Assurance Activity Report for MAGNUM-HW-CC

Version 1.3, 10 February 2023

MAGNUM-HW-CC Security Target

Version 1.3

collaborative Protection Profile for Network Devices Version 2.2e

Evaluated by:

intertek acumen security

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

NIAP

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Evertz Microsystems Ltd

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

The TOE Evaluation was Sponsored by:
Evertz Microsystems Ltd

Evaluation Personnel:
Shehan D. Dissanayake
Yogesh Pawar
Suvendu Das

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
1.0	30/11/2022	Initial Release
1.1	13/01/2023	Updated to address NIAP ECR comments
1.2	03/02/2023	Minor update to the TOE version in section 1, section 7.6.1, and to the references of other documents.
1.3	10/02/2023	Minor update to the ST version and to section 1.2

Contents

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	MAGNUM-HW-CC Security Target
ST Version	1.3
ST Date	February 10, 2023
ST Author	Acumen Security, LLC.
TOE Identifier	MAGNUM-HW-CC
TOE Version	MAGNUM-SDVN v21.10.4
TOE Developer	Evertz Microsystems Ltd. 5292 John Lucas Drive Burlington, Ontario CANADA
Key Words	Network Device

2 TOE Overview

The TOE is classified as a network device (a generic infrastructure device that can be connected to a network). The TOE hardware device is the Evertz MAGNUM-HW-CC which includes the MAGNUM-HW-CC (1 RU) with an Intel Xeon Silver 4309Y processor, running MAGNUM-SDVN firmware v21.10.4. The SDVN firmware is based on Ubuntu 20.04 TLS (Focal). The MAGNUM-HW-CC serves as the primary user and network interface device for the MAGNUM control application**.**

Evertz MAGNUM software (MAGNUM-SDVN 21.10) is a custom-developed application written primarily in python. MAGNUM-HW operates as a combination of an application layer and as part of the integrated Linux platform stack, using a customized Ubuntu operating system. The TOE version of MAGNUM (MAGNUM-HW-CC) is only operable on Evertz provided platforms and hardware.

The TOE is an infrastructure network device that provides secure remote management, auditing, and updating capabilities. The TOE provides secure remote management using an HTTPS/TLS web interface and an SSH command line interface. The TOE generates audit logs and transmits the audit logs to a remote syslog server over a mutually authenticated TLS channel. The TOE verifies the authenticity of software updates by verifying the digital signature prior to installing any update.

The scope of the evaluated functionality includes the following,

- Secure remote administration of the TOE via TLS and SSH
- Secure Local administration of the TOE
- Secure connectivity with remote audit servers
- Secure access to the management functionality of the TOE
- Identification and authentication of the administrator of the TOE

No other functionality is included within the scope of this evaluation.

The MAGNUM is a software module that unifies control and interfacing to Evertz and 3rd party media steaming devices. As a unified controller, the MAGNUM supports the following functionalities that are outside of the scope of this evaluation:

- MAGNUM serves as the control interface for Evertz's proprietary IPX media streaming switch fabric that allows the general user to establish, change, and tear down multicast IP video streams. MAGNUM may also serve as a general control interface for similar Evertz and third-party systems and devices.
- Equipment to prepare video for IP transport, or to convert it into other video formats, is outside the scope of this TOE. Such equipment includes, but is not limited to, cameras, KVMs, codecs, video servers and video displays. Equipment to perform functions such as embedding audio and/or other information within the video stream is also outside the scope of this TOE.
- MAGNUM issues commands (via dedicated internal API) to Evertz's proprietary IPX switching fabric and other production endpoints for the purpose of initiating, maintaining, and tearing down virtual routing paths. The MAGNUM-HW-CC device serves as the primary operational and administrative management interface to the closed multicast switching environment.
- MAGNUM provides Out-of-Band Management (OOBM) of Evertz IPX, EXE, and other 3rd party devices. To perform primary operational and administrative management functions on the closed multicast switching environment, Security Administrators may access MAGNUM software via direct

connection using a terminal session. Security Administrators may also access MAGNUM via a dedicated management workstation operating over an OOBM network to perform these OOB management functions. In addition to Security Administrators, general users may also access the MAGNUM software via a dedicated management workstation over an OOBM network.

Note: Sites may close this OOBM network or may operate MAGNUM within an existing OOBM, if the topology is compliant with the security parameters listed below.

1.2 TOE Description

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

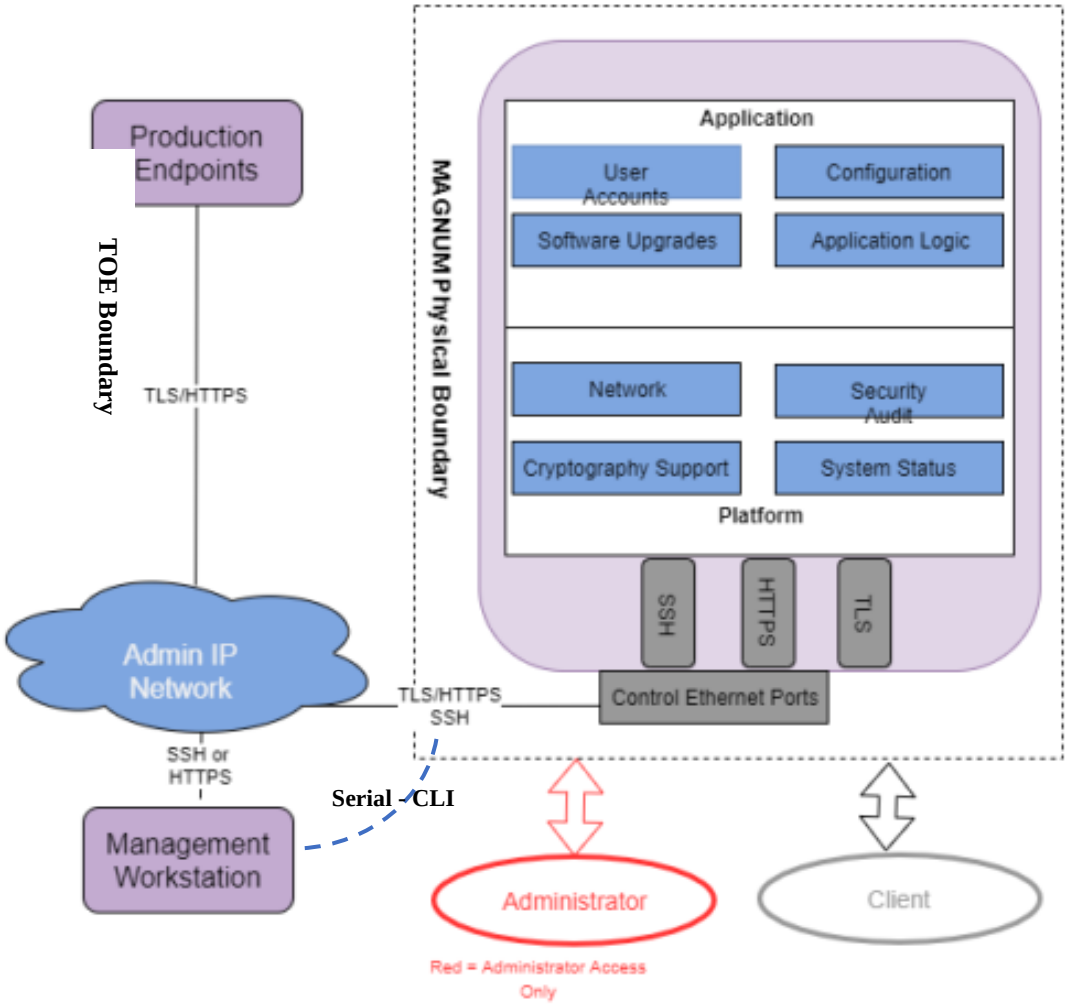


Figure 1 – Representative TOE Deployment

2.1.1 Physical Boundaries and IT Testing Environment Components

The physical boundaries of the TOE are outlined in section 1.2. All physical boundaries are required in the TOE Environment. The TOE is shipped to the customer via commercial courier. The IT Testing Environment components used to test the TOE are shown in Table 2 below.

Table 2 – IT Testing Environment Components

Component	Purpose/Description
Syslog server	• Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management workstation with web browser	• Supported browser: Chrome or Safari • Supporting TLSv1.2 • Supporting at least one of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
CRL Server	• Conformant with RFC 5280
DNS Sever	• Conformant with RFC 1035

2.1.2 Security Functions Provided by the TOE

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

1.2.1.1 Security Audit

The TOE generates audit records for security relevant events. Audit data are stored internally and are only accessible to privileged administrators. The TOE supports access to the TSF using administrator accounts for authentication and authorization to management and security functions.

The TOE also supports sending audit records to a remote Syslog server. Audit records sent to the remote server are protected by a TLS connection. Each audit record includes identity (username, IP address, or process), date and time of the event, type of event, and the outcome of the event.

1.2.1.2 Cryptographic Support

The TOE includes an OpenSSL library (Version 1.1.1k with Fedora Core 33 Patches) that implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS, HTTPs, and SSH connections for secure management and secure connections to a syslog and authentication servers. TLS and HTTPs are also used to verify firmware updates. The cryptographic services provided by the TOE are described below:

Table 3 – TOE Cryptographic Protocols

Cryptographic Protocol	Use within the TOE
HTTPS/TLS (client)	Secure connection to syslog FCS_HTTPS_EXT.1, FCS_TLSC_EXT.2
HTPS/TLS (server)	Remote management FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1
SSH(server)	Remote management FCS_SSHS_EXT.1
AES	Provides encryption/decryption in support of the TLS and SSH protocol. FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_SSHS_EXT.1
DRBG	Deterministic random bit generation use to generate keys. FCS_TLSS_EXT.1, FCS_RBG_EXT.1, FCS_SSHS_EXT.1
Secure hash	Used as part of digital signatures and firmware integrity checks. FCS_COP.1/Hash, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
HMAC	Provides keyed hashing services in support of TLS. FCS_COP.1/KeyedHash, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
EC-DH	Provides key establishment for TLS. FCS_CKM.2, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
ECDSA	Used to generate EC-DH components for key establishment for TLS. FCS_CKM.1, FCS_TLSS_EXT.1
RSA	Provide key generation and signature generation and verification (PKCS1_V1.5) in support of TLS. FCS_CKM.1, FCS_COP.1/SigGen, FCS_COP.1/SigVer, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1

The following table lists all SFRs for which a CAVP certificate is claimed, the CAVP algorithm list name and the CAVP Certificate number.

Table 4 – CAVP Algorithm Testing References

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #	TOE Cards
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	MAGNUM Cryptographic Module, version 21.10.0	RSA	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
	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	MAGNUM Cryptographic Module, version 21.10.0	ECDSA	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
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"	MAGNUM Cryptographic Module, version 21.10.0	Nor required	Not required	N/A
	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	MAGNUM Cryptographic Module, version 21.10.0	ECDSA	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
FCS_COP.1/ DataEncryption	AES used in [**CBC, CTR, GCM**] mode and cryptographic key sizes [**128 bits, 256 bits**]	MAGNUM Cryptographic Module, version 21.10.0	AES	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
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	MAGNUM Cryptographic Module, version 21.10.0	RSA	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
FCS_COP.1/ Hash	[**SHA-1, SHA-256, SHA-384, SHA-512**] and message digest sizes [**160, 256, 384, 512**] bits	MAGNUM Cryptographic Module, version 21.10.0	SHS	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
FCS_COP.1/ KeyedHash	[**HMAC-SHA-1, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512**] and cryptographic key sizes [**key size (in bits) used in HMAC**] and message digest sizes [**160, 256, 384, 512**] bits	MAGNUM Cryptographic Module, version 21.10.0	HMAC	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)
FCS_RBG_EXT.1	**CTR_DRBG (AES)**	MAGNUM Cryptographic Module, version 21.10.0	DRBG	A2455	Ubuntu 20.04 LTS (Focal) on Xeon Silver 4309Y (8C/16T)

1.2.1.3 Identification and Authentication

The TOE authenticates administrative users using a username/password combination. The TOE does not allow access to any administrative functions prior to successful authentication. The TOE validates and authenticates X.509 certificates for all certificate uses.

The TOE supports passwords consisting of alphanumeric and special characters and enforces minimum password lengths. The TSF supports certificates using RSA signature algorithms. Certificates are used to authenticate trusted channels, not administrators. The TOE only allows users to view the login warning banner prior to authentication. Remote administrators are locked out after a configurable number of unsuccessful authentication attempts.

1.2.1.4 Security Management

The TOE allows users with the Security Administrator role to administer the TOE over a remote web UI, remote CLI, or a local CLI. These interfaces do not allow the Security Administrator to execute arbitrary commands or executables on the TOE. Security Administrators can manage connections to an external Syslog server, as well as determine the size of local audit storage.

1.2.1.5 Protection of the TSF

The TOE implements several self-protection mechanisms. This protection includes self-tests to ensure the correct operations of cryptographic functions. Firmware upgrades, performed by a Security Administrator, must pass two authentication tests. The TOE does not provide an interface for the reading of secret or private keys. The TOE ensures timestamps, timeouts, and certificate checks are accurate by maintaining a real-time clock.

1.2.1.6 TOE Access

The TOE can be configured to display a warning and consent banner when an administrator attempts to establish an interactive session over the CLI (local or remote) or remote web UI. The TOE also enforces a configurable inactivity timeout for remote administrative sessions.

1.2.1.7 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel between itself and remote. The trusted channels utilize X.509 certificates to perform mutual authentication. The TOE initiates the TLS trusted channel with the remote server.

The TOE uses HTTPS/TLS and SSH to provide a trusted path between itself and remote administrative users. The TOE does not implement any additional methods of remote administration. The remote administrative users are responsible for initiating the trusted path when they wish to communicate with the TOE.

2.1.3 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- MAGNUM-HW-CC Security Administration Manual for Common Criteria, Magnum 21.10, Revision 03, January 13, 2023
- MAGNUM-HW 1RU Enterprise Class Server for MAGNUM User Manual, Version 2.2, September 2016
- Evertz MAGNUM-HW-CC Security Target, version 1.2

2.1.4 References

In additional to TOE documentation, the following reference may also be valuable when understanding and controlling the TOE:

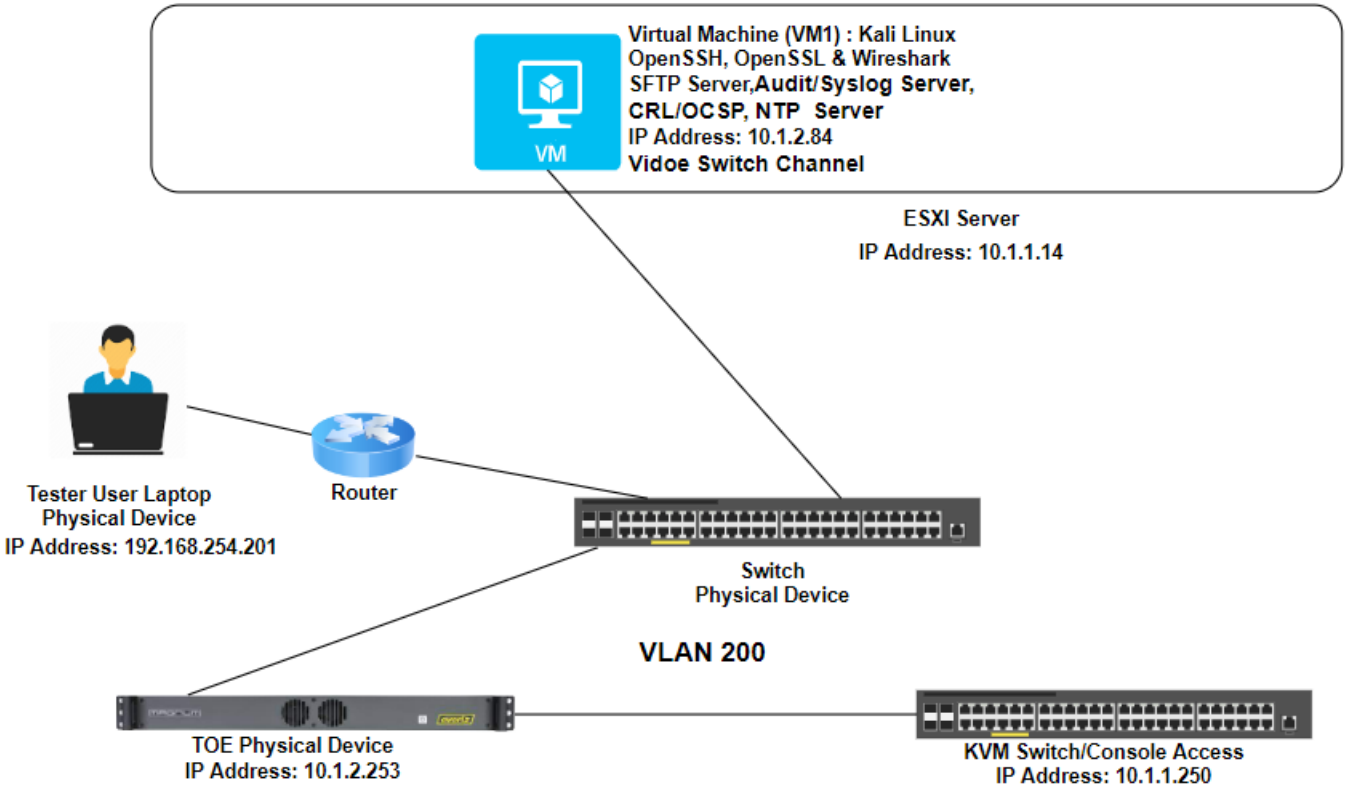
- collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP]

3 Assurance Activities Identification

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

4 Test Bed Descriptions

The figure below shows a logical view of the test setup.



4.1 Test Bed Component Information

The following table includes all information that is required to be documented for common criteria certification. This is typically collected during the dedicated TOE configuration sprint.

Name	OS	Version	Function	Protocols	Tools (version)
MAGNUM-HW-CC	MAGNUM-SDVN	v21.10.4	TOE	TLS and SSH	NA
Virtual Machine (VM1) (Evertz Magnum I)	Kali Linux	2021.4	SSH Client/ Server SFTP Server Audit Server CRL/OCSP/NTP Server/ IPX Vidoe switch Channel	SSH	Acumen-tlsc Acumen-tlss Acumen-sshs Rsyslogd OpenSSH, OpenSSL.
Tester User Laptop Physical machine	Windows	10	Test Workstation	SSH	Putty (0.76) Wireshark (3.6.0)
Switch	Cisco IOS	NA	Switch	IP	NA
ESXi Server			ESXi Server	HTTPs	NA
Router	Cisco IOS	NA	Router	IP	NA
KVM Console		NA	KVM Console	IP	NA

The testing was conducted between 05-March-2022 and 22-November-2022.

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 **FAU_GEN.1** section titled **TOE Summary Specification** in the Security Target to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys: **The TOE includes 3 different keys. When a key is destroyed or generated a log message is created and the keys are referred to as follows:** • **TLS keys – 'ssl/private/evertz-server.key'** • **SSH keys – 'ssh_host_rsa_key'** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.1.2 FAU_GEN.1 TSS 2

Objective	For distributed TOEs the evaluator shall examine the TSS to ensure that it describes which of the overall required auditable events defined in FAU_GEN.1.1 are generated and recorded by which TOE components. The evaluator shall ensure that this mapping of audit events to TOE components accounts for, and is consistent with, information provided in Table 1, as well as events in Tables 2, 4, and 5 (where applicable to the overall TOE). This includes that the evaluator shall confirm that all components defined as generating audit information for a particular SFR should also contribute to that SFR as defined in the mapping of SFRs to TOE components, and that the audit records generated by each component cover all the SFRs that it implements.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 1

Objective	The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection-based SFR sections as applicable, shall be provided from the actual audit record).
Evaluator Findings	The evaluator examined the section titled **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 table in that section contains a listing and description of each of the fields in generated audit records that contain the information required in FAU_GEN.1.2, as well as an example audit record. The evaluator next compared this list of events to the auditable events listed in the NDcPP. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.4 FAU_GEN.1 Guidance 2

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

Administrative Activity	**Method (Command/GUI Configuration)**	**Section**
login and logout	Logging in to Local Console: • Connect a VGA monitor and a USB keyboard	• Logging in to Local Console • Logging Out Of Local Console

			• Switch console sessions by pressing <CTRL><ALT><F1> through <CTRL><ALT><F6>. • Log in with username configshell and default password configshell to access a structured menu • Changing any settings requires entering configshell's password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings. • There also exists users etservice and etdev that access an open shell with limited permissions Logging out of Local Console: • Select logout at the bottom of the menu list • This will close the current administration session Logging in with SSH • Use Putty or a similar SSH client from a PC	• Logging in with SSH • Logging out of SSH • Logging in to Web Interface • Logging out of Web Interface	

			• Enter MAGNUM's IP address (use default port 22) • Log in with username configshell and default password configshell to access a structured menu • Changing any settings requires entering configshell's password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings • There also exists users etservice and etdev that access an open shell with limited permissions. Logging out of SSH: • Select logout at the bottom of the menu list • This will close the current SSH session Logging in to Web Interface: • Launch a web browser session • Enter the IP address of MAGNUM		

		• Log in with username admin and default password admin (other users can be created as well) Logging out of Web Interface: • Select the person icon on the top right of the web page. • Select Logout		
	Resetting passwords	Change Linux User Passwords: • Log in to the console as configshell and select Security • Select Change Linux User Passwords • Select the target user (the postgres user is internal but also has a password) • When prompted, enter configshell's password first, regardless of the target user • Enter the user's new password, twice for confirmation, adhering to the displayed password complexity requirements • Repeat this process for other users as necessary Change Web User Passwords: • Log in to the web interface as any user	• Change Linux User Passwords • Change Web User Passwords	

		• Select the configuration icon on the top right of the web page • Select Account from the left menu to modify the currently logged in account • Select Change Password • Complete all fields and select Save		
	Create CSR	• Log in to the console as configshell and select Security • Select Certificate Management • MAGNUM Security Administration Manual Page 21 of 60 • Select Create Certificate Signing Request • Update each field as appropriate for the particular device and organization • Select Create and Export • Select the destination, either /home/configshell via SFTP or USB Device • The file name is auto-generated during export	• Create Certificate Signing Request	
	Import Signed Server Certificate	• Log in to the console as configshell and select Security • Select Certificate Management	• Import Signed Server Certificate	

		• Select Import Signed Server Certificate • MAGNUM Security Administration Manual Page 22 of 60 • When prompted, enter configshell's password • Select the file's source, either /home/configshell via SFTP or USB Device • Select the correct certificate file (must be in PEM format with a .pem extension) • When prompted, reboot		
	Import Trusted CA Certificate	• Log in to the console as configshell and select Security • Select Certificate Management • Select Import Trusted CA Certificate • When prompted, enter configshell's password • Select the file's source, either /home/configshell via SFTP or USB Device • Select the correct CA certificate file (must be in PEM format with a .crt extension) • MAGNUM Security Administration Manual Page 25 of 60	• Import Trusted CA Certificate	

		• After the CA certificate is imported, the changes will take place immediately		
	Reset SSH Key	• Log in to the console as configshell and select Security • Select Reset SSH Key • Select Yes to proceed • When prompted, enter configshell's password • When prompted, reboot • MAGNUM Security Administration Manual Page 38 of 60 • A new key will be automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.	• Reset SSH Key	
	Upgrading Firmware	• Log in to the console as configshell and select System • Select Upgrade • When prompted, enter configshell's password • Select the file's source, either /home/configshell via SFTP or USB Device • Select the correct .efp file (the .sig file won't appear but it is expected to be beside the .efp file)	• Upgrading Firmware	

	• Consider the prompt, and select Yes to proceed • When prompted, enter configshell's password • Wait until the upgrade completes, and press q to return • When prompted, reboot • If the EFP is corrupted it will display the following message: • If the upgrade fails, contact Evertz Service Department	

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

Administrative Activity	**Method (Command/GUI Configuration)**	**Test Case(s)**
login and logout	Logging in to Local Console: • Connect a VGA monitor and a USB keyboard • Switch console sessions by pressing <CTRL><ALT><F1> through <CTRL><ALT><F6>. • Log in with username configshell and default password configshell to access a structured menu • Changing any settings requires entering	• FIA_UIA_EXT.1 Test #1 • FTA_SSL.4 Test #1 • FTA_SSL.4 Test #2

			configshell's password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings. • There also exists users etservice and etdev that access an open shell with limited permissions Logging out of Local Console: • Select logout at the bottom of the menu list • This will close the current administration session Logging in with SSH • Use Putty or a similar SSH client from a PC • Enter MAGNUM's IP address (use default port 22) • Log in with username configshell and default password configshell to access a structured menu • Changing any settings requires entering configshell's password each time, and that step is assumed in all instructions.		

			Security-sensitive changes are further protected by user prompts and warnings • There also exists users etservice and etdev that access an open shell with limited permissions. Logging out of SSH: • Select logout at the bottom of the menu list • This will close the current SSH session Logging in to Web Interface: • Launch a web browser session • Enter the IP address of MAGNUM • Log in with username admin and default password admin (other users can be created as well) Logging out of Web Interface: • Select the person icon on the top right of the web page. Select Logout		

	Resetting passwords	Change Linux User Passwords: • Log in to the console as configshell and select Security • Select Change Linux User Passwords • Select the target user (the postgres user is internal but also has a password) • When prompted, enter configshell's password first, regardless of the target user • Enter the user's new password, twice for confirmation, adhering to the displayed password complexity requirements • Repeat this process for other users as necessary Change Web User Passwords: • Log in to the web interface as any user • Select the configuration icon on the top right of the web page • Select Account from the left menu to modify the currently logged in account • Select Change Password • Complete all fields and select Save	• FIA_PMG_EXT.1.1 Test #1	

	Create CSR	• Log in to the console as configshell and select Security • Select Certificate Management • MAGNUM Security Administration Manual Page 21 of 60 • Select Create Certificate Signing Request • Update each field as appropriate for the particular device and organization • Select Create and Export • Select the destination, either /home/configshell via SFTP or USB Device The file name is auto-generated during export	• FIA_X509_EXT.3 Test #1	
	Import Signed Server Certificate	• Log in to the console as configshell and select Security • Select Certificate Management • Select Import Signed Server Certificate • MAGNUM Security Administration Manual Page 22 of 60 • When prompted, enter configshell's password	• FIA_X509_EXT.3 Test #2	

		• Select the file's source, either /home/configshell via SFTP or USB Device • Select the correct certificate file (must be in PEM format with a .pem extension) • When prompted, reboot		
	Import Trusted CA Certificate	• Log in to the console as configshell and select Security • Select Certificate Management • Select Import Trusted CA Certificate • When prompted, enter configshell's password • Select the file's source, either /home/configshell via SFTP or USB Device • Select the correct CA certificate file (must be in PEM format with a .crt extension) • MAGNUM Security Administration Manual Page 25 of 60 • After the CA certificate is imported, the changes will take place immediately	• FIA_X509_EXT.1.1/Rev Test #1a	
	Reset SSH Key	• Log in to the console as configshell and select Security • Select Reset SSH Key • Select Yes to proceed	• FMT_MTD.1/CryptoKeys Test #2	

		• When prompted, enter configshell's password • When prompted, reboot • MAGNUM Security Administration Manual Page 38 of 60 • A new key will be automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.		
	Upgrading Firmware	• Log in to the console as configshell and select System • Select Upgrade • When prompted, enter configshell's password • Select the file's source, either /home/configshell via SFTP or USB Device • Select the correct .efp file (the .sig file won't appear but it is expected to be beside the .efp file) • Consider the prompt, and select Yes to proceed • When prompted, enter configshell's password • Wait until the upgrade completes, and press q to return • When prompted, reboot	• FPT_TUD_EXT.1 Test #1	

		• If the EFP is corrupted it will display the following message: • If the upgrade fails, contact Evertz Service Department		

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

Verdict	Pass

5.1.2 FAU_GEN.2

5.1.2.1 FAU_GEN.2 TSS 1

Objective	The requirement for FAU_GEN.2 is already covered by the TSS requirements for FAU.GEN.1
Evaluator Findings	Refer to section 5.1.1 above
Verdict	Pass.

5.1.2.2 FAU_GEN.2 Guidance 1

Objective	The requirement for FAU_GEN.2 is already covered by the Guidance requirements for FAU.GEN.1
Evaluator Findings	Refer to section 5.1.1 above
Verdict	Pass

5.1.3 FAU_STG_EXT.1

5.1.3.1 FAU_STG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states that:

	Audit data is sent to external syslog server through secured, mutually authenticated TLS v1.2 sessions. A Security Administrator must configure an external syslog server (IP address/TCP Port number) on the TOE. A trusted certificate chain that is used to sign syslog server's certificate must be also uploaded to MAGNUM. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.2 FAU_STG_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS states that: **MAGNUM stores all audit data locally on SSD in a 20 GB non-executable partition, protected by Linux permissions. Only authorized administrators can access the stored audit data.** **To keep the local audit disk partition from overflowing old audit records on the local SSD are transmitted to the audit server once a connection is available. In the unlikely event that the disk partition fills up before enough records can be rotated away new entries are dropped.** **The TSF protects audit data from unauthorized modification and deletion through the restrictive administrative interfaces. The filesystem of the TSF is not exposed to the administrative user over the HTTPs GUI or the local CLI. The administrative user must be positively identified and authenticated prior to being allowed to clear the local audit log or change audit settings.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.3.3 FAU_STG_EXT.1 TSS 3

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

	but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes that 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 TOE is a standalone TOE that stores the Audit Data locally and the TSS states that: **To keep the local audit disk partition from overflowing old audit records on the local SSD are transmitted to the audit server once a connection is available.** **The TOE is not a distributed TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.4 FAU_STG_EXT.1 TSS 4

Objective	The evaluator shall examine the TSS to ensure that it details the behaviour of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behaviour of the TOE shall also be detailed in the TSS.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS states that: **In the unlikely event that the disk partition fills up before enough records can be rotated away new entries are dropped.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.1.3.5 FAU_STG_EXT.1 TSS 5

Objective	The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the

	TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.
Evaluator Findings	The evaluator examined the **FAU_STG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. Upon investigation, the evaluator found that the TSS states that: **The log data that is transmitted to the external syslog server and to the local audit store in real-time, simultaneously.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.6 FAU_STG_EXT.1 TSS 6

Objective	For distributed TOEs the evaluator shall examine the TSS to ensure it describes to which TOE components this SFR applies and how audit data transfer to the external audit server is implemented among the different TOE components (e.g. every TOE components does its own transfer or the data is sent to another TOE component for central transfer of all audit events to the external audit server).
Evaluator Findings	This requirement does not get applied to the TOE because the TOE is not a distributed TOE
Verdict	Pass

5.1.3.7 FAU_STG_EXT.1 TSS 7

Objective	For distributed TOEs the evaluator shall examine the TSS to ensure it describes which TOE components are storing audit information locally and which components are buffering audit information and forwarding the information to another TOE component for local storage. For every component the TSS shall describe the behaviour when local storage space or buffer space is exhausted.
Evaluator Findings	This requirement does not get applied to the TOE because the TOE is not a distributed TOE
Verdict	Pass

5.1.3.8 FAU_STG_EXT.1 Guidance 1

Objective	The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
Evaluator Findings	The evaluator examined the section titled **Secure Audit Servers** 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: **System log messages can be sent to a remote audit server. The remote audit server must listen on port 6514 for TLS connections, and its certificate chain must be trusted by MAGNUM in High Security Mode. All audit events are simultaneously sent to the remote server and the local store. If this or any outgoing client connection is unintentionally broken, MAGNUM will automatically reconnect within seconds.** **In addition, it was also found that there is a step-by-step configuration guide in the same section on how to add a remote syslog server.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.9 FAU_STG_EXT.1 Guidance 2

Objective	The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.
Evaluator Findings	The evaluator examined the section titled **Secure Audit Servers** 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: **System log messages can be sent to a remote audit server. The remote audit server must listen on port 6514 for TLS connections, and its certificate chain must be trusted by MAGNUM in High Security Mode. All audit events are simultaneously sent to the remote server and the local store.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.10 FAU_STG_EXT.1 Guidance 3

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

Evaluator Findings	The evaluator examined the section titled **Auditable Events** 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 Security Target states that: **The TSF shall [*drop new audit data*] when the local storage space for audit data is full.** And the AGD states that: **When the audit events in the system are full the TOE will drop new audit messages. If this highly unlikely event occurs, the administrators will have to manually clear the unnecessary files by login in to the shell as the 'configshell' user to make space or increase the disk space by attaching a new hard disk.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (Cryptographic Support)

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

5.2.1 FCS_CKM.1

5.2.1.1 FCS_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined the **FCS_CKM.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that: **The TSF supports 4096-bit RSA keys for generation of keys for TLS session signatures and ECDSA with NIST curves P-256, P-384, and P-521 to generate ECDH components for TLS key establishment.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.2 FCS_CKM.1 Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **Initial Setup** 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: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Random number generation using AES-256 CTR DRBG with SHA-256 hash** • **Key generation of RSA 4096-bit keys to support digital signatures** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement** • **SHA-512 used to verify file checksums and hash stored passwords** • **HMAC-SHA-1/256/384/512 used for TLS and SSH sessions and verification of firmware image** • **SSH rekey thresholds of 1 hour or 1 GB of data** • **Reject any SSL connection or TLS v1.0 or v1.1 connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: **#A2455** **Key Generation for FIPS PUB 186-4 RSA Schemes** For RSA key generation, this is validated by A2455 for the TOE model microarchitecture. **Key Generation for Elliptic Curve Cryptography (ECC)** For ECC (ECDSA) key generation, this is validated by A2455 for the TOE model microarchitecture. **Key Generation for Finite-Field Cryptography (FFC)** FCC schemes are not claimed, hence not applicable to the TOE. **FFC Schemes using "safe-prime" groups** (modified by TD0580) FFC-Safe prime groups are not claimed for the TOE, hence not applicable to the TOE. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.2 FCS_CKM.2

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

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
Evaluator Findings	The evaluator examined the **FCS_CKM.2** section titled **TOE Summary Specification** in the Security Target to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that: **The TOE acts as both sender and recipient for RSA and elliptic curve-based key establishment schemes that meet the following:** • **NIST Special Publication (SP) 800-56A Revision 2, "Recommendation for Pair Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" – for FCS_TLSC_EXT.1 connections to the audit server, FCS_TLSC_EXT.2 connections to video switches, and FCS_TLSS_EXT.1 connections to the remote administrators managing the TOE over web-GUI.** **or** • **RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specification Version 2.1". The TOE uses RSA-based key establishment for backwards compatibility for FCS_TLSC_EXT.1 connections to the audit server, FCS_TLSC_EXT.2 connections to video switches, and FCS_TLSS_EXT.1 connections to the remote administrators managing the TOE over web-GUI.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.2.2 FCS_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that:

	TLS Key establishment is performed with either RSA or ECDHE. The selection between key establishment schemes is determined by the TLS ciphersuite selection. **Ciphersuites allowed for TLS:** • **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_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246** • **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** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.2.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE **(modified by TD0580)**
Evaluator Findings	CAVP Certs: **#A2455** **Key Establishment Schemes** ***SP800-56A Key Establishment Schemes*** For elliptic-key based key exchange, this is validated as per CAVP A2455 (KAS-ECC-SSC Component) for the claimed TOE microarchitecture. This validated elliptic-key based key agreement is for TLS and SSH. ***RSA-based key establishment schemes*** The evaluator conducted testing using an independent known-good implementation during test cases for FCS_TLSS_EXT.1.1 using RSA public/private keys. The connections were successful. ***FFC Schemes using "safe-prime" groups*** The TOE does not claim FFC schemes, hence this test requirement is not applicable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3 FCS_CKM.4

5.2.3.1 FCS_CKM.4 TSS 1

Objective	The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are accounted for2). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.
Evaluator Findings	The evaluator examined the **FCS_CKM.4** section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS states that: **The TSF overwrites keys with random data followed by overwriting the contents with zeros. After each write operation, MAGNUM reads the data to confirm that it only the new data is stored (as opposed to a cached or older version of the data). If this test fails, the process is repeated until it succeeds. A sudden, unexpected power could disrupt zeroization and cause keys to not be zeroized. There are no other known circumstances where the TOE would not conform to these requirements.** The evaluator examined the **FCS_CKM.4** section titled **TOE Summary Specification** in the Security Target to verify that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found that the TSS states that: **Keys are stored on a separate disk partition that uses Linux file permission to ensure that no user or administrator access is allowed. The TOE does not provide full shell access and file permissions cannot be changed. No user has access to this partition. Keys are cleared when entering secure mode during device setup, and whenever the administrator selects this operation from the console.** **The following key is stored in the partition:** **The keys/CSPs used by the TOE, their storage location and format, and their associated zeroization method are as below:** • **EC Diffie-Hellman Keys** ○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***Key agreement and key establishment*** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **Firmware Update Key**

	○ Storage location and method: *Public key is stored in plaintext in a separate disk partition that uses Linux file permission. Private ke is not stored or used on the TOE.* ○ Usage: *Verification of firmware integrity when updating to new firmware versions using a SHA-512 hashed RSA signature.* ○ Zeroization: Linux 'cp' command replaces the public key file when importing a new file, i*nstructing a part of the code to destroy the abstraction that represents the key file.* • HTTPS/TLS Server/Host Key ○ Storage location and method: *Plaintext in a separate disk partition that uses Linux file permission* ○ Usage: *RSA and EC private key used in the HTTPS/TLS protocols* ○ Zeroization: *A single overwrite consisting of a pseudorandom pattern using the TSF's RBG, then overwritten again with zeroes. Copy in RAM is overwritten with zeroes when no longer needed..* • HTTPS/TLS session authentication key ○ Storage location and method: *Plaintext in RAM* ○ Usage: *HMAC Sha*-1, -256, or -384 key used for HTTPS/TLS session authentication. ○ Zeroization: *Overwritten with zeroes when no longer needed.* • HTTPS/TLS Session Encryption Key ○ Storage location and method: *Plaintext in RAM* ○ Usage: *AES (128, 256) key used for HTTPS/TLS session encryption* ○ Zeroization: *Overwritten with zeroes when no longer needed.* • SSH Server/Host key ○ Storage location and method: *Plaintext in a separate disk partition that uses Linux file permission* ○ Usage: *RSA private key used in the SSH protocol (key establishment, 2048- or 3072-bit)* ○ Zeroization: *A a single overwrite consisting of a pseudorandom pattern using the TSF's RBG, then overwritten again with zeroes. Copy in RAM is overwritten with zeroes when no longer needed.* • SSH Session Authentication Key ○ Storage location and method: *Plaintext in RAM* ○ Usage: *HMAC-SHA2-256 or HMAC-SHA2-2512 key used for SSH session authentication* ○ Zeroization: *Overwritten with zeroes when no longer needed.* • SSH Session Encryption Key ○ Storage location and method: *Plaintext in RAM* ○ Usage: *AES (128-, 256-bit) key used for SSH session encryption* ○ Zeroization: *Overwritten with zeroes when no longer needed.* • Locally Stored Passwords ○ Storage location and method: *SHA-512 Hashed in configuration file* ○ Usage: *User Authentication* ○ Zeroization: *Overwritten with pseudorandom pattern using the TSF's RBG/ zeros.*

	• **Configuration Encryption Key** ○ **Storage location and method:** ***Plaintext in a separate disk partition that uses Linux file permission*** ○ **Usage:** ***Configuration Encryption*** ○ **Zeroization:** ***Instructing a part of the code to destroy the abstraction that represents the key.*** **No direct interface/access is provided to view or modify the contents of these files.** **The TLS Session keys are zeroized from RAM when the associated TLS session is terminated.** **The DRBG state is zeroized using a single overwrite of zeros when the TSF is shutdown or restarted.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.3.2 FCS_CKM.4 TSS 2

Objective	The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).
Evaluator Findings	The evaluator examined the **FCS_CKM.4** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that the TSS states that: **This information is covered in the section above in FCS_CKM.4 TSS 1.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.3.3 FCS_CKM.4 TSS 3

Objective	Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.
Evaluator Findings	The evaluator examined the **FCS_CKM.4** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an

	encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that the TSS states that: **Keys are stored on a separate disk partition that uses Linux file permission to ensure that no user or administrator access is allowed. The TOE does not provide full shell access and file permissions cannot be changed. No user has access to this partition. Keys are cleared when entering secure mode during device setup, and whenever the administrator selects this operation from the console.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.3.4 FCS_CKM.4 TSS 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
Evaluator Findings	The evaluator examined the **FCS_CKM.4** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS states that: **A sudden, unexpected power could disrupt zeroization and cause keys to not be zeroized. There are no other known circumstances where the TOE would not conform to these requirements.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.3.5 FCS_CKM.4 TSS 5

Objective	Where the ST specifies the use of “a value that does not contain any CSP” to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
Evaluator Findings	The evaluator verified that ST does not specify the use of ‘a value that does not contain any CSP’ to overwrite keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.3.6 FCS_CKM.4 Guidance 1

Objective	A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined the section titled **FCS_CKM.4.1** in the Security Target 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 Security Target states that: **The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method** • **For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes]],** • **For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [** ○ **logically addresses the storage location of the key and performs a [single] overwrite consisting of [a pseudorandom pattern using the TSF's RBG, zeroes],** ○ **instructs a part of the TSF to destroy the abstraction that represents the key]** **that meets the following: No Standard** Upon further investigation as per the **Reset SSH Key** in the **MAGNUM Security Administration Manual for Common Criteria, rev02**, the evaluator found that the AGD states that: **Log in to the console as configshell and select Security --> Select Reset SSH Key --> Select Yes to proceed --> When prompted, enter configshell's password --> When prompted, reboot --> A new key will be automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.4 FCS_COP.1/DataEncryption

5.2.4.1 FCS_COP.1/DataEncryption TSS 1

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

Evaluator Findings	The evaluator examined the **FCS_COP.1/DataEncryption** section titled **TOE Summary Specification** in the Security Target to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS states that: **The TOE provides AES encryption/decryption in CBC, CTR and GCM modes with 128- and 256-bit keys.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.4.2 FCS_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify that it provides guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the AGD states that: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Random number generation using AES-256 CTR DRBG with SHA-256 hash** • **Key generation of RSA 4096-bit keys to support digital signatures** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement** • **SHA-512 used to verify file checksums and hash stored passwords** • **HMAC-SHA-1/256/384/512 used for TLS sessions and verification of firmware image** • **SSH rekey thresholds of 1 hour or 1 GB of data** • **Reject any SSL connection or TLS v1.0 or v1.1 connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.4.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Cert: **#A2455** **AES-CBC Known Answer Tests, AES-CBC Multi-Block Message Test, AES-CBC Monte Carlo Tests**

	AES-CBC cryptographic operations are validated under CAVP A2455 for the claimed microarchitecture. The CAVP certificate for AES-CBC apply to the algorithm implementation used for SSH and TLS. **AES-GCM Test** AES-GCM cryptographic operations are validated under CAVP A2455. **AES-CTR Known Answer Tests, AES-CTR Multi-Block Message Test, AES-CTR Monte-Carlo Test** AES-CTR cryptographic operations are validated under CAVP A2455 for the claimed microarchitecture. The CAVP certificate for AES-CTR apply to the algorithm implementation used for SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FCS_COP.1/SigGen

5.2.5.1 FCS_COP.1/SigGen TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the **FCS_COP.1/SigGen** section titled **TOE Summary Specification** in the Security Target to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS states that: **The TOE supports signature generation and verification with RSA 2048, 3072, 4096-bits in accordance with FIPS PUB 186-4, Section 5.5, using PKCS #1 v2.1.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.5.2 FCS_COP.1/SigGen Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **Initial Setup** 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: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Random number generation using AES-256 CTR DRBG with SHA-256 hash** • **Key generation of RSA 4096-bit keys to support digital signatures** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement** • **SHA-512 used to verify file checksums and hash stored passwords** • **HMAC-SHA-1/256/384/512 used for TLS sessions and verification of firmware image** • **SSH rekey thresholds of 1 hour or 1 GB of data** • **Reject any SSL connection or TLS v1.0 or v1.1 connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.5.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP RSA SigGen&SigVer (186-4) Certs: #**A2455** **RSA Signature Algorithm Tests** ***Signature Generation Test*** For the claimed TOE model microarchitecture, RSA SigGen operations for TLS are validated under CAVP A2455. ***Signature Verification Test*** RSA SigVer operations for TLS for the claimed TOE model microarchitecture are validated under CAVP A2455. **ECDSA Algorithm Tests** ECDSA Signature Generation Tests are not applicable because ECDSA cryptographic algorithms are not claimed in the ST for signature generation and verification. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.6 FCS_COP.1/Hash

5.2.6.1 FCS_COP.1/Hash TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	The evaluator examined the **FCS_COP.1/Hash** section titled **TOE Summary Specification** in the Security Target to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS states that: **Cryptographic hashing services are performed using Evertz's cryptographic module. Hashing is used for firmware integrity checks, password verification and security mode verification.** **The TOE provides cryptographic hashing services for. The TOE implements hashing in byte-oriented mode. The TOE uses hashing for the following security functions:** • **TLS connection establishment using SHA-1/256/384** • **Verifying executable file checksums SHA-512** • **Linux Passwords using salted SHA-512** • **Key generation using SHA-256 as specified in NIST SP 800-90 DRBG** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.6.2 FCS_COP.1/Hash Guidance 1

Objective	The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD states that: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Random number generation using AES-256 CTR DRBG with SHA-256 hash** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement** • **SHA-512 used to verify file checksums and hash stored passwords**

	• **HMAC-SHA-1/256/384/512 used for TLS sessions and verification of firmware image** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP Certs: **#A2455** **Short Messages Test - Bit-oriented Mode, Short Messages Test - Byte-oriented Mode, Selected Long Messages Test - Bit-oriented Mode, Selected Long Messages Test - Byte-oriented Mode, Pseudorandomly Generated Messages Test** TLS and SSH hashing services, and Password hashing services are validated under CAVP A2455 for the claimed TOE microarchitecture. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7 FCS_COP.1/KeyedHash

5.2.7.1 FCS_COP.1/KeyedHash TSS 1

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	The evaluator examined the **FCS_COP.1/KeyedHash** section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS states that: **MAGNUM uses OpenSSL software that has been patched to enforce FIPS modes using special environment variables. When these are set, the TSF will not allow ephemerally generated hashes and keys to be created that do not comply with these standards. The keyed-hash message authentication is performed internally by OpenSSL when it is used to perform message authentication.** **For HMAC-SHA-1:** • **Key length: 160 bits** • **Hash function used: SHA-1** • **Block size: 256 bits** • **Output MAC (message digest size): 160 bits**

	For HMAC-SHA-256: • **Key length: 256 - 512 bits** • **Hash function used: SHA-256** • **Block size: 512 bits** • **Output MAC (message digest size): 256 bits** **For HMAC-SHA-384:** • **Key length: 384 bits** • **Hash function used: SHA-384** • **Block size: 1024** • **Output MAC (message digest size): 384 bits** **For HMAC-SHA-512:** • **Key length: 512 bits** • **Hash function used: SHA-512** • **Block size: 1024 bits** • **Output MAC (message digest size): 512 bits** **HMACs are used for verification of the firmware image and encrypted password files during bootup.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.7.2 FCS_COP.1/KeyedHash Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function. Upon investigation, the evaluator found that the AGD states that: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Random number generation using AES-256 CTR DRBG with SHA-256 hash** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement**

	• **SHA-512 used to verify file checksums and hash stored passwords** • **HMAC-SHA-1/256/384/512 used for TLS sessions and verification of firmware image** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	CAVP HMAC Certs: **#A2455** TLS and SSH secure hashing services are validated under CAVP A2455 for the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8 FCS_RBG_EXT.1

5.2.8.1 FCS_RBG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.
Evaluator Findings	The evaluator examined the **FCS_RBG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS states that: **The TOE implements a DRBG in accordance with ISO/IEC 18031:2011 using a CTR DRBG with AES. The TSF seed the CTR_DRBG using 384-bits of data that contains at least 256 bits of entropy. The TSF gathers and pools entropy from one software-based noise source: haveged and the Linux Kernel entropy.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.2.8.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify that it contains appropriate instructions for configuring the RNG functionality. Upon investigation, the evaluator found that the AGD states that: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Random number generation using AES-256 CTR DRBG with SHA-256 hash** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP DRBG Certs: **#A2455** CAVP certificate number A2455 covers the claimed physical platform for the CTR-DRBG. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (HTTPS)

5.3.1 FCS_HTTPS_EXT.1

5.3.1.1 FCS_HTTPS_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.
Evaluator Findings	The evaluator examined the section titled **TOE Summary Specification** in the Security Target to verify that the TSS provides enough detail to explain how the implementation complies with RFC 2818. Upon investigation, the evaluator found that the TSS states that t**he TSF implements the server and client sides of the HTTPs protocol according to RFC 2818 by using a TLS session in place of a TCP connection**.

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

5.3.1.2 FCS_HTTPS_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.
Evaluator Findings	The evaluator examined the 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 section 3, sub-section "Web Interface" of the 'MAGNUM Security Administration Manual for Common Criteria states that **the Security Administrators can securely administer the Magnum via Web Graphical User Interface once the IP address is configured, and a valid Server Certificate is imported. The steps to configure IP address and import server certificates are described in the sections 8 and 14 in the same document.** The section 'Web Interface' also describes the supported web-browsers and the ciphersuites that they need to support for successful connectivity. Administrator can access the TOE by entering the IP address of the TOE in any of the web browser. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (SSH)

5.4.1 FCS_SSHS_EXT.1

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

Objective	The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims). The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file. If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to

	FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS states that: **The TSF implements SSH as a trusted channel for remote administrative connections to the CLI. Public key or password-based authentication is allowed. ssh-rsa, rsa-sha2-256, and rsa-sha2-512 are the only public key algorithms accepted for SSH connections. All connections using other public key algorithms are rejected.** The TSS also states that: **The TOE establishes a user identity by verifying that the SSH client's present public key matches the one that is stored within the SSH server's authorized keys file.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.2 FCS_SSHS_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that: **During an SSH session, the TOE reads the packet payload size from the TCP header to determine packets size. As packets are reassembled, the payloads are added. Any packets larger than 263KB are rejected.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.3 FCS_SSHS_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that:

	SSH transport is encrypted using AES CTR with key sizes of 128- or 256-bits. Data integrity is verified using HMAC-SHA256 or HMAC SHA512. All other MAC algorithms are rejected. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.4 FCS_SSHS_EXT.1.4 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled **Initial Setup** and **System Security Mode** in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that: **Details of all functions that are configured in High Security Mode can be found in Section 14. High Security Mode sets all cryptographic configurations for the TOE, including limiting cryptographic parameters to only the following:** **SSH cryptographic configurations:** • **AES CTR with 128-bit or 256-bit keys for encryption** • **SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512 for authentication** • **ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP512 for key exchange** • **HMAC-SHA2-256 and HMAC-SHA2-512 for SSH transport MAC algorithms** **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed.** **Putting the device in High Security Mode configures the TLS ciphers and all other cryptographic engine requirements needed in the evaluated configuration. No other configuration of cryptography is permitted on the TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

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

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

Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS states that: **Public key or password-based authentication is allowed. ssh-rsa, rsa-sha2-256, and rsa-sha2-512 are the only public key algorithms accepted for SSH connections. All connections using other public key algorithms are rejected.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.6 FCS_SSHS_EXT.1.5 TSS 2

Objective	The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. Upon investigation, the evaluator found that the TSS states that: **If an SSH client attempts a session with public key authentication and does not provide the proper key, the TOE will reject the authentication attempt and revert to password-based authentication.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.7 FCS_SSHS_EXT.1.5 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled **Initial Setup** and **System Security Mode** in the AGD to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD states that: **Details of all functions that are configured in High Security Mode can be found in Section 14. High Security Mode sets all cryptographic configurations for the TOE, including limiting cryptographic parameters to only the following:** **SSH cryptographic configurations:**

	• **AES CTR with 128-bit or 256-bit keys for encryption** • **SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512 for authentication** • **ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP512 for key exchange** • **HMAC-SHA2-256 and HMAC-SHA2-512 for SSH transport MAC algorithms** **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed.** **Putting the device in High Security Mode configures the TLS ciphers and all other cryptographic engine requirements needed in the evaluated configuration. No other configuration of cryptography is permitted on the TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.8 FCS_SSHS_EXT.1.6 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that: **Data integrity is verified using HMAC-SHA256 or HMAC SHA512. All other MAC algorithms are rejected.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.9 FCS_SSHS_EXT.1.6 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).
Evaluator Findings	The evaluator examined the section titled **Initial Setup** and **System Security Mode** in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that: **Details of all functions that are configured in High Security Mode can be found in Section 14. High Security Mode sets all cryptographic configurations for the TOE, including limiting cryptographic parameters to only the following:** **SSH cryptographic configurations:**

	• **AES CTR with 128-bit or 256-bit keys for encryption** • **SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512 for authentication** • **ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP512 for key exchange** • **HMAC-SHA2-256 and HMAC-SHA2-512 for SSH transport MAC algorithms** **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed.** **As per Section 14 System Security Mode:** **Putting the device in High Security Mode configures the TLS ciphers and all other cryptographic engine requirements needed in the evaluated configuration. No other configuration of cryptography is permitted on the TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.10 FCS_SSHS_EXT.1.7 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that: **Keys are exchanged using elliptic curve Diffie Hellman with NIST curves P-256, P-384 or P-521.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.11 FCS_SSHS_EXT.1.7 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** and **System Security Mode** in the AGD to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD states that:

	Details of all functions that are configured in High Security Mode can be found in Section 14. High Security Mode sets all cryptographic configurations for the TOE, including limiting cryptographic parameters to only the following: **SSH cryptographic configurations:** • **AES CTR with 128-bit or 256-bit keys for encryption** • **SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512 for authentication** • **ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP512 for key exchange** • **HMAC-SHA2-256 and HMAC-SHA2-512 for SSH transport MAC algorithms** **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed.** **As per Section 14 System Security Mode:** **Putting the device in High Security Mode configures the TLS ciphers and all other cryptographic engine requirements needed in the evaluated configuration. No other configuration of cryptography is permitted on the TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.12 FCS_SSHS_EXT.1.8 TSS 1

Objective	The evaluator shall check that the TSS specifies the following: a) Both thresholds are checked by the TOE. b) Rekeying is performed upon reaching the threshold that is hit first.
Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies that both thresholds are checked and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that: **The TSF will rekey the SSH if the session lasts longer than 60 minutes or if more than 1GB of data have been transferred.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.4.1.13 FCS_SSHS_EXT.1.8 Guidance 1

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

	the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD states that: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **SSH rekey thresholds of 1 hour or 1 GB of data** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (TLS)

5.5.1 FCS_TLSC_EXT.1

5.5.1.1 FCS_TLSC_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** 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: **When the TSF is configured with a server certificate with an RSA key, the TSF supports following restrictive TLS ciphersuites are supported:** • **TLS_RSA_WITH_AES_128_CBC_SHA** • **TLS_RSA_WITH_AES_256_CBC_SHA** • **TLS_RSA_WITH_AES_128_CBC_SHA256** • **TLS_RSA_WITH_AES_256_CBC_SHA256** • **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.5.1.2 FCS_TLSC_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** 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 TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **HMAC-SHA-1/256/384/512 used for TLS sessions and verification of firmware image** • **Reject any SSL connection or TLS v1.0 or v1.1 connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 FCS_TLSC_EXT.1.2 TSS 1

Objective	The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application configured reference identifier, including which types of reference identifiers are supported (e.g. application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier, including which types of reference identifiers are supported; whether IP addresses and wildcards are supported. Upon investigation, the evaluator found that the TSS states that: **When establishing a TLS connection, the MAGNUM client establishes the following reference identifiers:** • **Domain Name Service (DNS) in CN or SAN-DNS** • **IPv4 Address in SAN-IP** **The SAN field is mandatory when using SAN-IP. If there is no SAN-DNS field provided, the default fallback position is the Common Name (CN). When establishing reference identifiers, wildcards are supported for DNS only.** **MAGNUM supports wildcard in certificates. The wildcard must be in the left-most label of the presented identifier. And the wildcard only covers one level of subdomains. For the reference identifier without a left-most label as in the certificate, the connection will fail, i.e., awesome.com doesn't match *.awesome.com.** **Certificate pinning is not used.**

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

5.5.1.4 FCS_TLSC_EXT.1.2 TSS 2

Objective	Note that where a TLS channel is being used between components of a distributed TOE for FPT_ITT.1, the requirements to have the reference identifier established by the user are relaxed and the identifier may also be established through a "Gatekeeper" discovery process. The TSS should describe the discovery process and highlight how the reference identifier is supplied to the "joining" component. Where the secure channel is being used between components of a distributed TOE for FPT_ITT.1 and the ST author selected attributes from RFC 5280, the evaluator shall ensure the TSS describes which attribute type, or combination of attributes types, are used by the client to match the presented identifier with the configured identifier. The evaluator shall ensure the TSS presents an argument how the attribute type, or combination of attribute types, uniquely identify the remote TOE component; and the evaluator shall verify the attribute type, or combination of attribute types, is sufficient to support unique identification of the maximum supported number of TOE components.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.5.1.5 FCS_TLSC_EXT.1.2 TSS 3

Objective	If IP addresses are supported in the CN as reference identifiers, the evaluator shall ensure that the TSS describes the TOE's conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order. The evaluator shall also ensure that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify and found that the TOE does not support the IP addresses in the CN as reference identifiers. Based on these findings, this assurance activity is considered not applicable to the TOE.
Verdict	N/A

5.5.1.6 FCS_TLSC_EXT.1.2 Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **Allowed Subject Alt Names (DNS)** and **Allow Subject Alt Names (IP)** 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: **This option allows the administrator to configure a list of allowed Subject Alternative Names (also known as reference identifiers). In High Security Mode, all TLS connections (including both client and server connections) are authenticated by verifying the peer's certificate. If the peer's certificate does not contain a Subject Alternative Name field from the MAGNUM device's allowed list, the connection is blocked. If the allowed list is empty, this field is not checked during certificate authentication. If the peer's certificate does not have a Subject Alternative Names field, the Common Name field is checked instead, for backwards compatibility.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Allowed Subject Alt Names (DNS)** • **Select Add DNS Host to add new entries** • **Enter a valid DNS name (wildcards are supported)** • **Select Remove DNS Host to remove entries** • **Select Save and Apply when done** • **When prompted, reboot** **Allow Subject Alt Names (IP) option allows the administrator to configure a list of allowed Subject Alternative Names (also known as reference identifiers). In High Security Mode, all TLS connections (including both client and server connections) are authenticated by verifying the peer's certificate. If the peer's certificate does not contain a Subject Alternative Name field from the MAGNUM device's allowed list, the connection is blocked. If the allowed list is empty, this field is not checked during certificate authentication.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Allowed Subject Alt Names (IP)** • **Select Add IP to add new entries** • **Enter a valid IP address** • **Select Remove IP to remove entries** • **Select Save and Apply when done** • **When prompted, reboot** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.7 FCS_TLSC_EXT.1.4 TSS 1

Objective	The evaluator shall verify that TSS describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behaviour is performed by default or may be configured.
Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that: • **The TSF sends the client EC Diffie-Hellman secp256r1 NIST curve.** • **The TSF does not provide support for elliptic curves in the ClientHello message.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.8 FCS_TLSC_EXT.1.4 Guidance 1

Objective	If the TSS indicates that the Supported Elliptic Curves/Supported Groups Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves/Supported Groups Extension.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** 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 TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 FCS_TLSC_EXT.2

5.5.2.1 FCS_TLSC_EXT.2.1 TSS 1

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

Evaluator Findings	The evaluator examined the **FCS_TLSC_EXT.2** section titled **TOE Summary Specification** in the Security Target to verify that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that: **For trusted channels with the Evertz video switch (IPX), the TOE requires TLS with mutual authentication.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.2 FCS_TLSC_EXT.2.1 Guidance 1

Objective	If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the section titled **Configuration of IPX Channel** in the AGD to verify that it includes instructions for configuring the client-side certificates for TLS mutual authentication and the TSS indicates that mutual authentication using X.509v3 certificates is used. Upon investigation, the evaluator found that the AGD states that: **Log in to the Magnum through WebUI → Select the System type as SDVN → Click on Devices and Links → Click on Add Device(s) → Select the required Device Type → Select the Number of Devices → Enter device details and click on Add Device → The device is added** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3 FCS_TLSS_EXT.1

5.5.3.1 FCS_TLSS_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified are identical to those listed for this component. Upon investigation, the evaluator found that the TSS states that: **When the TSF is configured with a server certificate with an RSA key, the TSF supports following restrictive TLS ciphersuites are supported:**

	• **TLS_RSA_WITH_AES_128_CBC_SHA** • **TLS_RSA_WITH_AES_256_CBC_SHA** • **TLS_RSA_WITH_AES_128_CBC_SHA256** • **TLS_RSA_WITH_AES_256_CBC_SHA256** • **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** • **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.5.3.2 FCS_TLSS_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined the section titled **Initial Setup** and **System Security 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: **Details of all functions that are configured in High Security Mode can be found in Section 14. High Security Mode sets all cryptographic configurations for the TOE, including limiting cryptographic parameters to only the following:** **Ciphersuites allowed for TLS:** • **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_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246** • **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** **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed.** **As per the System Security Mode, Putting the device in High Security Mode configures the TLS ciphers and all other cryptographic engine requirements needed in the evaluated configuration. No other configuration of cryptography is permitted on the TOE.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.3 FCS_TLSS_EXT.1.2 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of how the TOE technically prevents the use of old SSL and TLS versions.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description of the denial of old SSL and TLS versions. Upon investigation, the evaluator found that the TSS states that: **The TSF only supports TLSv1.2 for HTTPS/TLS. Connection requests that include SSL 2.0, SSL 3.0, TLS 1.0 or TLS 1.1 are denied. If the TSF receives a ClientHello message that requests TLSv1.1 or earlier, the TSF sends a fatal handshake_failure message and terminates the connection.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.5.3.4 FCS_TLSS_EXT.1.2 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** 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 TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Reject any SSL connection or TLS v1.0 or v1.1 connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

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

Objective	If using ECDHE and/or DHE ciphers, the evaluator shall verify that the TSS lists all EC Diffie-Hellman curves and/or Diffie-Hellman groups used in the key establishment by the TOE when acting as a TLS Server. For example, if the TOE supports TLS_DHE_RSA_WITH_AES_128_CBC_SHA cipher and Diffie-Hellman parameters with size 2048 bits, then list Diffie-Hellman Group 14.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that, if using ECDHE or DHE ciphers, the TSS describes the key agreement parameters of the server Key Exchange message. Upon investigation, the evaluator found that the TSS states that: **MAGNUM supports cipher suites that use ECDHE or RSA keys for key exchange and RSA for authentication. These keys are generated by the OpenSSL implementation internally with OpenSSL's RSA command line utility. When acting as a TLS server, the TOE Key Exchange message parameters are 4096-bit RSA key or ECDSA over NIST curve secp256r1.**

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

5.5.3.6 FCS_TLSS_EXT.1.3 Guidance 1

Objective	The evaluator shall verify that any configuration necessary to meet the requirement must be contained in the AGD guidance.
Evaluator Findings	The evaluator examined the section titled **Initial Setup** in the AGD to verify that it contains any configuration necessary to meet the requirement. Upon investigation, the evaluator found that the AGD states that: **The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:** • **Key generation of RSA 4096-bit keys to support digital signatures** • **ECDSA keys with NIST curves P256 or P-384 to support ECDHE key agreement** • **Reject any SSL connection or TLS v1.0 or v1.1 connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.7 FCS_TLSS_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS describes if session resumption based on session IDs is supported (RFC 4346 and/or RFC 5246) and/or if session resumption based on session tickets is supported (RFC 5077).
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that: **The TSF supports session resumption based on session IDs and session tickets. Session tickets adhere to the structural format provided in section 4 of RFC 5077. Session tickets are encrypted according to the TLS negotiated symmetric encryption algorithm** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.8 FCS_TLSS_EXT.1.4 TSS 2

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that the session tickets are encrypted using symmetric algorithms consistent with FCS_COP.1/DataEncryption. The evaluator shall verify that the TSS identifies the key lengths and algorithms used to protect session tickets.

Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that: **Session tickets are encrypted according to the TLS negotiated symmetric encryption algorithm.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.9 FCS_TLSS_EXT.1.4 TSS 3

Objective	If session tickets are supported, the evaluator shall verify that the TSS describes that session tickets adhere to the structural format provided in section 4 of RFC 5077 and if not, a justification shall be given of the actual session ticket format.
Evaluator Findings	The evaluator examined the **FCS_TLSS_EXT.1** section titled **TOE Summary Specification** in the Security Target. Upon investigation, the evaluator found that the TSS states that: **Session tickets adhere to the structural format provided in section 4 of RFC 5077.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Identification and Authentication)

5.6.1 FIA_AFL.1

5.6.1.1 FIA_AFL.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability.
Evaluator Findings	The evaluator examined the **FIA_AFL.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary to restore this ability. Upon investigation, the evaluator found that the TSS states that: **An administrator can configure the number of unsuccessful attempts a remote administrator can make before a lock-out and can configure the length of time that the remote administrator is locked out. The attempts can range between 3 and 10, with a default of 10. The length of time can be configured between 1 and 60 minutes, with a default of 15. Additionally, a different Administrator**

	can log in and unlock the user, prior to the timeout period if needed. **The TOE maintains a counter for incorrect authentication attempts for each username. If the user enters an incorrect password the configured number of times, the username is changed to a locked state. Any attempt to authenticate from a remote interface using that username is denied and an error message is shown to the user. When the lockout time has expired or an administrator unlocks the user, the administrator is allowed to authenticate to the TOE again.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.2 FIA_AFL.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).
Evaluator Findings	The evaluator examined the **FIA_AFL.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS states that: **Lockouts are not enforced on the TOE's console interface. This ensures that authentication failures cannot lead to a situation where no administrator access is available.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.3 FIA_AFL.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.
Evaluator Findings	The evaluator examined the section titled **Account Lockout Duration** and **Account Lockout Threshold** in the AGD to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). Upon investigation, the evaluator found that the AGD states that:

	Configure how long console and web accounts are locked after too many failed login attempts. • **Log in to the console as configshell and select Security** • **Select Account Lockout Duration** • **When prompted, enter configshell's password** • **Enter the new account lockout duration (in minutes)** • **The change will take effect immediately** **Configure how many failed login attempts will temporarily lock console and web accounts.** • **Log in to the console as configshell and select Security** • **Select Account Lockout Threshold** • **When prompted, enter configshell's password** • **Enter the new account lockout threshold** • **The change will take effect immediately** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.4 FIA_AFL.1 Guidance 2

Objective	The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.
Evaluator Findings	The evaluator examined the section titled **Unlock SSH Accounts** and **Unlock Web Accounts** 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: **Unlock SSH user accounts that have been locked due to too many failed login attempts** • **Log in to the console as configshell and select Security** • **Select Unlock SSH Accounts** • **Select the user account to unlock** • **When prompted, enter configshell's password** • **The change will take effect immediately** **Unlock web user accounts that have been locked due to too many failed login attempts.** • **Log in to the console as configshell and select Security**

	• **Select Unlock Web Accounts** • **Select the web user account to unlock** • **When prompted, enter configshell's password** • **The change will take effect immediately** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2 FIA_PMG_EXT.1

5.6.2.1 FIA_PMG_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords.
Evaluator Findings	The evaluator examined the **FIA_PMG_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS states that: **MAGNUM enforces that passwords must meet minimum requirements (length, mix of number of lower/upper case letters, numbers as well as special characters, no common dictionary words. etc).** **The special characters the TSF supports include : "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", """, "'", "+", "-", ",", ".", "/", "\", ":", ";", "<", "=", ">", "?", "[", "]", "_", "`", "{", "|", "}", [space]. Administrators can configure a minimum password length between 8 and 15 characters. Guidance documentation recommends that Administrators set the minimum password length to 15 characters.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it: a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
Evaluator Findings	The evaluator examined the section titled **Minimum Password Length** and **Password Complexity** in the AGD to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong

	passwords and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD states that: **Configure the minimum password length for console and web users.** • **Log in to the console as configshell and select Security** • **Select Minimum Password Length** • **When prompted, enter configshell's password** • **Enter the new minimum password length** • **The change will take effect the next time a web or console user changes their password** **If this option is enabled using High Security Mode, all web and console user passwords must meet increased complexity requirements:** • **Minimum length 8 characters** • **Must use two of each: Upper case letters, Lower case letters, Numbers, Symbols** • **No reusing previous password** **The allowed character list is:** • **Upper case letters** • **Lower case letters** • **Numerals** • **Special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"]** • **Other special characters: [" ", "'", "`", "+", ",", "-", ".", "/", ":", ";", "<", "=", ">", "?", "[", "\", "]", "_", "`", "{", "|", "}", "~"]** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 FIA_UIA_EXT.1

5.6.3.1 FIA_UIA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a "successful logon".
Evaluator Findings	The evaluator examined the **FIA_UIA_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that:

	Authentication is based on username/password for the web interface and local console. Remote access of SSH can use password or SSH public key-based authentication. The TOE does not expose any interface, through any access method prior to successful login. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.2 FIA_UIA_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.
Evaluator Findings	The evaluator examined the **FIA_UIA_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that: **The TSF displays a warning banner after the user enters their username, but before the password prompt will accept login credentials from a user. This applies to direct console users as well as web users.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.3 FIA_UIA_EXT.1 TSS 3

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

5.6.3.4 FIA_UIA_EXT.1 TSS 4

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

Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.6.3.5 FIA_UIA_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.
Evaluator Findings	The evaluator examined the following section 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: • **Logging in to Local Console** • **Logging in with SSH** • **Logging in to Web Interface** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 FIA_UAU.7

5.6.4.1 FIA_UAU.7 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.
Evaluator Findings	The evaluator examined each AGD and verified that no preparatory steps are required to ensure that authentication data is not revealed while entering the credentials. **It was found during testing that when the user is entering their password over the local console, the TSF shows only asterisks (“*”).** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 FIA_X509_EXT.1/Rev

5.6.5.1 FIA_X509_EXT.1/Rev TSS 1

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

Evaluator Findings	The evaluator examined the **FIA_X509_EXT.1/Rev** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that:
	
	MAGNUM uses CRLs to validate certificates. When the TOE acts as a TLS client, the video switch or syslog server's certificates are validated during the TLS session connection handshake. Certificates are also checked for revocation when loaded onto the TOE. When acting as a TLS server, the TOE validates certificates when presented by the client. MAGNUM first checks Certificate Authorities (CAs), then CRLs, then SANs. The TOE verifies that the certificates presented as a TLS server must contain the TLS server extended key usage, TLS client certificates must have the TLS client extended key usage. The TOE does not support certificates for trusted updates or OCSP. This validation includes revocation checking for the full certificate chain regardless of whether the full chain or only a leaf certificate is presented.
	
	For an expired certificate, MAGNUM will deny the connection.
	
	During session establishment with MAGNUM, any byte modification in the certificate will lead to the failure of connection.
	
	The TSF additionally verifies:
	
	• **Each certificate (other than the first certificate) in the certificate chain has the Subject Type=CA flag set.**
	• **Each certificate is signed by:**
	  ○ **a certificate in the certificate chain, or**
	  ○ **a trusted root CA that has been installed in the TSF**
	
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.6.5.2 FIA_X509_EXT.1/Rev TSS 2

Objective	The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.
Evaluator Findings	The evaluator examined the **FIA_X509_EXT.1/Rev** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that: **The TOE uses a CRLs to verify whether the certificate or intermediate CA certificate has been revoked when a leaf certificate is presented to the TOE as part of the certificate chain during authentication.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.3 FIA_X509_EXT.1/Rev Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.
Evaluator Findings	The evaluator examined the section titled **Certificate Management** and **Show Certificate Revocation List** 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: • **X.509 certificates are used to authenticate all TLS connections. A client certificate is sent whenever the server requests one. This functionality cannot be disabled.** • **Only certificates in PEM format are supported (DER is not supported).** • **Certificate Revocation Lists (CRLs) are downloaded from CRL-DP extensions during each connection attempt, if the peer certificates define them (only for end-user and intermediate certificates, not for root CA certificates).** • **Recommend removing the Evertz default CA and CRL during system setup, to replace them with organization-specific certificates.** **The Show Certificate Revocation List allows the administrator to review CRLs. This option is useful before and after importing or removing CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is**

	revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first. • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Show Certificate Revocation List** • **Select the CRL to review** • **Review the CRL details, using the arrow keys to scroll down or right** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6 FIA_X509_EXT.2

5.6.6.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the **FIA_X509_EXT.2** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that: **As a TLS Client, the TOE uses CRL to determine whether the certificate is revoked or not. If the certificate fails a validity check, the connection attempt will fail and the trusted channel is not established.** **The FIA_X509_EXT.1 section titled TOE Summary Specification in the Security Target include additional information on how there is a certificate trust store which stores certificates loaded onto the TOE. This section also describes how CRL verification is done on certificates that are already in the trust store as well as on the certificates presented to the TOE during an TLS authentication step.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.2 FIA_X509_EXT.2 TSS 2

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

Evaluator Findings	The evaluator examined the **FIA_X509_EXT.2** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that: **The CRLs are obtained from a CRL distribution point over HTTP and are refreshed according to the CRL update-interval set in the TOE CLI. If the TOE is unable to reach the CRL DP it will not accept the certificate and the session associated with the certificate will be denied.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled **Initial Setup, Certificate Management, Create Certificate Signing Request**, **Import Signed Device Certificate, Export Server Certificate, Import Trusted CA Certificate, Import Certificate Revocation List** 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 states that: **The following steps are required after first boot to put MAGNUM into the Common Criteria evaluated configuration:** • **Observer Power-On Self Test passage** • **Configure IP addresses** • **Configure Date, Time, Time Zone** • **Enable High Security Mode** • **Remove the Evertz default CRL and CA** • **Import the organization's CAs and CRLs** • **Configure Secure Audit Servers** **The Certificate Management, states that:** • **X.509 certificates are used to authenticate all TLS connections. A client certificate is sent whenever the server requests one. This functionality cannot be disabled.** • **Only certificates in PEM format are supported (DER is not supported).** • **Certificate Revocation Lists (CRLs) are downloaded from CRL-DP extensions during each connection attempt, if the peer certificates define them (only for end-user and intermediate certificates, not for root CA certificates).**

	• **Recommend removing the Evertz default CA and CRL during system setup, to replace them with organization-specific certificates.** **The Create Certificate Signing Request, states that:** **MAGNUM initially powers on with a certificate signed by the default Evertz CA. It is recommended to replace this with organization-specific certificates, where a CSR is generated and signed by the organization's CA. This option allows an administrator to create and export a CSR. It is derived from the device's TLS key, which is unique to each device and automatically generated at first power-on, when entering High Security Mode, or when manually reset. The CSR is created with editable fields, but it is expected that the organization's CA will provide its own when creating a signed certificate for the device. The CSR will automatically include the device's current IP addresses in the SAN field.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Create Certificate Signing Request** • **Update each field as appropriate for the particular device and organization** • **Select Create and Export** • **Select the destination, either /home/configshell via SFTP or USB Device** • **The file name is auto-generated during export** **Import Signed Device Certificate:** **After the organization's CA signs a previously exported CSR to create a signed certificate, this option allows the administrator to import the certificate into MAGNUM. This certificate will identify the MAGNUM device to the other devices to which it connects.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Signed Server Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct certificate file (must be in PEM format with a .pem extension)** • **When prompted, reboot** **Export Server Certificate:** **Export the MAGNUM device's certificate used for all TLS connections, if a need for that arises. This only includes the device's public key, not the private key.** • **Log in to the console as configshell and select Security** • **Select Certificate Management**

	• **Select Export Server Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **The file name is auto-generated during export** **Import Trusted CA Certificate:** **Import and thereby trust a CA certificate. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. They must all be signed by a trusted intermediate or root CA. Each CA in the chain must be explicitly imported from here to be trusted.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Trusted CA Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CA certificate file (must be in PEM format with a .crt extension)** • **After the CA certificate is imported, the changes will take place immediately** **Import Certificate Revocation List:** **This option allows the administrator to import CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first. If the peer's end-entity or intermediate CA certificates include a CRL-DP extension, it will be downloaded at every connection attempt, and the connection will be denied if either the download fails or the downloaded CRL revokes a certificate along the peer's certificate chain.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Certificate Revocation list** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CRL file (must have a .crl extension)** • **The change will take effect for all new TLS connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.4 FIA_X509_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the section titled **Show Certificate Revocation List** and **Import Certificate Revocation List** in the AGD to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the AGD states that: **Show Certificate Revocation List:** **This option allows the administrator to review CRLs. This option is useful before and after importing or removing CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Show Certificate Revocation List** • **Select the CRL to review** • **Review the CRL details, using the arrow keys to scroll down or right** **Import Certificate Revocation List:** **This option allows the administrator to import CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first. If the peer's end-entity or intermediate CA certificates include a CRL-DP extension, it will be downloaded at every connection attempt, and the connection will be denied if either the download fails or the downloaded CRL revokes a certificate along the peer's certificate chain.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Certificate Revocation list** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CRL file (must have a .crl extension)** • **The change will take effect for all new TLS connections** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.6.6.5 FIA_X509_EXT.2 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Evaluator Findings	The evaluator examined the section titled **Initial Setup, Certificate Management, Create Certificate Signing Request, Import Signed Device Certificate, Export Server Certificate, Import Trusted CA Certificate, Import Certificate Revocation List, Show Certificate Revocation List and Import Certificate Revocation List** in the AGD. Upon investigation, the evaluator found that the AGD states that: **The following steps are required after first boot to put MAGNUM into the Common Criteria evaluated configuration:** • **Observer Power-On Self Test passage** • **Configure IP addresses** • **Configure Date, Time, Time Zone** • **Enable High Security Mode** • **Remove the Evertz default CRL and CA** • **Import the organization's CAs and CRLs** • **Configure Secure Audit Servers** **The Certificate Management, states that:** • **X.509 certificates are used to authenticate all TLS connections. A client certificate is sent whenever the server requests one. This functionality cannot be disabled.** • **Only certificates in PEM format are supported (DER is not supported).** • **Certificate Revocation Lists (CRLs) are downloaded from CRL-DP extensions during each connection attempt, if the peer certificates define them (only for end-user and intermediate certificates, not for root CA certificates).** • **Recommend removing the Evertz default CA and CRL during system setup, to replace them with organization-specific certificates.** **The Create Certificate Signing Request, states that:** **MAGNUM initially powers on with a certificate signed by the default Evertz CA. It is recommended to replace this with organization-specific certificates, where a CSR is generated and signed by the organization's CA. This option allows an administrator to create and export a CSR. It is derived from the device's TLS key, which is unique to each device and automatically generated at first power-on, when entering High Security Mode, or when manually reset. The CSR is created with editable fields, but it is expected that the**

	organization's CA will provide its own when creating a signed certificate for the device. The CSR will automatically include the device's current IP addresses in the SAN field. • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Create Certificate Signing Request** • **Update each field as appropriate for the particular device and organization** • **Select Create and Export** • **Select the destination, either /home/configshell via SFTP or USB Device** • **The file name is auto-generated during export** **Import Signed Device Certificate:** **After the organization's CA signs a previously exported CSR to create a signed certificate, this option allows the administrator to import the certificate into MAGNUM. This certificate will identify the MAGNUM device to the other devices to which it connects.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Signed Server Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct certificate file (must be in PEM format with a .pem extension)** • **When prompted, reboot** **Export Server Certificate:** **Export the MAGNUM device's certificate used for all TLS connections, if a need for that arises. This only includes the device's public key, not the private key.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Export Server Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **The file name is auto-generated during export** **Import Trusted CA Certificate:**

	Import and thereby trust a CA certificate. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. They must all be signed by a trusted intermediate or root CA. Each CA in the chain must be explicitly imported from here to be trusted. • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Trusted CA Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CA certificate file (must be in PEM format with a .crt extension)** • **After the CA certificate is imported, the changes will take place immediately** **Import Certificate Revocation List:** **This option allows the administrator to import CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first. If the peer's end-entity or intermediate CA certificates include a CRL-DP extension, it will be downloaded at every connection attempt, and the connection will be denied if either the download fails or the downloaded CRL revokes a certificate along the peer's certificate chain.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Certificate Revocation list** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CRL file (must have a .crl extension)** • **The change will take effect for all new TLS connections** **Show Certificate Revocation List:** **This option allows the administrator to review CRLs. This option is useful before and after importing or removing CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Show Certificate Revocation List** • **Select the CRL to review** • **Review the CRL details, using the arrow keys to scroll down or right**

	Import Certificate Revocation List: **This option allows the administrator to import CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first. If the peer's end-entity or intermediate CA certificates include a CRL-DP extension, it will be downloaded at every connection attempt, and the connection will be denied if either the download fails or the downloaded CRL revokes a certificate along the peer's certificate chain.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Certificate Revocation list** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CRL file (must have a .crl extension)** • **The change will take effect for all new TLS connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.6.7 FIA_X509_EXT.3

5.6.7.1 FIA_X509_EXT.3 TSS 1

Objective	If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.
Evaluator Findings	The ST does not claim "device-specific information" hence this assurance activity is considered not applicable to the TOE.
Verdict	N/A

5.6.7.2 FIA_X509_EXT.3 Guidance 1

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

Evaluator Findings	The evaluator examined the section titled **Create Certificate Signing Request** in the AGD to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD states that: **MAGNUM initially powers on with a certificate signed by the default Evertz CA. It is recommended to replace this with organization-specific certificates, where a CSR is generated and signed by the organization's CA. This option allows an administrator to create and export a CSR. It is derived from the device's TLS key, which is unique to each device and automatically generated at first power-on, when entering High Security Mode, or when manually reset. The CSR is created with editable fields, but it is expected that the organization's CA will provide its own when creating a signed certificate for the device. The CSR will automatically include the device's current IP addresses in the SAN field.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Create Certificate Signing Request** • **Update each field as appropriate (Email, Common Name, Organizational Unit, Organization, City/Locality, State/Province, Country, SAN IP, SAN DNS) for the particular device and organization** • **Select Create and Export** • **Select the destination, either /home/configshell via SFTP or USB Device** • **The file name is auto-generated during export** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

5.7 TSS and Guidance Activities (Security Management)

5.7.1 FMT_MOF.1/ManualUpdate

5.7.1.1 FMT_MOF.1/ManualUpdate TSS 1

Objective	For distributed TOEs it is required to verify the TSS to ensure that it describes how every function related to security management is realized for every TOE component and shared between different TOE components. The evaluator shall confirm that all relevant aspects of each TOE component are covered by the FMT SFRs.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.7.1.2 FMT_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	The evaluator examined the section titled **Upgrading Firmware** 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: **Administrators are required to contact Evertz to receive notifications of product updates directly or via an email blast.** **In High Security Mode, all firmware upgrade images (.efp files) will have their signatures (.sig files) verified before being installed. Evertz signs these firmware images at build-time. If the .efp file has been tampered with, the installation is aborted. Always keep the .sig file beside the .efp file.** • **Log in to the console as configshell and select System** • **Select Upgrade** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct .efp file (the .sig file won't appear but it is expected to be beside the .efp file)** • **Consider the prompt, and select Yes to proceed** • **When prompted, enter configshell's password** • **Wait until the upgrade completes, and press q to return** • **When prompted, reboot** • **If the EFP is corrupted it will display the following message:** • **If the upgrade fails, contact Evertz Service Department** **Since the upgrade is done by the local console and during upgradation no activity or services are allowed.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.3 FMT_MOF.1/ManualUpdate Guidance 2

Objective	For distributed TOEs the guidance documentation shall describe all steps how to update all TOE components. This shall contain description of the order in which components need to be updated if the order is relevant to the update process. The guidance documentation shall also provide warnings regarding functions of TOE components and the overall TOE that may cease to operate during the update (if applicable).
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.

Verdict	N/A

5.7.2 FMT_MOF.1/Functions

5.7.2.1 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	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.7.2.2 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 the **FMT_MOF.1/Functions** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE). Upon investigation, the evaluator found that the TSS states that: **The TSF gives the Security Administrator the ability to manage the security functions: auditing operations, administrative user accounts, password and session policies, advisory banners, software updates, as well as cryptographic functions.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.3 FMT_MOF.1/Functions Guidance 2

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

Evaluator Findings	The evaluator examined the section titled **Secure Audit Servers** and **Auditable Events** 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: **System log messages can be sent to a remote audit server. The remote audit server must listen on port 6514 for TLS connections, and its certificate chain must be trusted by MAGNUM in High Security Mode. All audit events are simultaneously sent to the remote server and the local store. If this or any outgoing client connection is unintentionally broken, MAGNUM will automatically reconnect within seconds.** • **Log in to the console as configshell and select Security** • **Select Secure Audit Servers** • **Select Add Server to add new entries** • **Enter a valid IP address** • **Add additional servers as needed** • **Remove a server by selecting it and erasing the IP address value** • **Select Save and Apply** • **When prompted, enter configshell's password** • **The change will take effect immediately** **Auditable Events states that:** **When the audit events in the system are full the TOE will drop new audit messages. If this highly unlikely event occurs, the administrators will have to manually clear the unnecessary files by login in to the shell as the 'configshell' user to make space or increase the disk space by attaching a new hard disk. User identity in auditable events is determined by the following:** • **For SSH sessions: When a user logs in via SSH an audit message indicating the user is generated that includes an SSH session ID. All audit events related to this session include the session ID.** • **All log events with 'configshell' are performed by user 'configshell' on the CLI. The configuration shell is only accessible by the user 'configshell'. Only one 'configshell' user is permitted access to the TOE. No concurrent 'configshell' users are allowed.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FMT_MTD.1/CoreData

5.7.3.1 FMT_MTD.1/CoreData TSS 1

Objective	The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
Evaluator Findings	The evaluator examined the **FMT_MTD.1/CoreData** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that: **The TSF displays a warning banner prior to user authentication. There are no administrative functions available for unauthorized users. All administrators must be authenticated and authorized to perform any activity that can alter TSF data.** The evaluator examined the **FMT_MTD.1/CoreData** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that: **The TSF implements the Security Administrator role to authorized administrators of the TOE. The TSF allows the Security Administrators to administer the TSF via the CLI (local and remote) and a web UI. The TSF permissions restrict access to these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role.** **The TOE is configured with specific user groups that can perform specific tasks. Only those in the admin group are able to access and perform updates. The filesystem ownership under Linux only allows certain users and groups to access the filesystem. Only authorized administrators can access the TOE's trust store and modify or delete certificates within the trust store. So, non-privileged users are not able to update the system files. Command line access is restricted such that regular users do not have access to command line scripts used to manage MAGNUM.** **The web admin and console admin user are statically created on the system. These users cannot be removed from the system.** **Administrator roles are statically assigned. The users admin, etservice, etdev, and the web admin are all in the Administrator role. Users created by the web interface (i.e. web users) are implicitly, automatically assigned into the ("regular") User role.** **Administrators can use console admin interface to administer the system locally or remotely using SSH. The web administrator can also administer MAGNUM over HTTPS.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.3.2 FMT_MTD.1/CoreData TSS 2

Objective	If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.
Evaluator Findings	The evaluator examined the **FMT_MTD.1/CoreData** section titled **TOE Summary Specification** in the Security Target to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that: **Only authorized administrators can access the TOE's trust store and modify or delete certificates within the trust store. So, non-privileged users are not able to update the system files. Command line access is restricted such that regular users do not have access to command line scripts used to manage MAGNUM.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.3 FMT_MTD.1/CoreData Guidance 1

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

Evaluator Findings	The evaluator examined the following section in the AGD to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the AGD includes configuration of the following in the respective sections:
	
	• **Audit Configuration**
	  ○ **Section titled 'Auditable Events, Secure Audit Servers'**
	
	• **TOE Banner**
	  ○ **Section titled 'Web Login Banner'**
	
	• **Session time-out**
	  ○ **Section titled 'Session Timeout'**
	
	• **TOE updates**
	  ○ **Section titled 'Upgrading Firmware'**

	• **X.509 Certificates**
	  ○ **Section titled 'Create Certificate Signing Request, Import Signed Server Certificate,Export Server Certificate, Import Trusted CA Certificate, Export Trusted CA Certificate, Remove Trusted CA Certificate, Import Certificate Revocation List, Remove Certificate Revocation List'**
	• **Basic Startup Configuration**
	  ○ **Section Titled 'Initial Setup, Configuring Date and Time, Configuring IP Addresses, System Security Mode'**
	• **Account Threshold**
	  ○ **Section Titled 'Account Lockout Duration, Account Lockout Threshold, Minimum Password Length, Password Complexity'**
	• **Identification/Authentication**
	  ○ **Sections titled 'Create and Remove Web Users, Change Web User Passwords, Unlock Web Accounts, Unlock SSH Accounts'**
	In addition, section 'Administrative Functions' in the guidance document specifies all the security functions are restricted to authorized security administrators.
	Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.3.4 FMT_MTD.1/CoreData Guidance 2

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

	This option allows the administrator to review the CA certificates trusted by a MAGNUM device. This option is useful before and after importing or removing trusted CA certificates. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. They must all be signed by a trusted CA. Each CA in the chain must be explicitly imported from here to be trusted. • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Show Trusted CA Certificates** • **Select a particular CA certificate to review** • **Review the certificate details, using the arrow keys to scroll down or right** The evaluator examined the section titled **Import Trusted CA Certificate, Export Trusted CA Certificate,** and **Remove Trusted CA Certificate** in the AGD to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD states that: **Import Trusted CA Certificate:** **Import and thereby trust a CA certificate. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. They must all be signed by a trusted intermediate or root CA. Each CA in the chain must be explicitly imported from here to be trusted.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Import Trusted CA Certificate** • **When prompted, enter configshell's password** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **Select the correct CA certificate file (must be in PEM format with a .crt extension)** • **After the CA certificate is imported, the changes will take place immediately** **Export Trusted CA Certificate:** **Export any trusted CA certificate, if a need for that arises.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Export Trusted CA Certificate** • **When prompted, enter configshell's password** • **Select the CA certificate to export** • **Select the file's source, either /home/configshell via SFTP or USB Device** • **The file name is kept the same after export**

	Remove Trusted CA Certificate: **Remove and thereby stop trusting a CA certificate. In High Security Mode, all CA certificates must have a corresponding CRL, which must be removed first. This is enforced by MAGNUM to ensure there are no stale CRLs.** • **Log in to the console as configshell and select Security** • **Select Certificate Management** • **Select Remove Trusted CA Certificate** • **Select the trusted CA certificate to remove and stop trusting** • **When prompted, enter configshell's password** • **The change will take effect for all new TLS connections** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4 FMT_MTD.1/CryptoKeys

5.7.4.1 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	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.7.4.2 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 those operations are performed.
Evaluator Findings	The evaluator examined the **FMT_MTD.1/CryptoKeys** section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how those operations are performed. Upon investigation, the evaluator found that the TSS states that: **The web UI and CLI allow the Security Administrator to perform the following TSF management functions:** • **Keys** ○ **Importing a Public Key (SSH public keys)**

	○ **TLS Key Reset (TLS keys cannot be imported. They are automatically generated when a CSR is generated, and can only be reset/replaced, not deleted. TLS keys are reset when a new CSR is generated.)** • **Cluster Key Import / Export / Reset Certificates** ○ **Create Certificate Signing Request (TLS keys are automatically generated when creating a CSR)** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.3 FMT_MTD.1/CryptoKeys Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the section titled **Reset SSH Key** and **Reset TLS Key and Certificate** 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: **Erase the device's current SSH Key and generate a new one during reboot.** • **Log in to the console as configshell and select Security** • **Select Reset SSH Key** • **Select Yes to proceed** • **When prompted, enter configshell's password** • **When prompted, reboot** • **A new key will be automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.** **Reset TLS Key and Certificate:** **In High Security Mode, MAGNUM encrypts all TLS connections with TLSv1.2. This option allows an administrator to change the private TLS key at any time. The new random key is chosen automatically. A new self-signed certificate will also be created, replacing any existing certificate identifying the device. The administrator should generate a new CSR and have it signed by a CA before MAGNUM reconnects to other devices.** • **Log in to the console as configshell and select Security** • **Select Reset TLS Key and Certificate** • **Select Yes to proceed** • **When prompted, enter configshell's password** • **When prompted, reboot**

	• **A new key and self-signed certificate are automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.** • **Create a new CSR, sign it, and import it before connecting MAGNUM to other devices** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5 FMT_SMF.1

5.7.5.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall examine the TSS, Guidance Documentation and the TOE as observed during all other testing and shall confirm that the management functions specified in FMT_SMF.1 are provided by the TOE. The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.
Evaluator Findings	The evaluator examined the **FMT_SMF.1** section titled **TOE Summary Specification** in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator found that the AGD states that: **The TSF implements the Security Administrator role to authorized administrators of the TOE. The TSF allows the Security Administrators to administer the TSF via the CLI (local and remote) and a web UI. The TSF permissions restrict access to these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role. The web UI and CLI allow the Security Administrator to perform the following TSF management functions:** The evaluator examined the section titled **FMT_SMF.1** in the TSS to verify that it describes the local administrative interface. **Administrators can use console admin interface to administer the system locally via local console port.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.2 FMT_SMF.1 TSS 2

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

	shall check that the TOE behaviour observed during testing of the configured SFRs is as described in the TSS and Guidance Documentation.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.7.5.3 FMT_SMF.1 Guidance 1

Objective	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.
Evaluator Findings	The evaluator examined the following sections in each AGD to verify that it describes the local administrative interface. Upon investigation, the evaluator mentioned the respective sections in each AGD for the points stated in the TSS as below: **The specific management capabilities available from the TOE include:** • **Ability to System Setup** ○ **Section 'Initial Setup'** ○ **Section 'Connection Security Options'** ○ **Section 'Data Purge'** • **Administrator Log In/Out of:** ○ **Section 'Logging in to Local Console, Logging Out Of Local Console'** ○ **Section 'Logging in with SSH, Logging out of SSH, Logging in to Web Interface, Logging out of Web Interface'** • **Web/User Interface Configuration:** ○ **Section 'Configuring Date and Time'** ○ **Section 'Configuring IP Addresses'** ○ **Section 'Audit Servers'** ○ **Section 'Session Timeout'** • **Transferring Files** ○ **Using FTPS Section 'Files Using SFTP'** ○ **Using SFTP Section 'Files Using SFTP'** ○ **Using SCP Section 'Files Using SFTP'** • **Editing the Login Banner**

	○ **Section 'Edit Login Banner'** • **Keys** ○ **Section 'Import Code Verification Public Key'** ○ **Section 'Reset SSH Key, Reset TLS Key and Certificate'** • **Cluster Key Import / Export / Reset Certificates** ○ **Section 'Create Certificate Signing Request'** ○ **Section 'Show Server Certificate, Import Signed Server Certificate, Export Server Certificate'** ○ **Section 'Show Trusted CA Certificates, Import Trusted CA Certificate, Export Trusted CA Certificate, Remove Trusted CA Certificate'** ○ **Section 'Show Certificate Revocation List, Import Certificate Revocation List, Remove Certificate Revocation List'** ○ **Section 'Allowed Subject Alt Names (DNS), Allow Subject Alt Names (IP)'** • **Administer Passwords** ○ **Linux User Section 'Minimum Password Length, Password Complexity'** ○ **Web User Section 'Change Web User Passwords'** • **Add / Delete** ○ **Section 'Create and Remove Web Users'** • **Audits** ○ **Section 'Export Logs'** • **Firmware** ○ **Section 'Check Version from Console'** ○ **Section 'Check Version from Web Interface'** • **Upgrade** ○ **Section 'Upgrading Firmware'** The evaluator examined the section titled '**Logging in to Local Console**' in the AGD to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD describes the steps associated

	with connecting to the serial port of a computer. This sufficiently ensures that the interface is a local interface. Based on these findings, this assurance activity is considered satisfied. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6 FMT_SMR.2

5.7.6.1 FMT_SMR.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.
Evaluator Findings	The evaluator examined the **FMT_SMR.2** section titled **TOE Summary Specification** in the TSS to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the TSS states that: **The TOE is configured with specific user groups that can perform specific tasks. Only those in the admin group are able to access and perform updates. The filesystem ownership under Linux only allows certain users and groups to access the filesystem. Only authorized administrators can access the TOE's trust store and modify or delete certificates within the trust store. So, non-privileged users are not able to update the system files. Command line access is restricted such that regular users do not have access to command line scripts used to manage MAGNUM.** **The web admin and console admin user are statically created on the system. These users cannot be removed from the system.** **Administrator roles are statically assigned. The users admin, etservice, etdev, and the web admin are all in the Administrator role. Users created by the web interface (i.e. web users) are implicitly, automatically assigned into the ("regular") User role.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6.2 FMT_SMR.2 Guidance 1

Objective	The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.
Evaluator Findings	The evaluator examined the section titled **Initial Setup, Logging in to Local Console, Logging in with SSH,** and **Logging in to Web Interface** 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 states that: **Initial Setup**

	The following steps are required after first boot to put MAGNUM into the Common Criteria evaluated configuration: • **Observer Power-On Self Test passage** • **Configure IP addresses** • **Configure Date, Time, Time Zone** • **Enable High Security Mode** • **Remove the Evertz default CRL and CA** • **Import the organization's CAs and CRLs** • **Configure Secure Audit Servers** **Logging in to Local Console:** **Most administrative actions are accomplished through the console menu. Failed login attempts on the local console do not trigger account lockouts. Only administrative users have access to the console menu, either locally or remotely. No unprivileged users are permitted access to the console menu.** • **Connect a VGA monitor and a USB keyboard** • **Switch console sessions by pressing <CTRL><ALT><F1> through <CTRL><ALT><F6>.** • **Log in with username configshell and default password configshell to access a structured menu** • **Changing any settings requires entering configshell's password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings.** • **There also exists users etservice and etdev that access an open shell with limited permissions** **Logging in with SSH:** **The console menu is available over SSH for remote administration. Too many failed login attempts over SSH will trigger account lockouts.** • **Use Putty or a similar SSH client from a PCEnter MAGNUM's IP address (use default port 22)** • **Log in with username configshell and default password configshell to access a structured menu** • **Changing any settings requires entering configshell's password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings.** • **There also exists users etservice and etdev that access an open shell with limited permissions** **Logging in to Web Interface:** **MAGNUM's application features are accessed with a web browser. Chrome and Safari are supported. Too many failed login attempts over the web interface will trigger account lockouts.** • **Launch a web browser session** • **Enter the IP address of MAGNUM**

	• **Log in with username admin and default password admin (other users can be created as well)** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (Protection of the TSF)

5.8.1 FPT_APW_EXT.1

5.8.1.1 FPT_APW_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.
Evaluator Findings	The evaluator examined the **FPT_APW_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. The evaluator also examined the TSS section 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 the authentication data stored by the TOE. The TSF does not store plaintext password. The salted SHA-512 hash of the password is saved to disk (using the Linux PAM cracklib module). Passwords for users of the web interface are stored in a PostgreSQL database and obfuscated using a salted Blowfish hash. Both the password file and the database reside on the filesystem, which is access controlled through Linux file permissions.** **MAGNUM also uses Linux permissions to prevent accessing the obscured forms of the passwords.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2 FPT_SKP_EXT.1

5.8.2.1 FPT_SKP_EXT.1 TSS 1

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

Evaluator Findings	The evaluator examined the **FPT_SKP_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that: **MAGNUM uses Linux file permissions to only allow the appropriate services programmatic access to protect private keys from being read.** **The TOE's keys associated with its certificate for TLS are stored in a disk partition with file permissions that do not allow user or administrator access. None of these services have methods to expose the key beyond their immediate use.** **The keys/CSPs used by the TOE, their storage location and format, and their associated zeroization method are as below:** • **EC Diffie-Hellman Keys** ○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***Key agreement and key establishment*** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **Firmware Update Key** ○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***Verification of firmware integrity when updating to new firmware versions using a SHA-512 hashed RSA signature.*** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **HTTPS/TLS Server/Host Key** ○ **Storage location and method:** ***Plaintext in a separate disk partition that uses Linux file permission*** ○ **Usage:** ***RSA and EC private key used in the HTTPS/TLS protocols*** ○ **Zeroization:** ***Instructing a part of the code to destroy the abstraction that represents the key.*** • **HTTPS/TLS session authentication key** ○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***HMAC Sha*-1, -256, or -384 key used for HTTPS/TLS session authentication.** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **HTTPS/TLS Session Encryption Key** ○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***AES (128, 256) key used for HTTPS/TLS session encryption*** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **SSH Server/Host key** ○ **Storage location and method:** ***Plaintext in a separate disk partition that uses Linux file permission*** ○ **Usage:** ***RSA private key used in the SSH protocol (key establishment, 2048- or 3072-bit)*** ○ **Zeroization:** ***Instructing a part of the code to destroy the abstraction that represents the key.*** • **SSH Session Authentication Key**

	○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***HMAC-SHA2-256 or HMAC-SHA2-2512 key used for SSH session authentication*** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **SSH Session Encryption Key** ○ **Storage location and method:** ***Plaintext in RAM*** ○ **Usage:** ***AES (128-, 256-bit) key used for SSH session encryption*** ○ **Zeroization:** ***Overwritten with zeroes when no longer needed.*** • **Locally Stored Passwords** ○ **Storage location and method:** ***SHA-512 Hashed in configuration file*** ○ **Usage:** ***User Authentication*** ○ **Zeroization:** ***Overwritten with pseudorandom pattern using the TSF's RBG/ zeros.*** • **Configuration Encryption Key** ○ **Storage location and method:** ***Plaintext in a separate disk partition that uses Linux file permission*** ○ **Usage:** ***Configuration Encryption*** ○ **Zeroization:** ***Instructing a part of the code to destroy the abstraction that represents the key.*** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FPT_STM_EXT.1

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

Objective	The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. If "obtain time from the underlying virtualization system" is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.
Evaluator Findings	The evaluator examined the **FPT_STM_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that:

	MAGNUM provides accurate timestamps that can be updated via manual configuration by the administrator. System time is used to provide accurate time/date stamps on audit records, to track administrator inactivity and for the validation of X.509 certificates used in TLS communications. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 FPT_STM_EXT.1 Guidance 1

Objective	The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication. If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.
Evaluator Findings	The evaluator examined the section titled **Configuring Date and 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: **Understanding logged audit events requires accurate time keeping. Reboot is required after changing the date or time.** • **Log in to the console as configshell and select System** • **Select and configure Time Zone** • **Select and configure Date** • **Select and configure Time** • **Reboot** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FPT_TST_EXT.1.1

5.8.4.1 FPT_TST_EXT.1.1 TSS 1

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

Evaluator Findings	The evaluator examined the **FPT_TST_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS states that: **The firmware is validated in the following three ways on startup:** • **The bootloader verifies a SHA-512 checksum of the kernel image before loading the image** • **MAGNUM invokes OpenSSL to display its version, which will trigger the built-in self-tests. This ensures that the crypto module has not been tampered with.** **These self-tests include:** ○ **SHA-256/284/521 KAT** ○ **HMAC-SHA-256/521 KAT** ○ **AES 128 GCM Encrypt and Decrypt KAT** ○ **AES 256 GCM Encrypt and Decrypt KAT** ○ **AES 128 CTR Encrypt and Decrypt KAT** ○ **RSA 4096 SHA-256 Sign and Verify KAT** ○ **DRBG AES-CTR-256 KAT (invoking the instantiate, reseed, and generate functions)** • **MAGNUM verifies SHA-512 chesksums of all non-configuration files, including executable and shared object files.** The evaluator examined the **FPT_TST_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that: **These tests verify that TOE firmware has not been modified and all cryptographic functions are working correctly.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 FPT_TST_EXT.1.1 TSS 2

Objective	For distributed TOEs the evaluator shall examine the TSS to ensure that it details which TOE component performs which self-tests and when these self-tests are run.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.8.4.3 FPT_TST_EXT.1.1 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined the section titled **Power-On Self Test** and **Firmware Integrity Check** 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: **A self test of the device's cryptographic modules is always performed at power-on.** **If the self test fails, please contact the Evertz Service Department.** **Firmware Integrity Check states that:** • **In High Security Mode, a firmware integrity check is performed at every power-on:** • **If the firmware integrity check fails, please contact the Evertz Service Department.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.4 FPT_TST_EXT.1.1 Guidance 2

Objective	For distributed TOEs the evaluator shall ensure that the guidance documentation describes how to determine from an error message returned which TOE component has failed the self-test.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.8.5 FPT_TUD_EXT.1

5.8.5.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that:

	The MAGNUM server is typically deployed in a closed network without direct access to the internet. In these instances, Administrators are required to contact Evertz to receive notification of production updates directly or via email blast. Operators may verify the current version using the CLI menu 'Version' or on the web interface Config Management->Current System Info. The evaluator examined the **FPT_TUD_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS, if a trusted update can be installed on the TOE with a delayed activation, describes how and when the inactive version becomes active. Upon investigation, the evaluator found that the TSS states that: **When the administrator selects the update file the TSF will ask if the file should be installed. When the administrator selects [yes] the TSF automatically verifies the digital signature prior to installing the update. In the event that an update file fails verification the update is rejected and an appropriate audit record is generated.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.2 FPT_TUD_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	The evaluator examined the **FPT_TUD_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes all TSF software update mechanisms for updating the system software, includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS states that: **When the administrator selects the update file the TSF will ask if the file should be installed. When the administrator selects [yes] the TSF automatically verifies the digital signature prior to installing the update. In the event that an update file fails verification the update is rejected and an appropriate audit record is generated.** The evaluator examined the **FPT_TUD_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification. Upon investigation, the evaluator found that the TSS

	states that: **Customers requiring secure delivery for site policy can request secure courier delivery of software updates. Digital delivery may be provided via File Transfer Protocol Secure (FTPS) using signed and hashed code. Instructions for FTPS transfer are found in [CC2] in the Transferring Files in High Security Mode section. When the administrator selects the update file the TSF will ask if the file should be installed. When the administrator selects [yes] the TSF automatically verifies the digital signature prior to installing the update. In the event that an update file fails verification the update is rejected and an appropriate audit record is generated.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.3 FPT_TUD_EXT.1 TSS 3

Objective	If the options 'support automatic checking for updates' or 'support automatic updates' are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.
Evaluator Findings	The evaluator examined the Security Target and found that the options 'support automatic checking for updates' or 'support automatic updates' are not chosen from the selection in FPT_TUD_EXT.1.2 Based on these findings, this assurance activity is considered satisfied.
Verdict	N/A

5.8.5.4 FPT_TUD_EXT.1 TSS 4

Objective	For distributed TOEs, the evaluator shall examine the TSS to ensure that it describes how all TOE components are updated, that it describes all mechanisms that support continuous proper functioning of the TOE during update (when applying updates separately to individual TOE components) and how verification of the signature or checksum is performed for each TOE component. Alternatively, this description can be provided in the guidance documentation. In that case the evaluator should examine the guidance documentation instead.
Evaluator Findings	Not applicable because the TOE is not a distributed TOE.
Verdict	N/A

5.8.5.5 FPT_TUD_EXT.1 TSS 5

Objective	If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular,

	authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.
Evaluator Findings	The evaluator examined the Security Target and found that the published hash is not used to protect the trusted update mechanism. Based on these findings, this assurance activity is considered satisfied.
Verdict	N/A

5.8.5.6 FPT_TUD_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version.
Evaluator Findings	The evaluator examined the section titled **Check Version from Console** and **Check Version from Web Interface** 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: • **Log in to the console as configshell** • **Select Version** • **Using the arrow keys, scroll through the installed packages list** • **Search by entering / (forward slash) then a search pattern** • **Search for "magnum-rootfs" to get the MAGNUM version** • **Press the q key to return to the main menu** **Check Version from Web Interface states that:** • **Log in to the web interface as admin** • **Select Configuration Management from the SDVN system** • **Select Current System Info** • **Scroll or search for "magnum-rootfs" to get the MAGNUM version** • **Click Close** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.7 FPT_TUD_EXT.1 Guidance 2

Objective	The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
Evaluator Findings	The evaluator examined the section titled **Firmware Integrity Check** 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: **In High Security Mode, a firmware integrity check is performed at every power-on:** **If the firmware integrity check fails, please contact the Evertz Service Department.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.8 FPT_TUD_EXT.1 Guidance 3

Objective	If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.
Evaluator Findings	The evaluator examined the Security Target & AGD and found that the published hash is not used to protect the trusted update mechanism. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.9 FPT_TUD_EXT.1 Guidance 4

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

5.8.5.10 FPT_TUD_EXT.1 Guidance 5

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

5.8.5.11 FPT_TUD_EXT.1 Guidance 6

Objective	If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.
Evaluator Findings	The evaluator examined the Security Target & AGD and verified that a certificate-based mechanism is not used for software update digital signature verification. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (TOE Access)

5.9.1 FTA_SSL_EXT.1

5.9.1.1 FTA_SSL_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings.
Evaluator Findings	The evaluator examined the **FTA_SSL_EXT.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies whether local administrative session locking or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that: **MAGNUM has a configurable timeout that can be modified using the console admin interface. The timeout is 15 minutes in secure mode, adjustable to anywhere between 1 and 60 minutes. When a timeout occurs, the user's session is terminated, and the user is logged out of the system. This applies to console, SSH, and web interactive sessions.**

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

5.9.1.2 FTA_SSL_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period.
Evaluator Findings	The evaluator examined the section titled **Account Lockout Duration, Account Lockout Threshold** and **Session Timeout** in the AGD to verify that it states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD states that: **Configure how long console and web accounts are locked after too many failed login attempts.** • **Log in to the console as configshell and select Security** • **Select Account Lockout Duration** • **When prompted, enter configshell's password** • **Enter the new account lockout duration (in minutes)** • **The change will take effect immediately** **Account Lockout Threshold states that:** • **Configure how many failed login attempts will temporarily lock console and web accounts.** • **Log in to the console as configshell and select Security** • **Select Account Lockout Threshold** • **When prompted, enter configshell's password** • **Enter the new account lockout threshold** • **The change will take effect immediately** **Session Timeout states that:** • **Log in to the console as configshell and select Security** • **Select Session Timeout** • **When prompted, enter configshell's password** • **Enter the new session timeout (in minutes)** • **The change will take effect for any new user logins** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FTA_SSL.3

5.9.2.1 FTA_SSL.3 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.
Evaluator Findings	The evaluator examined the **FTA_SSL.3** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that: **MAGNUM has a configurable timeout that can be modified using the console admin interface. The timeout is 15 minutes in secure mode, adjustable to anywhere between 1 and 60 minutes. When a timeout occurs, the user's session is terminated, and the user is logged out of the system. This applies to console, SSH, and web interactive sessions.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2.2 FTA_SSL.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.
Evaluator Findings	The evaluator examined the section titled **Account Lockout Duration, Account Lockout Threshold** and **Session Timeout** in the AGD to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD states that: **Configure how long console and web accounts are locked after too many failed login attempts.** • **Log in to the console as configshell and select Security** • **Select Account Lockout Duration** • **When prompted, enter configshell's password** • **Enter the new account lockout duration (in minutes)** • **The change will take effect immediately** **Account Lockout Threshold states that:** **Configure how many failed login attempts will temporarily lock console and web accounts.** • **Log in to the console as configshell and select Security** • **Select Account Lockout Threshold** • **When prompted, enter configshell's password**

	• **Enter the new account lockout threshold** • **The change will take effect immediately** **Session Timeout states that:** **Inactive console and web sessions are disconnected after a configurable session timeout** • **Log in to the console as configshell and select Security** • **Select Session Timeout** • **When prompted, enter configshell's password** • **Enter the new session timeout (in minutes)** • **The change will take effect for any new user logins** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3 FTA_SSL.4

5.9.3.1 FTA_SSL.4 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.
Evaluator Findings	The evaluator examined the **FTA_SSL.4** section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that: **On a local terminal, select "Logout" from the console admin interface to manually terminate an interactive session. On the command line interface, type 'exit' to manually terminate a remote interactive session via SSH, and on the WebGUI, select 'Logout' to manually exit a session.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.2 FTA_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	The evaluator examined the section titled **Logging Out of Local Console, Logging out of SSH** and **Logging out of Web Interface** 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:

	Logging Out of Local Console states that: **1. Select logout at the bottom of the menu list.** **2. This will close the current administration session** **Logging out of SSH states that:** **1. Select logout at the bottom of the menu list.** **2. This will close the current SSH session** **Logging out of Web Interface states that:** **1. Select the person icon on the top right of the web page** **2. Select Logout** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4 FTA_TAB.1

5.9.4.1 FTA_TAB.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).
Evaluator Findings	The evaluator examined the **FTA_TAB.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access. Upon investigation, the evaluator found that the TSS states that: **MAGNUM is managed locally through the local console and remotely over SSH and the HTTPS web interface. Administrators access the console through directly connected USB keyboard and VGA monitor.** **The TSF presents the access banner prior to authentication when a user connects to the remote web UI or local console CLI described in the FIA_UIA_EXT.1, FIA_UAU_EXT.2 description.**

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

5.9.4.2 FTA_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	The evaluator examined the section titled **Edit Login Banner** in the AGD to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that: **The message in MAGNUM's login banner can be customized, depending on each organization's requirements. The console and web login banners share the same message.** • **Log in to the console as configshell and select Security** • **Select Edit Login Banner** • **Edit the message as required. The editor is called "nano" (see https://www.nanoeditor.org/docs.php for details on how to use)** • **To save and exit press <CTRL>X, then Y, then <Enter>** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10 TSS and Guidance Activities (Trusted Path/Channels)

5.10.1 FTP_ITC.1

5.10.1.1 FTP_ITC.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	The evaluator examined the **FTP_ITC.1** section titled **TOE Summary Specification** in the Security Target to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator further examined the TSS section to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that:

	Trusted channels are established between the TOE and a remote audit server and video switches. The TOE initiates the connection for remote audit servers and video switches. **When using the stunnel program to communicate with video switches over TLS, the trusted certificate verifies the validity of the communication via mutual authentication of X.509 certificates. For the trusted channel communication between the TOE and the remote audit server does not use mutual authentication.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.2 FTP_ITC.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	The evaluator examined the section titled **Configuration of IPX Channel** 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: **Log in to the Magnum through WebUI → Select the System type as SDVN → Click on Devices and Links → Click on Add Device(s) → Select the required Device Type → Select the Number of Devices → Enter device details and click on Add Device → The device is added** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2 FTP_TRP.1/Admin

5.10.2.1 FTP_TRP.1/Admin TSS 1

Objective	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.
Evaluator Findings	The evaluator examined the **FTP_TRP.1/Admin** section titled **TOE Summary Specification** in the Security Target to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that: **MAGNUM only communicates with Administrative Users via Trusted Paths. For remote administration this is restricted to a GUI over HTTPS or the command line over SSH.**

	MAGNUM uses encryption and restricts the choices of ciphers, hashes, and key-exchange algorithms to those allowed by the NDcPP. Next, the evaluator compared the protocols identified in the TSS to the definition of the SFR. The evaluator found that the protocols listed in the TSS are consistent with the protocols listed in the definition of the SFR. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2.2 FTP_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	The evaluator examined the section titled **Logging in with SSH** and **Logging in to Web Interface** 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 states that: **Logging in with SSH** **The console menu is available over SSH for remote administration. Too many failed login attempts over SSH will trigger account lockouts.** • **Use Putty or a similar SSH client from a PC** • **Enter MAGNUM's IP address (use default port 22)** • **Log in with username configshell and default password configshell to access a structured menu** • **Changing any settings requires entering configshell's password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings.** • **There also exists users etservice and etdev that access an open shell with limited permissions** **Logging in to Web Interface states that:** **MAGNUM's application features are accessed with a web browser. Chrome and Safari are supported. Too many failed login attempts over the web interface will trigger account lockouts.** • **Launch a web browser session** • **Enter the IP address of MAGNUM** • **Log in with username admin and default password admin (other users can be created as well)** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 FAU_GEN.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Test Steps	• Trigger each auditable event on the TOE • Verify that each audit record is generated and contains the required information
Expected Test Results	• **The TOE should be able to generate audit records for each of the events described in the ST under the FAU_GEN.1.1 & FAU_GEN.1.2.** • **The audit records generated should match the proper format as specified in the guidance documentation.**
Pass/Fail with Explanation	Pass. • The TOE was able to generate audit records for each of the events described in the ST under the FAU_GEN.1.1 & FAU_GEN.1.2. • The audit records generated does matches the proper format as specified in the guidance documentation.

6.2 FAU_STG_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.

Test Steps	• Confirm secure connection with the audit server. • Send audit data to the audit server from the TOE. • Confirm that audit logs were sent to the syslog server. • Examine traffic to ensure it is not plaintext.
Expected Test Results	**Audit data from the TOE is protected by TLS when it is exported.**
Pass/Fail with Explanation	Pass. Audit data from the TOE is protected by TLS when it is exported. It can be verified with the packet capture. This meets the testing requirement.

6.3 FAU_STG_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option '**drop new audit data**' in FAU_STG_EXT.1.3).
Test Steps	• Fill the audit log • Log into TOE to generate logs and note the time • Verify that new audit logs are not generated
Expected Test Results	**The TOE stops logging when the local audit space is filled**
Pass/Fail with Explanation	Pass. The TOE drops new logs when the storage space is full. This meets the requirement.

6.4 FAU_STG_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '**overwrite previous audit records**' in FAU_STG_EXT.1.3)

Pass/Fail with Explanation	This test is not applicable since the TOE does not claim this functionality

6.5 FAU_STG_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The TOE behaves as specified (for the option '**other action**' in FAU_STG_EXT.1.3).
Pass/Fail with Explanation	This test is not applicable since the TOE does not claim this functionality

6.6 FAU_STG_EXT.1 Test #4

Item	Data
Test Assurance Activity	Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.
Pass/Fail with Explanation	This test is not applicable since the TOE is not a distributed TOE

6.7 FPT_STM_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: If the TOE supports direct **setting of the time by the Security Administrator,** then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Steps	• Confirm the current time on the TOE • Set a new time on the TOE via the remote GUI over TLS • Verify that the new time is set
Expected Test Results	**The TOE should support the manual setting of time.**
Pass/Fail with Explanation	Pass: The TOE supports the manual setting of time. This meets the testing requirement.

6.8 FPT_STM_EXT.1 Test #2

Item	Data
Test Assurance Activity	Test 2: If the TOE supports the **use of an NTP server**; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Pass/Fail with Explanation	The TOE does not claim NTP hence this test is not applicable

6.9 FPT_STM_EXT.1 Test #3

Item	Data
Test Assurance Activity	If **the audit component of the TOE consists of several parts with independent time information**, then the evaluator shall verify that the time information between the different parts are either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously.
Pass/Fail with Explanation	The TOE does not support independent time information, hence, this test is not applicable.

6.10 FTP_ITC.1 Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	• Configure the TOE to connect with a syslog server, this will configure a secure channel between the TOE and the IT entity • Initiate the connection between the TOE and the IT entity • Perform a packet capture of the traffic between the TOE and the IT entity Verify that the connection is not sent plaintext • Verify successful connection with the logs • Repeat this process for a connection with IPX
Expected Test Results	**External connections from the TOE are sent via an encrypted channel.**
Pass/Fail with Explanation	Pass. External connections to Syslog server and Video switch from the TOE are sent via an encrypted channel.

6.11 FTP_ITC.1 Test #2

Item	Data
Test Assurance Activity	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
Test Steps	This test case is covered in FTP_ITC.1_T1
Expected Test Results	**This test case is covered in FTP_ITC.1_T1**
Pass/Fail with Explanation	Pass. This test case is covered in FTP_ITC.1_T1

6.12 FTP_ITC.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Steps	This test case is covered in FTP_ITC.1_T1
Expected Test Results	**This test case is covered in FTP_ITC.1_T1**
Pass/Fail with Explanation	Pass. This test case is covered in FTP_ITC.1_T1

6.13 FTP_ITC.1 Test #4

Item	Data
Test Assurance Activity	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations: 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	Syslog Server Short Disconnect: • Configure the TOE to connect with a syslog server

	• Initiate the connection between the TOE and the Syslog Server • Verify that the connection is not sent plaintext using packet capture • Disconnect the connectivity between TOE and the syslog server for a short interval of around 2mins. • Reconnect the connectivity between TOE and the syslog server. From the TOE, continue to send data and verify that the data sent from the TOE is not sent in plaintext • Verify with the logs Syslog Server Long Disconnect: • Configure the TOE to connect with a syslog server • Initiate the connection between the TOE and the Syslog Server • Verify that the connection is not sent plaintext using packet capture • Disconnect the connectivity between TOE and the syslog server for a long interval of **5mins.** • Reconnect the connectivity between TOE and the syslog server. From the TOE, continue to send data and verify that the data sent from the TOE is not sent in plaintext • Verify with the Logs IPX Short Disconnect: • Initiate the connection between the TOE and the IPX • Verify that the connection is not sent plaintext using packet capture • Disconnect the connectivity between TOE and the syslog server for a short interval of around 40Seconds • Reconnect the connectivity between TOE and the syslog server. From the TOE, continue to send data and verify that the data sent from the TOE is not sent in plaintext • Verify with the Logs IPX Long Disconnect: • Initiate the connection between the TOE and the IPX • Verify that the connection is not sent plaintext using packet capture • Disconnect the connectivity between TOE and the syslog server for a long interval of 50 seconds. • Reconnect the connectivity between TOE and the syslog server. From the TOE, continue to send data and verify that the data sent from the TOE is not sent in plaintext • Verify with the Logs

Expected Test Results	**When physical connectivity with a syslog and IPX server is interrupted and then restored, the data is exchanged between both entities is never in plaintext, as can be shown by packet captures during and after the outage.**
Pass/Fail with Explanation	Pass. When physical connectivity with a syslog and IPX server is interrupted and then restored, the data is exchanged between both entities is never in plaintext, as can be shown by packet captures during and after the outage. This meets the testing requirement.

6.14 FIA_AFL.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Test Steps	• Obtain the value of lockout period and maximum authentication failure • Configure the value by changing of lockout period and authentication failure • Verify that when the user incorrectly authenticates after a set amount of times, the user is locked out via web • Verify that when the user incorrectly authenticates after a set amount of times, the user is locked out via SSH
Expected Test Results	**The TOE should not allow for access to the device if an account fails authentication after a configured number of attempts.**
Pass/Fail with Explanation	Pass: The TOE denied access to accounts after invalid authentication attempts. This meets testing requirements.

6.15 FIA_AFL.1 Test #2a

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any fs 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	• Configure the value by changing the lockout authentication failure • Verify that account is locked when maximum incorrect authentication attempt is reached for CLI • Using different administrator credentials unlock the offending user • Login with the now unlocked user credentials and verify that the user can successfully login. • Verify that account is locked when maximum incorrect authentication attempt is reached for WebUI • Using different administrator credentials unlock the offending user • Login with the now unlocked user credentials and verify that the user can successfully login.
Expected Test Results	**User can get into the system with correct credentials after the account is unlocked by the Administrator.**
Pass/Fail with Explanation	Pass: User can get into the system with correct credentials after the account is unlocked by the Administrator.

6.16 FIA_AFL.1 Test #2b

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g. any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: If the **time period** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorisation attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time period configured in Test 1 and show that an authorisation attempt using valid credentials results in successful access.
Test Steps	• Configure the value by changing the lockout authentication failure • Verify that account is locked when maximum incorrect authentication attempt is reached for CLI • Wait for lockout period to get over • Login with correct credentials and verify it allows to get into the system • Verify that account is locked when maximum incorrect authentication attempt is reached for WebUI • Wait for lockout period to get over • Login with correct credentials and verify it allows to get into the system

Expected Test Results	**User can get into the system with correct credentials after lockout period is done.**
Pass/Fail with Explanation	Pass. User can get into the system with correct credentials by waiting until the time period has expired.

6.17 FIA_PMG_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing.
Test Steps	• Set the minimum length between 8 characters respectively and update the configuration • Verify via logs that the configuration is updated. • Provide a password with the required characters "1234`~!@qwER" and verify that it passes. • Verify via logs that the password-reset was successful. • Provide a password with the required characters "5#6$7%8^tyUI" and verify that it passes. • Verify via logs that the password-reset was successful. • Provide a password with the required characters "90asDF&*()-=_+" and verify that it passes. • Verify via logs that the password-reset was successful. • Provide a password with the required characters "1234}]qwER[{" and verify that it passes. • Verify via logs that the password-reset was successful. • Provide a password with the required characters "12qwER\|:;"'" and verify that it passes. • Verify via logs that the password-reset was successful. • Provide a password with the required characters "12<>?,./qwER" and verify that it passes. • Verify via logs that the password-reset was successful. • Provide a password for WebUI with the required characters "1a2s#D$F" and verify that it passes. • Verify via logs that the password-reset was successful.
Expected Test Results	**The TOE accepts valid password combinations that meets the requirements on remote CLI**
Pass/Fail with Explanation	Pass. The TOE accepts valid password combinations that meets the requirements.

6.18 FIA_PMG_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
Test Steps	**SSH** • Provide a password that is less than 8 characters i.e 4 characters and verify that it fails • Provide a password 10 character password with no upper or lower case letters "123test321" and verify that it fails • Provide a password 9 character password with no digits "Corelight" and verify that it fails • Provide a password 10 character password with no special character "123TesT321" and verify that it fails **WebUI:** • Provide a password that is less than 8 characters i.e 4 characters and verify that it fails • Provide a password 10 character password with no upper or lower case letters "123test321" and verify that it fails • Provide a password 9 character password with no digits "Corelight" and verify that it fails • Provide a password 10 character password with no special character "123TesT321" and verify that it fails
Expected Test Results	**The TOE only accepts valid password combinations.**
Pass/Fail with Explanation	Pass: The TOE does not allow to change the password when the password combination is not matched. The TOE only accepts valid password combinations.

6.19 FIA_UIA_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.

Test Steps	Console: • Log onto the TOE local connection with incorrect credentials • Verify the failure via logs • Log onto the TOE local connection with correct credentials • Verify via logs SSH: • Log onto the TOE remote SSH CLI connection with incorrect credentials • Verify the failure via logs • Log onto the TOE remote SSH CLI with correct credentials • Verify via logs WebUI: • Log onto the TOE remote WebUI connection with incorrect credentials • Verify the failure via logs • Log onto the TOE remote WebUI with correct credentials. • Verify via logs
Expected Test Results	• **The TOE only allows an authorized user to gain access to the system via console.** • **Users with incorrect credentials are denied access as shown by TOE logs generated which states 'failed console login attempt by invalid user'.**
Pass/Fail with Explanation	Pass. • The TOE only allows an authorized user to gain access to the system via console, ssh and webui. • Console, SSH and WebUI users with incorrect credentials are denied access as shown by TOE logs.

6.20 FIA_UIA_EXT.1 Test #2

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

	Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
Test Steps	• Connect to the TOE remotely using ssh and verify the only option presented is the username/password entry and give incorrect credentials. • Verify authentication logs reflect failure. • Attempt to connect to the TOE with correct credentials remotely and verify that the previously enabled commands are now available. • Verify authentication logs reflect success.
Expected Test Results	• **No services except displaying a banner is available to a remote administrator attempting to login to the TOE via SSH** • **Log showing inability to access any services prior to login.**
Pass/Fail with Explanation	Pass. • No services except displaying a banner is available to a remote administrator attempting to login to the TOE via SSH • Log showing inability to access any services prior to login.

6.21 FIA_UIA_EXT.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
Test Steps	• Connect to the TOE via console. • Verify the only option presented is the username/password entry. • Attempt to connect to the TOE with incorrect credentials. • Verify authentication logs reflect failure. • Attempt to connect to the TOE with correct credentials. • Verify that the previously disabled commands are now available.

	• Verify authentication logs reflect success.
Expected Test Results	• **No services except displaying a banner is available to a local administrator attempting to login to the TOE.** • **Log showing inability to access any services prior to login.**
Pass/Fail with Explanation	Pass. • No services except displaying a banner is available to a local administrator attempting to login to the TOE. • Log showing inability to access any services prior to login.

6.22 FIA_UAU.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.
Test Steps	• Connect to the TOE via console with incorrect authentication credentials and verify that at most obscured feedback is provided. • Verify the logs. • Connect to the TOE via console with correct authentication credentials and verify that at most obscured feedback is provided. • Verify the logs
Expected Test Results	**The TOE should not provide anything other than obscured feedback, when entered credentials are correct authenticating information.**
Pass/Fail with Explanation	Pass. The TOE does not provide anything more than obscured feedback. This meets the testing requirements.

6.23 FMT_MOF.1/ManualUpdate Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Steps	• Login to the TOE via a lower privileged user. • Attempt to access configuration mode without the proper privilege and verify user is unable to access it. • Attempt to perform an update command and verify the command is rejected.
Expected Test Results	• **The TOE should reject attempts from an unprivileged user to update a legitimate image on the TOE.** • **Evidence (screenshot or CLI output) showing privilege level of the user.** • **Evidence (screenshot or CLI output) showing unsuccessful attempts.**
Pass/Fail with Explanation	Pass. An administrator without prior authentication is unable to update the TOE.

6.24 FMT_MOF.1/ManualUpdate Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Test Steps	This testing is covered by the requirements in FPT_TUD_EXT.1 Test #1.
Expected Test Results	**This testing is covered by the requirements in FPT_TUD_EXT.1 Test #1.**
Pass/Fail with Explanation	This testing is covered by the requirements in FPT_TUD_EXT.1 Test #1.

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

Item	Data
Test Assurance Activity	Test 1 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than

	the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Connect to the TOE as unprivileged user. • Attempt to modify the parameters involved with the syslog server and verify the command is rejected. • Verify via logs
Expected Test Results	• **The TOE should reject attempts from an unprivileged user to modify audit data on the TOE.** • **Evidence (screenshot or CLI output) showing privilege level of the user.** • **Evidence (screenshot or CLI output) showing unsuccessful attempts.**
Pass/Fail with Explanation	Pass. The TOE does not allow a user to modify parameters without prior authentication. • The TOE rejects the attempts from an unprivileged user to modify audit data on the TOE. • Evidence (screenshot or CLI output) showing privilege level of the user. • Evidence (screenshot or CLI output) showing unsuccessful attempts. This meets the testing requirement.

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

Item	Data
Test Assurance Activity	Test 2 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.
Test Steps	This testing is covered by the requirements in FAU_STG_EXT.1.
Expected Test Results	**This testing is covered by the requirements in FAU_STG_EXT.1.**
Pass/Fail with Explanation	This testing is covered by the requirements in FAU_STG_EXT.1.

6.27 FMT_MOF.1/Functions Test #3

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Login as unprivileged user • Perform an admin level task and observed that it failed • Show that when logged in with admin level user (configshell) it takes you to a different user interface.
Expected Test Results	**The TOE does not allow an user to modify parameters without prior authentication.**
Pass/Fail with Explanation	Pass. The TOE does not allow an user to modify parameters without prior authentication.

6.28 FMT_MOF.1/Functions Test #4

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection with prior authentication as Security Administrator. This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions with Security Administrator authentication shall be successful.
Test Steps	• Attempt to configure transmission of audit data with prior authentication as security administrator. This can be done in one test or in separate tests • The attempt(s) to determine the behavior of the selected functions with administrator authentication shall be successful
Expected Test Results	**The TOE allows an authorized administrator to configure the audit data security parameters.**
Pass/Fail with Explanation	Pass. The TOE allows an authorized administrator to configure the audit data security parameters.

6.29 FMT_MTD.1/CryptoKeys Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps	• Try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as security administrator • Attempts to perform related actions without prior authentication should fail
Expected Test Results	**The TOE should not allow a non-administrative user to modify cryptographic keys.**
Pass/Fail with Explanation	Pass. The TOE does not allow a non-administrative user to modify cryptographic keys.

6.30 FMT_MTD.1/CryptoKeys Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Test Steps	• Try to perform at least one of the related actions with prior authentication as security administrator. • Verify the attempt(s) is successful.
Expected Test Results	**The TOE allows an authorized administrator to make changes to the cryptographic keys.**
Pass/Fail with Explanation	Pass. The TOE allows an authorized administrator to make changes to the cryptographic keys.

6.31 FMT_SMF.1 Test #1

Item	Data
Test Assurance Activity	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Test Steps	The TSF shall be capable of performing the following management functions: • Ability to administer the TOE locally and remotely • Ability to configure the access banner • Ability to configure the session inactivity time before session termination or locking • Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates • Ability to configure the authentication failure parameters for FIA_AFL.1. • Ability to configure audit behavior (e.g., changes to storage locations for audit; changes to behavior when local audit storage space is full). • Ability to manage the cryptographic keys. • Ability to set the time which is used for timestamps. • Ability to import X.509v3 certificates to the TOE's trust store.
Expected Test Results	**All management functions identified in section 2.4.4 have been tested throughout the evaluation. Thus, this requirement has been met.**
Pass/Fail with Explanation	This test is performed in conjunction with other tests

6.32 FMT_SMR.2 Test #1

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

	FIA_UIA_EXT.1 Test #2, FIA_UIA_EXT.1 Test #3, FTA_SSL_EXT.1.1 Test #1, FTA_SSL.3 Test #1, FTA_SSL.4 Test #1 and FTA_TAB.1 Test #1
Expected Test Results	**This test is covered in below tests:** **FIA_UIA_EXT.1 Test #2, FIA_UIA_EXT.1 Test #3, FTA_SSL_EXT.1.1 Test #1, FTA_SSL.3 Test #1, FTA_SSL.4 Test #1 and FTA_TAB.1 Test #1**
Pass/Fail with Explanation	Pass: This test requirement has been performed in conjunction with other tests.

6.33 FTA_SSL.3 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Steps	SSH: • Configure a local time out period of 60 seconds on administrative sessions from CLI. • Log into the TOE via SSH. • Verify login time. • Verify login time using log. • Let the console set idle for 60 seconds and verify that the session was terminated and verify the logout time. • Configure a local time out period of 120 seconds on administrative sessions from CLI. • Log into the TOE via SSH. • Verify login time. • Verify login time using log. • Let the console set idle for 120 seconds and verify that the session was terminated and verify the logout time. WebUI: • Configure a local time out period of 240 seconds on administrative sessions from CLI. • Log into the TOE via WebUI. • Verify login time using log. • Let the console set idle for 240 seconds and verify that the session was terminated and verify the logout time.

Expected Test Results	• **The TOE should terminate idle remote sessions after the configured time.** • **Evidence (e.g., screenshot or CLI output) showing configuration of time out value.** • **Log showing the administrative log on (with time).** • **Evidence (e.g., screenshot or CLI output) showing administrator being terminated.** • **Log showing the termination of the connection.**
Pass/Fail with Explanation	Pass. The TOE terminates a session after the specified period of inactivity. • The TOE terminates the idle remote sessions after the configured time. • Evidence (e.g., screenshot or CLI output) showing configuration of time out value. • Log showing the administrative log on (with time). • Evidence (e.g., screenshot or CLI output) showing administrator being terminated. • Log showing the termination of the connection. This meets the testing requirement

6.34 FTA_SSL.4 Test #1

Item	Data
Test Assurance Activity	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	• Log onto the TOE through a local administrative interface. • Verify the logs reflect log in. • Using the instructions provided by the user guide log off. • Verify the logs reflect the log off.
Expected Test Results	• **The TOE should allow the user to terminate the directly connected administrative sessions** • **Evidence (e.g., screenshot or CLI output) showing logging into the TOE locally.** • **Evidence (e.g., screenshot or CLI output) showing the log out.** • **Log showing the log out.**
Pass/Fail with Explanation	Pass. The TOE allows the user to terminate the directly connected administrative sessions. • The TOE allows the user to terminate the directly connected administrative sessions • Evidence (e.g., screenshot or CLI output) showing logging into the TOE locally. • Evidence (e.g., screenshot or CLI output) showing the log out.

	• Log showing the log out. This meets the testing requirement.

6.35 FTA_SSL.4 Test #2

Item	Data
Test Assurance Activity	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps	SSH: • Log onto the TOE through a SSH administrative interface. • Verify the logs reflect login. • Using the instructions provided by the user guide log off. • Verify the logs reflect the log off. WebUI: • Log onto the TOE through a WebUI administrative interface. • Verify the logs reflect login. • Using the instructions provided by the user guide log off. • Verify the logs reflect the log off.
Expected Test Results	• **The TOE should allow the user to terminate the interactive remote sessions** • **Evidence (e.g., screenshot or CLI output) showing logging into the TOE remotely.** • **Evidence (e.g., screenshot or CLI output) showing the log out.** • **Log showing the log out.**
Pass/Fail with Explanation	Pass. The TOE allows the administrator to logout of the device. • The TOE allows the user to terminate the interactive remote sessions • Evidence (e.g., screenshot or CLI output) showing logging into the TOE remotely. • Evidence (e.g., screenshot or CLI output) showing the log out. • Log showing the log out. This meets the testing requirement.

6.36 FTA_SSL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Test Steps	• Log into the TOE via local console. • Configure new idle time of 60 seconds. • Perform the command to verify time. • Wait 62 seconds and attempt a command. • Verify that logs were created for configuring the timeout period. • Verify that logs were created for inactivity logout. • Configure new idle time of 120 seconds. • Perform the command to verify time. • Wait 122 seconds and attempt a command. • Verify that logs were created for configuring the timeout period. • Verify that logs were created for inactivity logout.
Expected Test Results	• **The TOE should terminate idle local sessions after the configured time.** • **Evidence (e.g., screenshot or CLI output) showing configuration of time out value.** • **Log showing the administrative log on (with time).** • **Evidence (e.g., screenshot or CLI output) showing administrator being terminated.** • **Log showing the termination of the connection.**
Pass/Fail with Explanation	Pass. The TOE terminates a local session after the specified time. • The TOE terminates idle local sessions after the configured time. • Evidence (e.g., screenshot or CLI output) showing configuration of time out value. • Log showing the administrative log on (with time). • Evidence (e.g., screenshot or CLI output) showing administrator being terminated. • Log showing the termination of the connection. This meets the testing requirements.

6.37 FTA_TAB.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.
Test Steps	• Configure access banners on TOE. • Log into the TOE via SSH. • Log into the TOE via console. • Log into the TOE via WebUI
Expected Test Results	• **When any user accesses the TOE through the console and SSH, the configured banner should be displayed prior to authenticating the TOE.** • **Evidence (e.g., screenshot or CLI output) showing configuration of access banners.** • **Log showing configuration of the access banners.** • **Evidence (e.g., screenshot or CLI output) from logon with access banners.**
Pass/Fail with Explanation	Pass. When any user accesses the TOE through the console and SSH, the configured banner is displayed at the credential page.

6.38 FTP_TRP.1/Admin Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	• Attempt to establish an SSH connection from a remote administrator. • Capture the traffic between the devices and verify that traffic was not sent in plaintext.
Expected Test Results	• **The TOE should establish communication between TOE and remote administrator via SSH and Web UI.** • **The Encrypted Packets in SSH connection in packet capture should confirm that the data is not sent in plain text.** • **Evidence (screenshot or CLI output) showing attempt to connect via the trusted paths**

	• **Log showing successful connection.**
Pass/Fail with Explanation	Pass. Remote administrative access to the TOE is over secure protected channels.

6.39 FTP_TRP.1/Admin Test #2

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Test Steps	This is covered by FTP_TRP.1/Admin_T1. In that test, the data was not sent in plaintext.
Expected Test Results	**This is covered by FTP_TRP.1/Admin_T1. In that test, the data was not sent in plaintext.**
Pass/Fail with Explanation	**This is covered by FTP_TRP.1/Admin_T1. In that test, the data was not sent in plaintext.**

6.40 FCS_SSHS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	Test 1: For each supported client **public-key** authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. **TD0631 Applied.**
Test Steps	• Configure the TOE to support SSH-RSA based SSH authentication method • Log into the TOE SSH with SSH-RSA based authentication • Verify authentication via packet capture • Configure the TOE to support RSA-SHA2-256 based SSH authentication method • Log into the TOE SSH with rsa-sha2-256 based authentication • Verify authentication via packet capture • Configure the TOE to support RSA-SHA2-512 based SSH authentication method • Log into the TOE SSH with RSA-SHA2-512 based authentication • Verify authentication via packet capture
Expected Test Results	**That user authentication succeeds when the correct public key is provided by the user.**

Pass/Fail with Explanation	Pass. The TOE allows a SSH client to connect with all the public key algorithms specified in the ST selection.

6.41 FCS_SSHS_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall choose one client **public key** authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. **TD0631 Applied.**
Test Steps	• Configure the SSH client with a new RSA-SHA2-256 based keypair for SSH without configuring the TOE • Log into the TOE SSH with RSA-based authentication • Verify authentication failure logs • Verify the connection via Packet capture.
Expected Test Results	**The attempt to log into the TOE without loading the public key onto the TOE should be unsuccessful**.
Pass/Fail with Explanation	Pass. The attempt to log into the TOE without loading the public key onto the TOE proved to be unsuccessful.

6.42 FCS_SSHS_EXT.1.2 Test #3

Item	Data
Test Assurance Activity	Test 1: If **password-based** authentication methods have been selected in the ST then using the guidance documentation, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that user authentication succeeds when the correct password is provided by the user.
Test Steps	• Log into the TOE via SSH with password authentication • Verify wire capture that SSH session was established
Expected Test Results	**That user authentication succeeds when the correct password is provided by the user.**
Pass/Fail with Explanation	Pass. User authentication succeeds when the correct password is provided by the user.

6.43 FCS_SSHS_EXT.1.2 Test #4

Item	Data

Test Assurance Activity	Test 2: If **password-based** authentication methods have been selected in the ST then the evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails.
Test Steps	• Attempt to Log into the TOE via SSH with correct username incorrect password-based authentication parameters (will fail) • Verify authentication logs reflect failures • Attempt to Log into the TOE via SSH with incorrect username correct password-based authentication parameters (will fail) • Verify authentication logs reflect failures
Expected Test Results	• **Failed login** • **Log showing failed login**
Pass/Fail with Explanation	Pass. TOE does not allow access to it with incorrect credentials. It only authenticates user with valid user credentials.

6.44 FCS_SSHS_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.
Test Steps	• Use a modified version of openSSH to start an SSH session with the TOE • The program will send an unusually large packet • Verify packet capture • Verify authentication logs reflect failures
Expected Test Results	**The large packets are dropped**
Pass/Fail with Explanation	Pass. The TOE rejects the large packet.

6.45 FCS_SSHS_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection. To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol

	negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.
Test Steps	• Connect to the TOE using AES-128 -CTR • Verify that the SSH session was encrypted using AES-128 via capture • Verify that the SSH session was encrypted using AES-128 via log • Establish an SSH session with the configured supported algorithms (AES-256-CTR) • Verify that the SSH session was encrypted using AES-256 via capture • Verify that the SSH session was encrypted using AES-256 via log
Expected Test Results	**The TOE supports successful negotiations when using the claimed cipher suites.**
Pass/Fail with Explanation	Pass. The TOE supports successful negotiations when using the claimed cipher suites.

6.46 FCS_SSHS_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Test objective: This test case is meant to validate that the TOE server will support host public keys of the claimed algorithm types. **TD0631 Applied.**
Test Steps	• Verify the Claimed Host key algorithms by TOE. Screenshot of the TOE with Claimed Host key algorithms by TOE • Established a session with the TOE using the rsa-sha2-512 host key algorithms. • Verify through packet capture that the SSH session was encrypted using host key algorithms. • Established a session with the TOE using the rsa-sha2-256 host key algorithms • Verify through packet capture that the SSH session was encrypted using host key algorithms. • Established a session with the TOE using the ssh-rsa host key algorithms • Verify through packet capture that the SSH session was encrypted using host key algorithms.
Expected Test Results	**The TOE allows client to connect using the supported Host public key algorithm**

Pass/Fail with Explanation	Pass. The TOE allows client to connect using the supported Host public key algorithm. This meets the testing requirements.

6.47 FCS_SSHS_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected. Test objective: This negative test case is meant to validate that the TOE server does not support host public key algorithms that are not claimed. **TD0631 Applied.**
Test Steps	• Verify the Claimed Host key algorithms by TOE • Established a session with the TOE using the non-supported host key algorithms (SSH-DSS) • Verify through logs and packet capture that the SSH session was not established
Expected Test Results	**Toe should reject the connection if the session is established using a non-supported host key algorithm.**
Pass/Fail with Explanation	Pass. Toe rejects the connection if the session is established using a non-supported host key algorithm. This meets the testing requirement.

6.48 FCS_SSHS_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	Test 1: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
Test Steps	• Establish an SSH session with the configured supported algorithms (*hmac-sha2-256*) • Verify that the SSH session was successfully negotiated using hmac-sha2-256 via capture • Verify that the message integrity algorithm used was as configured. • Establish an SSH session with the configured supported algorithms (*hmac-sha2-512*) • Verify that the SSH session was successfully negotiated using *hmac-sha2-512* via capture • Verify that the message integrity algorithm used was as configured.

Expected Test Results	**The TOE is able to make SSH connections with each claimed data integrity algorithm.**
Pass/Fail with Explanation	Pass. The TOE is able to make SSH connections with each claimed data integrity algorithm.

6.49 FCS_SSHS_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	Test 2: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
Test Steps	• Attempt to establish an SSH session using HMAC-MD5 • Verify via wireshark that the TOE does not continue negotiation • Verify logs
Expected Test Results	**The TOE rejects SSH connections using the HMAC-MD5 MAC for data integrity.**
Pass/Fail with Explanation	Pass. The TOE rejects SSH connections using the HMAC-MD5 MAC for data integrity.

6.50 FCS_SSHS_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
Test Steps	• Attempt to establish an SSH session using diffiehellman-group1-sha1 • Verify the connection is refused via packet capture • Verify that the SSH session was refused via log
Expected Test Results	**The TOE does not permit connections when using Diffie-hellman-group1-sha1.**
Pass/Fail with Explanation	Pass. The TOE does not permit connections when using diffiehellman-group1-sha1.

6.51 FCS_SSHS_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Test Steps	• Establish an SSH session with the ECDH-SHA2-NISTP256 based algorithms. • Verify that the SSH session was established via capture • Establish an SSH session with the ECDH-SHA2-NISTP384 based algorithms. • Verify that the SSH session was established via capture • Establish an SSH session with the ECDH-SHA2-NISTP521 based algorithms. • Verify that the SSH session was established via capture
Expected Test Results	**The TOE is able to make SSH connections with each claimed data key exchange method.**
Pass/Fail with Explanation	Pass. The TOE is able to make SSH connections with each claimed data key exchange method.

6.52 FCS_SSHS_EXT.1.8 Test #1t

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the **time-based threshold** and the traffic-based threshold. For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).
Test Steps	• Establish an SSH session with the TOE • Waiting for 1 hour for the rekey to occur based on time • Verify the reflected logs
Expected Test Results	**The TOE issues a rekey after the specified time.**

Pass/Fail with Explanation	Pass. The TOE issues a rekey after the specified time.

6.53 FCS_SSHS_EXT.1.8 Test #1b

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold and the **traffic-based** threshold. For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8). The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions). In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met: 1. An argument is present in the TSS section describing this hardware- based limitation and 2. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or WiFi radio chip is the root cause of such limitation, these chips must be identified.
Test Steps	• Establish an SSH session with the TOE • Continually send traffic via scp script • Wait for 1 GB file to transfer for the rekey to occur based on threshold • Verify the reflected logs

Expected Test Results	**The TOE issues a rekey after the specified traffic**
Pass/Fail with Explanation	Pass. The TOE issues a rekey after the specified traffic.

6.54 FCS_TLSC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps	• Connect with TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • Verify using pcap the required cipher suite TLS_RSA_WITH_AES_128_CBC_SHA • Connect with TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • Verify using pcap the required cipher suite TLS_RSA_WITH_AES_256_CBC_SHA • Connect with TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • Verify using pcap the required cipher suite TLS_RSA_WITH_AES_128_CBC_SHA256 • Connect with TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • Verify using pcap the required cipher suite TLS_RSA_WITH_AES_256_CBC_SHA256 • Connect with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • Verify using pcap the required cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • Connect with TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289 • Verify using pcap the required cipher suite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • Repeat all the testing for Evertz IPX Device.
Expected Test Results	• **TOE can successfully establish a connection with below 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_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246** • **TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246** • **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**
Pass/Fail with Explanation	Pass. • TOE is able to successfully establish a connection with both Syslog Server and IPX using below 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_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • 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

6.55 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Steps	• Create a server certificate with the Server Authentication EKU. • Attempt a connection from the TOE to a TLS server using a valid certificate that contains the Server Authentication EKU • Show the TOE accept the connection • Verify with Packet Capture • Create a server certificate that lacks the Server Authentication EKU • Attempt a connection from the TOE to a TLS server using an invalid certificate missing the Server Authentication EKU • Show the TOE rejects the connection • Verify with Packet Capture
Expected Test Results	**The TOE will reject the connection to a server using an invalid certificate**
Pass/Fail with Explanation	Pass. The TOE is accepting the connection with a server certificate which has Server Authentication EKU and the TOE rejects the connection when the certificate is missing the Server Authentication EKU.

6.56 FCS_TLSC_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall send a server certificate in the TLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite). The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Test Steps	• Use Acumen TLSC tool attempt a connection with a certificate that doesn't match the ciphersuite. • Verify the connection fails with packet capture. • Verify with logs
Expected Test Results	**The TOE will deny the connection if the certificate sent by the server does not match the ciphersuite.**
Pass/Fail with Explanation	Pass. The TOE denies the connection if the certificate sent by the server does not match the ciphersuite.

6.57 FCS_TLSC_EXT.1.1 Test #4a

Item	Data
Test Assurance Activity	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Test Steps	• Start the connection using the Acumen-TLSC tool with TLS_NULL_WITH_NULL NULL cipher suite and wait for the connection, the connection should fail. • Verify via packet capture that TOE denies the connection • Verify via Logs
Expected Test Results	**The TOE does not make the connection because the ciphersuite presented was TLS_NULL_WITH_NULL_NULL.**
Pass/Fail with Explanation	Pass. The TOE does not make the connection because the ciphersuite presented was TLS_NULL_WITH_NULL_NULL.

6.58 FCS_TLSC_EXT.1.1 Test #4b

Item	Data
Test Assurance Activity	Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Test Steps	• Run the AcumenTLS tool and attempt to make a connection with the TOE. • Verify the connection is refused via packet capture. • Verify the connection is refused via logs.

Expected Test Results	**Client rejects the connection when unsupported ciphersuite is sent in the server hello message. This can be verified by using logs and pcap.**
Pass/Fail with Explanation	Pass. Client rejects the connection when unsupported ciphersuite is sent in the server hello message. This can be verified with the help of logs and pcap.

6.59 FCS_TLSC_EXT.1.1 Test #4c

Item	Data
Test Assurance Activity	[conditional]: If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension** the evaluator shall configure the server to perform an ECDHE or DHE key exchange in the TLS connection using a non-supported curve/group (for example P-192) and shall verify that the TOE disconnects after receiving the server's Key Exchange handshake message.
Test Steps	• Connect TOE using acumen-tlsc tool using ECDHE key exchange using non-supported curve P-192 and observe the session disconnect. • Verify with packet capture. • Verify with logs.
Expected Test Results	**The TOE should reject a connection when an unsupported curve was used.**
Pass/Fail with Explanation	Pass. The TOE denied a connection when non-supported curve was used during the connection. This meets the testing requirements.

6.60 FCS_TLSC_EXT.1.1 Test #5a

Item	Data
Test Assurance Activity	Change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Steps	• Using acumen-tlsc tool, attempt a connection to a remote TLS server using a non-supported TLS version and verify that the TOE rejects the connection. • Verify the connection fails with packet capture. • Verify with logs
Expected Test Results	**The TOE should reject the connection if it is receiving Server Hello from a non-supported version TLS.**
Pass/Fail with Explanation	Pass. The TOE rejects a connection with a server which modified the server hello with non-supported TLS version. This meets the testing requirement.

6.61 FCS_TLSC_EXT.1.1 Test #5b

Item	Data

Test Assurance Activity	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Steps	• Attempt a connection from the TOE to a remote TLS server using acumen-tlsc tool that would allow the server's signature block to be modified. Verify that the connection fails. • Verify with packet capture. • Verify the TOE logs.
Expected Test Results	**The TOE should reject the connection when the signature block is modified.**
Pass/Fail with Explanation	Pass. The TOE rejects the connection when the signature block is modified. This meets testing requirements.

6.62 FCS_TLSC_EXT.1.1 Test #6a

Item	Data
Test Assurance Activity	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Attempt a connection to a modified TLS Server using acumen-tlsc tool. • Verify connection failed with packet capture that Client sends an alert after receiving modified Server Finished handshake message. • Verify with logs.
Expected Test Results	**Client rejects the connection when byte in the server finished message is modified. This can be verified by using logs and pcap.**
Pass/Fail with Explanation	Pass. The connection is not completed when a corrupted Server Finished message is received. This satisfies the testing requirement.

6.63 FCS_TLSC_EXT.1.1 Test #6b

Item	Data
Test Assurance Activity	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully and no application data flows.
Test Steps	• Attempt a connection to a modified TLS server using acumen-tlsc tool, that would allow sending a garbled message from the server after the server issues the ChangeCipherSpec message and verify that the TOE rejects the connection. • Verify with packet capture. • Verify with logs.
Expected Test Results	**Client rejects the TLS connection when garbled message is sent from the server. This can be verified by using logs and pcap.**

Pass/Fail with Explanation	Pass. The modified TLS connection was rejected by the client which contains garbled message. This meets the testing requirements

6.64 FCS_TLSC_EXT.1.1 Test #6c

Item	Data
Test Assurance Activity	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.
Test Steps	• Using Acumen TLSC tool run the command to send modified nonce data to TOE • Verify that the client rejects the Server Key Exchange handshake message. • Verify with logs.
Expected Test Results	**The modified TLS connection is rejected.**
Pass/Fail with Explanation	Pass. Client rejects the connection when we modified a byte in the server nonce in the Server Hello handshake message. This meets the testing requirement.

6.65 FCS_TLSC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.
Test Steps	• Configure a correct DNS based reference identifier for the server on the TOE • Create a server that presents a server certificate that does not contain an identifier in the Subject Alternative Name (SAN) and Common Name (CN) that does not matches the DNS reference identifier. • Attempt to connect to the server and observe that the connection fails. • Verify with packet capture.

	• Verify with TOE logs. • **TOE does not support IP CN so IP based testing is not required.**
Expected Test Results	**When a server certificate that does not contain an identifier in the Subject Alternative Name (SAN) and Common Name (CN) that does not matches the reference identifier is presented, the TOE should reject the connection.**
Pass/Fail with Explanation	Pass. When a server certificate is presented that does not contain an identifier in the Subject Alternative Name (SAN) and Common Name (CN) that does not matches the reference identifier, the TOE rejects the connection. This meets the testing requirement

6.66 FCS_TLSC_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.
Test Steps	• Configure the correct reference identifier in the TOE. • Create a server certificate with valid DNS CN and invalid DNS SAN. • Attempt to connect to the server • Verify with packet capture. • Verify with logs. • Repeat for IPv4 address in the CN and SAN
Expected Test Results	**When a server certificate is presented that contains an identifier in the Subject Alternative Name (SAN) that does not match and Common Name (CN) that matches the reference identifier, the TOE should reject the connection**
Pass/Fail with Explanation	Pass. When a server certificate is presented that contains an identifier in the Subject Alternative Name (SAN) that does not matches and Common Name (CN) that matches the reference identifier, the TOE rejects the connection. This meets the testing requirement

6.67 FCS_TLSC_EXT.1.2 Test #3

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.**

	If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
Test Steps	• Configure a correct DNS reference ID on the TOE • Create a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension • Attempt to connect to the server and verify that a connection is established • Verify with the packet capture. • Verify with logs. • TOE only supports DNS in CN, not IP addresses or FQDNs, so IP or FQDN based testing is not required.
Expected Test Results	**When a server certificate is presented that contains a CN that matches the reference identifier and does not contain the SAN extension the TOE should accept the connection.**
Pass/Fail with Explanation	Pass. When a server certificate is presented that contains a CN that matches the reference identifier and does not contain the SAN extension the TOE accepts the connection. This meets the testing requirement.

6.68 FCS_TLSC_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).
Test Steps	• Configure the correct DNS reference identifier in the TOE. • Create a server certificate with incorrect CN and valid SAN. • Attempt to connect to the server and verify that a connection is established • Verify with packet capture • Verify with logs • Repeat this for IPv4.
Expected Test Results	**When a server certificate is presented that contains a CN that does not matches the reference identifier and contain the SAN that matches the reference identifier, the TOE should accept the connection.**
Pass/Fail with Explanation	Pass. When a server certificate is presented that contains a CN that does not matches the reference identifier and contains the SAN that matches the reference identifier, the TOE accepts the connection. This meets the testing requirement.

6.69 FCS_TLSC_EXT.1.2 Test #5 (1)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
Test Steps	• Configure the correct reference identifier in the TOE. • Create a server certificate containing a wildcard that is not in the left-most label of CN. • Attempt a connection and verify that the connection fails • Verify with packet capture. • Verify with logs • Repeat above steps for SAN
Expected Test Results	**When the server presents a certificate containing a wildcard that is not in the left-most label of the presented identifier, the connection should fail.**
Pass/Fail with Explanation	Pass. When the server presents a certificate containing a wildcard that is not in the left-most label of the presented identifier, the connection fails.

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

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds, if wildcards are supported, or fails if wildcards are not supported.

	(Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps	• Configure the correct reference identifier on the TOE. • Create a server certificate with a wildcard in the leftmost label of CN. • Attempt to connect to the TOE and verify that the connection is successful. • Verify with packet capture that the connection was successful. • Verify with logs that the connection was successful. • Repeat above steps for SAN
Expected Test Results	**When the server presents a certificate containing a wildcard that is in the left-most label of the presented identifier, the connection succeeds.**
Pass/Fail with Explanation	Pass. When the server is presented with a certificate containing a wildcard that is in the left-most label of the presented identifier, the connection succeeds. This meets the testing requirement.

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

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps	• Configure the correct reference identifier on the TOE. • Create a server certificate with a wildcard in the leftmost label of CN. • Attempt to connect to the TOE and verify that the connection fails. • Verify with packet capture. • Verify with logs. • Repeat for SAN

Expected Test Results	**When the server presents a certificate containing a wildcard that is in the left-most label of the presented identifier but the reference identifier in the TOE is without a loft-most label as in the certificate, the connection fails.**
Pass/Fail with Explanation	Pass. When the server presents a certificate containing a wildcard that is in the left-most label of the presented identifier but the reference identifier in the TOE is without a left-most label as in the certificate, the connection fails.

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

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps	• Configure the correct reference identifier on the TOE. • Create a server certificate with a wildcard in the leftmost label of CN. • Attempt to connect to the TOE and verify that the connection fails. • Verify with packet capture. • Verify with logs. • Repeat for SAN
Expected Test Results	**Client should reject the TLS connection when certificate presented by the server contains wildcard that is in the left-most label and configured reference identifier in the TOE is with two left-most label.**
Pass/Fail with Explanation	Pass. TOE rejects the TLS connection when certificate presented by the server contains wildcard that is in the left-most label and configured reference identifier in the TOE is with two left-most labels. This meets the testing requirement.

6.73 FCS_TLSC_EXT.1.2 Test #6

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT**.

	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. [conditional] If IP address identifiers 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 asterisk (*) (e.g. CN=192.168.1.* when connecting to 192.168.1.20, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g. IPv4, IPv6). Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 6. **TD0634 Applied.**
Pass/Fail with Explanation	This test is NOT applicable to the TOE because the TOE does not claim IP addresses in the CN.

6.74 FCS_TLSC_EXT.1.2 Test #7a

Item	Data
Test Assurance Activity	If **the secure channel is used for FPT_ITT, and RFC 5280 is selected**, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier): The evaluator shall present a server certificate that does not contain an identifier in the Subject (DN) attribute type(s) that matches the reference identifier. The evaluator shall verify that the connection fails.
Pass/Fail with Explanation	This test is not applicable because FPT_ITT with RFC 5280 is not claimed

6.75 FCS_TLSC_EXT.1.2 Test #7b

Item	Data

Test Assurance Activity	If **the secure channel is used for FPT_ITT, and RFC 5280 is selected**, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier): The evaluator shall present a server certificate that contains a valid identifier as an attribute type other than the expected attribute type (e.g. if the TOE is configured to expect id-at-serialNumber=correct_identifier, the certificate could instead include id-at-name=correct_identifier), and does not contain the SAN extension. The evaluator shall verify that the connection fails. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass this test.
Pass/Fail with Explanation	This test is not applicable because FPT_ITT with RFC 5280 is not claimed

6.76 FCS_TLSC_EXT.1.2 Test #7c

Item	Data
Test Assurance Activity	If **the secure channel is used for FPT_ITT, and RFC 5280 is selected**, the evaluator shall perform the following tests. Note, when multiple attribute types are selected in the SFR (e.g. when multiple attribute types are combined to form the unique identifier), the evaluator modifies each attribute type in accordance with the matching criteria described in the TSS (e.g. creating a mismatch of one attribute type at a time while other attribute types contain values that will match a portion of the reference identifier): The evaluator shall present a server certificate that contains a Subject attribute type that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds.
Pass/Fail with Explanation	This test is not applicable because FPT_ITT with RFC 5280 is not claimed

6.77 FCS_TLSC_EXT.1.3 Test #1

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

Pass/Fail with Explanation	There are 2 trusted channels (syslog and video switch), and both these trusted channels use the same x509 certificate trust store.

6.78 FCS_TLSC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.
Pass/Fail with Explanation	Test covered by FCS_TLSC_EXT.1.1 Test #1, FIA_X509_EXT.1.1/Rev Test #1a, FIA_X509_EXT.1.1/Rev Test #2 and FIA_X509_EXT.1.1/Rev Test #3.

6.79 FCS_TLSC_EXT.1.3 Test #3

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

6.80 FCS_TLSC_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	If the TOE presents the **Supported Elliptic Curves/Supported Groups Extension**, the evaluator shall configure the server to perform ECDHE or DHE (as applicable) key exchange using each of the TOE's supported curves and/or groups. The evaluator shall verify that the TOE successfully connects to the server.
Test Steps	• Start a connection with the server using ECDHE cipher and secp256r1 curve. • Verify with packet capture that connection is established.
Expected Test Results	**The TOE should be able to establish a connection with the supported curves**

Pass/Fail with Explanation	Pass. The TOE can establish a connection with the supported curves. This meets the testing requirement.

6.81 FCS_TLSC_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a connection to a peer server that is configured for mutual authentication (i.e. sends a server Certificate Request (type 13) message). The evaluator observes that the TOE TLS client sends both client Certificate (type 11) and client Certificate Verify (type 15) messages during its negotiation of a TLS channel and that Application Data is sent. **TD Applied: TD0670**
Test Steps	• Established a connection with TLS_RSA_WITH_AES_128_CBC_SHA Established a connection with TLS_RSA_WITH_AES_128_CBC_SHA • Verify using packet capture that the server sends a server Certificate Request (Type 13) message • Verify using packet capture that the TOE sends both the client certificate (Type 11) and Client Certificate Verify (Type 15) message. • Verify using packet capture that the application data is encrypted
Expected Test Results	**During the negotiation of the TLS channel** • **The Client should send a server Certificate Request (Type 13) message** • **TOE should send both client certificate (Type 11) and Client Certificate Verify (Type 15) message.** • **The application data should be encrypted.**
Pass/Fail with Explanation	Pass. During the negotiation of the TLS channel • The Client sends a server Certificate Request (Type 13) message • TOE sends both the client certificate (Type 11) and Client Certificate Verify (Type 15) message. • The application data is encrypted. This meets the testing requirement.

All the remaining Test Cases for FCS_TLSC_EXT.2 are covered by FCS_TLSC_EXT.1 and FIA_X509_EXT.1 testing

6.82 FCS_TLSS_EXT.1.1 Test #1

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

Test Steps	• From an OpenSSL Client, establish a connection with the TOE over TLS with a particular ciphersuite • Capture the traffic between the Openssl client tool and the TOE • Verify that the session was established with the chosen ciphersuite • Repeat for each supported ciphersuite
Expected Test Results	**The TOE will make a connection with each of the supported ciphers**
Pass/Fail with Explanation	Pass. The TOE successfully connected with all claimed ciphers. This meets testing requirements.

6.83 FCS_TLSS_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall send a Client Hello to the server with a list of ciphersuites that does not contain any of the ciphersuites in the server's ST and verify that the server denies the connection. Additionally, the evaluator shall send a Client Hello to the server containing only the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the server denies the connection.
Test Steps	• Use the Acumen-tlss tool to perform the connection using the NULL_WITH_NULL_NULL ciphersuite • Record a wirecapture of the connection attempt • Record the audit logs of the connection attempt • From OpenSSL attempt to make connection with an unclaimed cipher that is TLS_RSA_WITH_NULL_MD5 • Record a wirecapture of the connection attempt • Record the audit logs of the connection attempt
Expected Test Results	**The TOE will reject the NULL connection**
Pass/Fail with Explanation	Pass. The TOE did not successfully connect with an unclaimed ciphersuite or a NULL ciphersuite. This meets testing requirements.

6.84 FCS_TLSS_EXT.1.1 Test #3a

Item	Data
Test Assurance Activity	Modify a byte in the Client Finished handshake message, and verify that the server rejects the connection and does not send any application data.
Test Steps	• Use the AcumenTLS tool to modify the client's finished handshake message in the client hello during the handshake process • Connect to the server via AcumenTLS

	• Verify that the connection was not successful and note the error. • Verify the same in the packet captures.
Expected Test Results	**The TOE denies a connection when it detects a modified client finished handshake message**
Pass/Fail with Explanation	Pass. The TOE denies a connection when it detects a modified client finished handshake message.

6.85 FCS_TLSS_EXT.1.1 Test #3b

Item	Data
Test Assurance Activity	(Test Intent: The intent of this test is to ensure that the server's TLS implementation immediately makes use of the key exchange and authentication algorithms to: a) Correctly encrypt (D)TLS Finished message and b) Encrypt every (D)TLS message after session keys are negotiated.) The evaluator shall use one of the claimed ciphersuites to complete a successful handshake and observe transmission of properly encrypted application data. The evaluator shall verify that no Alert with alert level Fatal (2) messages were sent. The evaluator shall verify that the Finished message (Content type hexadecimal 16 and handshake message type hexadecimal 14) is sent immediately after the server's ChangeCipherSpec (Content type hexadecimal 14) message. The evaluator shall examine the Finished message (encrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 11 22 33 44 55...) and confirm that it does not contain unencrypted data (unencrypted example in hexadecimal of a TLS record containing a Finished message, 16 03 03 00 40 14 00 00 0c...), by verifying that the first byte of the encrypted Finished message does not equal hexadecimal 14 for at least one of three test messages. There is a chance that an encrypted Finished message contains a hexadecimal value of '14' at the position where a plaintext Finished message would contain the message type code '14'. If the observed Finished message contains a hexadecimal value of '14' at the position where the plaintext Finished message would contain the message type code, the test shall be repeated three times in total. In case the value of '14' can be observed in all three tests it can be assumed that the Finished message has indeed been sent in plaintext and the test has to be regarded as 'failed'. Otherwise it has to be assumed that the observation of the value '14' has been due to chance and that the Finished message has indeed been sent encrypted. In that latter case the test shall be regarded as 'passed'.
Test Steps	• Initiate a connection to the TOE using acumen-tlss tool from the evaluator machine. • Verify that Client Finished Message is encrypted using packet capture.
Expected Test Results	**The TOE should be able to encrypt the finish message.**

Pass/Fail with Explanation	Pass. The Finished message is encrypted. This meets testing requirements.

6.86 FCS_TLSS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt.
Test Steps	• Attempt an SSL v2.0 connection to the TOE • Verify the failed connection with the logs. • Verify that the connection was denied with the packet capture. • Attempt an SSL v3.0 connection to the TOE • Verify the failed connection with the logs. • Verify that the connection was denied with the packet capture. • Attempt an TLS v1.0 connection to the TOE • Verify the failed connection with the logs. • Verify that the connection was denied with the packet capture. • Attempt an TLS v1.1 connection to the TOE • Verify the failed connection with the logs. • Verify that the connection was denied with the packet capture.
Expected Test Results	• **The TOE rejects the SSL v2.0 connection attempts which can be seen in both the logs and pcap.** • **The TOE rejects the SSL v3.0 connection attempts which can be seen in both the logs and pcap.** • **The TOE rejects the TLS v1.0 connection attempts which can be seen in both the logs and pcap.** • **The TOE rejects the TLS v1.1 connection attempts which can be seen in both the logs and pcap.**
Pass/Fail with Explanation	Pass. • The TOE rejects the SSL v2.0 connection attempts which can be seen in both the logs and pcap. • The TOE rejects the SSL v3.0 connection attempts which can be seen in both the logs and pcap. • The TOE rejects the TLS v1.0 connection attempts which can be seen in both the logs and pcap. • The TOE rejects the TLS v1.1 connection attempts which can be seen in both the logs and pcap.

6.87 FCS_TLSS_EXT.1.3 Test #1a

Item	Data
Test Assurance Activity	If **ECDHE ciphersuites** are supported: The evaluator shall repeat this test for each supported elliptic curve. The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single supported elliptic curve specified in the Elliptic Curves Extension. The Evaluator shall verify (though a packet capture or instrumented client) that the TOE selects the same curve in the Server Key Exchange message and successfully establishes the connection.
Test Steps	• Connect to the TOE using secp256r1 and verify that it is successful. • Verify with packet capture.
Expected Test Results	**The TOE should be able to establish the connection using the supported EC curves.**
Pass/Fail with Explanation	Pass. The TOE should be able to establish the connection using the supported EC curves.

6.88 FCS_TLSS_EXT.1.3 Test #1b

Item	Data
Test Assurance Activity	If **ECDHE ciphersuites** are supported: The evaluator shall attempt a connection using a supported ECDHE ciphersuite and a single unsupported elliptic curve (e.g. secp192r1 (0x13)) specified in RFC4492, chap. 5.1.1. The evaluator shall verify that the TOE does not send a Server Hello message and the connection is not successfully established.
Test Steps	• Connect to the TOE using secp256k1 and verify that it fails. • Verify the failure with packet capture. • Verify with logs.
Expected Test Results	**The TOE should reject the connection with the unsupported curves.**
Pass/Fail with Explanation	Pass. The TOE should reject the connection with the unsupported curves.

6.89 FCS_TLSS_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	If **RSA key establishment ciphersuites** are supported, the evaluator shall repeat this test for each RSA key establishment key size. If any configuration is necessary, the evaluator shall configure the TOE to perform RSA key establishment using a supported key size (e.g. by loading a certificate with the appropriate key size). The evaluator shall attempt a connection using a supported RSA key establishment ciphersuite. The evaluator shall verify (through a packet capture or instrumented client) that the TOE sends a certificate whose modulus is consistent with the configured RSA key size.

Test Steps	• Connect to the TOE using RSA 4096 bit key and verify that it is successful. • Verify with packet capture.
Expected Test Results	**The TOE should be able to establish a connection using each supported RSA key size.**
Pass/Fail with Explanation	Pass. The TOE was able to establish a connection using the supported RSA key size.

6.90 FCS_TLSS_EXT.1.4 Test #1

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

6.91 FCS_TLSS_EXT.1.4 Test #2a

Item	Data

Test Assurance Activity	If the **TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall conduct a successful handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then initiate a new TLS connection and send the previously captured session ID to show that the TOE resumed the previous session by responding with ServerHello containing the same SessionID immediately followed by ChangeCipherSpec and Finished messages (as shown in Figure 2 of RFC 4346 or RFC 5246).
Test Steps	• Use acumen-tlss tool to connect to the TOE • Verify a successful connection with the logs • Verify a successful connection using packet capture.
Expected Test Results	**Client should successfully reuse the previous session by responding with ClientHello containing the same SessionID.**
Pass/Fail with Explanation	Pass. Client successfully reused the previous session by responding with ClientHello containing the same SessionID. This meets the testing requirement.

6.92 FCS_TLSS_EXT.1.4 Test #2b

Item	Data
Test Assurance Activity	If the **TOE supports session resumption using session IDs according to RFC4346 (TLS1.1) or RFC5246 (TLS1.2)**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS): The evaluator shall initiate a handshake and capture the TOE-generated session ID in the Server Hello message. The evaluator shall then, within the same handshake, generate or force an unencrypted fatal Alert message immediately before the client would otherwise send its ChangeCipherSpec message thereby disrupting the handshake. The evaluator shall then initiate a new Client Hello using the previously captured session ID, and verify that the server (1) implicitly rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake (as shown in figure 1 of RFC 4346 or RFC 5246), or (2) terminates the connection in some way that prevents the flow of application data.
Test Steps	• Use the acumen-tlss tool to connect to the TOE. • Screenshot for New Session ID sent by the server in the first handshake in the PCAP packet number 2. • Screenshot shows Fatal Handshake Failure message error in PCAP packet number 3 • Screenshot shows that client has chosen old Session ID data at sequence number 4 • Screenshot shows that the server has implicitly rejected the session ID by sending a ServerHello containing a different SessionID and performing a full handshake in the PCAP packet capture number 5. • Verify audit records

Expected Test Results	**When the Client Hello is initiated using the same session ID as part of a new Client Hello message the TOE rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake**
Pass/Fail with Explanation	Pass. When the Client Hello is initiated using the same session ID as part of a new Client Hello message the TOE rejects the session ID by sending a ServerHello containing a different SessionID and performing a full handshake. This meets the testing requirement.

6.93 FCS_TLSS_EXT.1.4 Test #3a

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

6.94 FCS_TLSS_EXT.1.4 Test #3b

Item	Data
Test Assurance Activity	If the **TOE supports session tickets according to RFC5077**, the evaluator shall carry out the following steps (note that for each of these tests, it is not necessary to perform the test case for each supported version of TLS):

	The evaluator shall permit a successful TLS handshake to occur in which a session ticket is exchanged with the non-TOE client. The evaluator will then modify the session ticket and send it as part of a new Client Hello message. The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.
Test Steps	• Use the acumen-tlss tool to connect to the TOE. • Verify packet capture contains two TLS handshakes with the TOE sequence number 4 and 11 respectively. • Verify new session ticket number in the pcap packet number 5 and 12. • Screenshot for New Session Ticket message sent by the server in the first handshake in the PCAP packet number 5. • Screenshot shows that Session ticket has been modified in PCAP packet number 8 and hence, Server has chosen new Session Ticket data at PCAP packet number 12 • Verify audit records
Expected Test Results	**When the modified session ticket is sent as part of a new Client Hello message the TOE rejects the session ticket by performing a full handshake.**
Pass/Fail with Explanation	Pass. When the modified session ticket is sent as part of a new Client Hello message the TOE rejects the session ticket by performing a full handshake. This meets the testing requirement.

6.95 FPT_TST_EXT.1 Test #1

Item	Data
Test Assurance Activity	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this. 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	• Power on the TOE • Observe the output of the TOE start up • Ensure that evidence of the execution of self-tests are provided
Expected Test Results	**The TOE executes all required self-tests during bootup**

Pass/Fail with Explanation	Pass. The TOE executes all required self-tests during bootup. This meets the testing requirement.

6.96 FPT_TUD_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. (For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g. by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.) After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.
Test Steps	• Verify the current version of the TOE • Perform the image update • Verify the new version of the TOE • Verify with the logs.
Expected Test Results	**An administrator is able to update the TOE when using a legitimate image.**
Pass/Fail with Explanation	Pass. An administrator is able to update the TOE when using a legitimate image.

6.97 FPT_TUD_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator obtains or produces illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates:

	1) A modified version (e.g. using a hex editor) of a legitimately signed update If the TOE allows a delayed activation of updates the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs depending on the point in time when an attempted update is rejected. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps	• Verify the current version of the TOE • Attempt to update the TOE with a modified version of legitimately signed update. • Verify the attempt was unsuccessful. • Verify with the logs.
Expected Test Results	**The TOE should reject a modified version of legitimately signed update.**
Pass/Fail with Explanation	Pass. The TOE rejects a modified version of legitimately signed update. This meets the testing requirement.

6.98 FPT_TUD_EXT.1 Test #2 (b)

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

	• Attempt to update the TOE with an image that has not been signed. • Verify the attempt was unsuccessful. • Verify with the logs.
Expected Test Results	**The TOE should reject an update when the image has not been signed.**
Pass/Fail with Explanation	Pass. The TOE rejects an update when the image has not been signed. This meets the testing requirement.

6.99 FPT_TUD_EXT.1 Test #2 (c)

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

6.100 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data
Test Assurance Activity	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
Test Steps	• Upload a complete certificate validation (CA and ICA) chain to the TOE's trust store. • Initiate the connection to the syslog server. • Verify the successful connection via Packet capture. • Repeat the steps for IPX connectivity.
Expected Test Results	**When a complete certificate chain is present on the TOE the TLS should establish a successful connection.**
Pass/Fail with Explanation	Pass. When a complete certificate chain is present on the TOE the TLS establishes a successful connection.

6.101 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test Assurance Activity	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
Test Steps	• Remove the ICA certificate from the TOE's trust Store • Initiate the connection to the syslog server. • Show logs of unsuccessful connection • Verify the unsuccessful connection via Packet capture. • Repeat the steps for IPX connectivity.
Expected Test Results	**When an incomplete certificate chain is present on the TOE the TLS should not establish a connection.**
Pass/Fail with Explanation	Pass. When an incomplete certificate chain is present on the TOE the TLS session is not establishing a connection. This meets the testing requirement.

6.102 FIA_X509_EXT.1.1/Rev Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps	• Create a server certificate which is expired. • Attempt to connect to TLS server with an expired certificate from the TOE. • Show logs of unsuccessful connection • Verify the unsuccessful connection via Packet capture.
Expected Test Results	**The TOE should not accept a connection because of the expired certificate**
Pass/Fail with Explanation	Pass. The TOE rejects the connection when presented with an expired certificate. This meets the testing requirement.

6.103 FIA_X509_EXT.1.1/Rev Test #3

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 3: The evaluator shall test that the TOE can properly handle revoked certificates--conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e. the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails. Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.
Test Steps	• Configure the TOE to authenticate Root, intermediate and server certificate. • Configure the SAN information in the TOE (evertz.magnum.com) • Verify the valid certificate.

	• Create a server certificate which will have CRL distribution point (URI: http://10.1.2.84/Acumen_Root_ICA.crl) and the SAN field (evertz.magnum.com). • Create a CRL which will not have any revoked certificate • Attempt to make a connection (connection will pass). • Verify the same via packet capture. • Revoke the peer end entity certificate. • Attempt to make a connection (connection will fail). • Verify the reason for failure via logs. • Verify the reason for failure via packet capture. • Revoke the peer intermediate certificate. • Attempt to make a connection (connection will fail). • Verify the reason for failure via logs. • Verify the reason for failure via packet capture.
Expected Test Results	• **When attempting a connection with a revoked peer certificate the connection fails** • **When attempting a connection with a non-revoked peer certificate a successful connection is established** • **When attempting a connection with a revoked intermediate certificate the connection fails**
Pass/Fail with Explanation	Pass. • When attempting a connection with a revoked peer certificate the connection fails • When attempting a connection with a non-revoked peer certificate a successful connection is established • When attempting a connection with a revoked intermediate certificate the connection fails This meets the testing requirements.

6.104 FIA_X509_EXT.1.1/Rev Test #4

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator

	shall configure the CA to sign a CRL with a certificate that does not have the CRL sign key usage bit set and verify that validation of the CRL fails.
Test Steps	• Configure the trustpoint for Root CA and authenticate • Configure the trustpoint for intermediate CA and authenticate • Verify that intermediate CA does not have CRL Sign parameter in Key Usage section • Enroll CSR on the TOE • Attempt a connection with the peer (will fail) • Verify the reason for failure via logs • Verify the same via Packet Capture
Expected Test Results	• **The TOE should reject the connection when CA signing the CRL does not have the CRLsign key usage bit set** • **Evidence (screenshot or CLI output) showing addition of certificates** • **Log showing unsuccessful connection** • **Packet capture showing unsuccessful connection**
Pass/Fail with Explanation	Pass. • The TOE rejects the connection when CA signing the CRL does not have the CRLsign key usage bit set • Log showing unsuccessful connection with the error as “Unknown CA” • Packet capture showing unsuccessful connection with the error as “Unknown CA” This meets the testing requirement.

6.105 FIA_X509_EXT.1.1/Rev Test #5

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps	• Attempt a connection to a remote modified TLS server using acumen-tlsc tool that would perform the necessary modification on the server certificate. Verify that the TOE rejects the connection: • Verify that the connection fails with packet capture. • Verify with the help of logs.

Expected Test Results	**A connection with a server using a modified certificate fails.**
Pass/Fail with Explanation	Pass. The TOE rejects connections when the first 8 bytes of the certificate are modified. This meets the testing requirements.

6.106 FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• Attempt a connection to a remote TLS server with a modified certificate using acumen-tlsc tool and verify that it fails. • Verify with the help of packet capture. • Verify with logs.
Expected Test Results	**The TOE rejects connections when the last byte of the certificate is modified.**
Pass/Fail with Explanation	Pass. The TOE rejects the connections when the last byte of the certificate is modified. This meets the testing requirement.

6.107 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)
Test Steps	• Attempt a connection to a remote TLS server using acumen-tlsc tool and modify any byte in the public key of the certificate and verify that the connection is rejected. • Verify with the help of packet capture. • Verify with logs.
Expected Test Results	**The TOE rejects connections when the public key of the certificate is modified.**

Pass/Fail with Explanation	Pass. The TOE rejects the connections when the public key of the certificate is modified. This meets the testing requirement.

6.108 FIA_X509_EXT.1.1/Rev Test #8a

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain. **TD0527 (12/1 Update) has been applied.**
Test Steps	• Create a certificate chain with three certificates using EC curves. • Add only the RootCA on the TOE. • Attempt a connection from a remote server and verify that it is successful. • Verify the connection succeeds with packet capture.
Expected Test Results	**The TOE should make a successful EC connection with only the Root CA installed in the trusted store.**
Pass/Fail with Explanation	**EC curve is not supported as per the FCS_COP.1/SigGen**

6.109 FIA_X509_EXT.1.1/Rev Test #8b

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC Intermediate CA certificate needs to be provided, together with the leaf certificate, from outside the TOE to complete the chain (e.g. by storing only the EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid. **TD0527 (12/1 Update) has been applied.**

Test Steps	• Replace the Peer ICA in the earlier test with a modified certificate and signed by the trusted RootCA. • Attempt a connection from the remote server and verify that it fails. • Verify the failed connection with a packet capture. • Verify the failed connection with logs.
Expected Test Results	**The TOE should not allow a successful connection when the certificate chain uses an explicit format version of the Elliptic Curve**
Pass/Fail with Explanation	**EC curve is not supported as per the FCS_COP.1/SigGen**

6.110 FIA_X509_EXT.1.1/Rev Test #8c

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store. **TD0527 (12/1 Update) has been applied.**
Test Steps	• Add a subordinate CA certificate into a TOE's trust store, that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA and observe that it is rejected • Add a subordinate CA certificate into a TOE's trust store, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA and observe that it is accepted
Expected Test Results	• **The TOE should reject installation of subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA.** • **Evidence (screenshot or CLI output) showing installation of the certificates.**
Pass/Fail with Explanation	**EC curve is not supported as per the FCS_COP.1/SigGen**

6.111 FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that

	require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: *(i) as part of the validation of the leaf certificate belonging to this chain;* *(ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).*
Test Steps	• Create a certificate chain for a TLS server where an intermediate CA is missing the Basic Constraints extension • Load the certificate lacking the basic Constraints extension on the TOE and verify that it fails. • Verify with logs
Expected Test Results	**The TOE rejects certificates signed by a CA that does not contain the basicConstraints extension.**
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that does not contain the basicConstraints extension. This meets the testing requirement.

6.112 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) then the associated extendedKeyUsage rule testing may be omitted.

	The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: • a self-signed root CA certificate, • an intermediate CA certificate and • a leaf (node) certificate. The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: 1. As part of the validation of the leaf certificate belonging to this chain; 2. 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	• Create a certificate chain where an intermediate CA has the CA Flag set to False in the Basic Constraints extension • Load the certificate lacking the basic Constraints extension on the TOE and verify that it fails. • Verify with logs
Expected Test Results	**The TOE rejects certificates signed by a CA that has the CA flag in the basicConstraints extension set to FALSE.**
Pass/Fail with Explanation	Pass. The TOE rejects certificates signed by a CA that has the CA flag in the basicConstraints extension set to FALSE.

6.113 FIA_X509_EXT.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps	• Create a server certificate with a modified URL

	• Attempt to connect to the TOE using Openssl and verify that it fails. • Verify with packet capture. • Verify error in logs.
Expected Test Results	**The TOE should reject the certificates it cannot verify via CRL when the responder is not found**
Pass/Fail with Explanation	Pass. The TOE rejects certificates it cannot verify via CRL when the responder is not found. This meets the testing requirements.

6.114 FIA_X509_EXT.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.

Test Steps	• From the TOE, generate a CSR
	• Examine the CSR contents and ensure the CSR contains the following fields
	  ○ Public Key
	  ○ Common Name.
	  ○ Organization.
	  ○ Organizational Unit.
	  ○ Country.

Expected Test Results	**The TOE is able to generate a CSR with all of the requisite information.**
Pass/Fail with Explanation	Pass. The TOE is able to generate a CSR with all of the requisite information. This meets the testing requirement.

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

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

7.1.1.2 ADV_FSP.1 Activity 2

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass.

7.1.1.3 ADV_FSP.1 Activity 3

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

Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.2 AGD_OPE.1 Activity 2

Objective	The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The ST claims only one platform, and the operational guidance documents cover the configuration and use of this platform. 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

	examined the section **Initial Setup** in the AGD and 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, covers configuration of the in-scope functionality where additional configuration might be required. 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 XXXX of the AGD. The evaluator found that these sections describe how the Operational Environment must meet: OE.PHYSICAL is covered by an explicit statement in the CC Guide. Note that the evaluator believes, generally, speaking, that OE.NO_GENERAL_PURPOSE is unenforceable by an end-user for most (if not all) NDcPP targets because it assumes a user can modify the TOE. OE.NO_GENERAL_PURPOSE is in effect because the TOE is not provided with general-purpose computing capabilities. OE.TRUSTED_ADMIN is covered by an explicit statement in the CC Guide. OE.UPDATES is covered in the CC Guide under the 'Check Firmware Version' and 'Upgrading Firmware' sections in the CC Guide. OE.ADMIN_CREDENTIALS_SECURE – The CC Guide, throughout all sections, the document directs administrators to protect their administrator access credentials, respectively. The Security Target, section 6 - FCS_CKM.4 describes the credential securing methods used. OE.RESIDUAL_INFORMATION is covered in the CC guide as it covers methods to zeroize the device back to factory default states. OE.CONNECTIONS – the admin guide documents covers this in detail on the Magnum server usage.
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. There is only one operational environment claimed in the ST. The only claimed TOE platform in ST is covered by the operational guidance documents. 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, • Administer the TOE locally and remotely. • Configure the authentication failure parameters. • Update the Magnum, and to verify the updates using digital signature capability prior to installing those updates. • Resetting passwords. • Administrative login and logout. • Generate CSRs, import x509 certificates, and delete x509 certificates. • Configure the access banner. • Configure the session inactivity time before session termination or locking. • Configure remote audit server parameters. • Set the time which is used for time-stamps. The product delivery method is described in section 2 of the CC-Guide document. For testing, the evaluator received the physical product as specified in the CC-Guide. The evaluator performed the instructions supplied in the guide.

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

7.3.1.4 AGD_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Test #3. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.5 AGD_PRE.1 Activity 5

Objective	In addition, the evaluator shall ensure that the following requirements are also met. The preparative procedures must a) include instructions to provide a protected administrative capability; and b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections titled '**User Authentication Failure Parameters'** and **'User Password Management'** were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH/ WebGUI for remote administration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

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

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

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

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.

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

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

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

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

Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement.
	
	Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.
	
	• NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
	  ○ Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
	  ○ US-CERT: http://www.kb.cert.org/vuls/html/search
	• Community (Symantec) security community: https://www.securityfocus.com/
	• Tenable Network Security: http://nessus.org/plugins/index.php?view=search
	• Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories
	• Offensive Security Exploit Database: https://www.exploit-db.com/
	• Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
	• OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html

	• Google The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on the 03rd February 2023. • MAGNUM • Intel Xeon Silver 4309Y • Evertz • nginx 1.18.0-0 • openssh 8.2/ openssh 8.2p1-4ubuntu0.5 • rsyslog 8.2001.0-1 • openssl 1.1.1k • Linux Kernel 5.4.0 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, most issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. However, there are some residual vulnerabilities which the evaluator identified with the product. Most of them require local access to the TOE to exploit. Based on the A_PHYSICAL_PROTECTION assumption, it is assumed that the TOE is physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. The following vulnerabilities were identified as residual vulnerabilities which the evaluator had done thorough research including code reviews of the TOE. Some of these were excluded due to the low impact with a low CSVV base score and would require high attack complexity to exploit. CVE-2021-3618 CVE-2021-23017 CVE-2021-36368 CVE-2022-24903 CVE-2022-1292 CVE-2022-2068 CVE-2021-3712 CVE-2021-4160

	After research, it was identified that all of the vulnerabilities identified are either not applicable, patched, or are beyond basic attack potential. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.2 AVA_VAN.1 Activity 2

Objective	The evaluator shall perform the following activities to generate type 4 flaw hypotheses: • Fuzz testing ○ Examine effects of sending: ▪ mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443) ▪ mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE. Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis. ○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well-formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.
Evaluator Findings	The evaluator documented the fuzz testing results with respect to this requirement.

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

8 Conclusion

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

End of Document