testing tool to establish TLS connection using the following EC curves (secp256r1, secp384r1, and secp521r1). • The evaluator captures TLS packets. • The evaluator verifies that TLS connections successfully establish using supported EC curves.
Pass/Fail Explanation	TOE successfully establishes TLS connections using supported EC curves SECP256R1, SECP384R1, and SECP521R1.
Result	Pass

6.4.7 FCS_TLSS_EXT.1.3 Test #1b

Item	Data/Description
Test ID	FCS_TLSS_EXT.1.3_T1b
Objective	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 Flow	• The evaluator executes the Acumen test tool to initiate TLS connection to the TOE using unsupported EC curve SECP256K1. • The evaluator displays TOE logs. • The evaluator verifies TLS connection fails and server does not reply with Server Hello message.
Pass/Fail Explanation	TOE rejects TLS connection if client presented with Client Hello message with unsupported EC curve SECP256K1.
Result	Pass

6.4.8 FCS_TLSS_EXT.1.3 Test #2

Item	Data/Description
Test ID	FCS_TLSS_EXT.1.3_T1b

Objective	If **DHE ciphersuites** are supported, the evaluator shall repeat the following test for each supported parameter size. If any configuration is necessary, the evaluator shall configure the TOE to use a supported Diffie-Hellman parameter size. The evaluator shall attempt a connection using a supported DHE ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a Server Key Exchange Message where p Length is consistent with the message are the ones configured Diffie-Hellman parameter size(s).
Test Flow	N/A
Pass/Fail Explanation	N/A
Result	N/A

6.4.9 FCS_TLSS_EXT.1.3 Test #3

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.3_T3
Objective	If **RSA key establishment ciphersuites** are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.
Test Flow	• The evaluator displays the certificate on the TOE using RSA-2048 key. • The evaluator initiates TLS connection using certificate with RSA-2048 key. • The evaluator displays a successful connection using the RSA-2048 key. • The evaluator repeats test steps above with certificates that support RSA-3072 and RSA-4096 keys. • The evaluator initiates TLS connection using certificate with RSA-4096 key. • The evaluator displays a successful connection using the RSA-4096 key.
Pass/Fail Explanation	TOE successfully establishes TLS connections using supported RSA keys – RSA-2048, RSA-3072, and RSA-4096.
Result	Pass

6.4.10 FCS_TLSS_EXT.1.4 Test #1

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.4_T2a
Objective	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: a. implicitly rejects the SessionID by sending a ServerHello containing a different SessionID and by performing a full handshake (as shown in Figure 1 of RFC 4346 or RFC 5246), or terminates the connection in some way that prevents the flow of application data.
Test Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE and verify that the connection succeeds. • The evaluator displays connection logs from the TOE. • The evaluator displays the connection success in a packet capture.
Pass/Fail Explanation	N/A. The TOE does support session resumption based on session IDs and session tickets.
Result	N/A

6.4.11 FCS_TLSS_EXT.1.4 Test #2a

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.4_T2a
Objective	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).
Test Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE and verify that the connection succeeds. • The evaluator displays connection logs from the TOE. • The evaluator displays the connection success in a packet capture.
Pass/Fail Explanation	The TOE successfully resumes the second session from the original session ID.

Result	Pass

6.4.12 FCS_TLSS_EXT.1.4 Test #2b

Item	Data/Description
Test ID	FCS_TLSS_EXT.1.4_T2b
Objective	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.
Test Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE and verify that the connection succeeds. • The evaluator displays connection logs from the TOE. • The evaluator displays the connection success in a packet capture.
Pass/Fail Explanation	The TOE sends a new session ID when an unencrypted fatal Alert message is sent before the ChangeCipherSpec message.
Result	Pass

6.4.13 FCS_TLSS_EXT.1.4 Test #3a

Item	Data/Description
Test ID	FCS_TLSS_EXT.1.4_T3a
Objective	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.**

Test Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE and verify that the connection succeeds. • The evaluator displays connection logs from the TOE. • The evaluator displays the connection success in a packet capture.
Pass/Fail Explanation	The TOE reuses the session ticket to allow a session to be resumed.
Result	Pass

6.4.14 FCS_TLSS_EXT.1.4 Test #3b

Item	**Data/Description**
Test ID	FCS_TLSS_EXT.1.4_T3b
Objective	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.
Test Flow	• The evaluator uses the Acumen-tlss tool to initiate a connection to the TOE and verify that the connection succeeds. • The evaluator displays connection logs from the TOE. • The evaluator displays the connection success in a packet capture.
Pass/Fail Explanation	The TOE allows the session to be resumed after sending a modified session ticket.
Result	Pass

6.5 Test Cases (Update)

6.5.1 FPT_TST_EXT.1 Test #1

Item	**Data/Description**
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. For distributed TOEs the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.
Test Steps	The evaluator displays the output of the self-test application provided in the local console. The evaluator displays the GUI login interface of the TOE to indicate that cryptographic self-tests were passed
Expected Test Results	The TOE should display identical sha256 checksums and the self-test application output should all read ok. The TOE should also successfully initialize once the self-tests are passed.
Pass/Fail with Explanation	The TOE can successfully verify the integrity of the operating system and the HYCU application. The TOE was also successfully initialized after passing the self-tests .
Result	Pass

6.5.2 FPT_TUD_EXT.1 Test #1

Item	**Data/Description**
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	• The evaluator displays a hash of the TOE image from the vendor. • The evaluator displays a hash of the TOE image taken by the evaluator. • The evaluator attempts loading of the TOE image.
Expected Test Results	The evaluator should successfully be able to load TOE image to the virtual host.
Pass/Fail with Explanation	The TOE successfully allows an update of the TOE image.
Result	Pass

6.5.3 FPT_TUD_EXT.1 Test #2 (a)

Item	**Data/Description**

Test Assurance Activity	Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 1) A modified version (e.g. using a hex editor) of a legitimately signed update If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A The TOE only supports published hash for verification.

6.5.4 FPT_TUD_EXT.1 Test #2 (b)

Item	Data/Description
Test Assurance Activity	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 2) An image that has not been signed If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps	N/A
Expected Test Results	N/A

Pass/Fail with Explanation	N/A The TOE only supports published hash for verification.

6.5.5 FPT_TUD_EXT.1 Test #2 (c)

Item	Data/Description
Test Assurance Activity	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature) If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A The TOE only supports published hash for verification.

6.5.6 FPT_TUD_EXT.1 Test #3 (a)

Item	Data/Description
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 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.
Expected Test Results	N/A. The TOE does not verify the hash value of the update image.
Pass/Fail with Explanation	N/A. The TOE does not verify the hash value of the update image.

6.5.7 FPT_TUD_EXT.1 Test #3 (b)

Item	Data/Description
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 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.
Test Steps	N/A
Expected Test Results	N/A
Pass/Fail with Explanation	N/A. The TOE does not verify the hash value of the update image.

6.6 Test Cases (X509-Rev)

6.6.1 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data/Description
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	• The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence.
Expected Test Results	The TOE should successfully allow all of the certificates to be processed.
Pass/Fail with Explanation	The TOE allows a successful connection using the chain of certificates.
Result	Pass

6.6.2 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data/Description
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	• The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE.

	• The evaluator shows the connection attempt with packet capture evidence.
Expected Test Results	The TOE should reject the connection as the chain of certificates is broken.
Pass/Fail with Explanation	The TOE does not successfully allow a connection with a broken certificate chain.
Result	Pass

6.6.3 FIA_X509_EXT.1.1/Rev Test #2

Item	Data/Description
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	• The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence.
Expected Test Results	The TOE should reject the connection attempt with an expired certificate.
Pass/Fail with Explanation	The TOE successfully rejects the connection with an expired certificate.
Result	Pass

6.6.4 FIA_X509_EXT.1.1/Rev Test #3

Item	Data/Description
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	OCSP Intermediate Valid

	• The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence. Intermediate Revoked • The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence. Leaf Valid • The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence. Leaf Revoked • The evaluator shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence.
Expected Test Results	The TOE should successfully check for certificate revocation.
Pass/Fail with Explanation	The TOE successfully checks for certificate revocation with a valid chain of certificates.
Result	Pass

6.6.5 FIA_X509_EXT.1.1/Rev Test #4

Item	**Data/Description**
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 shows the valid chain of certificates on the TOE. • The evaluator attempts a connection to the TOE. • The evaluator shows the connection attempt with packet capture evidence.
Expected Test Results	The TOE should reject the connection with the missing OCSP signing flag.
Pass/Fail with Explanation	The TOE successfully rejects the connection as the OCSP responder certificate is missing the OCSP signing flag.
Result	Pass

6.6.6 FIA_X509_EXT.1.1/Rev Test #5

Item	**Data/Description**

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	• The evaluator uses acumen-tlsc tool to attempt a connection. • The evaluator displays log evidence of the connection attempt. • The evaluator displays packet capture evidence of the connection attempt.
Expected Test Results	The TOE does not connect due to a modified certificate.
Pass/Fail with Explanation	The TOE did not complete a successful connection after detecting the modified certificate.
Result	Pass

6.6.7 FIA_X509_EXT.1.1/Rev Test #6

Item	Data/Description
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	• The evaluator uses acumen-tlsc tool to attempt a connection. • The evaluator displays log evidence of the connection attempt. • The evaluator displays packet capture evidence of the connection attempt.
Expected Test Results	The TOE does not connect due to a modified certificate
Pass/Fail with Explanation	The TOE did not connect when a modified certificate was detected
Result	Pass

6.6.8 FIA_X509_EXT.1.1/Rev Test #7

Item	Data/Description
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	• The evaluator uses the acumen-tlsc tool to attempt a connection. • The evaluator displays log evidence of the connection attempt. • The evaluator displays packet capture evidence of the connection attempt.
Expected Test Results	The TOE will not connect due to a modified certificate.
Pass/Fail with Explanation	The TOE did not connect when a modified certificate was detected
Result	Pass

6.6.9 FIA_X509_EXT.1.1/Rev Test #8a

Item	Data/Description
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	• The evaluator shows the RootCA on the TOE highlighting the absence of the IntermediateCA. • The evaluator attempts a connection to the TOE. • The evaluator displays packet capture evidence.
Expected Test Results	The TOE should allow the certificates to authenticate the connection successfully.
Pass/Fail with Explanation	The TOE allows the TOE to process all of the certificates allowing a successful connection.
Result	Pass

6.6.10 FIA_X509_EXT.1.1/Rev Test #8b

Item	Data/Description
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	• The evaluator presents an Intermediate certificate that uses an explicit format version of the elliptic curve parameter in the public key information field and is signed by the trusted EC root CA. • The evaluator presents the Root and IntermediateCA to the TOE. • The evaluator confirms that the TOE treats the certificate as invalid. • The evaluator displays packet capture evidence.
Expected Test Results	The TOE should reject the validation since the Elliptic Curve parameters in the public key field are invalid.
Pass/Fail with Explanation	The TOE successfully declines the connection as the certificate is treated as invalid.
Result	Pass

6.6.11 FIA_X509_EXT.1.1/Rev Test #8c

Item	Data/Description
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	• The evaluator presents an Intermediate certificate that uses an explicit format version of the elliptic curve parameter in the public key information field and is signed by the trusted EC root CA. • The evaluator presents the Root and IntermediateCA to the TOE. • The evaluator confirms that the TOE treats the certificate as invalid.
Expected Test Results	The TOE should reject the validation of the IntermediateCA
Pass/Fail with Explanation	The TOE successfully declines loading of the Intermediate certificate

Result	Pass

6.6.12 FIA_X509_EXT.1.2/Rev Test #1

Item	Data/Description
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) (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	• The evaluator shows the valid chain of certificates on the TOE. • The evaluator shows the missing BasicConstraints section of the IntermediateCA. • The evaluator shows the evidence of the IntermediateCA being loaded to the TOE.
Expected Test Results	The TOE should reject validation of the IntermediateCA as it is missing the BasicContstraints section.
Pass/Fail with Explanation	The TOE successfully rejects the validation of the IntermediateCA.
Result	Pass

6.6.13 FIA_X509_EXT.1.2/Rev Test #2

Item	Data/Description
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	• The evaluator shows the valid chain of certificates on the TOE. • The evaluator shows the BasicConstraints section of the IntermediateCA set to false. • The evaluator shows the evidence of the IntermediateCA being loaded to the TOE.
Expected Test Results	The TOE should reject validation of the IntermediateCA as the BasicConstraints section is set to false.
Pass/Fail with Explanation	The TOE successfully rejects validation of the IntermediateCA.
Result	Pass

6.6.14 FIA_X509_EXT.2 Test #1

Item	Data/Description
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	• The evaluator attempts a connection where the certificate reaches out to a non-TOE IT entity. • The evaluator demonstrates evidence that the certificate was invalidated, and the connection fails.
Expected Test Results	The TOE does not allow a certificate to be validated when the OCSP responder is offline
Pass/Fail with Explanation	The TOE does not allow a certificate to be validated when the OCSP responder is offline.

Result	Pass

6.6.15 FIA_X509_EXT.3 Test #1

Item	Data/Description
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	• The evaluator generates a certificate request. • The evaluator shows evidence of the formatting of the generated certificate request.
Expected Test Results	The TOE should successfully allow a certificate request to be generated.
Pass/Fail with Explanation	The TOE successfully creates a certificate request in the proper format.
Result	Pass

6.6.16 FIA_X509_EXT.3 Test #2

Item	Data/Description
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	• The evaluator attempts a connection with a missing Intermediate CA. • The evaluator shows packet capture evidence of the connection attempt. • The evaluator attempts a connection with the intermediate CA loaded. • The evaluator shows packet capture evidence of the connection attempt.
Expected Test Results	The TOE should not allow successful validation due to an incomplete cert path. The evaluator will then demonstrate successful validation with a root and intermediate CA.
Pass/Fail with Explanation	The TOE does not allow importing a certificate for a for a certificate signing request if the CA chain is not complete. The TOE does allow successfully importing a correctly formed certificate chain.
Result	Pass

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 available to security administrators who have a valid purchase of the TOE. 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 'Evaluated Configuration' of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are: • Lenovo ThinkSystem SR630, Xeon Silver 4208 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 'Scope of the Evaluation' 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 'Evaluated Configuration' of the AGD. The evaluator found that these sections describe how the Operational Environment must meet: **COMPONENT** / **DESCRIPTION** Lenovo ThinkSystem SR630, Xeon Silver 4208 — TOE Hardware platform VMware ESXi 7.0 — Hypervisor

	VMware vCenter 7.0	Virtualization management
	LDAP/S server	Remote authentication
	SMTP/S server	Notifications
	HTTPS Webhooks	Auditing server
	DNS server	Name resolution
	Administrator Workstation	Management of the TOE
	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 section labeled 'Evaluated configuration' in the guidance documentation describes each of the devices in the operating environment and the supported platforms, including,

COMPONENT	DESCRIPTION
Lenovo ThinkSystem SR630, Xeon Silver 4208	TOE Hardware platform
VMware ESXi 7.0	Hypervisor
VMware vCenter 7.0	Virtualization management
LDAP/S server	Remote authentication
SMTP/S server	Notifications
HTTPS Webhooks	Auditing server
DNS server	Name resolution
Administrator Workstation	Management of the TOE

	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, • Enabling CC-compliant mode • Start and stop services • Update the TOE • Modify the behavior of the transmission of audit data to an external IT entity

	• Manage the cryptographic keys • Configure the cryptographic functionality • Manage the TOE's trust store and designate X509.v3 certificates as trust anchors. • Import/export/generate X.509v3 certificates to the TOE's trust store. • Set the time which is used for time-stamps (console only) • Setting minimum password length in the console • Running self-test on-demand • Configuring access banners • Ability to configure the session inactivity time before session termination or locking. 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. Section 18 titled 'Passwords on HYCU' were used to determine the verdict of this work unit. The AGD describes configuring the password via command line interface. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

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

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

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

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

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

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.

Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement.
	
	Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.
	
	• http://www.hycu.com
	• http://nvd.nist.gov/
	• http://www.us-cert.gov
	• http://www.securityfocus.com/
	• https://www.cvedetails.com/
	• www.exploitsearch.net
	• www.securiteam.com
	• http://nessus.org/plugins/index.php?view=search
	• http://www.zerodayinitiative.com/advisories
	• https://www.exploit-db.com
	• https://www.rapid7.com/db/vulnerabilities
	
	The evaluator performed the public domain vulnerability searches using the following key words. The vulnerability searches were performed on August 21st, 2023, September 21st, 2023, September 26th, 2023, October 25th 2023, December 20th 2023, and a final search on January 10th 2024.
	
	• HYCU for Enterprise Clouds
	• Lenovo ThinkSystem SR630, Xeon Silver 4208
	• HYCU Java Cryptographic Library
	• Keywords/Libraries/Components: Linux Kernel 4.18
	  ○ HYCU Enterprise for Cloud
	  ○ Bc-fips 1.0.2.1
	  ○ Bcpkix-fipx 1.0.5
	  ○ Bctls-fips-1.0.11.2
	  ○ Rocky Linux 8.6
	  ○ OpenSSL 1.1.1k
	  ○ java-1.8.0-openjdk-1.8.0.332.b09-2.el8_6
	  ○ X.509v3
	  ○ TLSv1.2
	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 Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0527: Updated to Certificate Revocation Testing (FIA_X509_EXT.1)	Y	
TD0528: NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	N	NTP is not included in the TOE.
TD0536: NIT Technical Decision for Update Verification Inconsistency	Y	
TD0537: NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	Y	
TD0546: NIT Technical Decision for DTLS – clarification of Application Note 63	N	DTLS is not being claimed.
TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Y	
TD0555: NIT Technical Decision for RFC Reference incorrect in TLSS Test	Y	
TD0556: NIT Technical Decisions for RFC 5077 question	Y	
TD0563: NIT Technical Decision for Clarification of audit date information	Y	
TD0564: NIT Technical Decision for Vulnerability Analysis Search Criteria	Y	
TD0569: NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	Y	
TD0570: NIT Technical Decision for Clarification about FIA_AFL.1	Y	
TD0571: NIT Technical Decision for Guidance on how to handle FIA_AFL.1	Y	
TD0572: NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Y	
TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Y	

TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Y	
TD0591: NIT Technical Decision for Virtual TOEs and hypervisors	Y	
TD0592: NIT Technical Decision for Local Storage of Audit Records	Y	
TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server	N	FCS_SSHS_EXT is not being claimed.
TD0632: NIT Technical Decision for Consistency with Time Data for vNDs	N	TOE does not obtain time from the underlying virtualization time
TD0633: NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	N	FCS_IPSEC is not being claimed
TD0634: NIT Technical Decision for Clarification required for testing IPv6	N	TOE does not support IP address identifiers in the SAN or CN
TD0635: NIT Technical Decision for TLS Server and Key Agreement Parameters	Y	
TD0636: NIT Technical Decision for Clarification of Public Key User Authentication for SSH	N	FCS_SSHC_EXT is not being claimed.
TD 0638: Technical Decision for Key Pair Generation for Authentication	Y	
TD 0639: NIT Technical Decision for Clarification for NTP MAC Keys	N	NTP is not included in the TOE.
TD 0670: NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Y	
TD0738: NIT Technical Decision for Link to Allowed-With List	Y	
TD0790: NIT Technical Decision: Clarification Required for testing IPv6	Y	
TD0792: NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	Y	

9 CAVP Algorithm Certificate Details

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	HYCU Java Cryptographic Library	RSA KeyGen	#A2933
	ECC schemes using "NIST curves" [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	HYCU Java Cryptographic Library	ECDSA KeyGen	#A2933
FCS_CKM.2	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"	HYCU Java Cryptographic Library	None: CCTL tested as per the PP/SD Evaluation Activities	Lab Evaluated
	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"	HYCU Java Cryptographic Library	KAS-ECC-SSC	#A2933
FCS_COP.1/ DataEncryption	AES used in [CBC, GCM] mode and cryptographic key sizes [128 bits, 256 bits]	HYCU Java Cryptographic Library	AES-CBC AES-GCM	#A2933
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	HYCU Java Cryptographic Library	RSA-SigGen	#A2933
	For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4	HYCU Java Cryptographic Library	ECDSA-SigGen	#A2933
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384] and message digest sizes [160, 256, 384] bits	HYCU Java Cryptographic Library	SHA-1 SHA2-256 SHA2-384	#A2933

FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384] and cryptographic key sizes [160, 256, and 384 bits] and message digest sizes [160, 256, 384] bits	HYCU Java Cryptographic Library	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384	#A2933
FCS_RBG_EXT.1	Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)	HYCU Java Cryptographic Library	Hash DRBG HMAC DRBG Counter DRBG	#A2933

10 Conclusion

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

End of Document