MMA10G-IPX Series v3.5 Security Target

Document Version: 1.1

2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

Version	Date	Changes
Version 0.1	Aug 05, 2024	Initial Release
Version 0.2	Aug 26, 2024	Updates as per GA responses
Version 0.3	Oct 07, 2024	QA review
Version 0.4	October 14,2024	Updates as per the QA review
Version 0.5	November 25, 2024	Finalize ST for Check-in
Version 0.6	January 13, 2025	Updates based on ECR comments for Check-in
Version 0.7	March 04, 2025	Updates based on review comments
Version 0.8	April 23, 2025	Finalize ST for Check-out
Version 0.9	May 09,2025	Final ST for Checkout
Version 1.0	June 09,2025	Address ECR comments
Version 1.1	June 19,2025	Address ECR comments

Contents

1 Introduction

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

1.1 Security Target and TOE Reference

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

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	MMA10G-IPX Series v3.5 Security Target
ST Version	1.1
ST Date	June 19, 2025
ST Author	Acumen Security, LLC.
TOE Identifier	MMA10G-IPX Series
TOE Version	v3.5
TOE Developer	Evertz Microsystems Ltd. 5292 John Lucas Drive Burlington, Ontario CANADA
Key Words	Network Device

1.2 TOE Overview

The TOE (Internet Protocol Crosspoint (IPX) switch) is a network-based audio video distribution system and is classified as a network device (a generic infrastructure device that can be connected to a network). It is a 10 Gigabit (Gb) Internet Protocol (IP) switch optimized for video-over-IP traffic (compressed or uncompressed). For the MMA10G and 3080 models, each IPX card occupies two (2) slots (16- and 32-port IPX cards) or four (4) slots (64-port IPX cards) in an Evertz Modular Crosspoint (EMX) frame. The 9080 models include the IPX cards and frame in a 1RU form factor. All IPX-compatible cards may be inserted into any IPX frame configuration provided there are sufficient contiguous free slots available.

Since video by nature has a unidirectional flow, and multiple copies of a single incoming video stream are often sent to multiple output destinations, the IPX exclusively uses multicast IP addressing. 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.

The TOE provides secure remote management using an HTTPS/TLS web interface. Administrators only may access IPX via a dedicated management workstation operating over an Out-of-Band Management (OOBM) network. Sites may close this OOBM network or may operate IPX within an existing OOBM, as long as the topology is compliant with the security parameters listed below. Users and administrators may also access IPX software via direct connection using a terminal session.

The TOE generates audit logs and transmits the audit logs to a remote syslog server over a TLS channel. The TOE verifies the authenticity of software updates by verifying the digital signature prior to installing any update.

The summary of the evaluated functionality provided by the TOE includes the following:

- Secure connectivity with remote audit servers and secure retention of audit logs locally.
- Identification and authentication of the administrator of the TOE.
- Secure remote administration of the TOE via TLS and secure Local administration of the TOE.
- Secure access to the management functionality of the TOE.
- Secure software updates.
- Secure communication with the non-TOE 'video switch control systems' via TLS.

The TOE hardware devices are the Evertz:

- MMA10G-IPX-16-CC running MMA10G-IPX-16-CC v3.5,
- MMA10G-IPX-32-CC running MMA10G-IPX-32-CC v3.5,
- MMA10G-IPX-64-CC running MMA10G-IPX-64-CC v3.5,
- 3080IPX-16-G3-CC running MMA10G-IPX-16-CC v3.5,
- 3080IPX-32-G3-CC running MMA10G-IPX-32-CC v3.5,
- 3080IPX-64-G6-CC running MMA10G-IPX-64-CC v3.5,
- 3080IPX-16-10G-CC running MMA10G-IPX-16-CC v3.5,
- 3080IPX-32-10G-CC running MMA10G-IPX-32-CC v3.5,
- 3080IPX-64-10G-CC running MMA10G-IPX-64-CC v3.5,
- 3080IPX-16-10G-HW-CC running MMA10G-IPX-16-CC v3.5,
- 3080IPX-32-10G-HW-CC running MMA10G-IPX-32-CC v3.5,
- 3080IPX-64-10G-HW-CC running MMA10G-IPX-64-CC v3.5,
- 3080IPX-16GE-CC running MMA10G-IPX-16-CC v3.5,
- 3080IPX-32GE-CC running MMA10G-IPX-32-CC v3.5,
- 3080IPX-64GE-CC running MMA10G-IPX-64-CC v3.5,
- 3080IPX-16GE-RJ45-CC running MMA10G-IPX-16-CC v3.5,
- 3080IPX-32GE-RJ45-CC running MMA10G-IPX-32-CC v3.5,
- 3080IPX-64GE-RJ45-CC running MMA10G-IPX-64-CC v3.5,
- 9080IPX-16-12RJ45-4SFP10GE-CC running MMA10G-IPX-16-CC v3.5,
- 9080IPX-16GE-12RJ45-4SFP-CC running MMA10G-IPX-16-CC v3.5,
- 9080IPX-32-28RJ45-4SFP10GE-CC running MMA10G-IPX-32-CC v3.5,
- 9080IPX-32-28RJ45-4SFP-CC running MMA10G-IPX-32-CC v3.5

and will be referred to as "IPX" throughout this document. The IPX appliances are Ethernet switches optimized for video content.

NOTE: All the devices listed above run on the same Freescale MPC8377E PowerQUICC II processor and use the same microarchitecture.

1.3 TOE Description

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

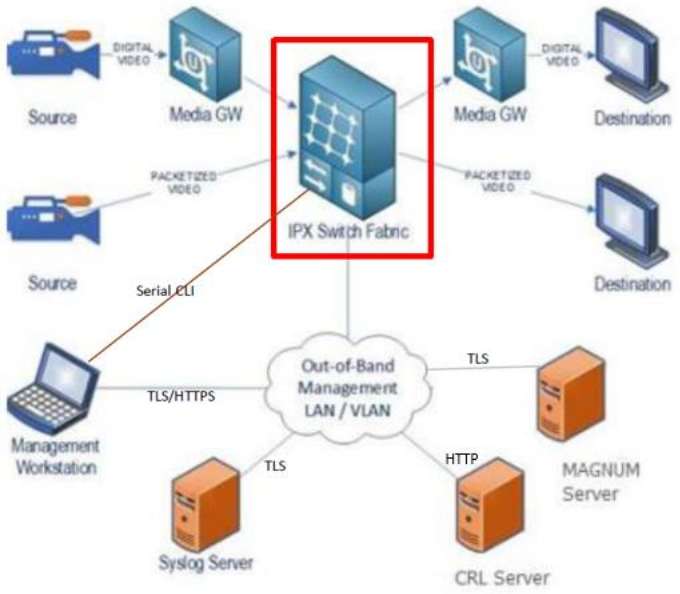

Figure 1 – Representative TOE Deployment

1.3.1 TOE Physical Boundaries

The physical boundaries of the TOE are outlined in section 1.2 and Table 2. The media and video components of the IT environment are NOT part of the TOE physical boundary. The TOE is shipped to the customer via commercial courier.

Table 2 – TOE Physical Boundary Components

Model	Software	AV/Broadcast	Supported Ports	Form Factor	Chassis Supported	Frame Controller	Processor
MMA10G-IPX-16-CC	MMA10G-IPX-16-CC v3.5	AV	16 SFP ports	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
MMA10G-IPX-32-CC	MMA10G-IPX-32-CC v3.5	AV	32 SFP ports	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
MMA10G-IPX-64-CC	MMA10G-IPX-64-CC v3.5	AV	64 SFP ports	modular	EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E

Model	Software	AV/Broadcast	Supported Ports	Form Factor	Chassis Supported	Frame Controller	Processor
3080IPX-16-G3-CC	MMA10G-IPX-16-CC v3.5	Broadcast	16 SFP ports (GbE or 10GbE)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-32-G3-CC	MMA10G-IPX-32-CC v3.5	Broadcast	32 SFP ports (GbE or 10GbE)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-64-G6-CC	MMA10G-IPX-64-CC v3.5	Broadcast	64 SFP ports (GbE or 10GbE)	modular	EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-16-10G-CC	MMA10G-IPX-16-CC v3.5	Broadcast	16 SFP ports (GbE or 10GbE)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-32-10G-CC	MMA10G-IPX-32-CC v3.5	Broadcast	32 SFP ports (GbE or 10GbE)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-64-10G-CC	MMA10G-IPX-64-CC v3.5	Broadcast	64 SFP ports (GbE or 10GbE)	modular	EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-16-10G-HW-CC	MMA10G-IPX-16-CC v3.5	Broadcast	16 SFP ports (GbE or 10GbE)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-32-10G-HW-CC	MMA10G-IPX-32-CC v3.5	Broadcast	32 SFP ports (GbE or 10GbE)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-64-10G-HW-CC	MMA10G-IPX-64-CC v3.5	Broadcast	64 SFP ports (GbE or 10GbE)	modular	EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-16GE-CC	MMA10G-IPX-16-CC v3.5	Broadcast	16 GbE ports (GbE only)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-32GE-CC	MMA10G-IPX-32-CC v3.5	Broadcast	32 GbE ports (GbE only)	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-64GE-CC	MMA10G-IPX-64-CC v3.5	Broadcast	64 GbE ports (GbE only)	modular	EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E

Model	Software	AV/Broadcast	Supported Ports	Form Factor	Chassis Supported	Frame Controller	Processor
3080IPX-16GE-RJ45-CC	MMA10G-IPX-16-CC v3.5	Broadcast	16 RJ45 GbE ports	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-32GE-RJ45-CC	MMA10G-IPX-32-CC v3.5	Broadcast	32 RJ45 GbE ports	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
3080IPX-64GE-RJ45-CC	MMA10G-IPX-64-CC v3.5	Broadcast	64 RJ45 GbE ports	modular	EMX1-FR EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E
9080IPX-16-12RJ45-4SFP10GE-CC	MMA10G-IPX-16-CC v3.5	Broadcast	12 RJ45 GbE ports 4 SFP ports (GbE or 10GbE)	1RU	N/A	None	PowerQUICC® II Pro MPC8377E
9080IPX-16GE-12RJ45-4SFP-CC	MMA10G-IPX-16-CC v3.5	Broadcast	12 RJ45 GbE ports 4 SFP ports (GbE or 10GbE)	1RU	N/A	None	PowerQUICC® II Pro MPC8377E
9080IPX-32-28RJ45-4SFP10GE-CC	MMA10G-IPX-32-CC v3.5	Broadcast	28 RJ45 GbEports 4 SFP ports (10GbE)	1RU	N/A	None	PowerQUICC® II Pro MPC8377E
9080IPX-32-28RJ45-4SFP-CC	MMA10G-IPX-32-CC v3.5	Broadcast	28 RJ45 GbE ports 4 SFP ports (GbE or 10GbE)	1RU	N/A	None	PowerQUICC® II Pro MPC8377E

The Required Environmental Components used to test the TOE are shown in Table 3 below:

Table 3- Required Environmental Components

Component	Required	Purpose/Description
Syslog Server	Yes	• Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting at least one of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management Workstation with web browser	Yes	• Google Chrome 50, or Firefox 38 • Supporting TLSv1.2 • Supporting Client Certificate authentication • Supporting Server Certificate authentication

Component	Required	Purpose/Description
		• Supporting at least one of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Local Management Workstation	Yes	Computer with terminal emulation software to access the console interface (CLI)
CRL Server	Yes	• Conformant with RFC 5280 • Provides a list of revoked certificates. • TOE uses the CRL server to check the revocation status of a server's presented certificate. • Communication between the TOE and the CRL server occurs over HTTP.
MAGNUM Client	Yes	• Provides remote management of the TOE's routing and switching of video signals • Supporting Mutual Authentication • Supporting TLSv1.2 with all of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Media Gateway	No	• Optional component for converting media streams. Not required for TOE operation.
Video Source devices	No	• Optional component for creating video streams that are sent to the TOE. Not required for TOE operation. • Supporting packetized or digital video
Video Destination devices	No	• Optional component for viewing video streams output by the TOE. Not required for TOE operation. • Supporting packetized or digital video

1.3.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v3.0e or NDcPP.

1.3.2.1 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:

- Startup and shutdown of the audit function
- Administrative login and logout events

- Changes to TSF data related to configuration changes
- Generation of a CSR and associated keypair
- Installation of a certificate
- Resetting passwords
- Failure to establish a HTTPS/TLS session
- Failure to establish a TLS session
- All use of the identification and authentication mechanism (local and remote connections to the TSF)
- Unsuccessful attempts to validate a certificate
- Initiation of a software update
- Result of a software update
- Changes to the time
- Modification of the behavior of the TSF
- Failure of self-tests
- Initiation and termination of the trusted channel
- Initiation and termination of the trusted path
- Attempts to unlock an interactive session
- Termination of a session by the session locking mechanism

The TOE stores generated audit data on itself and sends audit 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 TSF provides the capability to view audit data by using the Syslog tab in the web browser and local console. The log records the date and time, type, subject identity (IP address, hostname, and/or username), the outcome (success or failure), facility, application, and “message” (the log details). The previous audit records are overwritten when the allocated space for these records reaches the threshold on a FIFO basis.

1.3.2.2 Cryptographic Support

The TOE includes an OpenSSL library (Version 3.0.14 with Linux 4.19) that implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. The cryptographic implementation for IPX relies on the IPX Cryptographic Module version 3.5. These algorithms are used to provide security for the TLS/HTTPs connections for secure management and secure connections to a syslog and authentication servers. TLS and HTTPs are also used to verify firmware updates.

Table 4 – TOE Cryptographic Protocols

Cryptographic Protocol	Use within the TOE

HTTPS/TLS (client)	Secure connection to syslog FCS_HTTPS_EXT.1, FCS_TLSC_EXT.1
HTTPS/TLS (server)	Peer connections to MAGNUM and remote management FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2
AES	Provides encryption/decryption in support of the TLS protocol. FCS_COP.1.1/DataEncryption, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2
DRBG	Deterministic random bit generation use to generate keys. FCS_TLSS_EXT.1, FCS_TLSS_EXT.2, FCS_RBG_EXT.1
Secure hash	Used as part of digital signatures and firmware integrity checks. FCS_COP.1/Hash, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2
HMAC	Provides keyed hashing services in support of TLS. FCS_COP.1/KeyedHash, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2
EC-DH	Provides key generation and key establishment for TLS. FCS_CKM.1, FCS_CKM.2, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2
RSA	Provide key establishment, key generation and signature generation and verification (PKCS1_V1.5) in support of TLS. FCS_CKM.1, FCS_CKM.2, FCS_COP.1/SigGen, FCS_COP.1/SigVer, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards (refer to Table 16).

1.3.2.3 Identification and Authentication

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. (“Regular” IPX users do not access IPX directly; they control IP video switching through the IPX using a switch control system, such as Evertz’ Magnum. The switching of those IP video transport stream is outside the scope of the TOE.)

Once an Administrator attempts to access the management functionality of the TOE, the TOE prompts the Administrator for a username 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.

Remote administrators are locked out after a configurable number of unsuccessful authentication attempts.

The IPX requires a password-protected serial connection to perform initial configuration of the system IP address(es). Once each address is established, administrators use IP connectivity for all further administrative actions, including configuration, operations, and monitoring.

1.3.2.4 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 remotely
- Configure the access banner
- Configure the remote session inactivity time before session termination
- Update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Modify the behaviour of the transmission of audit data to an external IT entity
- Manage the cryptographic keys
- Re-enable an Administrator account
- Set the time which is used for time-stamps
- Manage the TOE's trust store and designate X509.v3 certificates as trust anchors
- Generate Certificate Signing Request (CSR) and process CA certificate response
- Configure the authentication failure parameters for FIA_AFL.1
- Administer the TOE locally
- Configure the local session inactivity time before session termination or locking

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. In IPX, only the admin role exists, since there is no provision for "regular" users to access IPX directly (as described above), and the portion of IPX they access and control are outside the scope of the TOE.

Primary management is done using the Webeasy web-based interface using 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 are managed from the web browser, which uses a menu-driven navigation system.

There is also a very simple serial-based connection (RS-232) that provides a simple menu interface. This is used to configure the IP interface (IP address, etc.). It is password-protected, and is typically only used once, for initial set-up.

1.3.2.5 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 are used as the time stamp that is applied to TOE generated audit records. 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. IPX automatically uses the digital signature mechanism to confirm the integrity of the product before installing the update.

1.3.2.6 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.

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

1.3.2.7 Trusted Path/Channels

The TOE allows the establishment of a trusted path between a video control system (such as Evertz' Magnum) and the IPX. The TOE also establishes a secure connection for sending audit data to a syslog server using TLS and other external authentication stores using TLS-protected communications.
The TOE uses HTTPS/TLS to provide a trusted path between itself and remote administrative users. The TOE does not implement any additional methods of remote administration. The remote administrative users are responsible for initiating the trusted path when they wish to communicate with the TOE.

1.3.3 TOE Documentation

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

- MMA10G-IPX Series v3.5 Security Target 1.1, June 19, 2025 [ST]
- IPX MMA10G-IPX v3.5 Supplemental Administrative Guidance for Common Criteria, version 1.1, June 19, 2025 [AGD]

1.3.4 References

In addition to the TOE documentation, the following references are applied within this ST:

- Collaborative Protection Profile for Network Devices, Version 3.0e [CPP_ND_V3.0E]

1.4 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 5 – Required Environmental Components

Components	Description

Syslog server	• Conformant with RFC 5424 (Syslog Protocol)
	• Supporting Syslog over TLS (RFC 5425)
	• Acting as a TLSv1.2 server
	• Supporting Client Certificate authentication
	• Supporting all of the following ciphersuites:
	  ○ TLS_RSA_WITH_AES_128_CBC_SHA
	  ○ TLS_RSA_WITH_AES_256_CBC_SHA
	  ○ TLS_RSA_WITH_AES_128_CBC_SHA256
	  ○ TLS_RSA_WITH_AES_256_CBC_SHA256
	  ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	  ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Components	Description
Management Workstation with web browser	• Google Chrome 50, or Firefox 38 • Supporting TLSv1.2 • Supporting Client Certificate authentication • Supporting all of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Local Management Workstation	• Computer with terminal emulation software to access the console interface (CLI)
CRL Server	• Conformant with RFC 5280 • Provides a list of revoked certificates. • TOE uses the CRL server to check the revocation status of a server's presented certificate. • Communication between the TOE and the CRL server occurs over HTTP.
MAGNUM Client	• Provides remote management of the TOE's routing and switching of video signals • Supporting Mutual Authentication • Supporting TLSv1.2 with all of the following ciphersuites: ○ TLS_RSA_WITH_AES_128_CBC_SHA ○ TLS_RSA_WITH_AES_256_CBC_SHA ○ TLS_RSA_WITH_AES_128_CBC_SHA256 ○ TLS_RSA_WITH_AES_256_CBC_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

1.5 Product Functionality not Included in the Scope of the Evaluation

The following product functionality is not included in the CC evaluation:

- SNMP Traps (Alarms)
- VistaLINK PRO module
- External Authentication Servers for administrator authentication

These functions are outside the TOE. Alarm monitoring is the sending of SNMP traps to an alarm monitoring system (which is assigned by an Administrator).

In addition, IPX provides IP video stream switching. This IP video switching does not provide security functionality and was therefore not evaluated and is outside the scope of the TOE. The nature of video encryption and decryption is that a video stream is encrypted at the sending end and decrypted at the receiving end; since IPX is a midpoint device and therefore does not perform encryption or decryption functionality. This functionality, while present in the TOE, was not evaluated.

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, April 2017 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 5, April 2017 (Conformant)

2.2 Protection Profile Conformance

This ST claims exact conformance to the following:

- collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E]

2.3 Conformance Rationale

This ST provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP TDs issued to date and applicable to NDcPP v3.0e have been considered. Table 6 identifies all applicable TDs.

Table 6 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0917 - NIT Technical Decision: Addition of FIPS PUB 186-5 for RSA	Yes	Applies to SFRs and Tests.
TD0900 - NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	Yes	Applies to SFR.
TD0899 - NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	Yes	Applies to Tests.
TD0886 - FAU_STG_EXT.1 Test 6	Yes	Applies to Tests.
TD0880 - NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	Yes	Applies to SFR.
TD0879 - NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	Yes	
TD0868 - NIT Technical Decision: Clarification of time frames in	No	Not claimed in ST.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8		
TD0836 - NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	Yes	Applies to SFR, Tests, and AA.

3 Security Problem Definition

The security problem definition has been taken directly from the claimed PP specified in Section 2.2 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 7 are drawn directly from the PP specified in Section 2.2.

Table 7 – Threats

ID	Threat
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 tunnelling 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. a 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 themselves into 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.

ID	Threat
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. Nonvalidated 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 includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2 Assumptions

The assumptions included in Table 8 are drawn directly from PP.

Table 8 – Assumptions

ID	Assumption
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.

ID	Assumption
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 a 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 and PP-Modules 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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.3 Organizational Security Policies

The OSPs included in Table 9 are drawn directly from the PP.

Table 9 – OSPs

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

4 Security Objectives

The security objectives have been taken directly from the claimed PP and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 10 – Security Objectives for the Operational Environment

ID	Objectives for the Operational Environment
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
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	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revisions 5, April 2017, and all international interpretations.

Table 11 – SFRs

Requirement	Description
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_STG_EXT.1	Protected Audit Event Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSS_EXT.1	TLS Server Protocol
FCS_TLSS_EXT.2	TLS Server Support for Mutual Authentication
FIA_AFL.1	Authentication Failure Handling
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU.7	Protected Authentication Feedback
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
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_STM_EXT.1	Reliable Time Stamps
FPT_TUD_EXT.1	Trusted Update

Requirement	Description
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_SSL_EXT.1	TSF-initiated Session Locking
FTA_TAB.1	Default TOE Access Banner
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1/Admin	Trusted Path

5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration identifier after a slash, e.g., /SigGen.
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
  Extended SFRs are identified by the addition of "EXT" after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1

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) Auditable events for the not specified level of audit; and
c) *All administrative actions comprising:*
   - *Administrative login and logout (name of Administrator account shall be logged if individual user accounts are required for Administrators).*
   - *Changes to TSF data related to 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 Administrator account shall be logged), no other actions*];
d) *Specifically defined auditable events listed in*Table 12.

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity ~~(if applicable)~~, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 12.

Table 12 – Security Functional Requirements and Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
FCS_TLSS_EXT.2	Failure to authenticate the client.	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate. • Any addition, replacement or removal of trust anchors in the TOE's trust store.	• Reason for failure of certificate validation. • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Functions	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1).	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session lock.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	• None. • None. • Reason for failure.
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	• None. • None. • Reason for failure.

5.2.1.2 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.

5.2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1
The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2
The TSF Shall be able to store generated audit data on the TOE itself. In addition [

- *The TOE shall consist of a single standalone component that stores audit data locally,*

].

FAU_STG_EXT.1.3

The TSF shall maintain a [*log file*] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4

The TSF shall be able to store [*nonpersistent*] audit records locally with a minimum storage size of [*2 log files with 1MB size each*].

FAU_STG_EXT.1.5

The TSF shall [*overwrite previous audit records according to the following rule: [on a circular (FIFO) basis]*] when the local storage space for audit data is full.

FAU_STG_EXT.1.6

The TSF shall provide the following mechanisms for administrative access to locally stored audit records [ability to view locally].

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

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 bits] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1;*
- *ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;*

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

Application Note: This SFR has been updated as per TD0917

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

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

- *RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2";*
- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision* 3, *"Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*

] ~~that meets the following: [assignment: list of standards].~~

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

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]];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [*
    - *logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]];*

that meets the following: *No Standard*

5.2.2.4 FCS_COP.1/DataEncryption Cryptographic Operations (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption
The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in* [*CBC, CTR, GCM*] *mode* and cryptographic key sizes [*128 bits, 256 bits*] that meet the following: *AES as specified in ISO 18033-3,* [*CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772*].

5.2.2.5 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen
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 [

- *For RSA: modulus 2048 bits or greater*

]

that meets the following: [

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,*

].

Application Note: This SFR has been updated as per TD0917

5.2.2.6 FCS_COP.1/Hash Cryptographic Operations (Hash Algorithm)

FCS_COP.1.1/Hash
The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [*SHA-1, SHA-256, SHA-384*] ~~and cryptographic key sizes~~ [~~*assignment: cryptographic key sizes*~~] and **message digest sizes [*160, 256, 384*] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.2.7 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash
The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [*HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384*] and cryptographic key sizes *[160 bits, 256 bits, and 384 bits used in HMAC]* **and message digest sizes [*160, 256, 384*] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.2.8 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 ~~protocol~~ using TLS.

5.2.2.9 FCS_RBG_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_DRBG (AES)]*.

FCS_RBG_EXT.1.2

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

5.2.2.10 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1
The TSF shall implement [TLS 1.2 (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*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and no other ciphersuites.

Application Note: The TOE supports non-mutual authentication in the role of a client when establishing connections to external syslog server (Audit Server).

FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [*the reference identifier per RFC 6125 Section 6 IPv4 address in the SAN, and no other attribute types*].

FCS_TLSC_EXT.1.3
The TSF shall not establish a trusted channel if the server certificate is invalid [

- *without any administrator override mechanism.*

].

FCS_TLSC_EXT.1.4
The TSF shall [*present the Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups*] in the Client Hello.

FCS_TLSC_EXT.1.5
The TSF shall [

- *present the signature_algorithms extension with support for the following algorithms: [*
  - *rsa_pkcs1 with sha256(0x0401),*

] and no other algorithms*;*].

FCS_TLSC_EXT.1.6
The TSF [*does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7
The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8
The TSF shall [*not use PSKs*].

FCS_TLSC_EXT.1.9 The TSF shall *[reject [TLS 1.2] renegotiation attempts]*.

5.2.2.11 FCS_TLSS_EXT.1 TLS Sever Protocol

FCS_TLSS_EXT.1.1
The TSF shall implement [*TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268*
- *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268*
- *TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246*
- *TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and no other ciphersuites.

Application Note: The TOE supports non-mutual authentication in the role of a server when providing remote administrative access via its web interface.

FCS_TLSS_EXT.1.2
The TSF shall authenticate itself using X.509 certificate(s) using *[RSA with key size [2048] bits]*.

FCS_TLSS_EXT.1.3
The TSF shall perform key exchange using: [

- *RSA key establishment with key size [2048] bits;*
- *EC Diffie-Hellman key agreement over NIST curves [secp256r1, secp384r1, secp521r1] and no other curves;*

].

FCS_TLSS_EXT.1.4
The TSF shall support [*no session resumption*].

FCS_TLSS_EXT.1.5
The TSF [*does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6
The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_TLSS_EXT.1.7
The TSF shall [*not use PSKs*].

FCS_TLSS_EXT.1.8
The TSF shall [*reject [TLS 1.2] renegotiation attempts]*.

5.2.2.12 FCS_TLSS_EXT.2 TLS Sever Support for Mutual Authentication

FCS_TLSS_EXT.2.1
The TSF shall support TLS communication with mutual authentication of TLS clients using X.509v3 certificates and shall [

- *reject the connection if the client either does not provide a client certificate at all or the client certificate cannot be successfully validated by the TOE (except for override mechanisms that might be defined in FCS_TLSS_EXT.2.2) ('hard fail')*].

Application Note: The TOE supports mutual authentication in the role of a server when establishing connections to MAGNUM (Video Control Server).

FCS_TLSS_EXT.2.2
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the client certificate is invalid. The TSF shall also [

- *not implement any administrator override mechanism*

].

FCS_TLSS_EXT.2.3
The TSF shall not establish a trusted channel if the identifier contained in a certificate does not match an expected identifier for the client. If the identifier is a Fully Qualified Domain Name (FQDN), then the TSF shall match the identifiers according to RFC 6125, otherwise the TSF shall parse the identifier from the certificate and match the identifier against the expected identifier of the client as described in the TSS.

FCS_TLSS_EXT.2.4
The TSF shall present a [*TLS 1.2*] Certificate Request message containing the following algorithms: [

- *rsa_pkcs1 with sha256(0x0401),*

] and no other algorithms.

5.2.3 Identification and Authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within *[3 to 20]* unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [unlocking the offending Administrator] is taken by an Administrator].*

5.2.3.2 FIA_PMG_EXT.1 Password Management

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

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters*:* [*"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", ["~", "`", " ", "_", "-", "+", "=", "{", "[", "}", "]", "|", "\", ":", ";", (''), (’), "<", ",", ">", ".", "?", "/", (space)]*];

b) Minimum password length shall be configurable to between [*15*] and [*20*] characters.

5.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

FIA_UIA_EXT.1.3
The TSF shall provide the following remote authentication mechanisms [*Web GUI password]* and [no other mechanism]. The TSF shall provide the following local authentication mechanisms [*password-based].*

Application Note: This SFR has been updated as per TD0900.

FIA_UIA_EXT.1.4
The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

5.2.3.4 FIA_UAU.7.1 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**.

5.2.3.5 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates** .
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- 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 DTLS/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 DTLS/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.*
  - *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.*

FIA_X509_EXT.1.2/Rev
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.

5.2.3.6 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*] 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*].

5.2.3.7 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions
The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*transmission of audit data to an external IT entity*] to *Security Administrators*.

5.2.4.2 FMT_MOF.1/ManualUpdate Management of Security Functions Behavior

FMT_MOF.1.1/ManualUpdate
The TSF shall restrict the ability to enable the function *to perform manual updates to Security Administrators.*

5.2.4.3 FMT_MTD.1/CoreData Management of TSF Data

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

5.2.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys
The TSF shall restrict the ability to *manage* the *cryptographic keys* to *Security Administrators*.

5.2.4.5 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 remotely;*
- *Ability to configure the access banner;*

- *Ability to configure the remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using* digital signature *capability prior to installing those updates;*
- [
  - *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
  - *Ability to manage the cryptographic keys;*
  - *Ability to re-enable an Administrator account;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
  - *Ability to generate Certificate Signing Request (CSR) and process CA certificate response;*
  - *Ability to configure the authentication failure parameters for FIA_AFL.1;*
  - *Ability to administer the TOE locally;*
  - *Ability to configure the local session inactivity time before session termination or locking;*

  ].

Application Note: This SFR has been updated as per TD0880.

5.2.4.6 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 remotely*

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FTP_APW_EXT.1 Protection of Administrator Passwords

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

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

5.2.5.2 FPT_SKP_EXT.1 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 keys, and private keys.

5.2.5.3 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2
The TSF shall [*allow the Security Administrator to set the time*].

5.2.5.4 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 verify the integrity of the TOE firmware and software;
- Prior to providing any cryptographic service and [*[before generation of RSA key pair, before uploading TOE's certificate, and before uploading CAs certificates]*] to verify correct operation of cryptographic implementation necessary to fulfil the TSF.
- [no other] self-tests *[none]* to demonstrate the correct operation of the TSF.

Application Note: This SFR has been updated as per TD0836

FPT_TST_EXT.1.2
The TSF shall respond to [*all failures*] *by* [*[pausing the system and rebooting it again]*].

5.2.5.5 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 [*no other TOE firmware/software version*].

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 means to authenticate firmware/software updates to the TOE using a [*digital signature*] prior to installing those updates.

5.2.6 TOE Access (FTA)

5.2.6.1 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

5.2.6.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 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 ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [*[video switch control system (such as Evertz MAGNUM)]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ disclosure **and detection of modification of the channel data**.

FTP_ITC.1.2
The TSF shall permit [*the TSF, **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 [*auditing services*].

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin
The TSF shall **be capable of using [*TLS, HTTPS*] to** provide a communication path between itself and **authorized** remote **Administrators** ~~users~~ that is logically distinct from other communication 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/Admin
The TSF shall permit remote **Administrators** ~~users~~ to initiate communication via the trusted path.

FTP_TRP.1.3/Admin
The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions.*

5.3 TOE SFR Dependencies Rationale for SFRs

The PP contain(s) all the requirements claimed in this ST. As such, the dependencies are not applicable since the PP has been approved.

5.4 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP, which is derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 13.

Table 13 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functionality specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey

5.5 Assurance Measures

The TOE satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Evertz Microsystems Ltd. to satisfy the assurance requirements. The following table lists the details.

Table 14 – TOE Security Assurance Measures

SAR Component	How the SAR will be met
ASE_TSS.1.1C Refinement	The TOE summary specification shall describe how the TOE meets each SFR. In the case of entropy analysis, the TSS is used in conjunction with required supplementary information on Entropy.
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.

SAR Component	How the SAR will be met
ALC_CMC.1 ALC_CMS.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ATE_IND.1	Vendor will provide the TOE for testing.
AVA_VAN.1	Vendor will provide the TOE for testing. Vendor will provide a document identifying the list of software and hardware components.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 15 – TOE Summary Specification SFR Description

Requirement	TSS Description
FAU_GEN.1	Audit records are created when an auditable event that belongs to a set of predefined events had occurred. The set of auditable events are sub-categorized into functional events and access events. Audit records are stored in log files in plaintext. 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. The TSF generates audit records for the following events: • Startup and shutdown of the audit function • Administrative login and logout events • Changes to TSF data related to configuration changes • Generation of a CSR and associated keypair • Installation of a certificate • Resetting passwords • Failure to establish a HTTPS/TLS session • Failure to establish a TLS session • All use of the identification and authentication mechanism (local and remote connections to the TSF) • Unsuccessful attempts to validate a certificate • Initiation of a software update • Result of a software update • Changes to the time • Modification of the behavior of the TSF • Failure of self-tests • Initiation and termination of the trusted channel • Initiation and termination of the trusted path • Attempts to unlock an interactive session • Termination of a session by the session locking mechanism Each audit record includes the date and time, type, subject identity (IP address, hostname, and/or username), the outcome (success or failure), and any additional information specified in column three of Table 12. The TOE only stores one certificate chain to support TLS. No other server certificates are stored. Logs of Administrator actions involving keys and certificates, such as generating keys, uploading and updating certificates, will reference the key as the "server private key", and the certificates as the "server certificate" and "CA certificates", along with their corresponding unique MD5 checksum values.

Requirement	TSS Description
FAU_GEN.2	None
FAU_STG_EXT.1	The TOE is a standalone TOE. IPX stores audit logs internally in real-time. The internal logs are stored unencrypted, but they are only accessible (and then read-only) via the web browser and console, which can only be used by Administrators. The TOE does not allow any deletion or modification of the logs manually via the web browser or console. IPX stores all audit data locally in a secure location; it is accessible to administrators using the "Syslog" tab on the web interface. Log information is also sent to an external Syslog server via 'Syslog over TLS using TLS v1.2'. Logs are sent to the Syslog servers in real-time. The [AGD] explains how to configure this connection. Configurations include adding the syslog server IP address/port number and uploading a trusted certificate chain to the TOE. The trusted channel with the Syslog server is described in greater detail in the FCS_TLSC_EXT.2 description. For local audit log storage, two log files are used, each with a maximum capacity of 1MB which is hardcoded and not configurable. Initially both files are empty, and entries are added to file 1. Once file 1 is full, newer entries will be added to file 2 until it becomes full, at which time content of file 1 will be cleared and entries added to file 1 again. The audit logs will keep getting forwarded to the secure syslog server in the event of an audit space is full. Audit logs are non-persistently saved in a memory file system which is the volatile memory. The maximum size of the volatile memory is 512MB and 256MB for the file system. The TOE overwrites previous audit records on a circular (FIFO) basis when the volatile memory /dev/shm/ftp/ storage space for audit is full.
FCS_CKM.1	The TSF supports generation of 2048-bit RSA keys for digital signatures in support of TLS sessions (FCS_TLSC_EXT.1 and FCS_TLSS_EXT.2) and the server certificate (FIA_X509_EXT.3). Generation of ECDSA keys with NIST curves of P-256 or P-384 or P-521 are also used to generate EC DH components for key establishment in TLS sessions (FCS_TLSC_EXT.1 and FCS_TLSS_EXT.2). The relevant NIST CAVP certificate numbers are listed in Table 16.
FCS_CKM.2	The TOE acts as both sender and recipient for elliptic curve Diffie-Hellman key establishment schemes that meet the following: • NIST Special Publication (SP) 800-56A revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" – for FCS_TLSC_EXT.1 connections to the audit server and FCS_TLSS_EXT.2 connections to the MAGNUM server. or • RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specification Version 2.1". The TOE uses RSA-based key establishment for backwards compatibility for FCS_TLSC_EXT.1 connections to audit server and FCS_TLSS_EXT.2 connections to the MAGNUM server.

Requirement	TSS Description
	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. The relevant NIST CAVP certificate numbers are listed in Table 16.
FCS_CKM.4	Cryptographic keys are destroyed by first overwriting the key file content with zeros. A read-verification is then performed to ensure that the entire content has really been changed to zeros and not any other values. If these steps fail, then the file will be overwritten again with zeros until the read-verify step succeeds. A sudden, unexpected power could disrupt zeroization and cause keys to not be zeroized. There are no other known circumstances where the TOE would not conform to these requirements. The keys/CSPs used by the TOE, their storage location and format, and their associated zeroization method are listed in the Table 17– Key Storage and Zeroization. To delete the plain-text keys stored on the non-volatile NOR flash storage, direct interface/access is provided to view or modify the contents of these files. The CLI provides Security Administrators with a menu item to destroy all CSPs, which would initiate key destruction. No direct interface/access is provided to view or modify the contents of the keys stored in the volatile memory. The TLS session keys stored on Flash are automatically destroyed when the TLS session ends. The DRBG state is zeroized using a single overwrite of zeros when the TSF is shutdown or restarted. The above destruction methods are followed in all configurations and circumstances.
FCS_COP.1/DataEncryption	The TOE provides AES encryption/decryption in CBC, CTR, or GCM mode with 128- and 256-bit keys. The TOE provides AES encryption and decryption in support of TLS v1.2 and RBG for secure communications.
FCS_COP.1/Hash	The TOE implements hashing in byte-oriented mode. The TOE provides cryptographic hashing services in support of TLS for SHA-1, SHA-256 and SHA-384. SHA-256 is used for firmware integrity checks during power-on-self-tests and upgrades. The locally stored passwords are salted using SHA-256. Key generation is performed using SHA-256 as specified in NIST SP 800-90 DRBG. The relevant NIST CAVP certificate numbers are listed in Table 16.
FCS_COP.1/KeyedHash	Keyed-hash message authentication is used as part of TLS protocol as part of the negotiated ciphersuites between peers. It is also used for firmware image integrity check where the hashed-value (HMAC-SHA-256) of the images is signed with Evertz's private key and the

Requirement	TSS Description
	result file (signature) is included in the firmware package file. During upgrade, the signature file is first decrypted using the public key stored on IPX, then the hashed value (HMAC-SHA-256) is re-calculated from the uploaded image file and then compared with the decrypted hash value (HMAC-SHA-256). These hashes must match for this validation to succeed. The following keyed-hash message authentication are used by IPX: • HMAC-SHA-1 with 160-bit key, message digest size of 160 bit and 160 bit message block size, • HMAC-SHA-256 with 256-bit keys, message digest sizes of 256 bits, and block size of 512 bits, and • HMAC-SHA-384 with 384-bit keys, message digest sizes of 384 bits, and block size of 1024 bits. The relevant NIST CAVP certificate numbers are listed in Table 16.
FCS_COP.1/SigGen	The TOE supports signature generation and verification with RSA 2048-bits with SHA-1/256/384 in accordance with FIPS PUB 186-4, using PKCS #1 v2.1. These signatures support TLS authentication and firmware verification. The TOE's server certificate is 2048-bits. The relevant NIST CAVP certificate numbers are listed in Table 16.
FCS_HTTPS_EXT.1	The TOE acts as a TLS/HTTPS server to provide web access to administrators. The TOE's HTTPS functionality is in accordance with all should statements in RFC 2818.
FCS_RBG_EXT.1	The TOE implements a DRBG in accordance with ISO/IEC 18031:2011 using a CTR DRBG with AES. The TSF seed the CTR_DRBG using 384-bits of data that contains at least 256 bits of entropy. The TSF gathers and pools entropy from two software-based noise source: haveged and the Linux Kernel entropy. The entropy sources are discussed in greater detail in the Entropy Assessment documentation. The relevant NIST CAVP certificate numbers are listed in Table 16.
FCS_TLSC_EXT.1 FCS_TLSS_EXT.1 FCS_TLSS_EXT.2	The TOE acts as a TLS/HTTPS server to provide web access to administrators. The TOE's HTTPS functionality is in accordance with all shall statements in RFC 2818. The TLS/HTTPS server connects over the TCP port 443. The TOE acts as a client when connecting to the syslog server and as a server when providing administrative access via TLS/HTTPS. The TLS client port is configurable between 0-65535. The TOE also acts as a TLS server when connecting to a video switch control system. For video switch control systems TLS trusted channels, the TOE requires TLS with mutual authentication. The TLS Server with mutual authentication connects over the TCP port 9672. The TSF only supports TLSv1.2 for HTTPS/TLS. Connection requests that include SSL 2.0, SSL 3.0, TLS 1.0 or TLS 1.1 are denied. If the TSF receives a ClientHello message that requests TLSv1.1 or earlier, the TSF sends a fatal handshake_failure message and terminates the connection.

Requirement	TSS Description
	The TOE performs X.509v3 certification validation. For all the TLS client and server connections, if the certificate verification fails for any reason (including a failure to establish a connection), the connection attempt fails, and the trusted channel is not established. There are no fallback authentication functions for failed certificate authentication. IPX specifies only a restricted set of ciphersuites that it supports during the negotiation phase with a client or a server. If no match of ciphersuites can be found with peer, TLS session will not be started. These ciphersuites cannot be configured or changed by an Administrator. The following ciphersuites are supported: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 Protocols that do not conform to TLS v1.2 are explicitly excluded in IPX's ciphersuites. IPX only supports ciphersuites that use RSA keys for authentication. These keys are generated with OpenSSL's RSA command line internally to the TSF. Elliptic curve Diffie Hellman and RSA are supported for key establishment in TLS for both client and server. The RSA key establishment uses 2048 bits. EC-DH key establishment uses NIST curves, P-256, P-384 and P-521. By default, the TOE presents the supported Elliptic Curve Extensions, secp256r1, secp384r1, and secp521r1 in the Client Hello. The TOE conforms to RFC 5246, section 7.4.3 for key exchange. All ciphers and elliptic curves on the TOE are hardcoded. The TOE does not accept any Diffie-Hellman (DHE) parameters other than those explicitly supported. When validating a client's certificate, IPX uses CRL (certification revocation list) to check for invalid certificates. CRL files which are signed by trusted CA certificated are imported to IPX. This CRL file will be used by IPX during certificate validation process to check for revocation status of the peer certificates. IPX allows configuration of an RFC6125 reference identifier from a peer it expects to connect with before connection is made. The reference identifier can be any string up to 64 bytes that is present in the peer certificate's DN and SAN field. The verification against peer certificate is implemented within OpenSSL using a bitwise comparison of the DN and SAN field. The TOE does not mandate SAN extension and checks SAN extension over CN when present. The TOE ignores CN when SAN is present. When SAN is not present, the TOE checks for CN. If the SAN is incorrect, the certificate will be rejected. It will not check for the CN. FQDN is supported in both SAN and CN while IP address is only supported in SAN. The IPX supports the following identifier types:

Requirement	TSS Description
	• DNS name in the SAN or CN. • IPv4 address in the SAN. The TOE enforces canonical format for IPv4 as defined in RFC 3986 for IPv4. SRV-ID and URI-ID types are not supported. IPX does not support certificate pinning. IPX supports wildcard in certificates. The wildcard must be in the left-most label of the presented identifier and 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. IPX does not support session resumption or session tickets. IPX does not use out-of-band provisioning of pre-shared keys (PSKs). IPX only supports the signature_algorithms extension (rsa_pkcs1 with sha256(0x0401) for TLS connections. If the claimed signature_algorithm is present in the 'CLIENT HELLO', then the connection is accepted otherwise denies the connection. By default, the signature_algorithms extension rsa_pkcs1 with sha256(0x0401) is supported on the TOE and in certificates generated via OpenSSL.
FIA_AFL.1	An administrator is able to configure the number of unsuccessful attempts a remote administrator makes before a lock-out. The attempts ranges between 3 and 20 attempts. The default number of attempts is 10. Each time the user enters an incorrect password a $failedCount variable is incremented. When the $failedCount variable reaches the configured limit, the username becomes locked and any future attempts to authenticate with this username are denied. The username will show the Lockout enabled on the Settings->Users page on the web interface. The user cannot login through any remote interface on the TOE until a different Administrator logs in and unlock the offending Administrator. Non administrative users can only be unlocked by an Administrator. Lockouts are not enforced on the TOE's console interface. This ensures that authentication failures cannot lead to a situation where no administrator access is available.
FIA_PMG_EXT.1	IPX enforces that passwords must meet minimum length requirements. IPX passwords can be composed of a mix of number, lower/upper case letters, and the following special characters "!"; "@"; "#"; "$"; "%"; "^"; "&"; "*"; "("; ")";"~"; "`"; "_"; "-"; "+"; "="; "{"; "["; "}"; "]"; "|"; "\"; ":"; ";"; ["]; [']; "<"; ","; ">"; "."; "?"; "/"; [space]. At least two characters from each category are required (upper case letter, lower case letter, number special character). Passwords must be at least a minimum length settable by the administrator between 15 and 20 characters.
FIA_UIA_EXT.1	The only accounts that the IPX will establish are Security Administrator accounts. Users only control the Video/Audio traffic handling on the IPX can be controlled indirectly via MAGNUM but no security relevant configuration cannot be done through Magnum. Administrators are identified and authenticated via username and password prior to performing any operations other than acknowledging the warning banner. The IPX Administrators user accounts module maintains Security

Requirement	TSS Description
	Administrator credentials. Since the only role that accesses the IPX directly is that of Security Administrator there is no assignment of roles required. Administrators is able to logon via the WebEasy interface using HTTPS or locally on the serial port. Both methods use username and password to authenticate the administrator. The Security Administrator is considered authenticated if the username and password match. Prior to successful identification and authentication on all interfaces, the TSF displays the TOE access banner specified in FTA_TAB.1. Users must acknowledge the warning banner before they login to the system.
FIA_UAU.7	None
FIA_X509_EXT.1/Rev	IPX uses OpenSSL for X.509 certificate validation. The certificate path is validated by ensuring that all the CA certificates have the basicConstraints extension and the path must terminate with a trusted CA certificate. The extendedKeyUsage on each certificate is also checked to ensure there is no inappropriate usage. Server certificates must have the Server Authentication purpose, client's certificates must have the Client Authentication purpose. Certificates for code signing and OCSP signing are not used or accepted by the TOE. Each certificate (other than the first certificate) in the certificate chain has the Subject Type=CA flag set. Certificates are not used for any purposes other than establishing TLS sessions. If certificates are uploaded to IPX for its own use those certificates are checked upon upload. When the TOE acts as a server, it does not perform verification of its server certificate. The TOE's client certificate is validated prior to use for authentication as well as upon upload. The certificate presented by remote TLS clients using mutual authentication is validated during the establishment of a TLS connection. For an expired certificate, IPX will deny the connection. IPX also uses CRL to verify whether the leaf certificate or intermediate CA certificate has been revoked. During session establishment with IPX, any byte modification in the certificate will lead to the failure of connection. The TSF verifies the validity of a certificate when: • A TLS client establishes a TLS connection with mutual authentication • A TLS server presents its certificates to the TOE as a part of a TLS connection If the Security Administrator loads a certificate that includes the basicConstraints extension with the CA flag set to TRUE (Subject Type = CA), the TSF does not perform certificate path validation.
FIA_X509_EXT.2	Instructions about generating/downloading CSR and loading certificate can be found in the AGD. The Administrator has the ability to upload either a complete certificate chain or an individual CA certificate to the IPX trust store. The same certificate will be used by IPX for both web service and MAGNUM control. The same CA will be used for certificate verification. IPX

Requirement	TSS Description
	enforces mutual authentication for MAGNUM clients and therefore requires client certificates to establish a connection. For MAGNUM, the CRLs are obtained from a CRL distribution point over HTTP and are refreshed according to the default CRL update-interval. The default interval is 2 hours. If the TOE is unable to reach the CRL DP it will not accept the certificate, and the session associated with the certificate will be denied. For the Syslog server, CRLs are obtained via the CRL upload option, where the Security Administrator uploads a CRL file. The 'Clear Cached CRL' option allows the removal of CRL files stored in the cache. The TOE will fail to validate a CRL if it is not signed by the currently active signing Certificate Authority (CA). In such cases, the associated certificate will be rejected, and the session associated with the certificate will be denied. If certificate verification fails for any reason (including a failure to establish a connection), the connection attempt fails, and the trusted channel is not established.
FIA_X509_EXT.3	The TSF allows Security Administrators to generate Certificate Signing Requests. The TSF requires the Security Administrator to specify the following values: • Common Name • Organization • Locality • State • Country • Key Length (2048) A CSR can be generated from the serial console menu. When validating certificates, each certificate from the chain is sequentially validated, terminating at the root CA. If any invalid certificate is found in this process, the validation fails.
FMT_MOF.1/Functions	The TOE restricts the ability to enable and disable the transmission of audit records to an external audit server to Security Administrators. The WebEasy interface allow the Security Administrator to perform the following TSF management functions: • View/Edit settings for sending audit data to the Syslog Server The Local console interface allow the Security Administrator to perform the following TSF management functions: • View settings for sending audit data to the Syslog Server Administrator can modify the behavior of transmitting audit data to an external audit server with the following configuration from the WebEasy interface:

Requirement	TSS Description
	• Login to the Management Web Application • Click “System” button from the displayed index page • Enter reference-identifier* (host name) of the target remote syslog server • Enter remote log server ip address • Enter remote log server log service port • Upload certificate chain applicable to TOE syslog server Certificate Authority • Click “Upload” button • Click “Apply” button at the top of the page
FMT_MOF.1/ManualUpdate	None
FMT_MTD.1/CoreData	IPX ensures that only secure values are accepted for security attributes. The TOE implements Role Based Access Control (RBAC). The Security Administrator is the only account that should be used. This account has the Administrator role. The TOE maintains the following roles: • Administrator • rw-user • ro-user The Security Administrator is the only account that should be used with the role of this account set to administrator role. There are no limitations/restrictions for the administrator role. There is no option to edit or modify the administrator role access. The Administrator has the ability to grant or remove permissions (which are also called ‘Restrictions’) to both ro-users and rw-users. By default, users with rw-user role can change the configuration of IPX, view the event log, and perform firmware upgrades. However, they are not authorized to change general system settings, manage user accounts, modify roles, or create new users. All permissions granted to rw-user role are subject to further restriction by the TOE’s Security Administrator. As part of the TOE’s evaluated configuration, it is required that the “upgrade” permission be disabled for the rw-user role. The users with ro-user role cannot change any IPX configuration settings, user settings or perform firmware upgrades. This role can only view IPX and user settings and view the event log. No administrative functionality is available prior to login. The TSF displays a warning banner prior to user authentication. The TOE maintains a trust store where the TOE’s certificate is stored. Only Security Administrators have access to the trust store. Security Administrators can upload a certificate chain. Uploading the certificate chain replaces the previously installed certificate chain.
FMT_MTD.1/CryptoKeys	The CLI allow the Security Administrator to perform the following TSF management functions on cryptographic keys: • Keys

Requirement	TSS Description
	○ TLS Key Generation (RSA 2048-bit keys are automatically generated when creating a CSR) ○ TLS Key Reset/Replacement (when a CSR is generated, previous RSA 2048-bit keys will be deleted and replaced by the new pair of keys. RSA 2048-bit keys cannot be imported from outside the TOE, and administrators cannot delete TLS keys manually.) The administrative interfaces provided by the TSF do not allow any of these functions to be accessed by unauthenticated or unauthorized users.
FMT_SMF.1 FMT_SMR.2	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. The (non-administrative) User can only view configurations. No administrative functionality is available prior to login. The TSF displays a warning banner prior to user authentication. The TSF implements the Security Administrator role to authorized administrators of the TOE. The TSF allows the Security Administrators to administer the TSF via a local CLI and a remote WebEasy interface. The TSF implements role-based access control of these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role. The WebEasy interface allow the Security Administrator to perform the following TSF management functions: • Control port IP configuration • Edit login banner • Reset certificates • Import certificates • Import Trusted CA certificate • Download a CSR • Configure WebEasy menu system timeout • Verify/Install Firmware Updates • View/Edit settings for sending audit data to the Syslog Server • View/Edit authentication failure parameters • Re-enable locked out Administrator accounts The following can only be performed from the local console interfaces: • Login to local console • Change Linux password for console account “customer” • Create certificate signing request CSR • Zeroize all Critical Security Parameters (CSP)

Requirement	TSS Description
	• Configure IPX date and time • Control port IP configuration • Configure console menu system timeout • Verify Firmware Updates Administrators can administer IPX locally through serial port connection. A console menu can be used to perform configurations tasks such as setting IP/system time/session timeout/generate certificate request/system reboot, etc. When a user account is created (by administrator), it must be assigned with a role that specifies the privileges the account will have. The administrator can choose to assign an existing role with pre-defined privileges or create a new role with customized privileges. Administrators can administer IPX remotely through its web interface, which runs on HTTPS. The web interface supports a broader set of the configuration settings that include configurations for certificate imports, syslog server, route mapping, etc. The administrative interfaces provided by the TSF do not allow any of these functions to be accessed by unauthenticated or unauthorized users.
FPT_APW_EXT.1	The TSF does not store plaintext password. Passwords are salted using SHA-256 and stored in a secure location which is not accessible to users. Secure (one-way) hash functions ensure that it's computationally impossible to recover a plaintext from its hashed value.
FPT_SKP_EXT.1	The TSF stores cryptographic keys in a directory (/etc/shadow) in flash memory. As there is no command line access, users cannot gain any direct access to these files. Information regarding the storage locations, usage, and method of storage of the cryptographic keys described in FCS_CKM.4 above.
FPT_STM_EXT.1	The TSF provides a reliable timestamp from the hardware clock on the TOE. Timestamps found in auditable log events use the system clock on IPX. In addition to the purpose of generating audit logs, this timestamp is used for the purposes of other time-sensitive operations on the TOE including cryptographic key regeneration intervals, local and remote session inactivity, X.509 certificate expiration validation. Administrators can, as needed, set the system time clock through serial port console menu after each card reboot. The new system time is also used to set the hardware clock, which is a clock that runs independently of any control program running in the CPU and even when IPX is powered off. During IPX system startup, system time is initialized to the time from the hardware clock.
FPT_TST_EXT.1	The TSF performs the following self-tests at power-on: • Firmware integrity check that compares the SHA256 checksum of the loaded firmware with a permanently stored hash value.

Requirement	TSS Description
	The TSF enables FIPS mode on the OpenSSL library by default at start-up, before generation of RSA key pair, before uploading TOE's certificate, and before uploading CAs certificates. Upon enabling FIPS mode the algorithm self-tests required by FIPS are performed. The OpenSSL library self-tests include: • SHA-256 KAT • HMAC-SHA-256 KAT • AES 128 GCM Encrypt and Decrypt KAT • AES 128 Encrypt and Decrypt KAT • RSA 2048 SHA-256 Sign and Verify KAT • ECDSA Pairwise Consistency Test • DRBG AES-CTR-256 KAT (invoking the instantiate, reseed, and generate functions) After loading the image, a hash value is computed from the memory partition containing the image. This hash value is compared with a pre-stored hash value at another location on flash. The pre-stored hash is not accessible through any interface for modification. The two hash values must match for the boot process to succeed. If any of the other checks fail, the TSF will display a failure message on the serial console and will perform a reboot. Administrators are instructed to contact Evertz service department for repair if the failure does not clear on reboot. These self-tests ensure the TOE software has the correct image and that cryptographic functions are performing appropriately. The OpenSSL library self-tests are also run during normal operation before generation of RSA key pair. If failures are seen by the Administrator, they should be immediately corrected.
FPT_TUD_EXT.1	The site administrators do not have access to install any applications on the TOE. The IPX embedded system can only be updated with the valid firmware release from Evertz. Security Administrators can verify the currently active version of the TOE using either the WebEasy interface or the local console. In the WebEasy interface, the active firmware version is displayed by selecting the “Upgrade” option from the top menu. The current version will appear under the “Firmware Upgrade” section. For the local console, the active TOE version is shown on the login screen immediately after a successful login. The TOE does not support delayed activation of updates. The current firmware version is displayed on both webpage and in serial console menu. Digital delivery of new IPX firmware is provided via File Transfer Protocol Secure (FTPS) using signed and hashed code. Firmware updates are only done from the IPX webpage interface under “upgrade”. IPX has only one firmware. It will be uploaded as soon as you press “Upgrade” button. During a firmware upgrade, IPX will first verify the digital signature of new firmware code with a local stored public key. The

Requirement	TSS Description
	TSF does not provide an interface to change the local stored public key to administrators. A SHA-256 hashed-value of the images is generated and then signed with Evertz's RSA 2048-bit private key. The result file (signature) is included in the firmware package together with the actual firmware binary. During upgrade, the signature file is first decrypted using the public key stored on IPX, then the hashed value is re-calculated from the uploaded image binary file and then compared with the decrypted hash value. If the hashes match, IPX proceeds to verify the firmware binary header against an Evertz-defined proprietary format. If there are no mismatches, the new firmware overwrites the existing version. If the digital signature fails, the upgrade fails and a log event is generated. If the digital signature succeeds, the upgrade proceeds and the updated firmware is installed onto the TOE.
FTA_SSL.3	Security Administrators can configure a maximum allowable period of inactivity for a Security Administrator session on the WebEasy interface (remote). If there is no user interaction with the IPX for the specified amount of time, the session is terminated. The TSF polls the session timeout every 60 seconds, so the timeout occurs after the set time plus 60 seconds. The initial, default session timeout is 15 minutes. When the session is terminated, any unsaved changes will be discarded.
FTA_SSL.4	Security Administrators terminates their own sessions by clicking "Logout" at the upper right hand of the WebEasy screen or typing "X" to exit the console.
FTA_SSL_EXT.1	Security Administrators configures a maximum allowable period of inactivity for a Security Administrator session on the local console. If there is no user interaction with the IPX for the specified amount of time, the session is terminated. The allowable inactivity timeout ranges from 1 to 60 minutes. The initial, default session timeout is 15 minutes. When the session is terminated, any unsaved changes will be discarded.
FTA_TAB.1	IPX is managed locally through the local console and remotely over the HTTPS web interface. Administrators access the console through directly connected USB keyboard and VGA monitor. The TSF presents the access banner prior to authentication when a user connects to the remote WebEasy interface or local console CLI described in the FIA_UIA_EXT.1 description. The TSF enables Security Administrators to alter the warning banner by navigating to the "System" tab on the web browser and scrolling toward the bottom to the "Warning Banner" section. From here the Security Administrator is able to modify the "Agree" text and/or the "Disagree" text. The "Disagree" text shows up when a user "disagrees" with the Security Banner text. The banner can provide warnings against unauthorized access to the TOE as well as any other information that the Security Administrator wishes to communicate. Users who select "Disagree" are not permitted access to the TSF.

Requirement	TSS Description
FTP_ITC.1	The TSF communicates with the external syslog server using TLS v1.2 as described in the descriptions of FAU_STG_EXT.1 and FCS_TLSC above. The TSF initiates the trusted channel with the Syslog server. The TSF communicates with a MAGNUM server (Video Switch Server) through TLS v1.2 protocol with X.509 certificate-based mutual authentication as well as described in the FCS_TLSS above. The MAGNUM server initiates the trusted channel with the TOE. The TOE's routing and switching of video signals is controlled by MAGNUM via remote administration over the TCP port 9672.
FTP_TRP.1/Admin	The TSF provides a trusted path for remote administration using HTTPs/TLS as described in FCS_HTTPS_EXT.1 and FCS_TLSS_EXT.1 descriptions. IPX uses encryption and restricts the choices of ciphers, hashes, and key-exchange algorithms to those allowed by the NDcPP.

6.1 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified in the table below.

Table 16 – CAVP Algorithm Certificate References

SFRs	Algorithm in ST	Implementation Name	CAVP Alg	CAVP Cert
FCS_CKM.1	RSA schemes using cryptographic key sizes of [2048 bits] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1	IPX Cryptographic Module version 3.5	RSA KeyGen (FIPS186-4) (Modulo 2048)	A6450
	ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", AppendixB.4		ECDSA KeyGen (FIPS186-4) Curve P-256,P-384,P-521) ECDSA KeyVer (FIPS186-4) Curve P-256,P-384,P-521)	A6450
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography	IPX Cryptographic Module version 3.5	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in the ETR and AAR accordingly.	This testing was performed in conjunction with FTP_TRP.1/Admin Test #1 and FTP_ITC.1 Test #1 to demonstrate correct operation.

	Specifications Version 2.2”			
	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”		KAS-ECC-SSC Sp800-56Ar3 (Domain Parameter Generation Methods: P-256, P-384, P-521)	A6450
FCS_COP.1/ DataEncryption	GCM *mode* and cryptographic key sizes 128 bits, 256 bits that meet: *AES as specified in ISO 18033-3 and* GCM as specified in ISO 19772	IPX Cryptographic Module version 3.5	AES-GCM (Key length 128,256)	A6450
	CBC *mode* and cryptographic key sizes 128 bits, 256 bits that meet: *AES as specified in ISO 18033-3,* CBC as specified in ISO 10116.		AES-CBC (Key length 128,256)	
	CTR *mode* and cryptographic key sizes 128 bits, 256 bits that meet: *AES as specified in ISO 18033-3,* and CTR as specified in ISO 10116.		AES-CTR (Key length 128,256)	
FCS_COP.1/SigGen	RSA Digital Signature Algorithm using key sizes of 2048 bits that meets FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	IPX Cryptographic Module version 3.5	RSA SigGen (FIPS186-4) (Modulo: 2048) RSA SigVer (FIPS186-4) (Modulo: 2048)	A6450
FCS_COP.1/Hash	[SHA-1, SHA-256 and SHA-384] and message digest sizes [160, 256	IPX Cryptographic Module version 3.5	SHA-1 SHA-256 SHA-384	A6450

	and 384] bits that meet the following: ISO/IEC 10118-3:2004.			
FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384] and cryptographic key sizes [160 bits, 256 bits and 384 bits] and message digest [160, 256, 384] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"	IPX Cryptographic Module version 3.5	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384	A6450
FCS_RBG_EXT.1	CTR_DRBG (AES) in accordance with ISO/IEC 18031:2011 with a minimum of 256-bits	IPX Cryptographic Module version 3.5	Counter DRBG (AES-256)	A6450

6.2 Cryptographic Key Destruction

The table below describes the key zeroization provided by the TOE and as referenced in FCS_CKM.4.

Table 17 – Key Storage and Zeroization.

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
EC Diffie-Hellman Keys	Key agreement and key establishment	Plaintext in RAM	Overwritten with zeroes when no longer needed
Firmware Update Key	Verification of firmware integrity when updating to new firmware versions using a HMAC-SHA-256 hashed RSA signature	Public key is stored in plaintext in the Flash disk. Private key is not stored or used on the TOE.	Public key file is replaced when importing a new file, by overwriting the old key with zeroes
HTTPS/TLS Server/Host Key	RSA and EC private key used in the HTTPS/TLS protocols	Plaintext in the Flash Disk	Copy in RAM is also overwritten with zeroes when no longer needed.
HTTPS/TLS session authentication key	HMAC SHA-1, -256, or -384 key used for HTTPS/TLS session authentication.	Plaintext in RAM	Overwritten with zeroes when no longer needed.
HTTPS/TLS Session Encryption Key	AES (128, 256) key used for HTTPS/TLS session encryption	Plaintext in RAM	Overwritten with zeroes when no longer needed.
Locally Stored Passwords	User Authentication	Salted using SHA-256	Overwritten with zeroes when no longer needed.
Configuration Encryption Key	Configuration Encryption	Plaintext in the Flash Disk	Overwritten with zeroes when no longer needed.

7 Acronym Table

Acronyms should be included as an Appendix in each document

Table 18 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CC	Common Criteria
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DTLS	Datagram Transport Layer Security
EP	Extended Package
GUI	Graphical User Interface
IP	Internet Protocol
NDcPP	Network Device Collaborative Protection Profile
NIAP	Nation Information Assurance Partnership
OCSP	Online Certificate Status Protocol
PP	Protection Profile
RSA	Rivest, Shamir & Adleman
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TD	Technical Decision
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification