National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

MMA10G-IPX Series v3.5

Report Number: **CCEVS-VR-VID11576-2025**

Dated: **June 25, 2025**

Version: **1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant

Lisa Mitchell

Linda Morrison

Lori Sarem

Common Criteria Testing Laboratory

Rupendra Kadtan

Chaitanya Muzumdar

Fathi Nasraoui

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the MMA10G-IPX Series v3.5 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in June 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the Collaborative Protection Profile for Network Devices, Version 3.0e [CPP_ND_V3.0E].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	MMA10G-IPX Series v3.5
Protection Profile	*Collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E]
Security Target	*MMA10G-IPX Series v3.5 Security Target*, Version 1.1, June 19, 2025
Evaluation Technical Report	*Evaluation Technical Report for MMA10G-IPX Series v3.5*, Version 1.1, 06/19/2025
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Evertz Microsystems Ltd.
Developer	Evertz Microsystems Ltd.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Sheldon Durrant, Lisa Mitchell, Linda Morrison, Lori Sarem The MITRE Corporation

3 Architectural Information

3.1 TOE Description

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 mutually authenticated 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 system’ 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.

3.2 Physical Boundaries

The physical boundaries of the TOE are outlined in 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

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	modular	EMX3-FR EMX6-FR	EMX-FC	PowerQUICC® II Pro MPC8377E

			(GbE or 10GbE)				
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
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	1RU	N/A	None	PowerQUICC® II Pro MPC8377E

			4 SFP ports (10GbE)				
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 cipher suites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o 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 • Supporting at least one of the following cipher suites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o 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 cipher suites:

Component	Required	Purpose/Description
		○ 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

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 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. 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.

4.2 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

4.3 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.

4.4 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 can be 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.

4.5 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.

4.6 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.

4.7 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.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

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

That information has not been reproduced here and the NDcPP30e should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within [CPP_ND_V3.0E].
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- *MMA10G-IPX v3.5 Supplemental Administrative Guidance for Common Criteria*, Document Version 1.1, June 19, 2025

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the proprietary *Test Plan for MMA10G-IPX Series V3.5*, Version 0.4, June 19, 2025, as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in [CPP_ND_V3.0E]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration is the MMA10G-IPX-16-CC running MMA10G-IPX-16-CC Version 3.5. All other TOE models listed in Section 3.2 are included by equivalency.

The Required Environmental Components used to test the TOE are shown in Table 5 below:

Table 5 - 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: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o 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 • Supporting at least one of the following ciphersuites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o 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: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA

Component	Required	Purpose/Description
		○ 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

8.2 Excluded Functionality

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.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev. (5) and CEM version 3.1 Rev. (5). The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in [CPP_ND_V3.0E]. Additionally, the evaluation team performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the MMA10G-IPX Series v3.5 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluation team performed an assessment of the Assurance Activities specified in [CPP_ND_V3.0E].

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluation team performed the Assurance Activities specified in [CPP_ND_V3.0E] related to the examination of the information contained in the TOE Summary Specification.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluation team performed the Assurance Activities specified in [CPP_ND_V3.0E] related to the examination of the information contained in the operational guidance documents.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in [CPP_ND_V3.0E] and recorded the results in a Test Report, summarized in the ETR and AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluation team. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not uncover any residual vulnerabilities.

The evaluation team searched the following sources:

- National Vulnerability Database (https://nvd.nist.gov/view/vuln.search)
- MITRE CVE site (http://cve.mitre.org/cve)
- CVE Security Vulnerability Database (https://www.cvedetails.com/vulnerability-search.php)
- Evertz Website (https://evertz.com/)

The searches were performed on 06 February, 23 April, 5 May and 10 June 2025 with the following search terms:

- Evertz
- Evertz MMA10G
- Evertz MMA10G -IPX
- linux_kernel 4.19.325
- libcurl 8.12.1
- Lighttpd 1.4.76
- Evertz 3080IPX

- Evertz 9080IPX
- PowerQUICC MPC8377E
- PHP 8.2.27
- Syslog-ng 3.31.2
- OpenSSL 3.0.14
- FMO 3.0.9

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *MMA10G-IPX v3.5 Supplemental Administrative Guidance for Common Criteria*, Document Version 1.01, June 19, 2025. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled. In particular, it is important that steps are followed in the Configuration Guidance documentation to disable the ability of the rw_user role to perform updates, as [CPP_ND_V3.0E] restricts this function to the Administrator role.

Evaluation activities are strictly bound by the assurance activities described in [CPP_ND_V3.0E] and its accompanying Supporting Document. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: *MMA10G-IPX Series v3.5 Security Target*, Version 1.1, June 19, 2025.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1 Revision 5.
2. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
3. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
4. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
5. *Collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E].
6. *MMA10G-IPX Series v3.5 Security Target*, Version 1.1, June 19, 2025.
7. *Assurance Activity Report for MMA10G-IPX Series v3.5*, version 1.6, June 19, 2025.
8. *Evaluation Technical Report for MMA10G-IPX Series v3.5*, version 1.3, June 19, 2025.
9. *Test Plan for MMA10G-IPX Series V3.5*, Version 0.4, June 19, 2025.
10. *Vulnerability Assessment for Evertz MMA10GIPX Servies V3.5*, Version 1.6, June 10, 2025.
11. *IPX MMA10G-IPX v3.5 Supplemental Administrative Guidance for Common Criteria*, Version 1.1, June 19, 2025.
12. *Evertz MMA10G-IPX Equivalency Analysis*, Version 1.4, 05/09/2025.