National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



TM

Validation Report

for the

MMA10G-EXE Series

Report Number: CCEVS-VR-11670-2026

Dated: October 20, 2026

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

Jenn Dotson

Lisa Mitchell

Jaemond Reyes

Lori Sarem

Charles Schmidt

Joe Walton

The MITRE Corporation

Common Criteria Testing Laboratory

Fathi Nasraoui

Rupendra Kadtan

Intertek Acumen Security LLC

Table of Contents

1 Executive Summary 5

2 Identification 6

3 Architectural Information 7

3.1 TOE Description 7
3.2 TOE Evaluated Platforms 7
3.3 TOE Architecture 11
3.4 Physical Boundaries 12

4 Security Policy 14

4.1 Security Audit 14
4.2 Cryptographic Support 14
4.3 Identification and Authentication 15
4.4 Security Management 16
4.5 Protection of the TSF 17
4.6 TOE Access 17
4.7 Trusted Path/Channels 17

5 Assumptions & Clarification of Scope 18

5.1 Assumptions 18
5.2 Clarification of Scope 18

6 Documentation 19

7 TOE Evaluated Configuration 20

7.1 Evaluated Configuration 20
7.2 Excluded Functionality 20

8 IT Product Testing 21

8.1 Developer Testing 21
8.2 Evaluation Team Independent Testing 21

9 Results of the Evaluation 22

9.1 Evaluation of Security Target (ASE) 22
9.2 Evaluation of Development Documentation (ADV) 22
9.3 Evaluation of Guidance Documents (AGD) 22
9.4 Evaluation of Life Cycle Support Activities (ALC) 23
9.5 Evaluation of Test Documentation and the Test Activity (ATE) 23
9.6 Vulnerability Assessment Activity 23
9.7 Summary of Evaluation Results 24

10 Validator Comments & Recommendations 25

11 Annexes 26

12 Security Target 27
13 Glossary 28
14 Bibliography 29

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the MMA10G-EXE Series solution, provided by Evertz Microsystems Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government, and no warranty of the TOE is either expressed or implied.

The evaluation was performed by the Acumen Security Common Criteria Testing Laboratory (CCTL) in Rockville, MD, and completed in October 2026. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, 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, 6 December 2023.

The TOE is the MMA10G-EXE Series. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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. 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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.

The technical information included in this report was obtained from the *MMA10G-EXE Series Security Target*, version 1.2, October 1, 2026, and analysis performed by the Validation team.

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) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Accreditation Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology 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-EXE Series
Protection Profile	*collaborative Protection Profile for Network Devices*, Version 3.0e, 6 December 2023
Security Target	*MMA10G-EXE Series Security Target*, version 1.2, October 1, 2026
Evaluation Technical Report	*Evaluation Technical Report for MMA10G-EXE Series v1.11*, version .07, 13 October 2026
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)	Intertek Acumen Security Rockville, MD
CCEVS Validators	Jenn Dotson, Lisa Mitchell, Jaemond Reyes, Lori Sarem, Charles Schmidt, Joe Walton

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The MMA10G-EXE Series switches are comprised of TOE firmware version 1.11 based on Linux 6.12 (CIP SLTS). The TOE appliances are Ethernet switches optimized for video content.

3.1 TOE Description

The MMA10G-EXE Series switches are Internet Protocol (IP) switches optimized for video-over-IP traffic (compressed or uncompressed). The TOE is classified as a network device (a generic infrastructure device that can be connected to a network). Models of the TOE included in the evaluation provide identical functionality. The only differences between them are the supported speed, the physical size, and the number of physical interfaces supported, and the processor.

The TOE builds on the capabilities of the existing Evertz line of video routing switches. Video routers receive video signals in various formats, such as Serial Digital Interface (SDI), Serial Data Transport Interface (SDTI), or Asynchronous Serial Interface (ASI), and switch dedicated physical input ports to dedicated physical output ports based on external commands.

The TOE provides the same capability within the context of packet-based networks using shared network infrastructure. The TOE provides a packet-based switching fabric from a video perspective, rather than relying on traditional packet-based network architecture.

3.2 TOE Evaluated Platforms

The TOE firmware is version 1.11 based on Linux 6.12 (CIP SLTS).

The TOE hardware devices are defined below:

Table 2: TOE Models

Model	AV/ Broadcast	Supported Ports	Form Factor **	Chassis Supported	Frame Controller	Processor
MMA10G-EXE16	AV	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
MMA10G-EXE26	AV	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)

MMA10G-EXE36	AV	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
MMA10G-EXE3.0	AV	16x DD QSFP cages per line card	9	EXE	EXE3-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-16-10G-A1	Broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-16-25G-A1	Broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-26-10G-A1	Broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-26-25G-A1	Broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-36-10G-A1	Broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-36-25G-A1	Broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-16-10G-A2	Broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-16-25G-A2	Broadcast	16 x QSFP28 cages per line card	16	EXE	EXE16-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)

EXE2.0-26-10G-A2	Broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-26-25G-A2	Broadcast	16 x QSFP28 cages per line card	26	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-36-10G-A2	Broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
EXE2.0-36-25G-A2	Broadcast	16 x QSFP28 cages per line card	36	EXE	EXE-FC-NCS	Intel(R) Xeon(R) CPU E3-1505M v5 (Skylake)
NATX-8-100G-CC	Broadcast	4 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
NATX-16-100G-CC	Broadcast	8 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
NATX-32-100G-1-CC	Broadcast	16 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
NATX-64-100G-2-CC	Broadcast	32 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-8-CC	AV	4 x DD QSFP (QSFP200G	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-16-CC	AV	8 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)

MMA10G-NATX-32-CC	AV	16 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-64-CC	AV	32 x DD QSFP (QSFP200G)	1	DragonFire frame	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-IPX128	AV	32 x QSFP+	3 or 6	EV Frame	Ev3-FC or Ev6-FC	Intel(R) Core(TM) i3-6102E (Skylake)
3080IPX-48-25G-CC	AV/broadcast	12 x QSFP+	3 or 6	EV Frame	Ev3-FC or Ev6-FC	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-128-CC	AV	32 x DD QSFP (QSFP200G and QSFP 400G))	1	Dragon Fire 2	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-LT-SFP-CC	AV	32xSFP + 8x DD QSFP	1	Dragon Fire	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-LT-QSFP-CC	AV	12xQSFP + 4x DD QSFP	1	Dragon Fire	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
MMA10G-NATX-LT-MP-CC	AV	32xSFP + 8x DD QSFP	1	Dragon Fire	N/A	Intel(R) Core(TM) i3-6102E (Skylake)
NATX-LT-1G-32SFP-6QSFPDD-CC	Broadcast	32xSFP + 8x DD QSFP	1	Dragon Fire	N/A	Intel(R) Core(TM) i3-6102E (Skylake)

**Form Factor: ** The number of line-card slots the chassis can hold, indicating the system's capacity.

3.3 TOE Architecture

The TOE consists of a device as specified in Section 3.2.

A typical TOE installation will also include a standard video routing switch software platform (such as Evertz Magnum) to route data between program streams in a manner sufficient to meet broadcast video standards for signal availability and integrity. Equipment to prepare video for IP transport, or to convert it into other video formats, and non-network-based video switching/processing, 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 TOE via a dedicated management workstation operating over an Out-of-Band Management (OOBM) network. Sites may close this OOBM network or may operate TOE within an existing OOBM as long as the topology is compliant with the security parameters listed below. Users and administrators may also access TOE software via direct connection using a terminal session.

The TOE generates audit logs and transmits the audit logs to a remote syslog server over an 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 systems’ via TLS

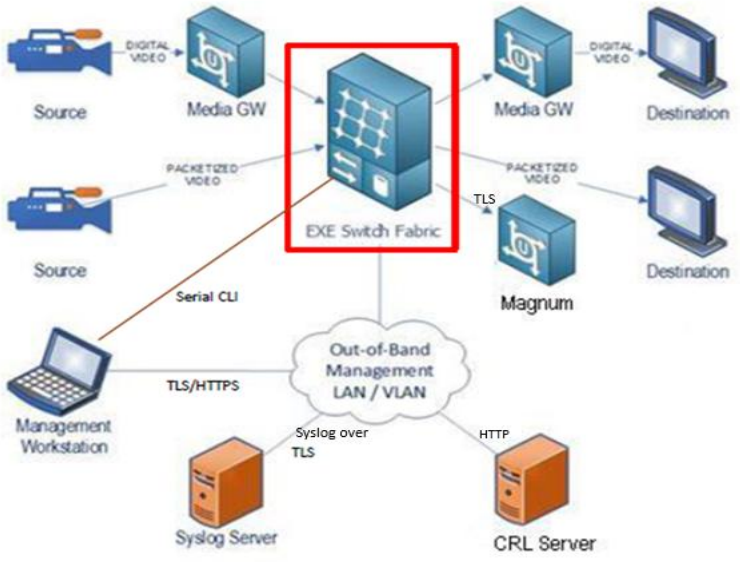


Figure 1 – Representative TOE Deployment

3.4 Physical Boundaries

The physical boundaries of the TOE are outlined in Section 3.3. The media and video components of the IT environment are NOT part of the TOE physical boundary. The required environmental components are shown Table 3 below:

Table 3 – TOE Physical Boundary 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, or Firefox • Supporting TLSv1.2 • Supporting Server Certificate authentication • Supporting at least one of the following ciphersuites: o TLS_RSA_WITH_AES_128_CBC_SHA

Component	Required	Purpose/Description
		○ 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	Yes	• Provides remote management of the TOE's routing and switching of video signals. • Supporting Mutual Authentication • Supporting at least one of the following ciphersuites: ○ 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 operations
Video Source devices	No	• Optional component for creating video streams that are sent to the TOE. Not required for TOE operations. • Supporting packetized or digital video streams.
Video Destination devices	No	• Optional component for receiving video streams that are sent from the TOE. Not required for TOE operations. • Supporting packetized or digital video streams

4 Security Policy

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

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. The Audit events generated by the TOE can be found in Section 1.3.2.1 of the ST.

The TOE can store the generated audit data on itself, and it can be configured to send syslog events to a syslog server, using a TLS protected collection method. Logs are classified into various predefined categories. The logging categories help describe the content of the messages that they contain. Access to the logs is restricted to only Security Administrators, who are authorized to edit them, 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 local console. The log records the time, host name, 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 3.5.4 with FIPS version 3.1.2 and Linux 6.12 (CIP SLTS) that implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS/HTTPS connections for secure management and secure connections to syslog and MAGNUM clients. TLS and HTTPS are also used to verify firmware updates. The cryptographic implementation for TOE relies on the EXE Cryptographic Module version 1.11. The cryptographic services provided by the TOE are further described below.

Table 4 – TOE Cryptographic Protocols

Cryptographic Protocol	Use within the TOE
HTTPS/TLS (client)	Secure connection to syslog 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_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 establishment for TLS. FCS_CKM.2, FCS_TLSC_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2
ECDSA	Provides components for EC-DH key establishment. FCS_CKM.1, FCS_CKM.2, 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_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” TOE users do not access TOE directly; they control IP video switching through the TOE using a switch control system, such as Evertz’s MAGNUM. The switching of those IP video transport streams 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. If the user fails to provide the correct authentication credentials, the user will be locked out after a configurable threshold until the user is manually unlocked by an Administrator.

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 TOE 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. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

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:

- 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 administer the TOE locally;
- 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 manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to configure the local session inactivity time before session termination or locking.

All these management functions are restricted to Security Administrators who are authorized to administer the TOE via a local CLI and a remote web interface. Administrators are individuals who manage specific types of administrative tasks. The TOE implements role-based access control of these management functions to users that have been identified, authenticated, and authorized with the Security Administrator role.

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 these services can be managed from the interface, 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 self-testing to ensure that its cryptographic functions operate correctly and that the TOE software is running the correct image.

An administrator initiates update processes from the web interface for all update installations. TOE automatically uses the RSA 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 described 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 and local console interface prior to allowing any administrative access to the TOE.

4.7 Trusted Path/Channels

The TOE allows the establishment of a trusted channel between a video control system (such as Evertz' Magnum) and the TOE. The TOE also establishes a secure connection for sending syslog data to a syslog server using TLS. 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 document:

- *collaborative Protection Profile for Network Devices*, version 3.0e, 6 December 2023 (NDcPP30e)

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 ST. 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 clarification. 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 assurance activities specified in the NDcPP30e and performed by the evaluation team).
- 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 Guides specified in Section 6, additional customer documentation was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP30e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

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

- *MMA10G-EXE Series Security Administrative Guide Addendum for Common Criteria*, version 0.4, September 17, 2026

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 TOE Evaluated Configuration

7.1 Evaluated Configuration

The IT Testing Environment Components used to test the TOE are detailed in Section 3.4. In addition, the platforms listed in Table 2 as detailed in Section 3.2 are within the scope of the evaluated platforms.

7.2 Excluded Functionality

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

- SNMP Traps (Alarms)
- SNMP
- VistaLINK PRO module
- Network Time Protocol (NTP) Server
- External Authentication Servers for administrator authentication (LDAP/LDAPS)
- SSH is by default disabled in CC Mode
- Rest API

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

In addition, TOE 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 TOE is a midpoint device and, therefore, does not perform encryption or decryption functionality. This functionality, while present in the TOE, was not evaluated.

8 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-EXE3.0*, version 1.6, 25 September 2026 and *Test Plan for NATX-32-100G-1-CC*, version 1.6, 25 September 2026, as summaries in the *Assurance Activity Report for MMA10G-EXE Series*, version 0.9, October 14, 2026.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the NDcPP30e. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. Specifically, the tested devices, test tools, and the test environment are documented in Section 4 of the AAR.

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 ETR. The reader of this document can assume that all assurance 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 MMA10G-EXE Series to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target (ASE)

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-EXE Series that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

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 (ADV)

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 and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the NDcPP30e related to the examination of the information contained in the TSS.

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.

9.3 Evaluation of Guidance Documents (AGD)

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 guide was assessed during the design and testing phases of the evaluation to ensure it was complete.

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.

9.4 Evaluation of Life Cycle Support Activities (ALC)

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 (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the NDcPP30e and recorded the results in the Test Reports, summarized in the AAR.

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.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the AVA report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluation team searched the following sites:

- https://av.evertz.com/
- https://nvd.nist.gov/
- https://www.cve.org/
- http://www.cvedetails.com/vulnerability-search.php

The Evaluation team performed the public-domain vulnerability searches using the following key words. Keyword searches were last performed on September 17, 2026:

MMA10G-EXE16	3080IPX-48-25G-CC	libcap-2.73
MMA10G-EXE26	MMA10G-NATX-128-CC	libconfuse-3.3
MMA10G-EXE36	MMA10G-NATX-LT-SFP-CC	libcurl-8.15.0
MMA10G-EXE3.0	MMA10G-NATX-LT-QSFP-CC	libtasn1-4.20.0
EXE2.0-16-10G-A1	MMA10G-NATX-LT-MP-CC	libxcrypt-4.4.38
EXE2.0-16-25G-A1	NATX-LT-1G-32SFP-6QSFPDD-CC	libxml2-2.13.8

EXE2.0-26-10G-A1	MMA10G-EXE Series 1.11	lighttpd-1.4.82
EXE2.0-26-25G-A1	EXE Cryptographic Module 1.11	nettle-3.10.1
EXE2.0-36-10G-A1	atftp-0.8.0	openssh-10.2p1
EXE2.0-36-25G-A1	binutils-2.45	openssl-3.5.4
EXE2.0-16-10G-A2	cjson-1.7.19	perl-5.40.2
EXE2.0-16-25G-A2	cpio-2.15	php-8.5.3
EXE2.0-26-10G-A2	dhrystone-2	python3-3.13.11
EXE2.0-26-25G-A2	dropbear-2025.88	python-urllib3-2.5.0
EXE2.0-36-10G-A2	expat-2.7.1	rpcbind-1.2.7
EXE2.0-36-25G-A2	glibc-2.41-70-g1502c248d58cb99a203731707987a4342926e830	rsync-3.4.1
NATX-8-100G-CC	gnupg2-2.5.18	rsyslog-8.2510.0
NATX-16-100G-CC	grub2-2.12	sqlite-3.51.0
NATX-32-100G-1-CC	iperf3-3.20	stunnel-5.76
NATX-64-100G-2-CC	iproute2-6.18.0	tar-1.35
MMA10G-NATX-8-CC	iptables-1.8.11	tcpreplay-4.5.2
MMA10G-NATX-16-CC	jitterentropy-library-3.6.1	thrift-0.13.0
MMA10G-NATX-32-CC	keyutils-1.6.3	wget-1.25.0
MMA10G-NATX-64-CC	libargon2-20190702	xxhash-0.8.3
MMA10G-IPX128		openssl FIPS provider 3.1.2

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 testing 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 highlights that the evaluated configuration is dependent upon the TOE being configured per the instructions in the Guidance document defined in Section 6. Note that the configuration includes setting the Session Handling to “Strict” mode in accordance with Section 2.4.10.4 of the Guidance document. No other versions of the TOE and software, either earlier or later, were evaluated.

The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Per NIAP/CCEVS Publication #6, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Annexes

Not applicable.

12 Security Target

MMA10G-EXE Series Security Target, version 1.2, October 1, 2026

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, April 2017.
2. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, April 2017.
3. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, April 2017.
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 (NDcPP30e).
6. *MMA10G-EXE Series Security Target,* version 1.2, October 1, 2026.
7. *MMA10G-EXE Series Security Administrative Guide Addendum for Common Criteria*, version 0.4, September 17, 2026.
8. *Assurance Activity Report for MMA10G-EXE Series*, version 0.9, October 14, 2026.
9. *Evaluation Technical Report for MMA10G-EXE Series v1.11*, version 0.7, October 13, 2026.
10. *Test Plan for MMA10G-EXE3.0*, version 1.6, 25 September 2026.
11. *Test Plan for NATX-32-100G-1-CC*, version 1.6, 25 September 2026.
12. *Vulnerability Assessment for MMA10G-EXE Series*, version 0.8, October 19, 2026.
13. *Evertz MMA10G EXE Equivalency Analysis*, version 1.4, October 1, 2026.