NETWORK DEVICE COLLABORATIVE PROTECTION PROFILE V2.6 SECURITY TARGET FOR MAGNUM-SC-CC

1 December 2017

Evertz Microsystems Ltd
5292 John Lucas Dr. Burlington, Ontario, Canada

Table of Contents

Table of Figures

Table of Tables

DOCUMENT REVISION HISTORY

VERSION	DATE	REVISION DESCRIPTION	AUTHOR
0.1	4/18/17	Based on previous ASPP	B. Mathews
0.2	4/19/17	Numerous corrections	B. Mathews
1.0	4/21/17	Add SSH to 6.2.1, standardize Section 6 formatting	B. Mathews
1.1	4/21/17	Change to Software Version	B. Mathews
1.2	4/24/17	Change to CPU Specs	B. Mathews
1.3	4/24/17	Corrected List of Ciphersuites	B. Mathews
1.4	4/26/17	Corrected List of Ciphersuites (again)	B. Mathews
2.0	5/24/17	Changes Based on Comments on IPX ST	B. Mathews
2.1	6/5/17	Eliminated Some Ciphersuites for CAVP Certification	B. Mathews
2.2	6/8/17	Eliminated SSH	B. Mathews
2.3	6/26/17	Corrections & Enhancements per NIAP	B. Mathews
2.4	8/2/17	Updates per TD0223-8 & add CAVP Cert. #s	B. Mathews
2.5	11/1/17	Corrected several minor omissions, discrepancies and typos.	B. Mathews
2.6	12/1/17	Corrected several minor omissions, discrepancies and typos.	B. Mathews

1 Introduction

This document is to demonstrate the compliance of one (1) product of Evertz Microsystems, Ltd. with the Network Device collaborative Protection Profile (NDcPP) version 1.0. The device is MAGNUM-SC-CC (hereinafter referred to as "MAGNUM"), which is a hardware and software package used to control one or more external video switching and endpoint devices (which lie outside the accreditation boundary of this product). MAGNUM is a control system used with a variety of video equipment, generally video switches of various types. MAGNUM consists of control and management applications embedded in a customized Linux operating system, running on a server-grade computer.

1.1 Security Target (ST) and Target of Evaluation (TOE) Reference

ST Title		**Evertz MAGNUM-SC-CC PPAS v2.6 Security Target**	
ST Document Number		2.6	
ST Version		2.6	
ST Issue Date		10/1/2017	
TOE Identification			
Component Type	**Subcomponent Type**	**Hardware Version**	**Firmware Version**
Server	MAGNUM-SC-CC	1.0	MAGNUM-SDVN-1.16.0

Table 1. ST and TOE Reference

2 Target of Evaluation (TOE) Overview

2.1 Physical Scope of the TOE

The MAGNUM-SC-CC hardware device is the Evertz MAGNUM-SC-CC (1 RU) running MAGNUM software. The MAGNUM-SC-CC serves as the primary user and network interface device for the MAGNUM control application.

Evertz MAGNUM software is a custom-developed application written primarily in python. MAGNUM operates as a combination of an application layer and as part of the integrated Linux platform stack, using a customized Linux distribution. The TOE version of MAGNUM is only operable on Evertz-provided platforms and hardware.

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.

Traditional packet-based networks do not support the extremely high standards for signal integrity and fault tolerance required for broadcast video. Evertz's solution to this problem has been to develop a packet-based switching fabric from a video perspective, rather than rely on traditional packet-based network architecture. Since video by nature has a unidirectional flow, and also since it is normal for multiple copies of a single incoming video stream to be sent to multiple output destinations, Evertz

focuses exclusively on multicast IP addressing. Unicast is not feasible for streaming video in an enterprise production environment.

Multicast switching can be challenging, especially for non-automated systems. Momentary delays and signal loss are common in these networks but are unacceptable in broadcast environments. Evertz has instead approached the problem from a video perspective. MAGNUM-SC-CC controls all Evertz multicast group definitions, such as JOIN and LEAVE commands, using Evertz's proprietary Synergy multicast protocol. MAGNUM compiles and delivers these commands within the context of traditional "vertical interval" switching architectures for legacy broadcast routing architectures, so as to route data seamlessly between program streams in a manner sufficient to meet broadcast video standards for signal availability and integrity.

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.

2.2 Logical Scope of the TOE (Overview)

The NDcPP-compliant TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Secure Management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

These features are described in more detail in the subsections below.

2.2.1 Security Audit

The TOE's Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. Very broadly, the Audit events generated by the TOE include:

- Establishment of a Trusted Path or Channel Session
- Failure to Establish a Trusted Path or Channel Session
- Termination of a Trusted Path or Channel Session
- Failure of Trusted Channel Functions
- Identification and Authentication
- Unsuccessful attempt to validate a certificate
- Any update attempt
- Result of the update attempt
- Management of TSF data
- Changes to Time

The TOE can store the generated audit data on itself and it can be configured to send syslog events to a syslog server, using a TLS protected collection method. Logs are classified into various predefined categories. The logging categories help describe the content of the messages that they contain. Access to the logs is restricted to only Security Administrators, who has no access to edit them, only to copy or delete (clear) them. Audit records are protected from unauthorized modifications and deletions.

The logs can be viewed by using the "Retrieve Logs" menu item from the "Help" drop-down menu. The log records the time, host name, facility, application and "message" (the log details). New audit records are dropped when the allocated space for these records reaches the threshold, which is why the use of a syslog server is important.

2.2.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; cryptographic hashing and software integrity testing using SHS; keyed hashing services using HMAC-SHA; random-bit generation using DRBG; cryptographic key establishment using RSA-based key establishment schemes; digital signature using RSA. The TOE implements secure protocols TLS (Server and Client) and TLS/HTTPS (Server). The algorithm certificate references are listed in the table below.

Algorithm	Description	Mode Supported	CAVP Cert. #
AES	Used for symmetric encryption/decryption FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_COP.1(1)	CBC (128 and 256 bits)	4651
SHS (SHA-1, SHA-256)	Cryptographic hashing services and software integrity test FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_COP.1(1) FCS_COP.1(3)	Byte Oriented	3810
HMAC (HMAC-SHA-1, HMAC-SHA-256)	Keyed hashing services FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_COP.1(1) FCS_COP.1(4)	Byte Oriented	3079
DRBG	Deterministic random bit generation services in accordance with NIST SP 800-90A Rev 1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_RBG_EXT.1	CTR_DRBG (AES 256)	1569
RSA	Signature Verification and key transport FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_CKM.1 FCS_CKM.2 FCS_COP.1(2)	FIPS PUB 186-4 Key Generation (2048-bit key)	2537

Table 2. CAVP Certification References

2.2.3 Identification and Authorization

All Administrators wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services other than the display of the warning banner. Once an Administrator attempts to access the management functionality of the TOE, the TOE prompts the Administrator for a user name and password for password-based authentication. The identification and authentication credentials are confirmed against a local user database. Only after the Administrator presents the correct identification and authentication credentials will access to the TOE functionality be granted. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

The TOE provides the capability to set password minimum length rules. This is to ensure the use of strong passwords in attempts to protect against brute force attacks. The TOE also accepts passwords composed of a variety of characters to support complex password composition. During authentication, no indication is given of the characters composing the password.

2.2.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure session or a local console connection. The TOE provides the ability to perform the following actions:

- Administer the TOE locally and remotely
- Configure the access banner
- Configure the cryptographic services
- Update the TOE and verify the updates using digital signature capability prior to installing those updates
- Specify the time limits of session inactivity

All of these management functions are restricted to an Administrator, which covers all administrator roles. Administrators are individuals who manage specific type of administrative tasks.

Primary management is done using the local console or remotely via HTTPS. This provides a network administration console from which one can manage various identity services. These services include authentication, authorization and reporting. All of these services use a menu-driven navigation system.

2.2.5 Protection of the TSF

The TOE will terminate inactive sessions after an Administrator-configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE provides protection of TSF data (authentication data and cryptographic keys). In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. This time can be set by and Administrator using the “Date” and “Time” selections from the System Configuration menu, or can be set to follow an external NTP server. The TOE also ensures firmware updates are from a reliable source. Finally, the TOE performs testing to verify correct operation.

In order for updates to be installed on the TOE, an administrator initiates the process from the web interface. Magnum automatically uses the digital signature mechanism to confirm the integrity of the product before installing the update.

2.2.6 TOE Access

Aside from the automatic Administrators session termination due to inactivity describes above, the TOE also allows Administrators to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

Regardless of the type of connection the TOE will display an Administrator-specified banner on the web browser management interface prior to allowing any administrative access to the TOE.

2.2.7 Trusted Paths/Channels

Magnum allows the establishment of a trusted path between a itself and various video control switches (such as Evertz' IPX); it can also link to an additional Magnum (for primary / backup control arrangements). The TOE also establishes a secure connection for sending syslog data to a syslog server using TLS and other external authentication stores using TLS-protected communications.

3 TOE Description

3.1 MAGNUM-SC-CC Component Description

MAGNUM is a software package. MAGNUM-SC is MAGNUM software pre-installed on an Evertz-provided server. MAGNUM-SC-CC is the "high security" version of MAGNUM-SC ("CC" stands for "Common Criteria").

COMPONENT	PART NUMBER	DESCRIPTION
MAGNUM	**MAGNUM-SC-CC**	(1) Evertz MAGNUM-SC-CC (19.0" W x 1.75" H x10.1" D), Single AC Power, supporting High-Security Version of MAGNUM Control Software

Table 3. MAGNUM Description

The EMX frames are passive (except for the door-mounted fans, which are the only powered equipment permanently attached to the frame). The frames mount power supplies, frame controllers and IPX cards. The frame controllers serve as a passthrough proxy to distribute Ethernet-based control connections to the individual IPX cards within the EMX frame chassis. The controllers also provide limited Simple Network Management Protocol (SNMP) alarm information, such as the card type, slot location, and the status of power supplies and fans.) Details are in the "Notify" section of the IPX Manual.

The SFP ports are unencrypted. Sites requiring enclave-based data security will deploy physical security controls to isolate the video network enclave. Where operational mission requires that video needs to cross a logical enclave boundary, Evertz stipulates a network architecture deploying third-party software or hardware encryption at the video transmitting and video receiving endpoints.

3.2 Component Interconnectivity

The TOE consists of the MAGNUM-SC-CC software, ancillary services and hardware (physical server). The MAGNUM-SC-CC communicates via (2) 1000BASE-T ports and (2) 10G SFP ports. In each case the second port is for optional redundancy.

3.3 Non-Scope Elements

3.3.1 Network Connectivity

The nature of the physical network connection is considered outside the scope of the TOE, as the available network elements (IP switches, IP routers, etc.) which may be used in establishing that link are site-specific. Evertz stipulates that any connection must meet organizationally-specific security requirements for the location(s) where the equipment is deployed.

3.3.2 Video Switches

The purpose of the MAGNUM control system is to control a variety of video equipment, including:

- Analog Video Routing Switches
- Digital Video Routing Switches (SDI)
- Digital Video Routing Switches (ASI)
- Digital Video Routing Switches (IP)
- Video Tally Switches
- KVM Routing Switches
- Audio Routing Switches
- Video Master Control Systems
- Video Branding Systems
- Multiviewers
- Video Transport Systems

These will be referred to as “video switches.” These are outside the scope of the TOE.

3.4 TOE Component Reference Images

3.4.1 MAGNUM-SC_CC Reference images

Figure 1. MAGNUM-SC-CC Front View

Figure 2. MAGNUM-SC-CC Rear View

3.5 Usage and Major Security Features of the TOE

3.5.1 System Architecture / IT Environment

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-SC-CC device serves as the primary operational and administrative management interface to the closed multicast switching environment.

Users and administrators may access MAGNUM software via direct connection using a terminal session. Administrators only may access MAGNUM via a dedicated management workstation operating over an

Out-of-Band Management (OOBM) network. Sites may close this OOBM network or may operate MAGNUM within an existing OOBM, as long as the topology is compliant with the security parameters listed below.

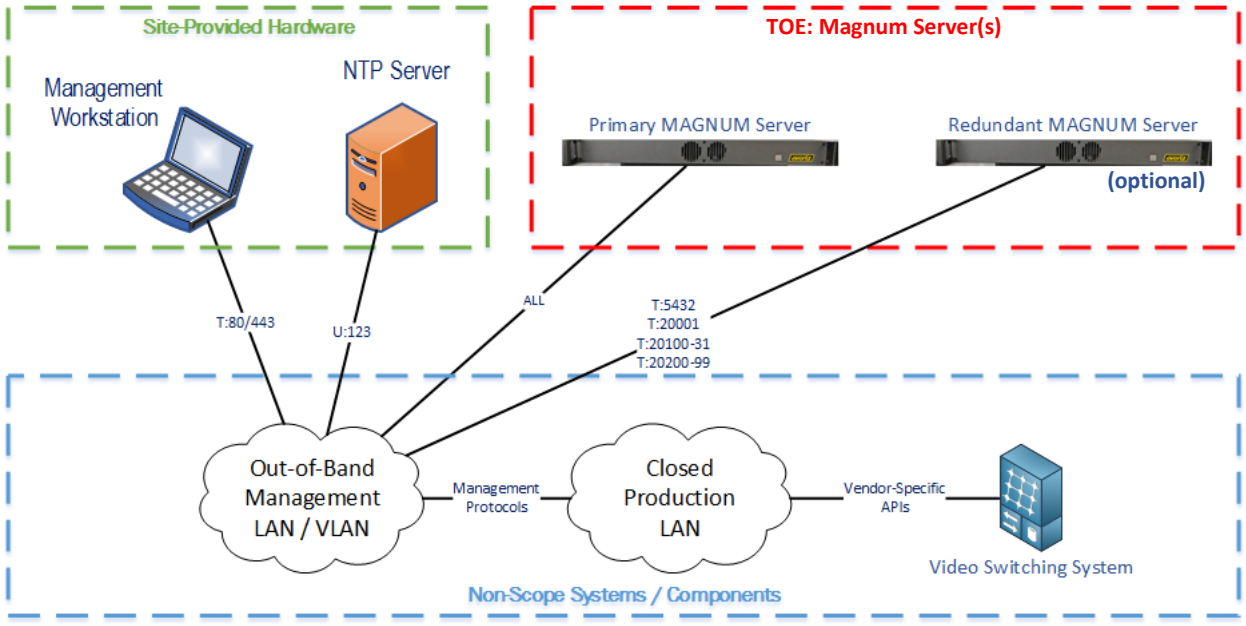

Figure 3. TOE Topology

3.5.1.1 Parts, Protocols and Services (PPS)

The MAGNUM-SC-CC environment supports the following Ports, Protocols, and Services:

Port	Behavior	Service	Protocol
U:123	Open	NTP	NTP
U:5404 -- 5407	TLS Encrypted	Cluster Manager	Corosync
T:80	Redirect to T:443	Web Server (nginx)	HTTP
T:443	TLS Encrypted	Web Server (nginx)	HTTPS
T:4000 – 4099	TLS Encrypted	MAGNUM Quartz Service	Quartz device interface(s)[1]
T:5432	TLS Encrypted	Database (postgresql)	SQL
T:8210	TLS Encrypted	MAGNUM Authentication Service	HTTPS Interface for Authentication API
T:8766	TLS Encrypted	MAGNUM Cucumber Service	Cucumber panel device interface[1]
T:12006	TLS Encrypted	MAGNUM Multiviewer Service	Evertz Multiviewer API (control)[1]
T:12019	TLS Encrypted	MAGNUM Multiviewer Service	Multiviewer Service Remote System Control API[1]
T:20001	TLS Encrypted	MAGNUM Backup Service	Backup Service Interconnect[2]
T:20100 – 20131	TLS Encrypted	MAGNUM EP3 Service	EP3 Interconnect[2]
T:20200 – 20299	TLS Encrypted	MAGNUM Driver Service	Driver Service Interconnect[2]
T:31001	TLS Encrypted	MAGNUM Multiviewer 3rd Party Service	Evertz Multiviewer Control Interface (for 3rd Party devices)[1]

LEGEND			
API	Application Programing Interface	**T**	Transmission Control Protocol
HTTP	Hypertext Transfer Protocol	**TLS**	Transport Layer Security
HTTPS	HTTP-Secure	**U**	User Datagram Protocol
NTP	Network Time Protocol		

[1]**Device control interface for production system device**

[2]**Redundant MAGNUM device interface**

Table 4. Magnum Environmental PPS

3.5.1.2 Security Architecture

3.5.1.2.1 Auditing

Audit data are stored internally and are only accessible to privileged administrators. The TOE supports role-based access control (RBAC) for authentication and authorization to management and security functions.

Audit records may also be stored externally on a Syslog server.

3.5.1.2.2 Authentication

Due to the closed nature of the deployed network, the TOE does not support the ability to use external authentication servers for user authentication. MAGNUM authenticates administrative users directly to local onboard databases.

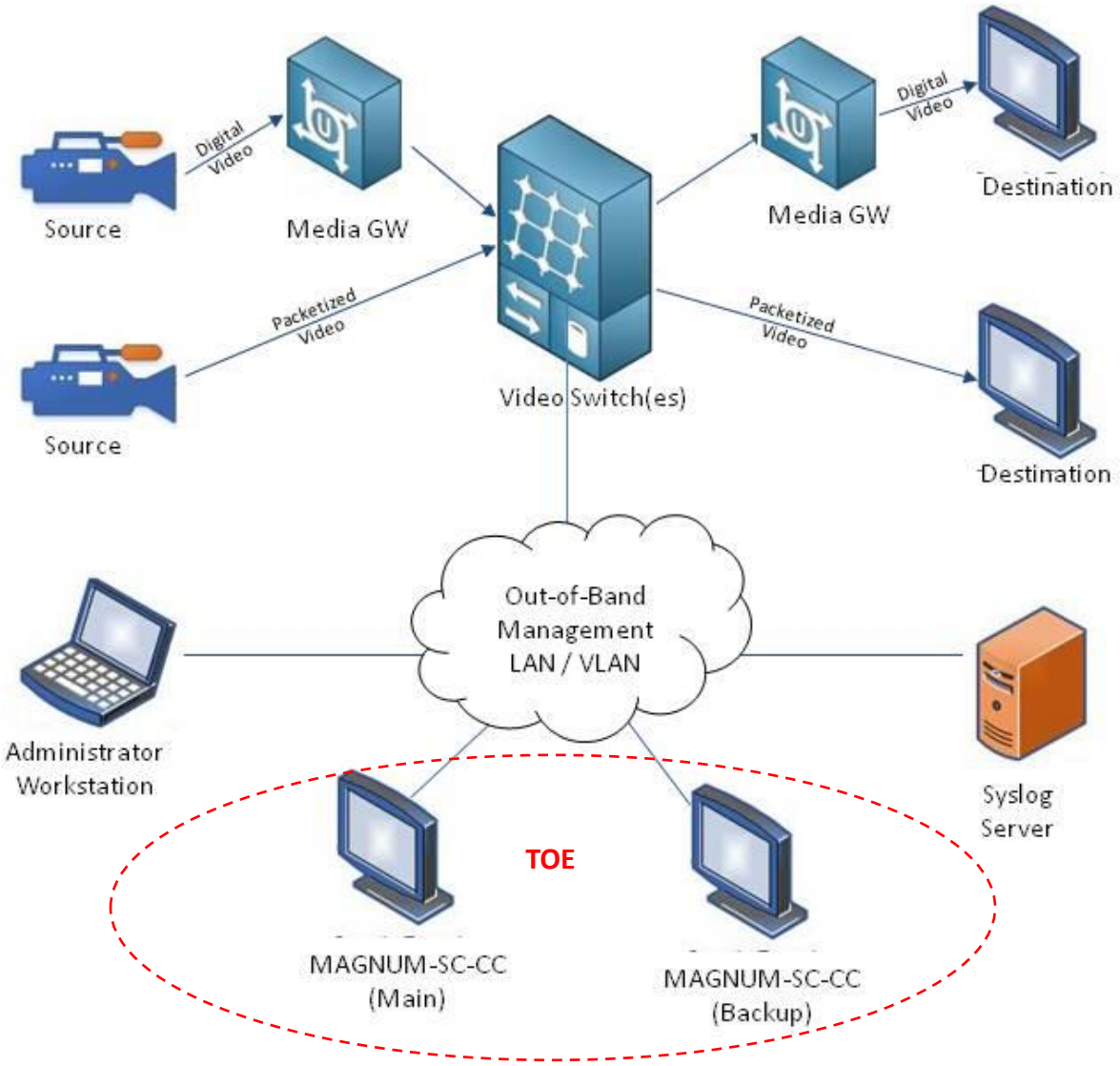

Figure 4. TOE System Architecture

3.5.2 Physical Design

The physical MAGNUM-SC-CC "box" is a 1 RU, server-grade computer:

Motherboard: Gigabyte MB10-DS3
CPU: 1x Intel Xeon CPU D-1541, 16 Threads, 2.1 - 2.7 GHz
Memory: Innodisk M4R0-AGSQGCRG, ECC DDR4, 64GB
Solid State Disk: 2x Intel SSDSC2BA200G401, 200 GB, RAID 1
Network Interfaces: 2x 1 Gbps Ethernet, 2x 10 Gbps SFP

3.5.3 System Design

3.5.3.1 Operational Control

The MAGNUM-SC-CC hardware controller communicates with one or more video switches Ethernet. Administrative users have the option of managing MAGNUM via either web browser using HTTPS or via local console at the hardware device. Both the management channel and the video switch communication channel are authenticated and encrypted at the application layer when the device is configured for High Security Mode. Please see the *Magnum-SDVN Security Administration Manual* for further information.

3.5.3.2 System Management

Initial configuration of the MAGNUM-SC-CC hardware device must occur via local console. Once initial device configuration is complete, administrators may use the web browser or local console connectivity for all further administrative actions, including configuration, operations, and monitoring.

MAGNUM provides for a redundant/backup hardware terminal using dedicated configuration transfer protocols as illustrated in Table 4, MAGNUM Environment PPS and Figure 3, TOE Topology.

3.5.4 TOE Documentation

Evertz Microsystems, Ltd. publishes manuals detailing the installation configuration and operation of IPX Magnum control software. These are available to customers both on paper and as electronic copies.

CATEGORY	PRODUCT	MANUAL
MAGNUM	MAGNUM-SC-CC	MAGNUM User Manual, Version 1.3, April 2016
		MAGNUM-SDVN Management and Control of Evertz IP Switch Fabrics and Gateways User Manual, Version 0.1, November 2014
		MAGNUM-SDVN Security Administration Manual, Version 14 April 18, 2017

Table 5. List of Evertz Operating Manuals

3.5.1 MAGNUM-SC-CC Hardware

Evertz MAGNUM software is a Linux-based application that can be provided on many computing platforms, including Evertz-manufactured control panels. This TOE requires that MAGNUM software be deployed on a dedicated, custom-built Evertz-owned platform (model MAGNUM-SC-CC); collectively, this product is known as MAGNUM-SC-CC. The MAGNUM-SC-CC features an embedded Operating System (OS) and includes the following interfaces:

- Ethernet (2x RJ45, 1000BaseT)
- Ethernet (2x SFP, 10G SFP)
- USB (2x USB 3.0 connectors)
- VGA Output

For local console access a standard video display would be connected via the VGA output and a keyboard and mouse would be connected via USB.

The MAGNUM-SC-CC device has three components: the MAGNUM software package, an embedded customized Linux distribution, and an Evertz customized hardware platform.

3.5.1.1 MAGNUM-SC-CC Hardware I/O Interface

The MAGNUM-SC-CC features the following I/O Interfaces and controls:

NAME	NUM	PORT/CONTROL TYPE		FUNCTION
		PHYSICAL	PROTOCOL	
Ethernet	2	SFP	10G SFP	IP Link to Devices, Security Administrators
Ethernet	2	RJ45	1000BASE-T	IP Link to Devices, Security Administrators
USB	2	USB Type A	USB 3.0	Keyboard/Mouse Human Interface Devices (HIDs)
VGA output	1	DE15	VGA	Legacy Analog Video Display Connection

Table 6. MAGNUM-SC-CC Hardware I/O

3.5.2 TOE Interconnectivity

The MAGNUM-SC-CC, the OOBM systems, and the production components in a given installation communicate with each other over standard Layer 2 Ethernet. The logical connectivity between MAGNUM, production systems, users and various ancillary components are part of the TOE, while physical connectivity lies outside of the scope of this TOE. It is specified that deployment of the secure version of these products will include the use of secure network connection(s) for control purposes.

3.5.3 TOE Operational Environment

MAGNUM is a device/component management application specifically designed to operate broadcast and enterprise video switching/routing equipment. Typically, such video equipment is deployed either in an extended series of point-to-point, non-Ethernet connections (such as optical fiber, Serial Digital Interface (SDI), High Density Multimedia Interface (HDMI), HDBaseT, or similar video-specific interfaces) or via an integrated, Ethernet-based switch fabric such as Evertz's IPX product.

MAGNUM does not have the ability to route multimedia stream data and operates exclusively via OOBM. MAGNUM both issues operational commands to production video equipment and serves as the primary interface for production devices to report to external services, such as logging tools. (Certain external services, such as NTP services, may connect directly into the production environment.)

MAGNUM may lie within the same production network as the video equipment or it may be isolated therefrom. In the case of non-Ethernet connectivity for the video system, MAGNUM may be located on a standard production network at the discretion of the site/mission owner.

It is not necessary for MAGNUM to be located on an enterprise OOBM network, although sites may choose to do so. Sites requiring multi-factor or LDAP-integrated authentication and authorization must

place MAGNUM on a dedicated/isolated OOBM network, as MAGNUM does not support these capabilities currently.

3.5.4 TOE Applications

Typical applications of IPX applications include:

- Security Cameras
- Multiviewer Displays
- Teleconferencing
- Video Production
- Video Storage
- Video Distribution

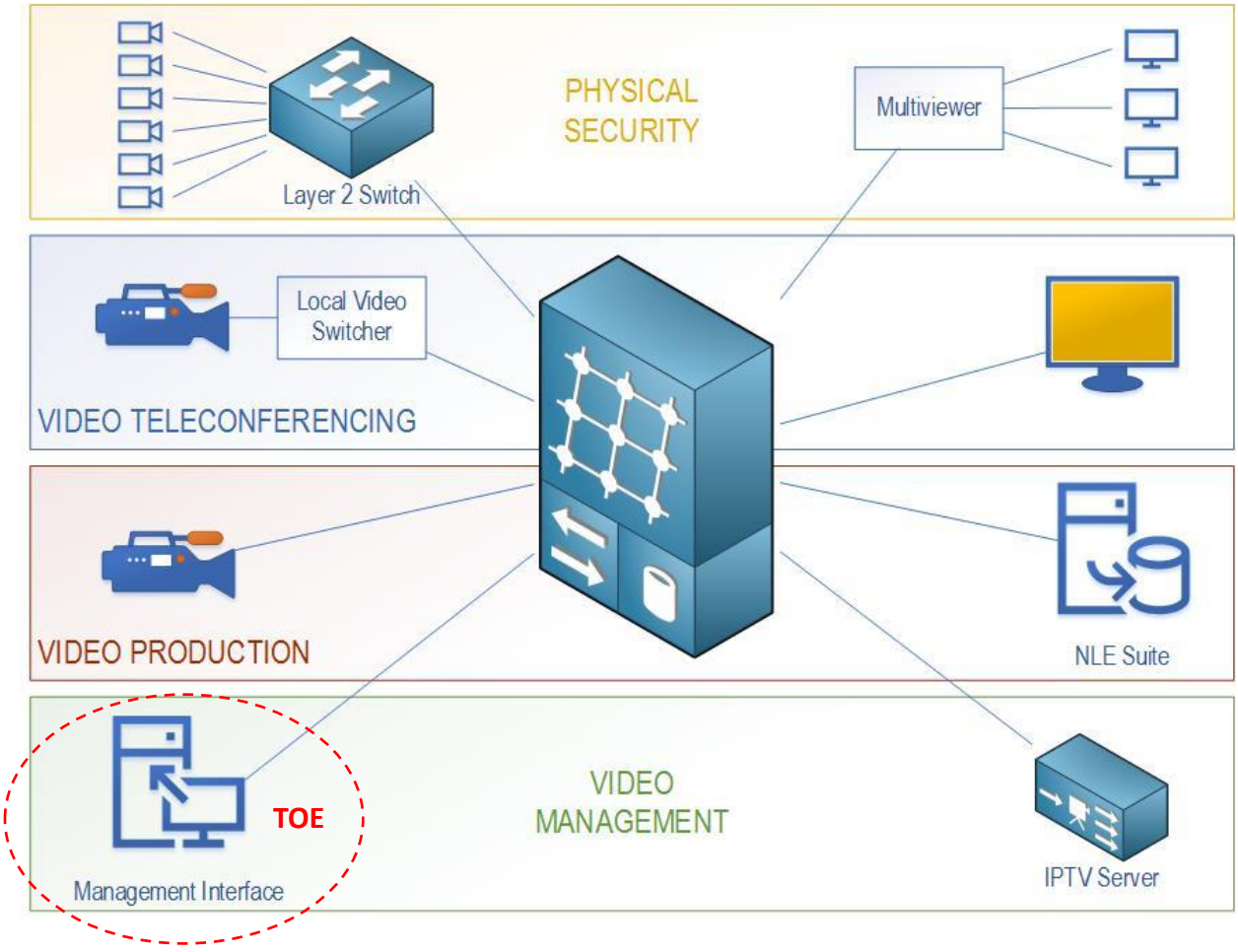

Figure 5. Examples of Typical Video Switch / Magnum Uses

3.5.5 TOE Management Overview

3.5.5.1 Operational Control

- Core routing
- System interlinking
- Multi-view display operation
- Facility Master Control
- Signal transport optimization
- Tally management
- Dynamic signal formatting[1]

3.5.5.2 User Interface

Operators access the application via web browser. Standard users are able to perform basic system functions such as routing and switching. Accessing administrative functions, such as system configurations, device updates, or access controls, requires elevated privileges and is reserved for system administrators only.

3.5.5.3 Administrative Interface

Although local console access is permitted, the primary and preferred method for system operation is via web browser. All management is via an OOBM network, as depicted in Figure 3, TOE Topology. Authorized administrators have full access to MAGNUM via the encrypted browser interface.

3.5.5.4 System Management

MAGNUM writes alarms and information to its internal logfile. Authorized privileged users have the ability to search the logs for specific details and / or export to an offline aggregator tool.

Administrators have the ability to manually offload logs using the administrator console. The *Magnum-SDVN Security Administration Manual* contains instructions for this process.

3.6 Logical Scope of the TOE

The figure below depicts the logical scope of the TOE.

[1] Dynamic formatting requires the use of additional components not included in this TOE.

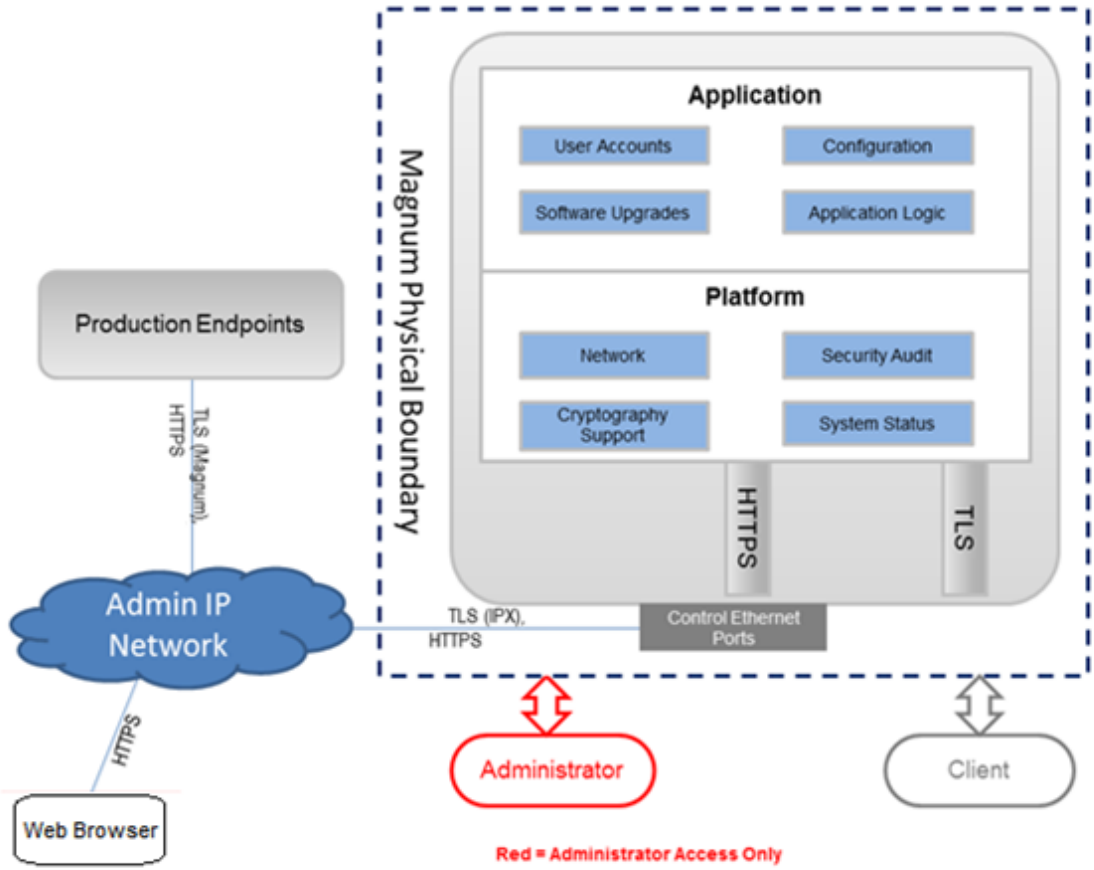

Figure 6. TOE Logical Scope and Workflow

3.6.1 Role Based Access Control

The TOE provides functional module authorization to administrative users through two defined roles:

- **User:** Provides rights to create, change and remove logical cross connections within the IPX. The "User" only has access to the system through the Magnum interface. Specific users may have access to all or only some of the ports under the control of the CO / Administrator.
- **Cryptography Officer (CO) / Administrator:** Provides all access rights and sets up secure communications.

	Functional Module	User	CO/Admin
Operational Modules	Device Control	✓	✓
	Port Configuration	✓	✓
	Port Naming	✓	✓
	Establish Sub-Users	✓	✓
	Administer Sub-Users	✓	✓
Security Modules	Network		✓
	Services		✓
	Administer All Accounts		✓
	Cryptographic Support		✓
	Self-Test		✓
	Security Audit		✓
	Firmware Upgrades		✓

Table 7. Role- Based Access to TOE Functional Module Settings

3.6.2 TOE Functional Modules

MAGNUM has seven functional modules, of which six are considered to be part of the Target Security Function (TSF). All modules are described here in order to provide context for the TOE functionality.

3.6.2.1 MAGNUM-SC-CC Functional Modules

The following MAGNUM functional modules are part of the TSF:

1. **User Accounts:** Used to manage all user accounts (both CO/Admin accounts and User accounts) and their assigned roles. MAGNUM has a default administrative user account with default login credentials, which must be changed at the time of installation by placing the device into High Security mode.

2. **Configuration:** Used to manage operator-created configurations for non-TSF (operational IP virtual cross connects, typically streaming video) settings, which can be saved in flash memory. A saved configuration can be loaded at startup.

3. **Network:** Used to manage the network interface settings for the non-TSF ports, including IP address, DNS and NTP.

4. **Software Upgrades:** Used to manage upgrades of the TOE software.

5. **Cryptography Support:** Used to manage the cryptographic module and keys.

6. **Security Audit:** Used to manage the recognition, recording and transmission of information related to security activities.

The following functional module is not part of the TSF:

1. **System Status:** Used to record non-security audit information (on the "health" and status of the system) on an external Syslog server. N.B.: External syslog connectivity is disabled in High Security mode.

3.7 Conformance Claims (ASE_CCL)

3.7.1 Common Criteria Claims

The following conformance claims are made for the TOE and ST:

- **CC v3.1, Rev. 3 Conformant**
  The ST and TOE are conformant to Common Criteria version 3.1, Revision 4.

- **Part 2 Extended**
  The ST is Common Criteria Part 2 extended.

- **Part 3 Conformant**
  The ST is Common Criteria Part 3 Conformant.

- **PP Conformant**
  The ST complies to the NDcPP (Collaborative Protection Profile "Security Requirements for Network Devices"), Version 1.0, with additional requirements drawn from Appendix C of the NDcPP.

3.7.2 NIAP Technical Decisions

Magnum conforms to the requirements of the following NIAP Technical Decisions. For each Technical Decision listed, the relevant SFR(s) are referenced, along with a brief description in red of the TD's effect (if any) on the Security Target.

- 0228 NIT Technical Decision for CA certificates - basicConstraints validation
  FIA_X509_EXT.1.2 Test change only; no change to the Security Target.

- 0227 NIT Technical Decision for TOE acting as a TLS Client and RSA key generation
  FCS_CKM.1 - Makes a client-side requirement optional; Magnum already does this.

- 0226 NIT Technical Decision for TLS Encryption Algorithms
  FCS_TLSC_EXT.2.1 & FCS_TLSS_EXT.2.1 One ciphersuite no longer mandatory; slight wording change only.

- 0201 – NIT Technical Decision for Use of intermediate CA certificates and certificate hierarchy depth
  FCS_TLSS_EXT.1.1 Removed the mandatory selection – only a slight wording change to Magnum.

- 0191 – NIT Technical Decision for Using secp521r1 for TLS communication
  FCS_TLSS_EXT.2.3 Wording change for some options; did not change our wording.

- 0188 – NIT Technical Decision for Optional use of X.509 certificates for digital signatures
  FPT_TUD_EXT.1 Made optional what we were doing anyway; no change to us.

- 0187 – NIT Technical Decision for Clarifying FIA_X509_EXT.1 test 1
  FIA_X509_EXT.1.1 Test change only; no change to the Security Target.

- 0185 – NIT Technical Decision for Channel for Secure Update.
  FTP_ITC.1 Expanded TSS description to explicitly state how updates are secured.

- 0184 – NIT Technical Decision for Mandatory use of X.509 certificates
  FIA_X509_EXT.[1,2 & 3] X.509 is Mandatory; Magnum already uses X.509 certificates.

- 0183 – NIT Technical Decision for Use of the Supporting Document
  No specific SFRs – This clarifies that evaluators do not have to evaluate SFRs that are n/a to the TOE.

- 0181 – NIT Technical Decision for Self-testing of integrity of firmware and software.
  FPT_TST_EXT.1 This simply says testing must abide by the SFR.

- 0169 – NIT Technical Decision for Compliance to RFC5759 and RFC5280 for using CRLs
  FIA_X509_EXT.1.1 Wording change to some optional selections; Magnum's selection did not change.

- 0155 – NIT Technical Decision for TLSS tests using ECDHE in the NDcPP v1.0.
  FCS_TLSS_EXT.2.3 Testing change for ECDHE, which is not used by Magnum.

- 0153 – NIT Technical Decision for Auditing of NTP Time Changes in the NDcPP v1.0 and FW cPP v1.0
  FAU_GEN.1: Added clarification that Magnum audits NTP time discontinuities.

- 0152 – NIT Technical Decision for Reference identifiers for TLS in the NDcPP v1.0 and FW cPP v1.0
  FCS_TLSC_EXT.2 Magnum already does this.

- 0151 – NIT Technical Decision for FCS_TLSS_EXT Testing - Issue 1 in NDcPP v1.0.
  FCS_TLSS_EXT.1 Test change only; no change to the Security Target.

- 0143 – NIT Technical Decision for Failure testing for TLS session establishment in NDcPP and FWcPP
  FCS_TLSS_EXT.1 Test change only; no change to the Security Target.

- 0130 – NIT Technical Decision for Requirements for Destruction of Cryptographic Keys
  FCS_CKM.4.1 Considerable text change; Magnum was already complaint.

- 0125 – NIT Technical Decision for Checking validity of peer certificates for HTTPS servers
  FCS_HTTPS_EXT.1.3 Wording change; Magnum is already compliant.

- 0117 – NIT Technical Decision for FIA_X509_EXT.1.1 Requirement in NDcPP
  FIA_X509_EXT.1.1 Added clarification in TSS that Magnum's X.509 certificate validation includes revocation checking.

- 0116 – NIT Technical Decision for a Typo in reference to RSASSA-PKCS1v1_5 in NDcPP and FWcPP
  FCS_COP.1.1(2) Typo correction.

- 0112 – NIT Technical Decision for TLS testing in the NDcPP v1.0 and FW cPP v1.0.
  (General) Test clarificcation only; no change to the Security Target.

- 0111 – NIT Technical Decision for third party libraries and FCS_CKM.1 in NDcPP and FWcPP
  FCS_CKM.1 Magnum complies with FIPS 186-4, so this is n/a.

- 0095 – NIT Technical Interpretations regarding audit, random bit generation, and entropy in NDcPP
  FAU_STG_EXT.1, FCS_COP.1 & FCS_RBG_EXT.1.1 Magnum is already compliant.

- 0094 – NIT Technical Decision for validating a published hash in NDcPP
  FPT_TUD_EXT & FMT_MOF Application note clarifications; Magnum is already compliant.

4 Definition of the Security Problem

This section identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with “assumption” specifying a unique name. Threats are identified as T.threat with “threat” specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with “osp” specifying a unique name.

The security problem & the associated assumptions, threats, etc are taken directly from the NDcPP v. 1.0.

4.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may not be able to provide all of its security functionality.

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	**The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.**
A.LIMITED_FUNCTIONALITY	**The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).**
A.NO_THRU_TRAFFIC_PROTECTION	**A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).**
A.TRUSTED_ADMINISTRATOR	**The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious**

	administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	**The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.**
A.ADMIN_CREDENTIALS_SECURE	**The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.**

Table 8. Operational Environment Assumptions

4.1.1 Threat Model

The table below shows the threats that are to be countered by the TOE, its operational environment, or a combination of the two.

Threat Name	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	**Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.**
T.WEAK_CRYPTOGRAPHY	**Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.**
T.UNTRUSTED_COMMUNICATION_CHANNELS	**Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.**
T.WEAK_AUTHENTICATION_ENDPOINTS	**Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselvesinto the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.**

T.UPDATE_COMPROMISE	**Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.**
T.UNDETECTED_ACTIVITY	**Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.**
T.SECURITY_FUNCTIONALITY_COMPROMISE	**Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.**
T.PASSWORD_CRACKING	**Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.**
T.SECURITY_FUNCTIONALITY_FAILURE	**A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.**

Table 9. Threat Model

4.2 Organizational Security Policies (OSP)

An organizational security policy is a set of rules, practices and procedures imposed by an organization to address its security needs. The table below shows the OSPs that are to be enforced by the TOE, its operational environment or a combination of the two.

Threat Name	Threat Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements or any other appropriate information to which users consent by accessing the TOE.

Table 10. Organizational Security Policies

5 Security Objectives (ASE_OBJ)

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

5.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v1.0 does not define any security objectives for the TOE

5.2 Security Objectives for the Operational Environment (OE)

All of the assumptions stated in Section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-TOE security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Those objectives are described in the table below:

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

Environment Security Objective	IT Environment Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access The TOE must be Protected on any other platform on which they reside

Table 11. Security Objectives for the Environment

6 Security Requirements

This section specifies the requirements for the TOE. The security functional requirements correspond to the security functions implemented by the TOE, as required by the PP.

6.1 TOE Security Functional Requirements (SFR)

This sub-section specifies the SFRs for the TOE. It organizes the SFRs by CC classes as per the table below.

CC Functional		Security Functional Requirements	
Class	**Description**	**TOE SFR**	**Description**
FAU	Security Audit	FAU_GEN.1	Audit Data Generation
		FAU_GEN.2	User Identity Association
		FAU_STG_EXT.1	External Audit Trail Storage
FCS	Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
		FCS_CKM.2	Cryptographic Key Establishment
		FCS_CKM.4	Cryptographic Key Destruction
		FCS_COP.1(1)	Cryptographic Operation (AES Data Encryption/Decryption)
		FCS_COP.1(2)	**Cryptographic Operation (Signature Generation and Verification)**
		FCS_COP.1(3)	Cryptographic Operation (Hash Algorithm)
		FCS_COP.1(4)	Cryptographic Operation (Keyed-Hash Algorithm)
		FCS_RBG_EXT.1	Random Bit Generation
		FCS_TLSC_EXT.2	Explicit: TLS (Client)
		FCS_TLSS_EXT.1	Explicit: TLS (Server)
		FCS_HTTPS_EXT.1	Explicit: HTTPS
FIA	Identification and Authentication	FIA_PMG_EXT.1	Password Management
		FIA_UIA_EXT.1	User Identification and Authentication
		FIA_UAU_EXT.2	Password-Based Authentication Mechanism
		FIA_UAU.7	Protected Authentication Feedback
		FIA_X509_EXT.1	X.509 Certificate Validation
		FIA_X509_EXT.2	X.509 Certificate Authentication
		FIA_X509_EXT.3	X.509 Certificate Requests

FMT	Security Management	FMT_MOF.1(1) / Trusted Update	Management of Security Functions Behavior
		FMT_MOF.1(1) / AdminAct	Administrators Modify Security Behavior
		FMT_MOF.1(2) / AdminAct	Administrators Enable/Disable Security Functions
		FMT_MOF.1 / LocSPace	Administrators Configure Audit Storage
		FMT_MTD.1	Management of TSF Data
		FMT_SMF.1	Specification of Management Functions
		FMT_SMR.2	Restrictions on Security Roles
FPT	Protection of the TSF	FPT_SKP_EXT.1	Protection of TSF Data (for Reading of All Symmetric Keys)
		FPT_APW_EXT.1	Protection of Administrator Passwords
		FPT_TST_EXT.1	TSF Testing
		FPT_TUD_EXT.1	Trusted Update
		FPT_STM.1	Reliable Time Stamps
FTA	TOE Access	FTA_SSL_EXT.1	TSF-Initiated Session Locking
		FTA_SSL.3	TSF-Initiated Termination
		FTA_SSL.4	User-Initiated Termination
		FTA_TAB.1	Default TOE Access Banners
FTP	Trusted Path/Channels	FTP_ITC.1	Inter-TSF Trusted Channel
		FTP_TRP.1	Trusted Path

Table 12. TOE Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1 FAU.GEN.1 – Audit Data Generation

FAU_GEN1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) *All administrative actions comprising:*
   - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
   - *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
   - *Generating import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
   - *Resetting passwords (name of related user account shall be logged).*
   - *Starting and stopping services (if applicable)*
   - No other actions
d) Specifically defined auditable events listed in the table below.

Requirement	Auditable Event
FAU_GEN.1.1	Start-up of the audit functions
	Shut-down of the audit functions
	… others handled by other audit requirements already
FIA_UIA_EXT.1	Web login
	Web logout
	Local Linux login
	Local Linux logout
	Remote Linux login
	Remote Linux logout
FIA_UAU_EXT.2	Local Linux login
	Local Linux logout
FIA_X509_EXT.1	TLS certificate verification
FMT_MOF.1(1)/TrustedUpdate	Attempt to update firmware
FMT_MTD.1	Enter secure mode
	Edit login banner
	Change Linux user password
	Expire web all user passwords
	Web user changing own password
	Create web user
	Delete web user
	Import signed certificate (CSR response)
	Import trusted CA certificate
	Remove trusted CA certificate
	Import CRL file
	Remove CRL file
	Configure allowed Subject Alt Names
	Configure device IP address
FPT_TUD_EXT.1	Result of attempt to update firmware
FPT_STM.1	Changing time / date / time zone
FTA_SSL.3	Terminate remote interactive session after timeout (web)
	Terminate remote interactive session after timeout (Linux)
FTA_SSL.4	Remote administrator terminated own session (web)
	Remote administrator terminated own session (Linux)
FTP_ITC.1	TLS connection initiated
	TLS connection terminated
	TLS connection failed to establish

FTP_TRP.1	Remote administrator session initiated (web)
	Remote administrator session terminated (web)
	Remote administrator session failed (web)
	Remote administrator session initiated (Linux)
	Remote administrator session terminated (Linux)
	Remote administrator session failed (Linux)
FAU_STG_EXT.3	Log rotated to prevent filling storage space
FMT_MOF.1(1)/Audit	Configure IP of remote audit server
FMT_MTD.1/AdminAct	Import update verification public key
	Reset disk encryption key
	Reset TLS private key
FCS_HTTPS_ EXT.1	Failure to establish HTTPS session (server side)
FCS_TLSC_EXT.2	TLS connection failed to establish (client side)
FCS_TLSS_EXT.1	TLS connection failed to establish (server side)

Table 13. TOE security Functional Requirements and Auditable Events

The Evertz administrative guide lists all of these auditable events with associated formats.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- For each audit type, based on the auditable event definitions of the functional components listed in the PP/ST, *information specified in column two of Table 16.* TSF Overview
- below.

Auditable Event	**Audit Record Content***	**Associated SFRs**
Start-up of the audit functions	<audit-process-info> start	FAU_GEN.1
Shut-down of the audit functions	<audit-process-info> <stop-reason>	FAU_GEN.1
Web login	Authenticated user <user-name> <token-info> <origin-ip-addr>	FIA_UIA_EXT.1
Web logout	User logged out <user-name> <token-info> <origin-ip-addr>	FIA_UIA_EXT.1
Local Linux login	Session opened for <user-name>	FIA_UIA_EXT.1 FIA_UAU_EXT.2
Local Linux logout	Session closed for <user-name>	FIA_UIA_EXT.1 FIA_UAU_EXT.2
Remote Linux login	Accepted password for <user-name> from <origin-ip-addr> session opened	FIA_UIA_EXT.1 FTA_SSL.4 FTP_TRP.1

Remote Linux logout	Received disconnect from <origin-ip-addr> session closed for <user-name>	FIA_UIA_EXT.1 FTA_SSL.4 FTP_TRP.1
TLS certificate verification	Cert verification error <reason>	FIA_X509.EXT.1
Attempt to update firmware	Performing action from <origin-ip-addr> upgrade server <efp-name>	FMT_MOF.1(1) / Trusted Update
Enter secure mode	Enabling high security mode from local terminal	FMT_MTD.1
Edit login banner	Editing login banner from <origin-ip-addr>	FMT_MTD.1
Change Linux user password	Performing action from <origin-ip-addr> change linux password <user-name>	FMT_MTD.1
Expire web all user passwords	Performing action from <origin-ip-addr> expire all web passwords	FMT_MTD.1
Web user changing own password	Modified user <user-name> from <origin-ip-addr>	FMT_MTD.1
Create web user	Created user <user-name> from <origin-ip-addr>	FMT_MTD.1
Delete web user	Deleted user <user-name> from <origin-ip-addr>	FMT_MTD.1
Import signed certificate (CSR response)	Import signed server certificate	FMT_MTD.1
Import trusted CA certificate	Import trusted CA certificate <cert-file-name>	FMT_MTD.1
Remove trusted CA certificate	Remove trusted CA certificate <cert-file-name>	FMT_MTD.1
Import CRL file	Import CRL <crl-file-name> issued by <issuing-CA-cert-file-name>	FMT_MTD.1
Remove CRL file	Remove CRL <crl-file-name>	FMT_MTD.1
Configure allowed Subject Alt Names	Configure allowed <san-type> SAN settings	FMT_MTD.1
Configure device IP address	Performing action from <origin-ip-addr> save network settings <settings-info>	FMT_MTD.1
Result of attempt to update firmware	Success or <reason-for-failure>	FPT_TUD_EXT.1
Changing time / date / time zone	<old-timestamp> Performing action from <origin-ip-addr> change time <new-timestamp>	FPT_STM.1
Terminate remote interactive session after timeout (web)	Web user timed out <user-name> <token-info>	FTA_SSL.3
Terminate remote interactive session after timeout (Linux)	Received disconnect from <origin-ip-addr> session closed for <user-name>	FTA_SSL.3
TLS connection initiated	<connection-id> accepted connection from <origin-ip-addr> connected to <target-ip-addr>	FTP_ITC.1
TLS connection terminated	<connection-id> connection closed	FTP_ITC.1
TLS connection failed to establish	<connection-id> error <reason>	FTP_ITC.1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.1
Remote administrator session failed (web)	Failed to authenticate user <user-name> <origin-ip-addr>	FTP_TRP.1
Remote administrator session failed (Linux)	Failure <reason> session closed for <user-name>	FTP_TRP.1

Log rotated to prevent filling storage space	<log-file-name> <max-size> log rotating <rotated-log-file-name>	FAU_STG_EXT.3
Configure IP of remote audit server	Performing action from <origin-ip-addr> configure remote audit server <target-ip-addr>	FMT_MOF.1(1) / Audit
Import update verification public key	Performing action from <origin-ip-addr> import code verification public key <checksum-of-key>	FMT_MTD.1 / AdminAct
Reset disk encryption key	Performing action from <origin-ip-addr> reset disk encryption key <checksum-of-key>	FMT_MTD.1 / AdminAct
Reset TLS private key	Performing action from <origin-ip-addr> erase and create TLS key <checksum-of-key>	FMT_MTD.1 / AdminAct
Failure to establish HTTPS session (server side)	<connection-id> accepted connection from <origin-ip-addr> error <reason>	FCS_HTTPS_EXT.1

*In addition to <time-stamp> + <device-name> + <app-name>, which is common to all entries.

Table 14. TOE Auditable Events AND Data Fields

6.1.1.2 FAU_GEN.2 – User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_STG_EXT.1 – External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit generated audit data to an external IT entity using a trusted channel according to **FTP_ITC.1 – Inter-TSF Trusted Channel**.

Note: for the purpose of this ST, the external IT entity is an organizationally-provided syslog server.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself.

FAU_STG_EXT.1.3 The TSF shall drop new audit data when the local storage space for audit data is full.

6.1.2 Cryptographic Support (FCS)

6.1.2.1 FCS_CKM.1 – Cryptographic Key Generation (Refined)

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm:

- ***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***

6.1.2.2 FCS_CKM.2 – Cryptographic Key Establishment (Refined)

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** algorithm:

- ***RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establisment Schemes Using Integer Factorization Cryptography"***

  Note: Magnum supports the following ciphersuites, in order of preference:

  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_CBC_SHA

6.1.2.3 FCS_CKM.4 – Cryptographic Key Zeroization

FCS_CKM.4.1 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**, destruction of reference to the key directly followed by a request for garbage collection];
- 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-pass** overwrite consisting of **zeroes**,
  - instructs a part of the TSF to destroy the abstraction that represents the key

that meets the following: No Standard.

6.1.2.4 FCS_COP.1(1) – Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1(1) The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm

- AES-CBC (as defined in NIST SP 800-38A) mode; and

and cryptographic key sizes 256-bit and 128-bit.

6.1.2.5 FCS_COP.1(2) – Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1(2) The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) *2048* bits,

that meet the following:

- 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. FCS_COP.1(3) – Cryptographic Operation (Hash Algorithm)

6.1.2.6 FCS_COP.1(3) – Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1(3) The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ that meet the following: ISO/IEC 10118-3:2004.

6.1.2.7 FCS_COP.1(4) – Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1(4) The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm HMAC-SHA-1, HMAC-SHA-256 and cryptographic key sizes 256 bits and message digest size 256 bits, that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".

6.1.2.8 FCS_RGB_EXT.1 –Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_CRBG (AES).

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from *one* software-based noise source with a minimum of 256 bits of entropy at least equal to the greatest security strength, according ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions" of keys and hashes that it will generate.

6.1.3 Identification and Authorization (FIA)

6.1.3.1 FIA_PMG_EXT.1 – Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- *Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: "~", "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", """, "`", "+", "-", ",", ".", "/", "\", ":", ";", "<", "=", ">", "?", "[", "]", "_", "`", "{", "|", "}", [space].*
- *Minimum password length shall be settable by the Security Administrator, and support passwords of 15 characters or greater.*

6.1.3.2 FIA_UIA_EXT.1 – User Identification and Authorization

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authorization process:

- Display the warning banner in accordance with FTA_TAB.1;
- No other actions

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

6.1.3.3 FIA_UAU_EXT.2 – Extended: Password-Based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism to perform administrative user authentication.

6.1.3.4 FIA_UAU.7 – Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress at the local console.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MOF.1(1)/TrustedUpdate – Management of Security Functions Behavior

FMT_MOF.1.1(1)/TrustedUpdate The TSF shall restrict the ability to enable the functions *to perform manual update* to *Security Administrators*.

6.1.4.2 FMT_MTD.1 – Management of TSF Data (for General TSF Data)

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.

6.1.4.3 FMT_SMF.1 – Specification of Management Functions

FMT_SMF.1.1 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*
- *No other capabilities.*

6.1.4.4 FMT_SMR.2 – Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely;*

are satisfied.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_SKP_EXT.1 – Extended: Protection of TSF Data (for reading of all symmetric keys

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric key and private keys.

6.1.5.2 FPT_APW_EXT.1 – Extended: Protection of Security Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent reading of plaintext passwords.

6.1.5.3 FPT_TST_EXT.1 – TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF:

- *Kernel integrity check that compares the SHA512 checksum of the kernel against permanently stored hash values*
- *Firmware integrity check that compares the SHA512 checksum of every executable and library file against permanently stored hash values*
- *Security mode verification that compares the SHA512 checksum of security-policy configuration files against stored hash values*
- *Correct operation of cryptographic functions by explicitly invoking OpenSSL's FIPS self-test*
- *Presence of certificate and public key files.*

6.1.5.4 FPT_TUD_EXT.1 – Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide *Security Administrators* the ability to query the currently executing version of the TOE firmware/software and the most recently installed version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide *Security Administrators* the ability to manually initiate updates to TOE firmware/software and no other update mechanism.

FPT_TUD_EXT.1.3 The TSF shall provide a means to authenticate firmware/software updates to the TOE using a digital signature mechanism prior to installing those updates.

6.1.5.5 FPT_STM.1 – Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.6 TOE Access (FTA)

6.1.6.1 FTA_SSL_EXT.1 – TSF-Initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, terminate the session after a Security Administrator–specified time period of inactivity.

6.1.7 FTA_SSL.3 – TSF-Initiated Termination

FTA_SSL.3.1 **Refinement:** The TSF shall terminate a **remote** interactive session after *a Security Administrator –configurable time interval of session inactivity*.

6.1.7.1 FTA_SSL.4 – User-Initiated Termination

FTA_SSL.4.1 **Refinement:** The TSF shall allow **Administrator**-initiated termination of the **Administrator's** own interactive session.

6.1.7.2 FTA_TAB.1 – Default TOE Access Banners

FTA_TAB.1.1 **Refinement:** Before establishing **an administrative user** session the TSF shall display a **Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

6.1.8 Trusted Path/Channels (FTP)

6.1.8.1 FTP_ITC.1 – Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall be **capable of using** TLS to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities:**

- **Video Switches**
- **Other Magnum Servers**
- **Audit Server**

that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2 Refinement: The TSF shall permit **the TSF, or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- *Controlling video switches,*
- *Coordinating with other Magnum servers (primary/backup),*
- *Audit logging.*

6.1.8.2 FTP_TRP.1 – Trusted Path

FTP_TRP.1.1 The TSF shall be **capable of using**

- TLS,
- HTTPS

to provide a communication path between itself and **authorized remote administrators** that is logically distinct from other communications paths and provides assured identification of its end points and protection of the communicated data from *disclosure and provides detection of modification of the channel data*.

FTP_TRP.1.2 Refinement: The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 Refinement: The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

6.2 Optional Requirements (Annex A)

6.2.1.1 FMT_MOF.1.1/Admin Act – Management of Security Functions Behavior

The following optional requirements are added because they describe auditing functions performed by Magnum.

FMT_MOF.1.1(1)/AdminAct

The TSF shall restrict the ability to modify the behavior of the functions *TOE Security Functions to Security Administrators*.

FMT_MOF.1.1(2)/AdminAct

The TSF shall restrict the ability to enable, disable the functions services to Security Administrators.

6.2.1.2 FMT_MOF.1.1/LocSpace – Management of Security Functions Behavior

FMT_MOF.1.1/LocSpace

The TSF shall restrict the ability to ***determine the behavior of*** *the functions audit functionality when Local Audit Storage Space is full to Security Administrators.*

6.3 Selection-Based Requirements (Annex B)

Magnum performs TLS server-side tasks when communicating with video switches. When communicating via the web, HTTPS is required. Therefore, FCS_HTTPS and FCS_TLSS applies for these functions.

Magnum serves as the client for TLS-based syslog communication. Therefore, FCS_TLSC applies for this function.

When multiple Magnums are used (main and backup), the Main acts as a TLS server and the backup acts as a TLS client.

Magnum uses x.509 Certificates. Therefore, FIA_X509 applies for these functions.

6.3.1 Cryptographic Support (FCS)

6.3.1.1 FCS_HTTPS_EXT.1 – HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 The TSF shall establish the connection only if the peer presents a valid certificate during handshake.

6.3.1.2 FCS_TLSC_EXT.2 – TLS Client Protocol with authentication

FCS_TLSC_EXT.2.1 The TSF shall implement one or more of the following protocols: TLS1.2 (RFC 5246) supporting the following ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.2.3 The TSF shall only establish a trusted channel if the peer certificate is valid.

FCS_TLSC_EXT.2.4 The TSF shall present the Supported Elliptic Curves Extension in the Client Hello with the following NIST curves: none and no other curves.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

6.3.1.3 FCS_TLSS_EXT.1 – TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.1.1 The TSF shall implement one or more of the following protocols: TLS1.2 (RFC 5246) supporting the following ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1.

FCS_TLSS_EXT.1.3 The TSF shall generate key establishment parameters using RSA with key size 2048 bits and no other size and no other**.**

6.3.1.4 FIA_X509_EXT.1 – X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3.
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
    - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*
    - *Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

6.3.1.5 FIA_X509_EXT.2 – X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for TLS, HTTPS and no additional uses**.**

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall: not accept the certificate**.**

6.3.1.6 FIA_X509_EXT.3 – X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and Common Name, Organization, Organizational Unit, and Country**.**

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

7 TOE Security Assurance Requirements

The TOE meets the security assurance requirements of NDcPP v1.0. The following table is the summary of those requirements:

Assurance Class	**Assurance Components**
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – sample (ATE_IND.1)
Vulnerability assessment	Vulnerability survey (AVA_VAN.1)

Table 15. TOE Security Assurance Requirements

8 TOE Summary Specification (TSS)

8.1 Target Security Function (TSF) Overview

The table below summarizes the security functions provided by the TOE.

SECURITY FUNCTION	TOE SCOPE DESCRIPTION
Security Audit (FAU)	IPX generates audit logs that consist of various auditable events or actions. This includes logins, use of trusted channel/path and cryptographic operations. Each audit event contains an associated date/time stamp, a label for the type of event, a user ID (if applicable) and a description of the event. IPX stores audit logs internally. The internal logs are stored unencrypted, but they are only accessible (and then read-only) via the web browser, which can only be used by Administrators.. Logs information is also sent (using TLS 1.2) to an external Syslog server assuming one is connected and configured (the Syslog server is beyond the scope of the TOE). The IPX manual explains how to do this.
Cryptographic Support (FCS)	The cryptographic module protects the management interfaces (TLS/HTTPS). It uses the following cryptographic algorithms: AES128 & 256 (Symmetric Cipher), RSA with 2048 bit keys (Asymmetric Cipher), SHA256 (Hashed MAC), RSA with 2048 bit keys (Digital Signatures), X509 (Certificate Encoding) and DRBG-AES-256-CTR Mode (Random number generation). In addition SNMPv3 is used exclusively for alarms.
Identification and Authentication (FIA)	The only accounts that the IPX will establish are Security Administrator accounts; Users only control the IPX indirectly via Magnum. CO/Administrative users are identified and authenticated via user name and password prior to performing any operations. The IPX CO/Administrators user accounts module maintains Security Administrator credentials. Since the only role that accesses the IPX directly is that od Security Administrator there is no assignment of roles required. Passwords of 15 characters or more are supported.
I Security Management (FMT)	IPX 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. IPX ensures that only secure values are accepted for security attributes A Security Administrator can change passwords, and can add, edit and/or delete Security Administrator accounts. The (non-administrative) User has no direct access or control over IPX; a (non-administrative) User may only access an IPX card through Magnum.

SECURITY FUNCTION	TOE SCOPE DESCRIPTION
Protection of the TSF (FPT)	IPX prevents the unauthorized modification of TSF data. This protection includes self-tests to ensure the correct operation of cryptographic functions. Firmware upgrades (only performed by a Security Administrator) are impossible unless the new firmware first passes two separate authentication tests.The IPX relies on trusted channels to protect communications between itself and other trusted services, such as syslog. Communications between the IPX and a remote administrative user are protected via a trusted path.
TOE Access (FTA)	Security Administrators can configure a maximum allowable period of inactivity for a Security Administrator session. If there is no user interaction with the IPX for the specified amount of time, the session is terminated. The initial, default session timeout is 15 minutes. Magnum also provides for a login banner message to be displayed by the management interfaces to advise Security Administrators regarding the appropriate use of Magnum, and the penalty for its misuse.
Trusted Path/Channels (FTP)	Magnum only communicates with Administrative Users via Trusted Paths. For remote administration this is restricted to a GUI over HTTPS. Magnum only communicates with other devices via Trusted Channels (using TLS).

Table 16. TSF Overview

8.2 TSS Items Requiring Further Specification

8.2.1 Security Audit (FAU)

8.2.1.1 FAU_GEN.1 – Audit Data Generation

Audit records are created when an auditable event that belongs to a set of predefined events had occurred. The set of auditable events can be sub-categorized into functional events and access events.

In general, the following event categories trigger an audit record:

- Starting and stopping services
- Authentication attempts
- Initiating and terminating sessions and connections
- Modifying users
- Modifying keys and certificates
- Changing system configuration
- Changing network configuration
- Time Changes (including NPT server time discontinuities)

Audit records are stored plaintext in /var/log/ for each application, rotated at size thresholds into similarly named compressed files. Each entry contains a timestamp of when the event had occurred as well as a message body with description of the event. Log entries are sorted based on chronological order.

8.2.1.2 FAU_GEN.2 – User Identity Association

Each audit event is associated with the user/application that has triggered that event. This user/application is identified by the username used for login or by the application name. For access log events, IP address/hostname may also be included.

8.2.1.3 FAU_STG_EXT.1 – External Audit Trail Storage

Audit data is sent to external syslog server through secured TLS sessions. For this to happen, an external syslog server should be configured (IP address/TCP Port number). A trusted certificate chain that is used to sign syslog server's certificate must be also uploaded to Magnum.

Magnum stores all audit data locally on SSD in a non-executable partition, protected by Linux-based disk encryption.

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.

8.2.2 Cryptographic Support (FCS)

8.2.2.1 FCS_CKM.1 – Cryptographic Key Generation

The TOE supports 2048-bit RSA keys. Key generation is invoked from the platform by first securely wiping any existing key (according to FIPS requirements), then calling "openssl genrsa -out $key_path 2048" (with openssl in FIPS mode).

Magnum uses the following OpenSSL module:

- MAGNUM OpenSSL Cryptographic Module 1.16.0

RSA keys are only used for TLS.

8.2.2.2 FCS_CKM.2 – Cryptographic Key Establishment

The TOE acts as both sender and recipient for RSA-based key establishment schemes. The underlying platform provides key confirmation services.

In the case of a decryption error, the TOE response is dependent on the stage of the connection process. If the connection has not been established, the TOE prevents a connection from occurring. If the connection has already been established, the TOE drops the packet(s) in question and logs the error internally.

To address the issue of side-channel attacks, the TOE does not reveal the particular error that occurred through other channels, either through message content or timing variations.

8.2.2.3 FCS_CKM.4 – Cryptographic Key Destruction

Magnum overwrites keys with random data followed by overwriting the contents with zeros. After each write operation, Magnum reads the data to confirm that is indeed what was written verifies that what was written (as opposed to a cached or older version of the data). If this test fails the process is repeated until it succeeds.

Keys are always stored on an encrypted disk partition, so they are never in plaintext. The "zeros" used for overwriting are logical zeros, so the content on the physical disk is still encrypted. 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:

- The private RSA key matching the server certificate, which is used for HTTPS web interface, and IPX and remote audit server connection;

This cryptographic key is stored in plaintext in a disk partition that no user has access to. No direct interface/access is provided to view or modify the contents of these files.

8.2.2.4 FCS_COP.1(1) – Cryptographic Operation(AES Data Encryption/Decryption)

The secure version of the Magnum application software forming this TOE is not configurable WRT cryptographic operation. In other words, the system defaults to the selected cryptographic modes and is not alterable when the system is placed into High Security mode.

8.2.2.5 FCS_COP.1(2) – Cryptographic Operation (Signature Generation and Verification)

The TOE implements hashing in byte-oriented mode. HMACs are used for verification of the firmware image and encrypted password files during bootup. The Linux and Web passwords are saved in a partition of the NOR flash memory separate from the firmware image and all executable files. The TOE uses hashing for the following security functions:

- TLS connection establishment
- Verifying executable file checksums
- Linux Passwords
- Web Passwords

8.2.2.6 FCS_COP.1(3) – Cryptographic Operation (Hash Algorithm)

Cryptographic hashing services are performed using Evertz's cryptographic module. Hashing is used for firmware integrity checks, password verification and security mode verification.

8.2.2.7 FCS_COP.1(4) – Cryptographic Operation (Keyed-Hash Algorithm)

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 - 512 bits
- Hash function used: SHA-1
- Block size: 512 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

8.2.2.8 FCS_RBG_EXT.1 – Random Bit Generation

As determined in *Evertz Microsystems Magnum Entropy Assessment Report*, 10 JAN 2017, the Linux kernel on which the IPX application is built uses */dev/random* as the entropy source for all random numbers. The functions which obtain random numbers from the RBG are:

- Haveged
- Linux Kernel Entropy

Please see the *Evertz Microsystems Entropy Assessment Report* for IPX for further information, such as seeding parameters.

8.2.2.9 FCS_TLSC_EXT.2 – Explicit: TLS (Client)

Magnum TLS client-side is used to export audit records, and to connect to one or more video switches. Mutual authentication is used when connecting to video switches over port 9672. Its operation is identical to the server-side (see below).

8.2.2.10 FCS_TLSS_EXT.1 – Explicit: TLS (Server)

Magnum specifies only a restricted set of cipher suites that it supports during the negotiation phase with its peer. If no match of cipher suites can be found with peer, TLS session will not be started. Protocols that do not conform to TLS1.2 are explicitly excluded in Magnum's ciphersuites

Magnum only supports cipher suites that use RSA keys for key exchange and authentication. These keys are generated by the OpenSSL implementation internally with OpenSSL's RSA command line utility. The four ciphersuites used by Magnum are:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256

Magnum uses CRL (certification revocation list) to check for invalid certificates. CRL files which are signed by trusted CA certificated can be imported to Magnum. This CRL file will be used by Magnum during certificate validation process to check for revocation status of the peer certificates.

Magnum allows configuration of reference identifier from peer it expects to connect with before connection is made. The verification against DN/SAN peer certificate is implemented within OpenSSL.

For browser-based management, MAGNUM must respond to the request presented by the user/operator browser. Administrators do not have the ability to modify the available ciphersuites, as these are hard-coded at the application layer. The MAGNUM SDVN Security Manual describes configuration procedures for the allowed SANs. When establishing a TLS connection, the MAGNUM client establishes the following reference identifiers:

- Domain Name Service (DNS)
- IP Address
- Email address

If there is no SAN field provided, or if there is a mismatch, 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.

8.2.2.11 FCS_HTTPS_EXT.1 – Explicit: HTTPS

HTTPS is basically HTTP running on top of TLS sessions. HTTPS uses TLS to securely establish the encrypted session.

Magnum functions as an HTTPS server only. HTTPS is used implementation to provide a secure interactive webpage interface for remote administrative functions, and to support secure exchange of user authentication parameters during login. The internal application is "stunnel."

Certificates (Magnum's own certificate or a trusted CA certificate) can be uploaded onto Magnum prior to establishing connection with peers. These certificates are used in the TLS handshaking process and is taken care of by TLS protocol implementation.

8.2.3 Identification and Authorization (FIA)

8.2.3.1 FIA_PMG_EXT.1 – Password Management

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).

Valid passwords are stored as hashed values in a PostgreSQL database.

8.2.3.2 FIA_UIA_EXT.1 – User identification and Authentication

Warning banner is displayed before login prompt becomes ready to accept login credentials from user. Users must acknowledge the warning banner before they can login to the system. This applies to direct console users as well as web users.

Authentication is based on username/password. Prior to successful login, no interface is exposed to allow unauthorized access.

8.2.3.3 FIA_UAU_EXT.2– Password-Based Authentication Mechanism

Console users rely on the PAM module provided by Linux. Web user passwords are stored (hashed) and verified in a PostgreSQL database.

8.2.3.4 FIA_UAU.7 – Protected Authentication Feedback

Console authentication displays no characters while the user enters a password. Web authentication shows only asterisks ("*").

8.2.3.5 FIA_X509_EXT.1 – X.509 Certificate Validation

MAGNUM uses CRLs to validate certificates. Certificates are validated during the connection handshake. MAGNUM first checks Certificate Authorities (CAs), then CRLs, then SANs. This validation includes revocation checking.

MAGNUM only supports certificates that have been loaded by an authorized system administrator within the local Evertz network environment. As a purpose-built ecosystem, MAGNUM will not operate non-Evertz hardware. Administrators should ensure that the CRL reflects the certificates loaded onto the IPX or other Evertz hardware which the system is intended to manage.

For an expired certificate, Magnum will deny the connection. Magnum also uses CRL to verify whether the certificate or intermediate CA certificate has been revoked. During session establishment with Magnum, any byte modification in the certificate will lead to the failure of connection.

8.2.3.6 FIA_X509_EXT.2 – X.509 Certificate Authentication

Instructions for configuring MAGNUM to operate with X.509 certificates are found in the MAGNUM SDVN Security Manual.

MAGNUM only has one certificate to present. If the certificate fails a validity check, the connection attempt fails and the trusted channel is not established.

The following trusted channels are supported:

- MAGNUM-SC-CC to another MAGNUM-SC-CC
- MAGNUM-SC-CC to an Evertz video switch compatible with Common Criteria (suffix "-CC" in Equipment ID). As of this writing these include:
  - MMA10G-IPX-16-CC
  - MMA10G-IPX-32-CC
  - MMA10G-IPX-64-CC

MAGNUM may also control 3rd-party devices as long as such devices support TLS v1.2. In such cases, MAGNUM can support a trusted channel to such devices. The configuration and deployment of 3rd-party devices lies outside the scope of the TOE and this ST.

8.2.3.7 FIA_X509_EXT.3 – X.509 Certificate Requests

Magnum uses its openssl based cryptographic module to generate a Certificate Request Message. This requires the specification of the public key, Common Name, Organization, Organizational Unit, and Country. This information is configurable via the console admin interface. Magnum uses the following key usage and extended key usage parameters:

- keyUsage = critical,nonRepudiation,digitalSignature,keyEncipherment
- ExtendedKeyUsage = clientAuth,serverAuth

Magnum uses its openssl based cryptographic module to verify certificates when the TOE is configured in a security mode to verify certificates by a Certificate Authority (CA). Magnum requires all certificates in the chain to be presented by the peer during connection attempts.

8.2.4 Security Management (FMT)

8.2.4.1 FMT_MOF.1(1) / Trusted Update – Management of Security Functions Behavior

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. So, non-privileged users are not able to update the system files.

8.2.4.2 FMT_MTD.1 – Management of TSF Data

Magnum is managed by the console admin interface or through the web interface. The TOE is configured with user accounts that restrict access to users that are not administrators. Any management function that is performed in console admin interface requires the administrator to enter the appropriate administrator password. Command line access is restricted such that regular users do not have access to command line scripts used to manage Magnum. The web interface is also controlled by access permissions and so only users given access to manage Magnum can do so. No administrative functionality is available through either interface prior to login.

8.2.4.3 FMT_SMF.1 – Specification of Management Functions

The *MAGNUM-SDVN Security Administration Manual* describes the management functions required by this PP. The following management capabilities are described in the manual:

- System Setup
  - Entering High Security Mode
  - Disabling USB Storage on the BIOS
  - Changing Connection in Security Mode
  - Bypass Options (Not Recommended)
  - Full Data Purge

- Administrator Log In/Out of:
  - Local Terminal
  - Remote Terminal
  - Web Interface

- Configuration:
  - Date & Time
  - IP Addresses
  - Clustering
  - Remote Audit Servers
  - Session Timeout

- Transferring FIles
  - Using FTPS
  - Using SFTP
  - Using SCP

- Editing the Login Banner

- Keys
  - Importing a Public Key
  - Disk Encryption Key Reset
  - TLS Key Reset
  - Cluster Key Import / Export / Reset

- Certificates
  - Create Certificate Signing REquest
  - Import / Export / Show Server Certificates
  - Import / Export / Show Truseted Certificates
  - Import / SHow / Remove Certificate Revocation List

- Allowed Subject Alt Names
  - DNS
  - Ip
  - E-Mail

- Administer Passwords
  - Set Password Minimum Length
  - Linux User
  - Web User
    - Add / Delete
    - Change Web Users' Passwords

- Audits
  - Export Logs

- Firmware
  - Check Firmware Version
    - From Terminal
    - From Web
  - Upgrade

8.2.4.4 FMT_SMR.2 – Restrictions on Security Roles

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. The web administrator can also administer Magnum over HTTPS.

8.3 Protection of the TSF (FPT)

8.3.1.1 FPT_SKP_EXT.1– Protection of TSF Data (for Reading of All Symmetric Keys)

Magnum uses three mechanisms to protect private keys from being read:

- Full disk encryption (LUKS)
- Linux file permissions to only allow the appropriate services programmatic access
- None of these service have methods to expose the key beyond their immediate use.

8.3.1.2 FPT_APW_EXT.1 – Protection of Administrator Passwords

The salted SHA512 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 as a salted Blowfish hash. Both the password file and the database reside on the filesystem, which is encrypted by LUKS disk encryption.

All password prompts either obscure the typed password so that it cannot be seen or refrain from echoing the typed password. Magnum does not store any passwords in plaintext format. Magnum also uses Linux permissions to prevent accessing the obscured forms of the passwords.

8.3.1.3 FPT_TST_EXT.1 – TSF Testing

The firmware is validated in the following three ways on startup:

- Magnum verifies SHA512 checksums of the bootloader components (kernel and initrd images)
- Magnum invokes the openssl to display its version, which will trigger the built-in self-tests. This ensures that the crypto module has not been tampered with.
- Magnum verifies SHA512 chesksums of all non-configuration files, including executable and shared object files.

These tests verify that TOE firmware has not been modified and all cryptographic functions are working correctly.

8.3.1.4 FPT_TUD_EXT.1 – Trusted Update

If the TOE has been implemented in accordance with this ST, then site administrators will not have access to an external network. 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 procedures described in the MAGNUM-SDVN Security Administration Manual in the Checking Version section.

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 the MAGNUM SDVN Security Administration Manual in the Transferring Files in High Security Mode section. In the event that an update file fails verification the update is rejected and an appropriate audit record is generated.

As an embedded application on an embedded OS, the application does not have the ability to be uninstalled completely. in accordance with the guidance in MAGNUM SDVN Security Administration Manual under the heading “Full Data Purge,” sites requiring a full data purge should shred the physical disk and request a new disk from Evertz if desired.

Binaries are not changed except by update. Checksums of all files are verified on boot, ensuring that no executables have been modified.

Administrative users (terminal and web) have the option to view current versions. Instructions for doing so are found in the MAGNUM-SDVN Security Administration Manual in the Checking Version section.

8.3.1.5 FPT_STM.1 – Reliable Time Stamps

Magnum can provide accurate timestamps via manual configuration by the administrator or by synchronizing with a NTP server. The NTP messages are authenticated using symmetric keys with SHA1 encoding. 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.

8.4 TOE Access (FTA)

8.4.1.1 FTA_SSL_EXT.1– TSF-Initiated Session Locking

Magnum has a configurable timeout that can be modified using 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 both console and web interactive sessions.

8.4.1.2 FTA_SSL.3 – TSF-Initiated Termination

Magnum has a configurable timeout that can be modified using 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 both console and web interactive sessions.

8.4.1.3 FTA_SSL.4 – User-Initiated Termination

On a terminal, select "Logout" from the console admin interface. From a web interface first select the "User" icon, then select "Logout."

8.4.1.4 FTA_TAB.1 – Default TOE Access Banner

Magnum is managed by the local console admin interface or through the HTTPS web interface.

From the console admin interface, under the Security menu, select “Edit Login Banner”. When modifications are complete, press Ctrl+X to save and exit the editor.

8.5 Trusted Path/Channels (FTP)

8.5.1.1 FTP_ITC.1– Inter-TSF Trusted Channel

A trusted channel using TLS is created when certificates are imported into Magnum and the device. Thus, when using the stunnel program to communicate with other services, the trusted certificate verifies the validity of the communication via mutual X.509 certificates.

8.5.1.2 FTP_TRP.1 – Trusted Path

Magnum only communicates with Administrative Users via Trusted Paths. For remote administration this is restricted to a GUI over HTTPS.

Magnum uses encryption and restricts the choices of ciphers, hashes, and key-exchange algorithms to those allowed by the NDcPP.

Appendix A. Glossary of Terms

TERM	DEFINITION
10G	10 Gigabit
AES	Advanced Encryption Standard
API	Application Programming Interface
ASLR	Address Spece Layout Randomization
AV	Audio-Video, Audiovisual
CA	Certificate Authority
CBC	Cipher Block Chain
CC	Common Criteria
CMC	CBC-mask-CBC
CO	Cryptography Officer
CRL	Certificate Revocation List
CTR	Counter (mode)
CWDM	Coarse Wave Division Multiplexing
DEP	Data Executable Prevention
DFB	Distributed Feedback
DHE	Diffie-Hellman Exchange
DN	Distinguished Name
DNS	Domain Name Service
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
DVI	Digital Video Interface
DWDM	Dense Wave Division Multiplexing
ECDHE	Elliptic Curve Diffie-Hellman Exchange
ECDSA	Elliptic Curve Digital Signature Algorithm
EMX	Evertz Modular Crosspoint
FIPS	Federal Information Processing Systems
FTPS	File Transfer Protocol Secure
Gb	Gigabit
GCM	Galois/Counter Mode
HDMI	High Density Multimedia Interface
HID	Human Interface Device
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input / Output
IAW	In Accordance With
IP	Internet Protocol
IPTV	IP Television
IPX	Internet Protocol Crosspoint
IT	Information Technology
km	Kilometer(s)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
max	Maximum
NDcPP	Network Device collaborative Protection Profile
NIST	National Institute of Standards and Technology
NLE	Non Linear Editor, Non Linear Editing

nm	Nanometer(s)
NMS	Network Management System
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OID	Object Identifier
OOBM	Out of Band Management
OS	Operating System
PP	Protection Profile
PPAS	Protection Profile for Application Security
PPS	Ports. Protocols, and Services
RA	Registration Authority
RBAC	Role Based Access Control
RFC	Request For Comment
RJ-45	Radio Jack (45)
RS-232	Recommended Standard 232
RSA	Rivest-Shamir-Adelman
RU	Rack Unit (1.75”)
S/MIME	Secure Multipurpose Internet Mail Extensions
SAN	Subject Alternative Name
SDI	Serial Digital Interface
SDVN	Software Defined Video Networking
SFP	Small Form-Factor Pluggable
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
ST	Security Target
T:	TCP / Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	Target Security Function
U:	UDP / User Datagram Protocol
USB	Universal Serial Bus
VGA	Video Graphics Array
VLAN	Virtual Local Area Network
WRT	With Respect To