MMA10G-EXE SERIES II

Security Administrative Guide Addendum for Common Criteria

Version 1.5, August 12, 2024

EVERTZ MICROSYSTEMS LTD.
5292 John Lucas Drive
Burlington, Ontario
Canada L7L5Z9

Phone:	+1 905-335-3700		
Sales:	sales@evertz.com	Fax:	+1 905-335-3573
Tech Support:	service@evertz.com	Fax:	+1 905-335-7571
Web Page:	www.evertz.com	Twitter:	𝕏@EvertzTV

This page left intentionally blank !

Table of Contents

Table of Figures

1. Introduction

1.1 Audience

This document is targeted to administrators configuring the EXE Firmware, specifically for the following Evertz supplied EXE Series hardware devices,

- MMA10G-EXE16
- MMA10G-EXE26
- MMA10G-EXE36
- EXE2.0-16-10G-A1
- EXE2.0-16-25G-A1
- EXE2.0-26-10G-A1
- EXE2.0-26-25G-A1
- EXE2.0-36-10G-A1
- EXE2.0-36-25G-A1
- EXE2.0-16-10G-A2
- EXE2.0-16-25G-A2
- EXE2.0-26-10G-A2
- EXE2.0-26-25G-A2
- EXE2.0-36-10G-A2
- EXE2.0-36-25G-A2
- NATX-8-100G-CC
- NATX-16-100G-CC
- NATX-32-100G-1-CC
- NATX-64-100G-2-CC
- MMA10G-NATX-8-CC
- MMA10G-NATX-16-CC
- MMA10G-NATX-32-CC
- MMA10G-NATX-64-CC
- MMA10G-IPX128
- 3080IPX-48-25G-CC

This document assumes the administrator is an IT staff who has general IT experience as specified in the guidelines document CPP_ND_V2.2E section 4.2.4.

1.2 Objective

The objective of this document is to provide preparative and administrative measures for setting up the **EXE system in common criteria evaluated state**. It highlights the measures and administrative steps that are necessary to be undertaken to **configure and maintain** the EXE in the CC evaluated configuration. CC evaluated configuration is the configuration which is in line with the requirements defined in the Security Target (ST). This document is intended to cover all the ST requirements as summarized in chapter 3. Administrator should note that this document does not mandate configuration settings for the features that are outside the scope of CC evaluation.

Reference Number	Document Name	Resource Location
[1]	RFC 5424: Syslog Protocol	https://tools.ietf.org/html/rfc5424
[2]	RFC 5425: Transport Layer Security	https://tools.ietf.org/html/rfc5425
[3]	RFC 5280: X509 PKI Cert and CRL Profile	https://tools.ietf.org/html/rfc5280

1.3 Operational Environment

Component	Usage/Purpose
Syslog Server	A Syslog Server is required to offload audit logs. The syslog server shall meet the following: • Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management Workstation	The management workstation which is to be used for the management of the EXE device must be capable of supporting the following: • Use to manage Supporting TLSv1.2. • Supporting at least one of the following ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

CRL Server	• Conformant with RFC 5280.
Evertz Magnum Server	Evertz Magnum Server provides remote management of EXE's routing and switching of video signals. The communication channel between the EXE and the Magnum Server must be secured with following parameters: • Supporting TLSv1.2 with at least one of the following cipher suites: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Media Gateway	Media Gateways are component which converts media streams.
Video Destination Devices	Video Destination Devices are components which are used for viewing video steams output by EXE.
Video Source Devices	The Video Source Devices are components which feeds the video streams into the network

Note: *In the Common Criteria Evaluated Configuration, the use of a Syslog Server and a CRL Server which complies with the requirements above in the environment is a must. The Management workstation and the Magnum Server that are used must comply with the above stated requirements. While the media gateways, video destination devices, and video source devices stated above are supported, please note that in the Common Criteria evaluation performed for the MMA10G-EXE Series II, communication channels that are used for the communication with these devices were not tested.*

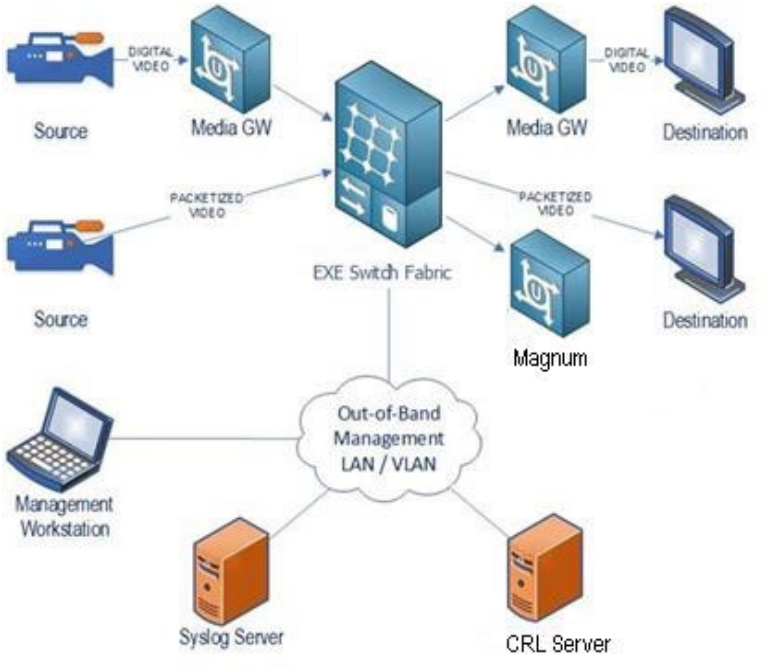


Figure 1 Typical EXE Network Topology Overview

2. Secure Installation

2.1 Obtaining and installing the CC Certified Firmware

2.1.1 Secure Delivery Verification

Before installing the Evertz EXE unit, you should take steps to ensure the unit has not been tampered with during transit. Perform the following checks to verify the integrity of the unit prior to installation.

1. Courier - Evertz only uses bonded couriers such as UPS, FedEx or DHL. Verify the shipment was received using a bonded courier.
2. Shipping information - Verify the shipment information against the original purchase order or evaluation request.
3. Verify the shipment has been received directly from Evertz.
4. External packaging - Verify the Evertz branded packing tape sealing the packaging is intact and the packaging has not been cut or damaged to allow access to the unit.
5. Internal packaging - Verify the unit is sealed in an undamaged. verify the internal box packaging is intact.
6. Warranty seal - Verify the unit's warranty seal is intact. The chassis cannot be opened without destroying the warranty seal.

If any concerns were identified while verifying the integrity of the unit, contact the supplier immediately.

2.1.2 Device Registration

Once the product is received and secure delivery is ensured, contact the Evertz sales team to register the product.

2.1.3 Physical security Requirements

Common Criteria compliant operation requires that you use the EXE in its Secure mode of operation and that you follow secure procedures for installation and operation of the unit. You must ensure that:

1. The EXE is installed in a secure physical location.

2. Physical access to the EXE unit is restricted to authorized operators.

2.1.4 Installing the unit

The documentation shipped with your unit includes a Start Guide and a model specific Hardware Supplement. The configuration guides, user guides, and administrative guides can be obtained after registering the product online.

Downloading the Common Criteria Certified firmware

The validated MMA10G-EXE firmware version is version 1.5.

The EXE is typically deployed in a closed network without direct access to the internet. In these instances, Administrators are required to contact Evertz to receive notification of production updates directly or via email blast.

Operators may verify the current version using the web interface.

Customers requiring secure delivery for site policy can request secure courier delivery of software updates. Digital delivery may be provided via secure file transfer, i.e., Microsoft OneDrive, etc.

2.2 Physical Installation

For physical installation steps related to EXE, administrators are advised to contact Evertz Support Team. Preparation of the physical site and network are not in the scope of this document.

2.3 Initial Configuration

The EXE should be given basic configuration through a local serial console connection prior to being connected to any network. The local console provides the local administrative access to the device. The subsequent section assumes that the administrator has sufficient knowledge in performing a serial connection from a workstation to EXE through necessary tools.

Once the administrator has successfully connected to a serial console and logged in with default supplied credentials, administrator is required to perform the following basic configuration steps to make the EXE operational in a target EXE network environment:

- Network Configuration
- System Utilities

2.3.1 Configuring the ‘recovery’ user for local console

The user ‘recovery’ is not available by default. The administrators shall use default IP and credentials to access the EXE via web GUI to create the recovery user.

Using the WebGUI, create an administrative user with the username ‘**recovery**’ to be used as the primary user for configuration via local console. Refer to section 3.1 for user configuration.

Note:

While any other user has the capability to access the local console, only the users with the ‘administrator’ role have the ability to modify device configurations. However, ONLY the ‘recovery’ user to be used for configuration over local console in the common criteria evaluated state. System administrators are responsible for strictly following these guidelines to be compliant with Common Criteria. Any other administrative user can be used in emergency situations and in situations where the ‘recovery’ user is locked out.

2.3.2 Accessing the EXE

Login via Web GUI

Steps

1. Using a web browser login to the EXE by entering “https://<IP address of the EXE>“.
2. Log in with username of the administrative user and the password.

Terminating Web Session

Prerequisites

- User already signed into the web session.

Steps

1. Click “**Logout**” button on top right corner.

Note: *No Configuration is required to obscure the password.*

Login via Local Serial Connection

Prerequisites

- Administrator is equipped with tools capable of making a serial connection to EXE:
    - o Serial Cable (Evertz 2x3 rainbow cable)
    - o Workstation
    - o Serial Connection Program (Putty, etc.)

Steps

1. Obtain the serial connection port (COM) in workstation.
2. Run your serial connection program (e.g.: Putty).
3. Set the parameters of serial connection.
    - o COM Port
    - o Bits Per Second: 115200
    - o Data Bits: 8
    - o Stop Bits: 1
    - o Flow Control: None
4. Confirm successful serial connection by ensuring that the login banner is displayed which is followed by the login prompt.
5. Login to the CLI using “recovery” user credentials.

Note:

Administrators can administer EXE locally through serial port connection. A console menu can be used to perform configurations tasks such as setting IP/system time/system reboot, etc.

Terminating Serial Console Connection

Prerequisites

- Successful local serial console connection to EXE.
- User has successfully logged in to the serial terminal using supplied credential.

Steps

1. Use the following until termination of the serial console connection.

   # X

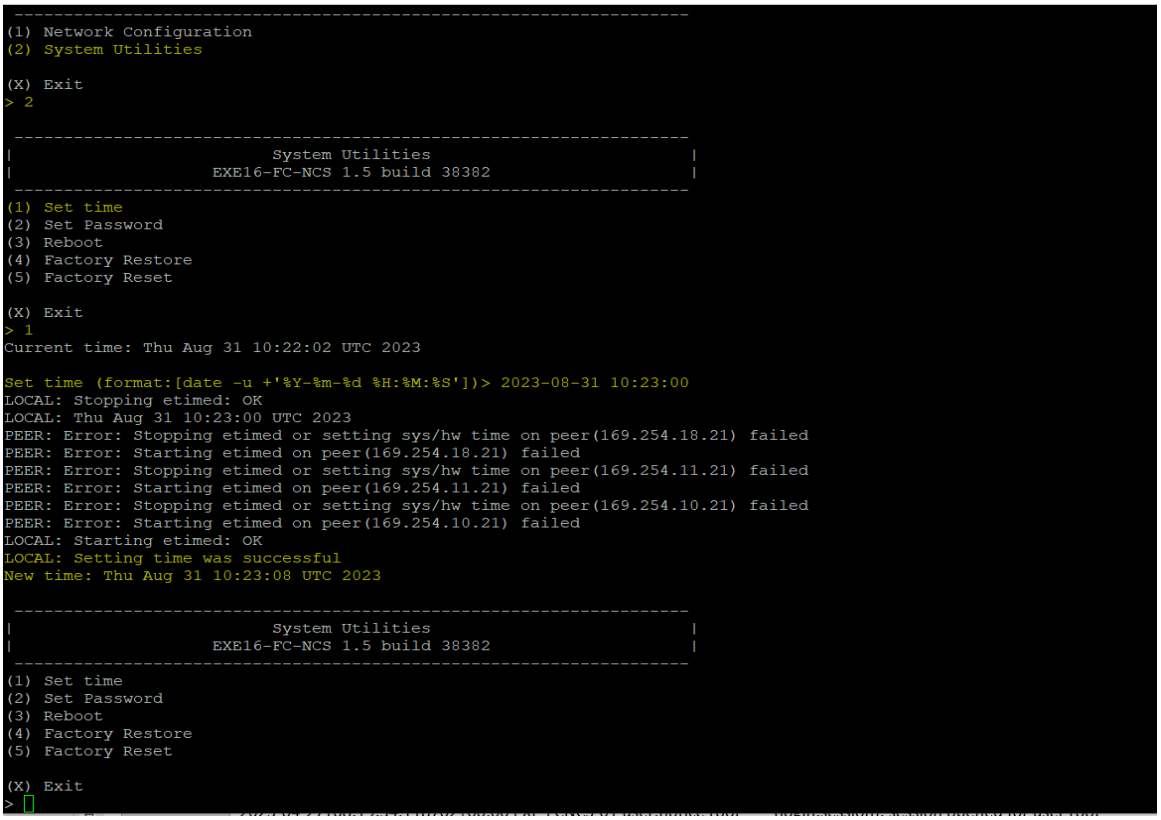
2.3.3 Configure System Date and Time

Prerequisites

- Successful local serial console connection to EXE.

Steps

1. Log in to the EXE serial console using “recovery” credentials.
2. Use the following to set the date of system.



Once in the ‘Set Time’ section, time can be set by using the following format:

`YYYY-MM-DD hours:minutes:seconds`

3. Press ENTER to apply the settings.

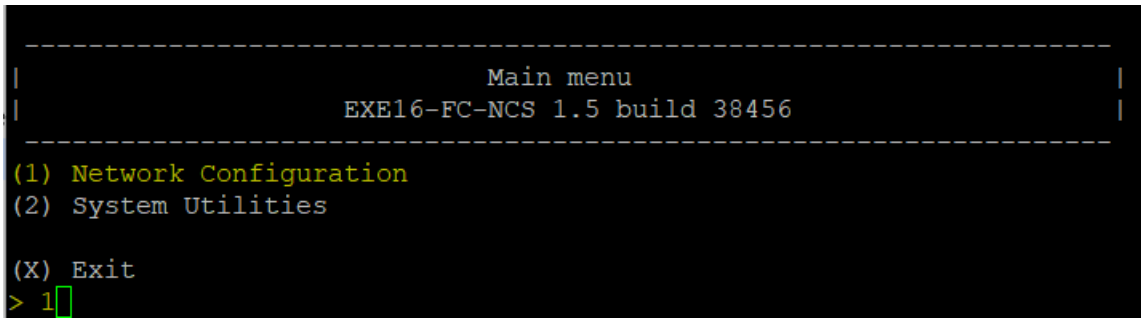
2.3.4 Network Configuration

Prerequisites

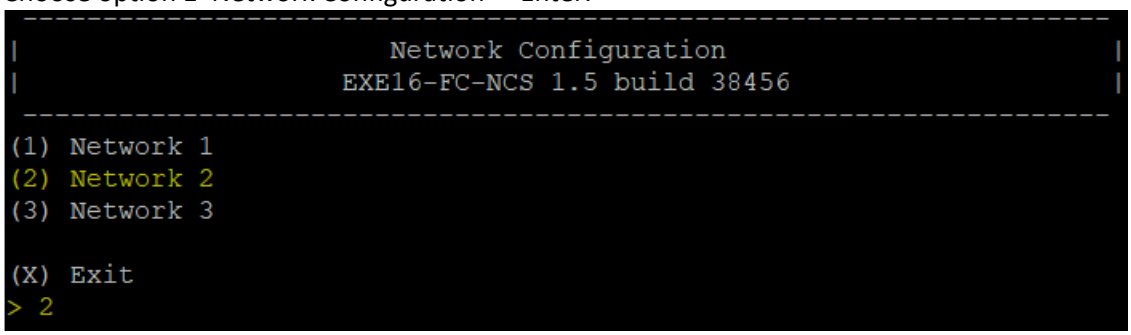
- Successful local serial console connection to EXE.
- Equipped with the following information regarding the EXE local network infrastructure:
  - IP Address Assigned for EXE Device by the network administrator.
  - Subnet Mask of the EXE network
  - Gateway of EXE network

Steps using serial console.

1. Login to the EXE serial console using “recovery” user credentials.
2. Use the following to set the network parameters.



Choose option 1 ‘Network Configuration’ > Enter.



Choose option 2 ‘Network 2” > Enter, you will get below screen to enter required IP Configuration Parameters.

```
Status:
ip:
netmask:
gateway:

Configure:
ip: 0.0.0.0
netmask: 0.0.0.0
gateway: 0.0.0.0

(1) Set IP
(2) Set Netmask
(3) Set Gateway

(X) Exit
>
```

Press option 1 ‘Set IP’ to enter IP Address of device, similarly you can press option 2/3 ‘Set Netmask’ / ‘Set Gateway’ to enter the required details as per below.

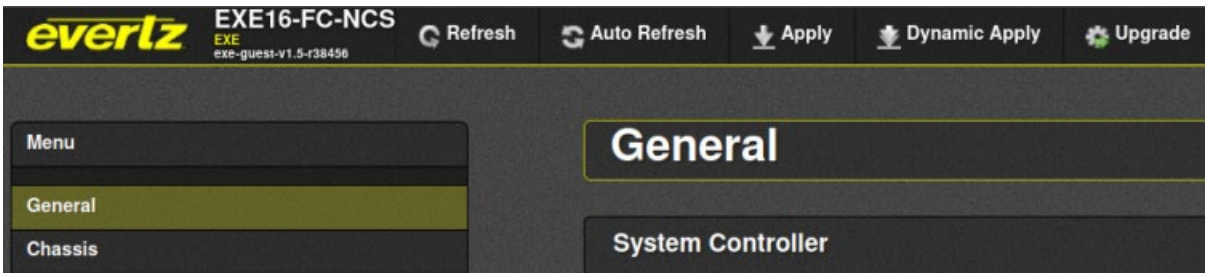
```
(1) Set IP
(2) Set Netmask
(3) Set Gateway

(X) Exit
> 1
Set IP> 1.1.1.1
notice: ctrl_net_red:ip changed from '0.0.0.0' to '1.1.1.1'
```

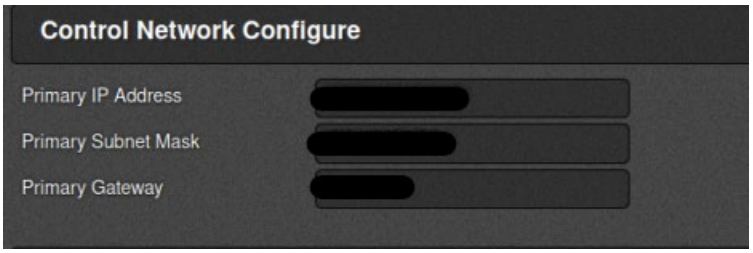
Note:

- *If we want to come out from the current selected option to previous option, we need to press “X”.*
- *Above example is for configuring the primary interface (Network 1), similarly secondary (Network 2) and service(Network 3) interfaces can be configured.*

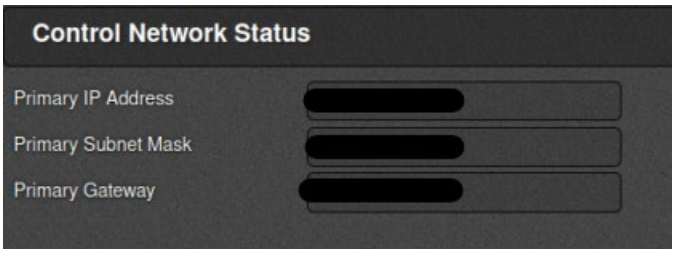
Steps using Web Access.

1. Login to the EXE Web Access using “root” credentials.
2. In the General Tab go to section "Control Network Configure" to set values of network parameters.





3. For reading the active configuration used by the system, go to section "Control Network Status" in the General Tab.



2.4 Secure Configuration

2.4.1 Configure Secure Mode

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**General**" menu.
3. Select System Controller → Secure Mode drop-down list.
4. Select "**Enabled**" option, Confirm the pop-up dialog.
5. Click "**Apply**" button at the top of the displayed page*

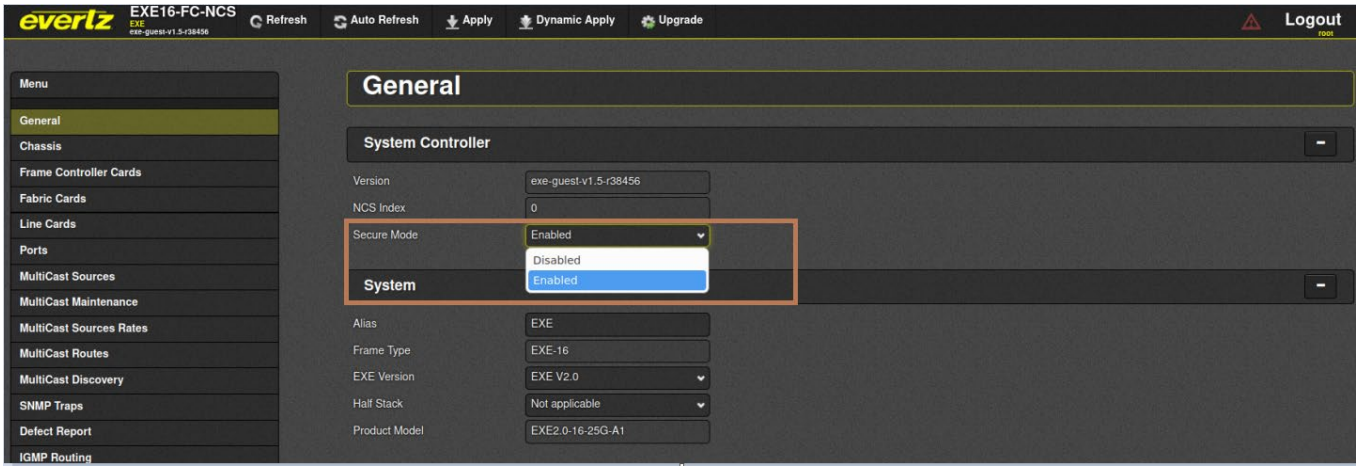


Figure 2: Enabling Secure Mode

6. Once the setting is applied, Reboot the device for the changes to take effect.

2.4.2 Verify Power-On Self-Tests

EXE performs FIPS power-up self-test to ensure all applications are in compliance with FIPS 140-2 Security Policy.

Prerequisites

- Completion of prior steps.
- Successful local serial console connection to EXE.

Steps

1. Reboot EXE
2. Verify that Signature Image verification and fips-self-test check are successful during console output on serial interface (refer to screenshots below for details) or in the syslog.

Successful Signature Image Verification

Look for line "**Starting power-on image sha256 checksum self-test**" followed by **"OK"**

```
[   36.507986] Run check for /etc/init.d/S024halfstack_auto-migrate
[   36.554902] Run check for /etc/init.d/S024mlnx_fw_update_ncs
[   36.601760] Run check for /etc/init.d/S025scrub_boot_images
[   36.643174] Runnning /etc/init.d/S025scrub_boot_images
Starting power-on image sha256 checksum self-test: OK
Starting scrub_boot_images : OK
[   38.354817] Run check for /etc/init.d/S026sensors_config_ncs
[   38.423195] Run check for /etc/init.d/S027smartd
[   38.465833] Runnning /etc/init.d/S027smartd
Starting smartd : [   38.559793] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: Rx/Tx
OK
Starting acpid: OK
```

Figure 3: Signature Image Verification

Unsuccessful Signature Image Verification

Instead of "**OK**" the output would be "**FAILED**". If the image verification fails, reboot the system after a few minutes. These few minutes will allow the image to be recovered from a redundant image. If the system does not boot up beyond this point, then the administrator is required to contact Evertz product support for further resolution.

Successful Self-Test Verification

EXE supports fips self-test during boot phase as well as during critical cryptographic operations.

Self-Test Verification During Boot

Look for line "**Enabling fipscheck: OK**" during boot up, if it is displayed, it is deemed that fips self-test during boot have run and succeeded.

```
Starting syslog compression: OK
Enabling fipscheck: OK
Generating 2048-bit rsa key... [   56.789769] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: Rx/Tx
OK
Starting sshd: OK
Starting stunnel: OK
Preparing snmpd security certificates: OK
Starting snmpd: OK
```

Figure 4: Self-Test Verification

Unsuccessful Self-Test Verification During Boot

If fips self-test verification during boot failed following output is produced in console or syslog

"**Enabling fipscheck: Failed"**

The system allows you to boot beyond this point, but it is not operable in CC evaluated state. The administrator is required to contact Evertz product support for further assistance and resolution.

Self-Test Verification During Critical Operation

Look for line "**FIPS object module self-test succeeded**."

```
2020-05-30T19:54:56.361518+00:00 3080IPX-128-1E-BE-95 user.info sshd 13642 - - FIPS object module self-test succeeded.
2020-05-30T19:54:56.367396+00:00 3080IPX-128-1E-BE-95 auth.info sshd 13642 - - FIPS mode initialized
2020-05-30T19:54:56.444144+00:00 3080IPX-128-1E-BE-95 auth.info sshd 13642 - - Accepted publickey for root from 10.50.4.33
2020-05-30T19:54:56.529167+00:00 3080IPX-128-1E-BE-95 user.notice root - - - (login:session): session opened for user root
2020-05-30T19:54:56.671428+00:00 3080IPX-128-1E-BE-95 user.info python2 13676 - - FIPS object module self-test succeeded.
```

Figure 5: Self-Test during critical operation.

***Note:** Self-test checks are done dynamically as applications start every time. During the bootup the FIPS self-tests are done. If the self-test verification passes during the bootup, the following audit message will be generated.*

If self-test verification fails during any critical operation, the following output is produced in console or syslog, and applications that require FIPS support will fail to start.

"**FIPS object module self-test failed.**"

Please contact Evertz product support for further assistance and resolution.

2.4.3 Verify Secure Mode Banners

Once secure mode is activated default banners will be displayed during serial console access as well as web-console access. The administrator should verify this activation before proceeding to subsequent steps.

Verify Serial Console Banner

Prerequisites

- Completion of prior steps
- Successful local serial console connection to EXE

Steps

1. A default banner displaying that the system is secured and specifying purpose and acceptance criteria will be displayed on console screen.

```
You are accessing a U.S Government (USG) Information System (IS) that is provided for USG-authorized use
 only.
By using this IS (which includes any device attached to this IS), you consent to the following condition
s:
-The USG routinely intercepts and monitors communications on the IS for purposes including, but not limi
ted to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM
), law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, and are subject to routine monitoring
, interception, and search, and may be disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g. authentication and access controls) to protect USG interests--
not for your personal benefit or privacy.
-Notwithstanding the above, this IS does not constitute consent to PM, LE or CI investigative searching
or monitoring of the content of privileged communications, or work product, related to personal represen
tation or services by attorneys, psychotherapists, or clergy, and their assistants.  Such communications
 and work product are private and confidential.  See User agreement for details.


EXE-FCNCS-01 login:
```

Figure 6: Verify Secure Banner

Verify Web Console Banner

Prerequisites

- Completion of prior steps

Steps

1. Access Management Web Application from workstation browser
2. A default banner displaying that the system is secured and specifying purpose and acceptance criteria will be displayed on the web page.

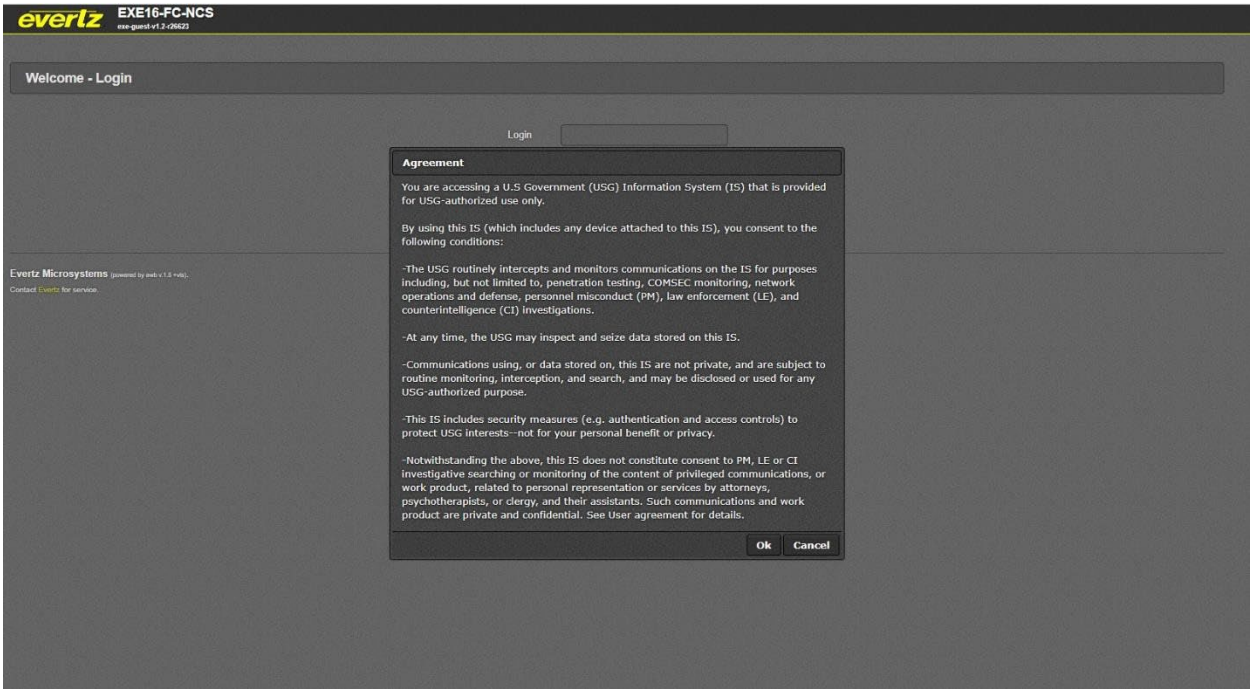


Figure 7: Verify Secure Access Banner

Once the user has enabled secure mode, it is mandatory to click “OK” to the agreement text displayed in the web console to administer EXE. If not, web console access is denied for that session.

2.4.4 FIPS Mode

EXE does not allow or provide interfaces for the administrator to configure/enable/disable fips mode separately, rather the functionality is enabled by default through the selection of secure mode.

2.4.5 Self-Test

EXE does not allow or provide interfaces for the administrator to configure/enable/disable self-test separately, rather during the boot up as well as during critical cryptographic operations the self-tests are run before hand and status of success and failure is audited through audit events.

Self-Test Outcomes/Errors

- “Enabling fipscheck: OK”: Successful self-test
- “Enabling fipscheck: Failed”: Failure self-test

2.4.6 Data Encryption/Decryption Modes

EXE only supports AES encryption and decryption in CBC and GCM modes with key sizes 128 and 256 for TLS. AES_CTR_384 is used for Random Bit Generation. All these modes and key sizes are supported by default and EXE does not allow or provide interfaces for the administrators to configure data encryption and decryption parameters. Parameters are hard coded implicitly in accordance with the CC evaluation criteria.

2.4.7 Cipher Suites

EXE does not allow or provide interfaces for the administrator to configure/enable/disable cipher suites. Rather EXE by default supports the following cipher suites in compliance with CC evaluation criteria implicitly. No configuration is needed or possible in both cipher suites selection and RNG.

- 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

2.4.8 Key Parameters

EXE accepts 2048-bits, 3072-bits, and 4096-bits RSA keys from the TLS Clients and TLS Servers (with mutual authentication) but EXE only generates 2048-bit RSA keys during Certificate Signing Request generation. EXE does not allow or provide interfaces for the administrator to configure key parameters such as the RSA key size or elliptic curves. Parameters are hard coded implicitly in accordance with the CC evaluation criteria.

2.4.9 Hash and Keyed-Hash Algorithms

EXE does not allow or provide interfaces for the administrator to configure Hash or Keyed Hash algorithm parameters; Parameters are configured implicitly in accordance with the CC evaluation criteria. By default, EXE supports SHA-1, SHA-256, SHA-384 hash algorithms and HMAC-SHA1 with 160-bit key, HMAC-SHA256 with 256-bit key, HMAC-SHA384 384-bit key keyed hash algorithms.

2.4.10 Configure Access Controls

EXE supports the following features for provision of access control:

- Preventing unauthorized access.
- Password strength & complexity configuration.
- Session-timeout configuration.
- Maximum login attempts enforcement.

Unauthorized Access Prevention

By default, EXE class of switches supports unauthorized access prevention using username/password combinations. The administrator can access and configure the EXE class of switches through the following methods:

- Management Web Application
- Local Serial Port Communication

The above access methods are protected from unauthorized access using username and password access protection. In addition to this the EXE provides additional layers of security through the following:

- Password strength & complexity support
- Automatic session-timeout support
- Maximum login attempts enforcement (Please note, this is applicable only to web application, for serial console connection maximum login attempt enforcement is not applicable)

Secure Passwords

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Settings**" button at the bottom right of the displayed index page.
3. Click **"Login**" tab at the displayed **Settings** page.
4. Under "**Password**" section select "**Password Strength**" to "**Strong**".
5. Click "**Apply**" button.

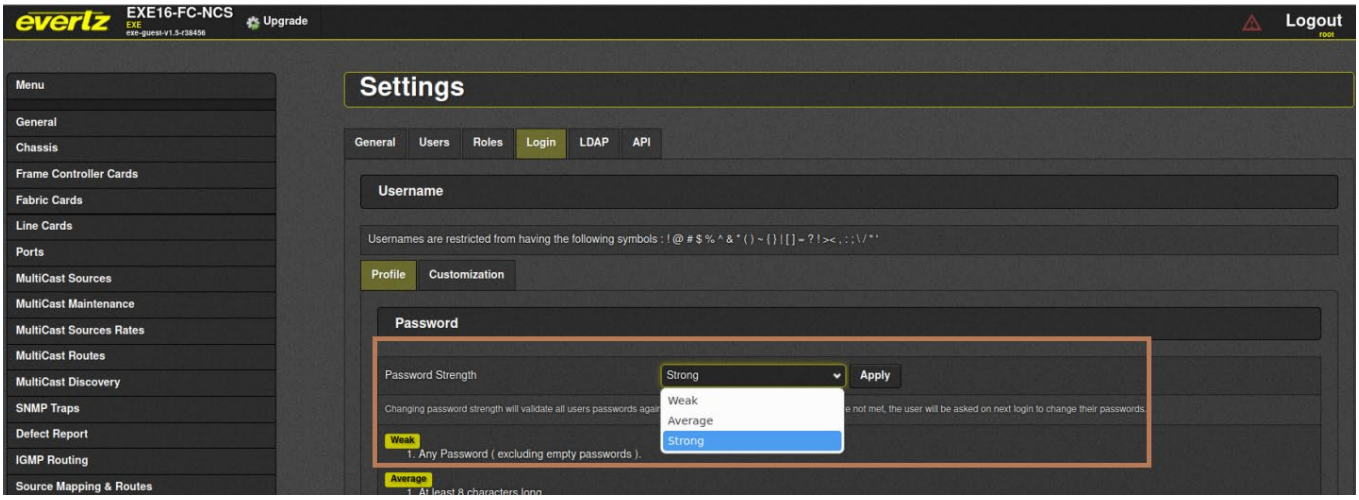


Figure 8: Secure Passwords

Once the above choice is made, EXE mandates following in terms of password requirement,

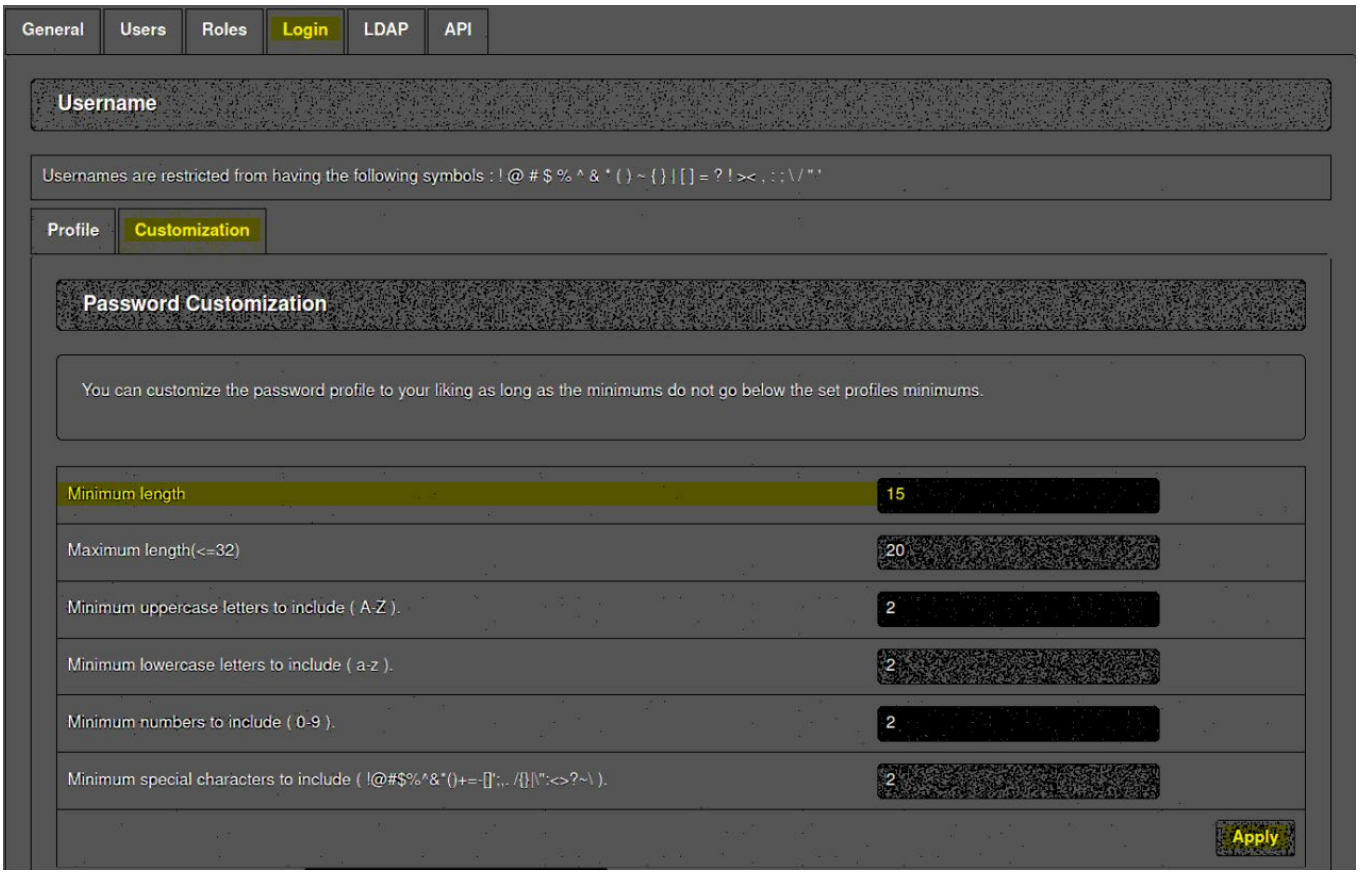
a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*"!", "@", "#", "$", "%", "^", "&", "*", "(", ")", ["~", "`", "_", "-", "+", "=", "{", "[", "}", "]", "|", "\", ":", ";", (''), (')*, "<", ",", ">", ".", "?",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

b) Minimum password length is set to 15 characters by default.

To configure minimum password length between 15 to 20 characters,

a) Click on "Customization" Tab

b) Enter the desired password length in the field for “minimum length” as shown in below image:



c) Click on “Apply” tab to finalize changes.

Note:

Once the password complexity setting is applied, it will be applied to both console and WebGUI user logins.

Set Session Timeout

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click “**Settings**” button at the bottom right of the displayed index page.
3. Click **“Login**” tab at the displayed **Settings** page.
4. Under “**Session**” set “**Timeout**” to well under 300.
5. Click “**Apply**” button.

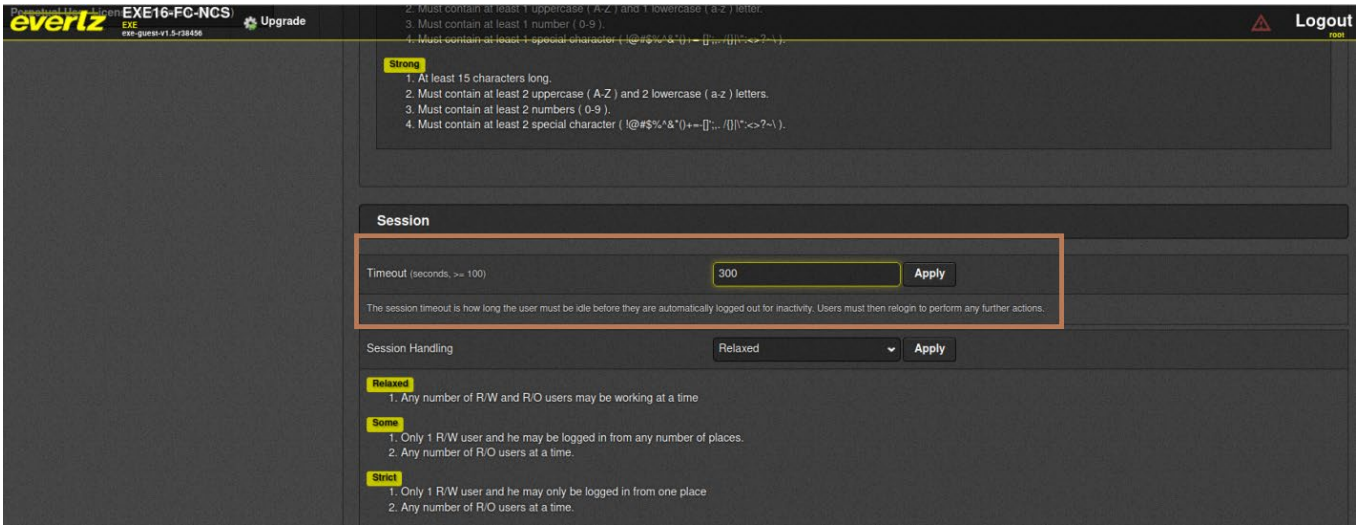


Figure 9: Set Session Timeout

Note:

Once the session timeout setting is applied, it will be applied to both console and WebGUI sessions.

Configure Session Handling

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Settings**" button at the bottom right of the displayed index page.
3. Click **"Login**" tab at the displayed **Settings** page.
4. Scroll down to Session segment.
5. Set "**Session Handling**" to "**Strict**".
6. Click "**Apply**" button.

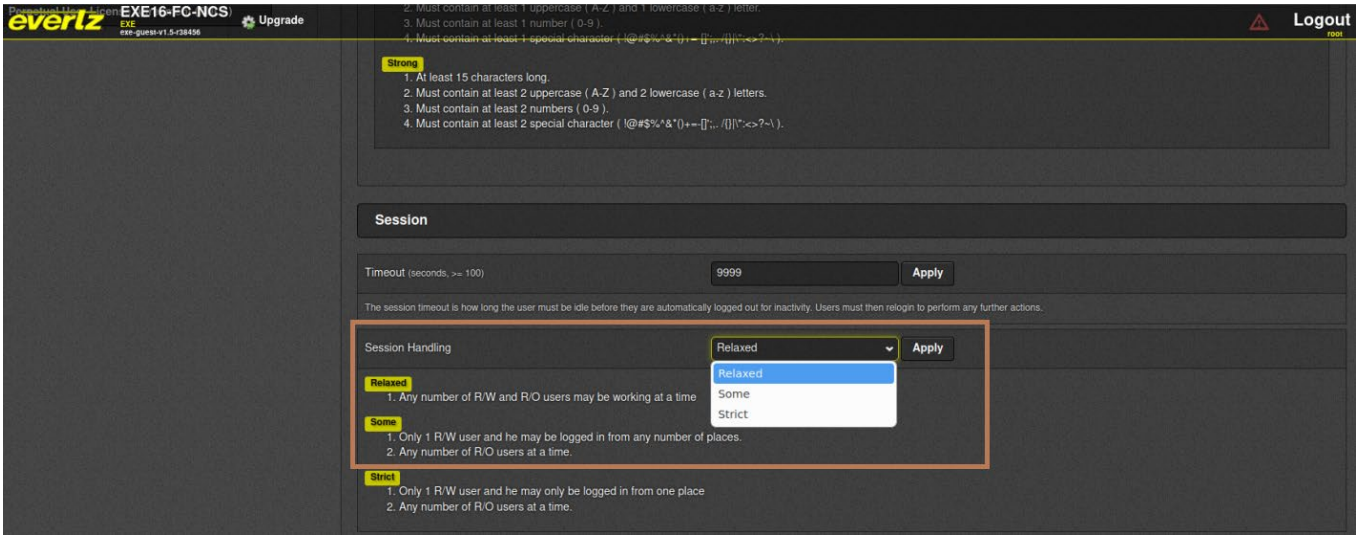


Figure 10: Strict Session Handling

Note:

Once the session handling setting is applied, it will be applied to both console and WebGUI sessions.

Limit Login Attempts

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Settings**" button at the bottom right of the displayed index page.
3. Click **"Login**" tab at the displayed **Settings** page.
4. Scroll down to **Login** segment at the bottom of the **Settings** page.
5. Set "**Max Failed Login Attempts**" to an acceptable value between "**3**" and "**20**".
6. Click "**Apply**" button.

Note:

Above limit login attempt is applicable for WebGUI session. It is not applicable for local console sessions.
This ensures that authentication failures cannot lead to a situation where no administrator access is available.

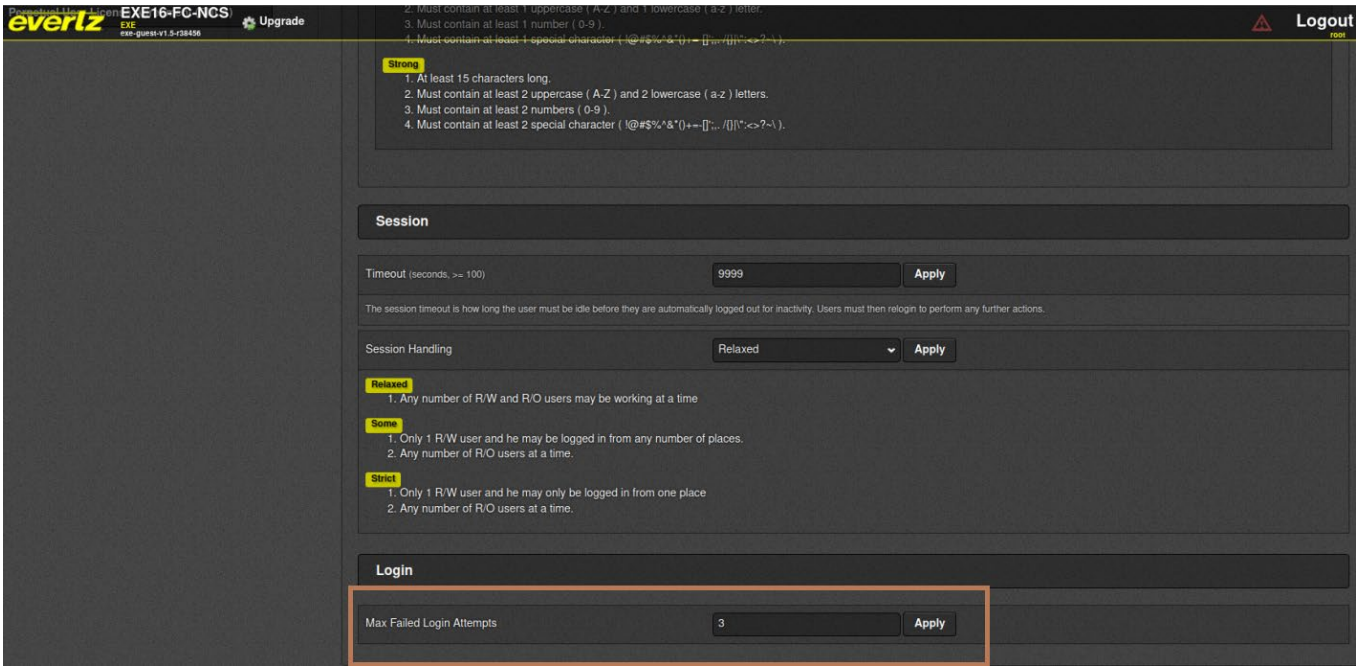


Figure 11: Set Max Attempts

Configure Secure Access Banner

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Perpetual User License Agreement (PULA)"** menu from menu list on left.
3. Insert applicable text in "**Agreement Text**".
4. Insert applicable text in "**Disagreement Text**".
5. Click "**Apply**" button at the top of the page.

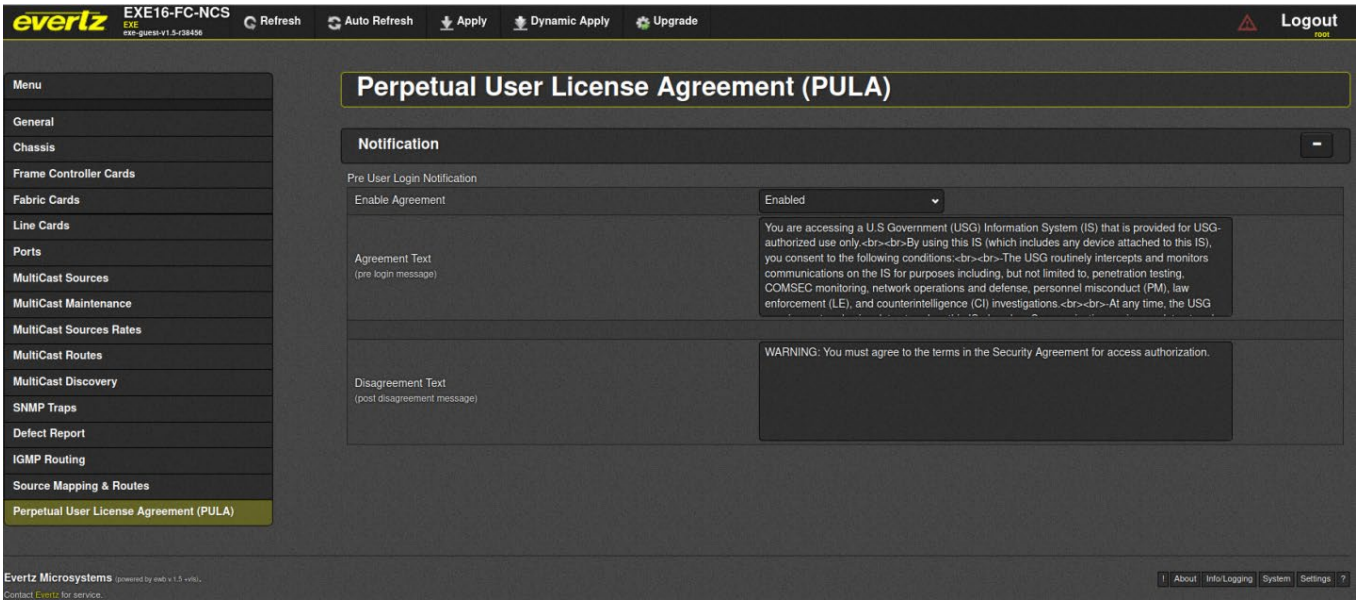


Figure 12: Configure Access Banner

For verification of Banner Change, see prior section on banner verification.

Disable the following features in CC evaluated configuration.

Disable REST API

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**settings**" button from bottom-right of the displayed index page.
3. Click "**API**" tab in the displayed "**Settings**" page.
4. Click "**EV**" tab under "APIs" segment.
5. Select "**Enabled**" to "**OFF**" position.
6. Click "**Apply**".
7. Repeat steps 5 to 6 for tabs "**PT**" and "**RT**".

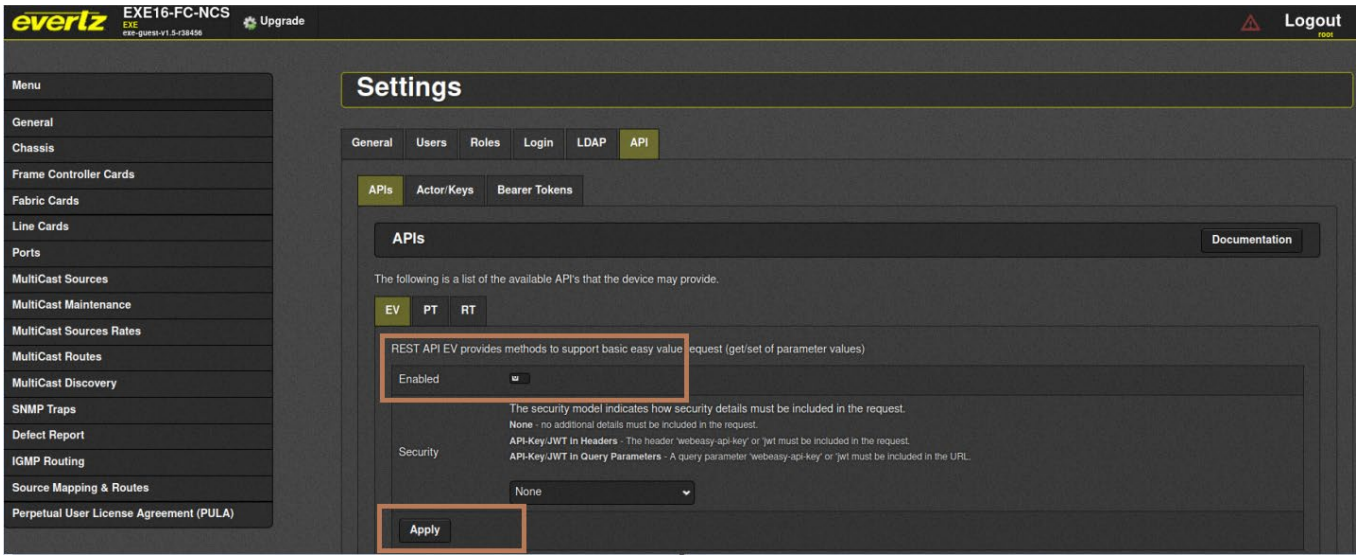
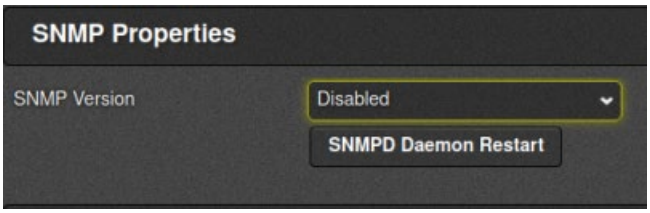


Figure 13: Disable REST API

Disable SNMP

General>SNMP Properties>Version set to "Disabled".



Disable NTP

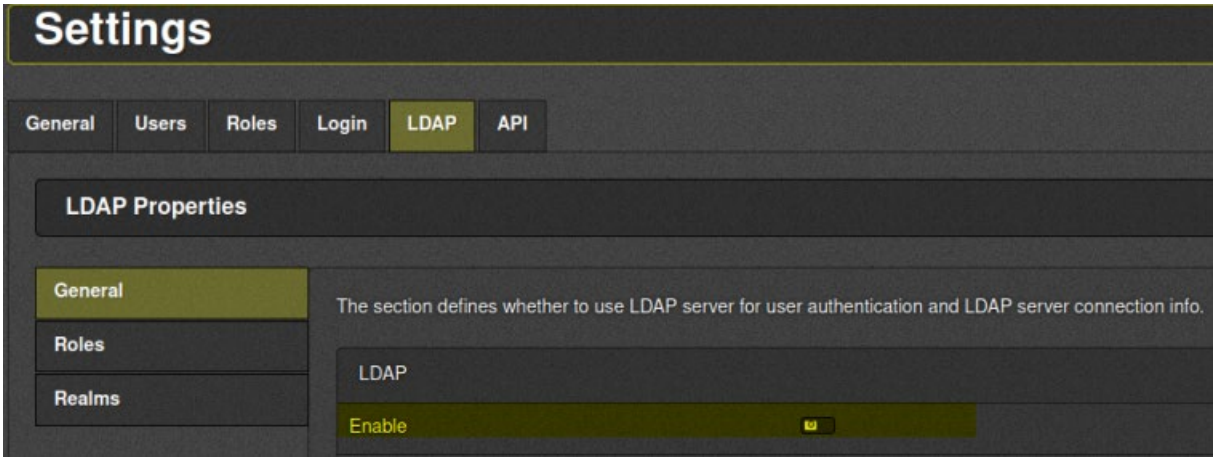
General>Time Server Configure>Time Server 0,1,2>IP empty them.

Disable LLDP streaming

Info/Logging>Log Streaming>LLDP>Enable set to "Disabled".

Disable LDAP

Settings>LDAP>LDAP Properties>General>LDAP>Enable to off state.



2.4.11 Configure TLS Server

In EXE, both WebGUI and Synergy Server (Magnum) use TLS Server capabilities to provide secure communication between the clients and server. The TLS Server comes with the following functionalities:

- Supports ONLY TLSv1.2
- SSLv3 and SSLv2 ARE NOT supported.
- Implicit cipher suite selection
- Implicit Key-Exchange selection

For communication with Synergy Server (Magnum), TLS communication with mutual authentication is used. For both Synergy Server and the WebGUI, a client certificate that is generated using a CSR should be used.

Create Certificate Signing Request & Download

Prerequisites

- None

Steps

1. Login to the EXE **Management Web Application**.
2. Click on "**General**" Tab from left side menu items.
3. Click on "**Download**" button of "**CSR Regenerate And Download**" under Certificates section.

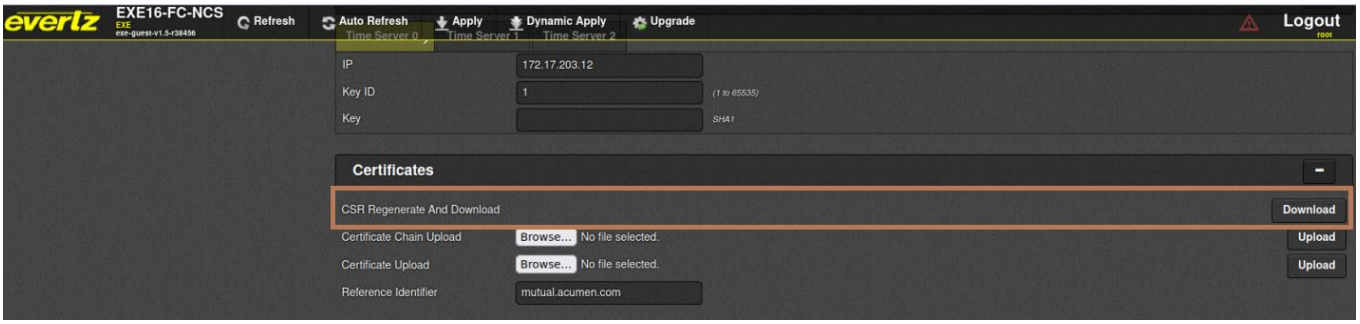


Figure 14: Generating and Downloading a CSR

Note: Reference-Identifier

*Only host names are used for reference identifiers, the product does not support IPV4 and IPv6 addressing in reference identifier. EXE allows configuration of 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 CN/SAN field. The verification against CN/SAN peer certificate is implemented within OpenSSL. A wildcard in the left-most label in the certificate will allow a successful connection, but a reference identifier without a left-most label as in the certificate, the connection will fail, i.e., awesome.com doesn't match *.awesome.com.*

Reference identifier is only used for synergy server communication with mutual authentication. No additional configuration is required for mutual authentication. The EXE will use mutual authentication for connection requests that are received from the configured reference identifier.

EXE does not allow the configuration of CSR parameters; the following default parameters are used. These parameters will be customizable starting v1.7.-

- Country Name: Canada
- State or Province Name: Ontario
- Locality Name: Burlington
- Organization Name: Evertz Microsystems Ltd.
- Organizational Unit Name: EXE
- Common Name: Configured primary IP address of EXE

- Email Address: support@evertz.com

Signing the CSR using a Public or Organizational Certificate Authority

The recommended practice is to use a public Certificate Authority (such as Verisign) or an Organizational Certificate Authority applicable to your organization to act as a CA for issuing EXE specific certificates.

Note:

- *Inquire about the policies pertaining to your organization from Organization's Cryptographic officer, Information Officer, or someone in similar capacity.*

Prerequisites

- Administrator has completed steps prior.

Steps

1. Submit the CSR generated in previous step to your Certificate Authority
2. Request your CA to provide the following.
    a. Signed Certificate for the CSR in PEM format.
    b. Certificate chain ordered by root CA on top in PEM format.

Upload Certificate Chain

Prerequisites

- Completion of prior steps
- Equipped with certificate chain applicable to the EXE Certificate Authority. The certificate chain should be in PEM format with ordering of root certificate at the top followed by hierarchical.
- Intermediate certificates if any.

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**General**" menu from Menus listed on left of the displayed index page.
3. Scroll down to "**Certificate**" section.
4. Click "**Choose File**" button of "**Certificate Chain Upload**" segment and select the trusted certificate chain provided by your CA from your file system.
5. Click "**Upload**".
6. A message informing the status of the upload will be displayed.

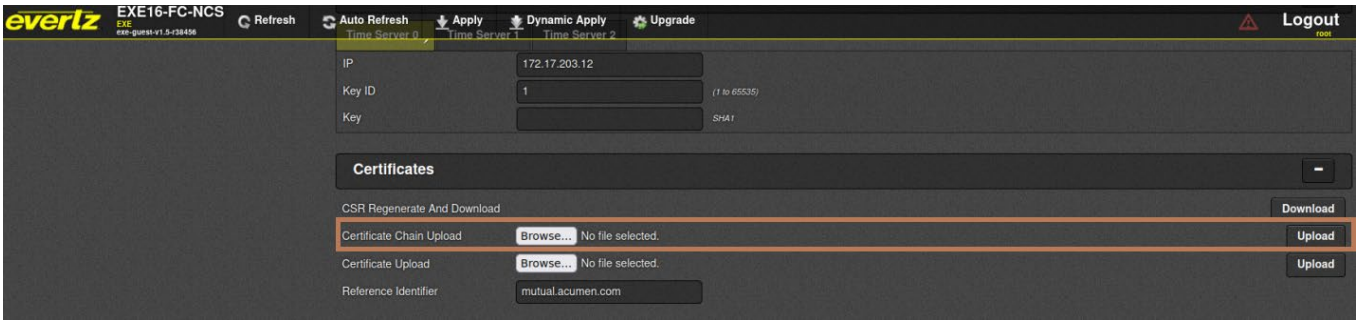


Figure 15: Upload Cert Chain

Note:

The above certificate chain is used for both synergy server as well as https web server.

EXE supports only one trust chain to be permitted at any given time. Subsequent upload overrides the previous trust chain. Multiple trust chains are not supported by EXE.

By default, Magnum and EXE use Default Evertz Root CA chain to make synergy communication between Magnum and EXE seamless, but they should be replaced according to this section.

Upload SSL Certificate

Prerequisites

- Completion of prior steps
- Equipped with signed certificate obtained from EXE's Certificate Authority

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**General**" menu from Menus listed on left of the page.
3. Scroll down to "**Certificates**" section.
4. Click "**Choose File**" button of "**Certificate Upload**" segment and select the CA signed SSL certificate provided by your CA from your file system.
5. Click "**Upload**".
6. Wait for Upload success status to be displayed.
7. Reboot EXE.

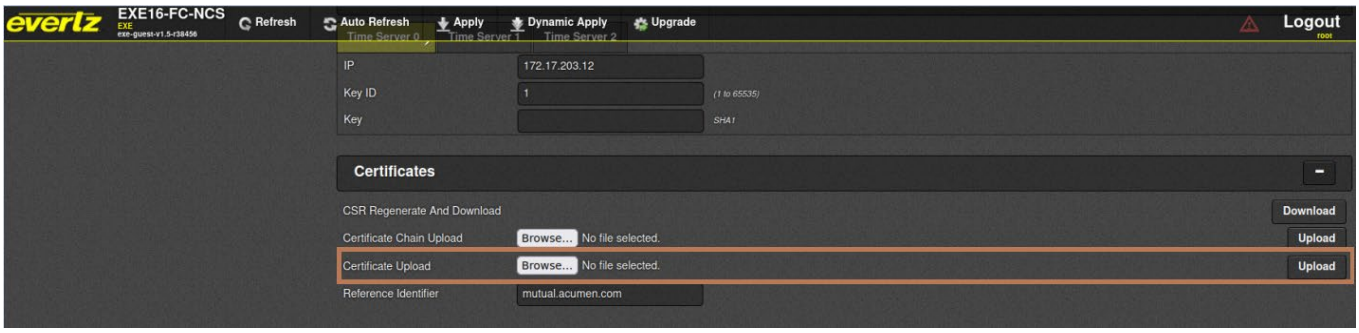


Figure 16: Upload SSL Certificate

Note:

The above certificate is used for both synergy server as well as https web server.

For all the TLS client and server connections, with the exception of 'revocation status verification failures', if the certificate verification fails for any other 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. The administrators must refer to the audit logs to identify what caused the failure. The detailed audit log description can be found in the 'Audit Events' section below. If the EXE is unable to reach a CRL Distribution Point, it will accept the certificate and the session associated with the certificate will be established, however, a log is generated indicating the reason for validation failure. The administrators must refer to the audit logs to identify what caused the failure.

By default, Magnum and EXE use Default Evertz Root CA chain signed certificate to make synergy communication between Magnum and EXE seamless, but they should be replaced according to this section.

In case of an unexpected connection failure of the synergy server communication channel, the synergy server will wait for the connection from the TLS client (Evertz Magnum device, 3rd party video routers/source devices). If no data is received, the synergy server will reset the connection after the TCP session timeout limit is reached. For connection recovery instructions with Evertz Magnum, please refer to the Evertz Magnum CC guide. For recovery information of the channels with other 3rd party video source and destination streaming devices, please refer to the administrative guidance documents of those specific devices.

2.4.12 Configure TLS Client

EXE supports secure TLS client configuration in compliance with the CC evaluation criteria. The rsyslog service client acts as a TLS client in the EXE system. TLS client capabilities are not used for any other functionality except remote rsyslog audit event functionality.

Prerequisites

- Completion of prior steps.
- Equipped with Certificate chain in PEM format obtained from EXE syslog server Certificate.

Authority.

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Info/Logging**" button from bottom-right of the displayed index page.
3. Scroll down to "**Log Streaming**" section of the displayed logging page.
4. Select "**Enabled**" under **Enable.**
5. Enter reference-identifier* (host name) of the target remote syslog server.
6. Enter remote log server IP address.
7. Enter remote log server log service port.
8. Select logging "Level".
9. Upload certificate chain applicable to EXE's syslog server Certificate Authority.
10. Click "**Upload**" button.
11. Click "**Apply**" button at the top of the page.

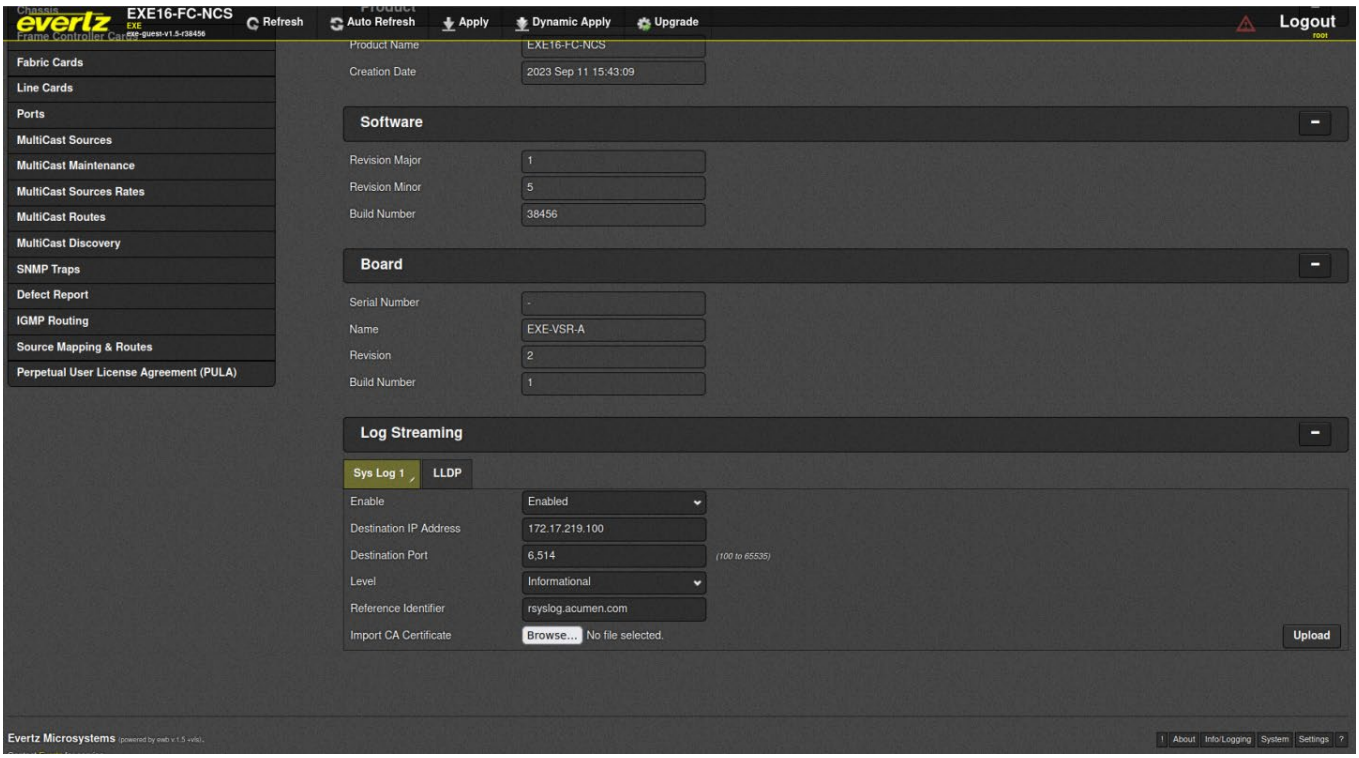


Figure 17: Secure Log Service

Once the above steps are complete, it is safe to assume that secure log upload is configured.

Note: Reference-Identifier*

Only host names are used for reference identifiers, EXE does not support IPv4 or IPv6 addressing in reference identifier. EXE allows configuration of 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 CN/SAN field.

*The verification against CN/SAN peer certificate is implemented within OpenSSL. A wildcard in the left-most label in the certificate will allow a successful connection, but a reference identifier without a left-most label as in the certificate, the connection will fail, i.e., awesome.com doesn't match *.awesome.com.*

Note:

For both TLS Server and TLS client only single certificate chains can be installed at any given time. Subsequent updates will override the previous certificate chains in the EXE certificate store.

For all the TLS client and server connections, with the exception of 'revocation status verification failures', if the certificate verification fails for any other 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. If the EXE is unable to reach a CRL Distribution Point, it will accept the certificate and the session associated with the certificate will be established, however, a log is generated indicating the reason for validation failure. The administrators must refer to the audit logs to identify what caused the failure. The detailed audit log description can be found in the 'Audit Events' section below.

3. Secure Management

3.1 User Management

EXE provides user management functionalities through Web interface. The Administrator is allowed to manage user accounts as required; the following section describes user management specifics as in compliance with the CC evaluated configuration. Contact Evertz for the default user accounts credentials.

Prerequisites

- Completion of prior steps

Steps

1. Login to the EXE "**Management Web Application**".
2. Click "**Settings**" displayed at the bottom of the displayed page.
3. Select "**Users**" tab.
4. The following screen will be displayed.

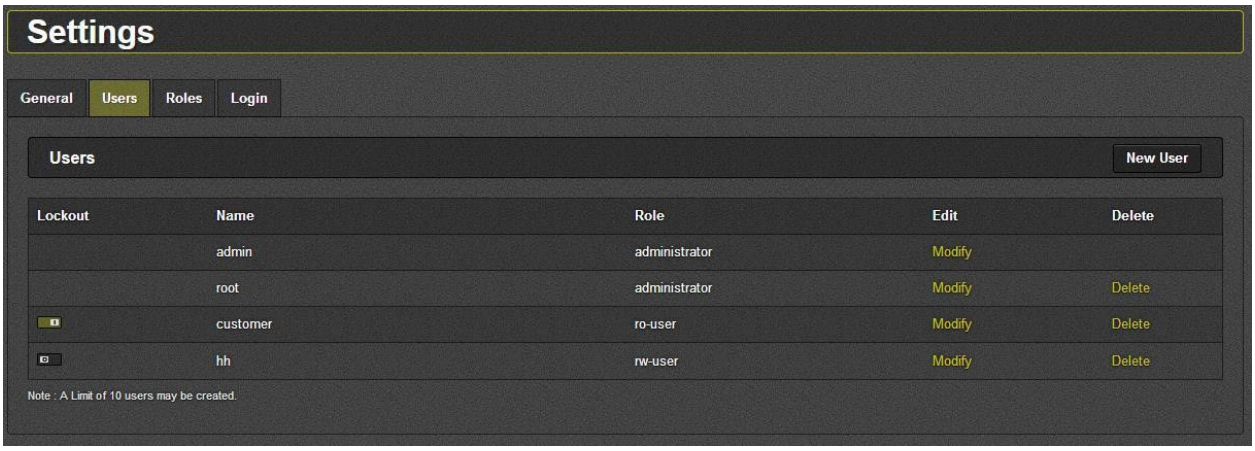


Figure 18: User Management

Following segment provide abstract description on user-management within the EXE;

Lockout: This button shows if the user is locked out for hitting the maximum number of failed authentication attempts. If the button is to the right (as shown for customer), the user is locked out and is not able to login. If the button is to the left (as shown for hh), the user is able login. An Administrator can move the button back to the "unlocked" position to allow a locked-out user to login in again.
Name: This field displays all usernames added to the system.

Role: This field lists the role user is assigned.

Edit: The *Modify* button is used to change role for given user. All roles can be modified except *admin*, which has full access by default.

New User: This control is used to add new users to the system. A name must be given to the user and a role selected from the drop-down menu. New roles can also be created in the *Roles* menu (as explained

in the section further below). The only accounts that should be established are the Security Administrator accounts.

Figure 19: New User Creation

Note: *The administrative accounts are used to manage and administer user accounts and assign roles. During initial login, there is a default administrative user account with default login credentials which must be changed by the user to meet organizational security requirements. Console serial access account with username "recovery" password can be changed by creating an administrator account with name "recovery" if not created already and changing its password. It is recommended that a new administrative account be created and used for day-to-day administration of EXE. The default account, with an updated password should be reserved as a back-up administrator if a lock-out occurs to the administrator on the web interface.*

New User: Confirmation Dialog

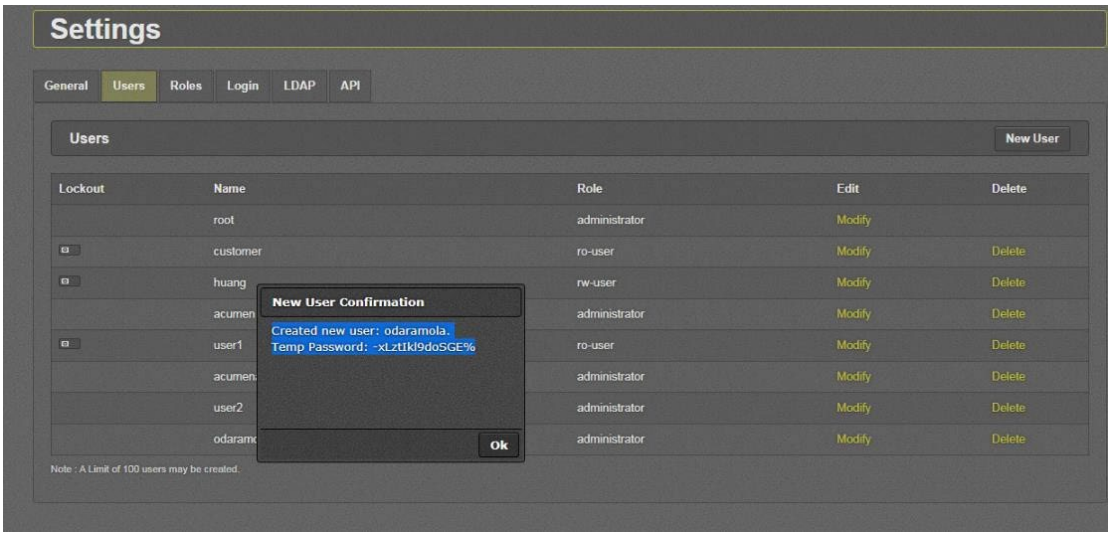


Figure 20: New User Confirmation

Roles: By default, there are three non-deletable roles on the system, administrator, rw-user, and ro-user. The Security Administrator is the only account that should be used with the role of this account set to administrator role.

1. **Administrator**: There are no limitations/restrictions for the administrator role.
2. **rw-user:** Users with this role can change the configuration of EXE, view the event log, and can perform firmware upgrades; but cannot create users with administrator access, cannot change general settings, cannot change user settings, and cannot change roles.
3. **ro-user:** Users with this role cannot change any EXE configuration settings, nor can they change any user settings. This role can only view EXE configurations, user settings, and event logs.

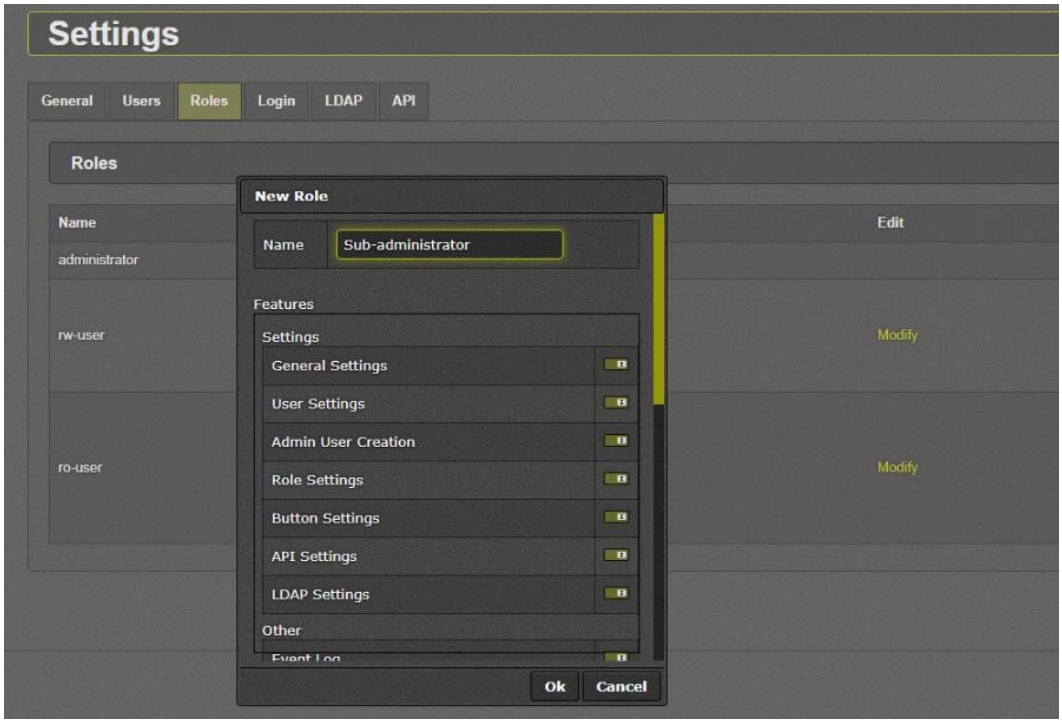


Figure 21: New Role Creation

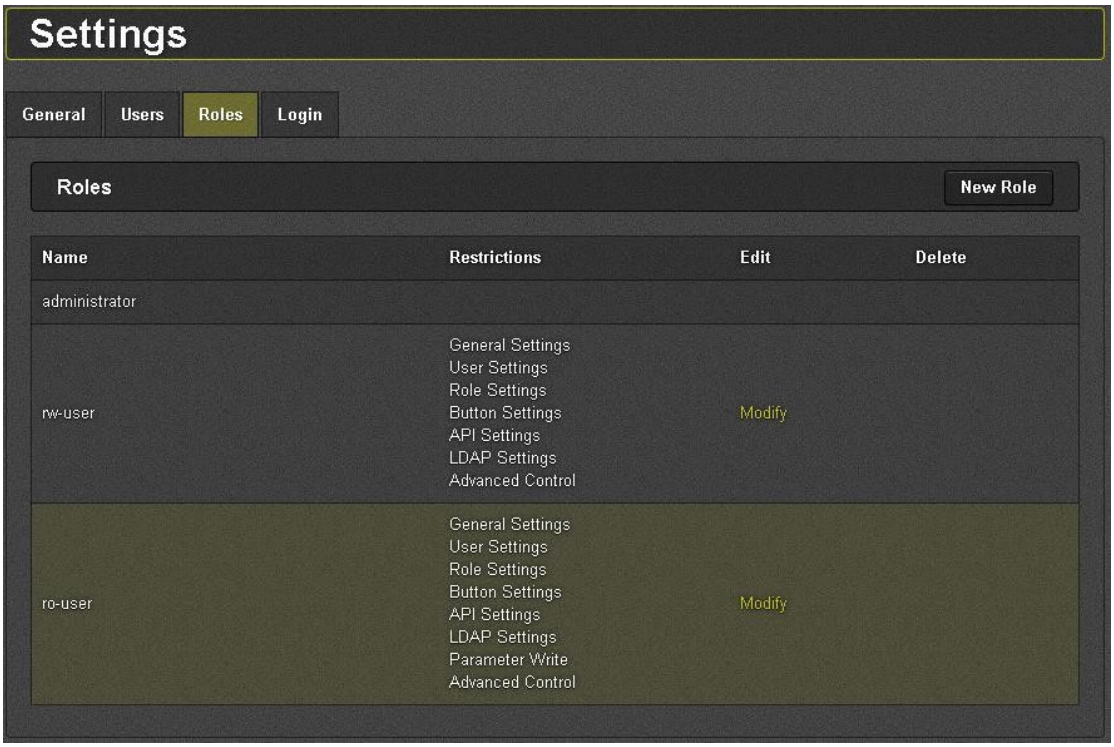


Figure 22: Roles Overview

Name: This field displays the names of all roles added to the system.

Restrictions: This field lists the restrictions given to each role. Blank indicates that no restriction is given to that role.

Delete: This control is used to permanently delete a role. All users that belong to the deleted role will be moved to ro-user role.

3.2 Certificate Management

- X.509 certificates are used to authenticate all TLS connections. A client certificate is sent whenever the server requests one. This functionality cannot be disabled.
- Only certificates in PEM format are supported (DER is not supported).
- Certificate Revocation Lists (CRLs) are downloaded from CRL-DP extensions during each connection attempt, if the peer certificates define them (only for end-user and intermediate certificates, not for root CA certificates).
- Recommend replacing the Evertz default CA and CRL during system setup, to replace them with organization-specific certificates.
- 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 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 EXE. Each certificate (other than the leaf 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 EXE for its own use those certificates are checked upon upload. When the EXE acts as a server for the WebGUI, it does not perform verification of its server certificate. When the EXE acts as a server for the Synergy (Magnum connection), it performs verification of every certificate in the chain, including its own certificate. The certificate presented by remote TLS clients using mutual authentication is validated during the establishment of a TLS connection.
- For an expired certificate, EXE will deny the connection.
- EXE also uses CRL to verify whether the leaf certificate or intermediate CA certificate has been revoked. During session establishment with EXE, any byte modification in the certificate will lead to the failure of connection. The CRLs are obtained from a CRL distribution point over HTTP and are refreshed according to the default CRL update-interval. This interval is not configurable. If the EXE is unable to reach the CRL DP it will accept the certificate and the session associated with the certificate will be established. An audit log is generated indicating that the CRL download failed.

3.3 Key/Cipher Management

All actions related to key management are done implicitly without the user's knowledge or involvement.

3.3.1 Zeroing Crypto Material

EXE implicitly does crypto shredding in compliance with the CC evaluation criteria during TLS Server configuration and subsequent actions.

The EXE class of switches comes with inbuilt tools to facilitate crypto shredding capability during end-of life of product.

Prerequisites

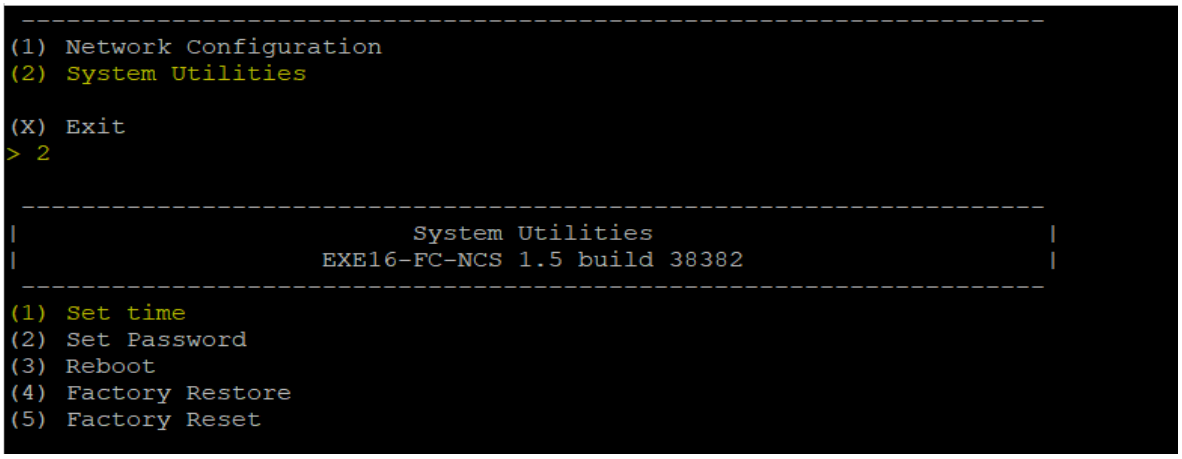
- EXE is no longer to be operational in Secure Environment or to be disposed permanently due to following motives.
    - Defect Product
    - Old Product
    - No further use in the EXE environment
- Local serial console connection

Steps

1. Login to the Console as the recovery user into the recovery menu.
2. Use the option **'System Utilities' >** '**Factory Reset**' to zeroize the Crypto material including private keys.

Please note that using Factory Reset option will wipe the existing configuration. Ensure that the configuration is backed up prior to using this option.

3. This will reboot EXE. Administrators should ensure that the EXE is back in Secure Mode to ensure that it is being used in the CC evaluated configuration.



Note: *Once Factory Reset command is executed successfully all sensitive key material and crypto specific data will be disposed PERMANANTLY during the reboot. The deletion is a straight-forward process and should not result in any delays. If the reboot process gets interrupted (due to power failure), the keys might not get permanently deleted. In such scenarios, the above steps will have to be repeated.*

4. Performing Secure Upgrade

EXE supports secure upgrade to facilitate a robust and capable update of mechanisms in line with the standards set by the Common Criteria for Network Device Protection Profile. EXE supports the following features during any secure upgrade:

- Multiple firmware version support simultaneously and simplified switch process between firmware versions.
- If the integrity or authenticity of the current image is faulted, the EXE will fail to boot.
- During the secure upgrade process, the integrity of the image is verified. If the verification fails, the failed image file is not created/mounted to the system and the image will not be available to be selected as the next boot image. The current boot image and the next boot image will remain to be the same current operational image.
- Image authenticity verification is done using digital Signature verification.
- Image Integrity validation is done using Signature verification and file corruption analysis.

4.1 Upgrade

Prerequisites

- Obtain the image file of the intended version of the EXE firmware from the Evertz secure website.

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Upgrade**" menu on top of the displayed page.
3. Scroll to "**Image Settings**" Section.
4. Find a slot which is empty. If None of the **Image Slots** are empty, click **Delete** button from a suitable Image slot.

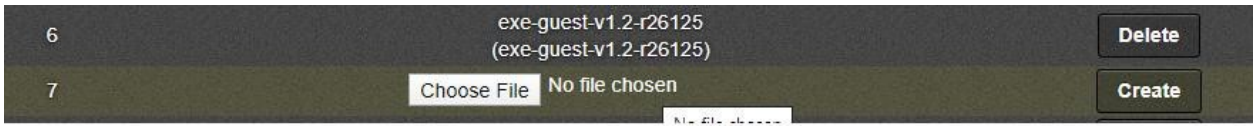


Figure 23: Selecting the image file to Upgrade.

5. Click "**Choose File**" displayed in the Image Slot row, Select the image file to be upgraded to.
6. Click "**Create**" button.
7. Confirm the popup dialog.
8. Wait for "**Processing**" status "**Message**" text to turn to "Image [N] created successfully using <filename>".

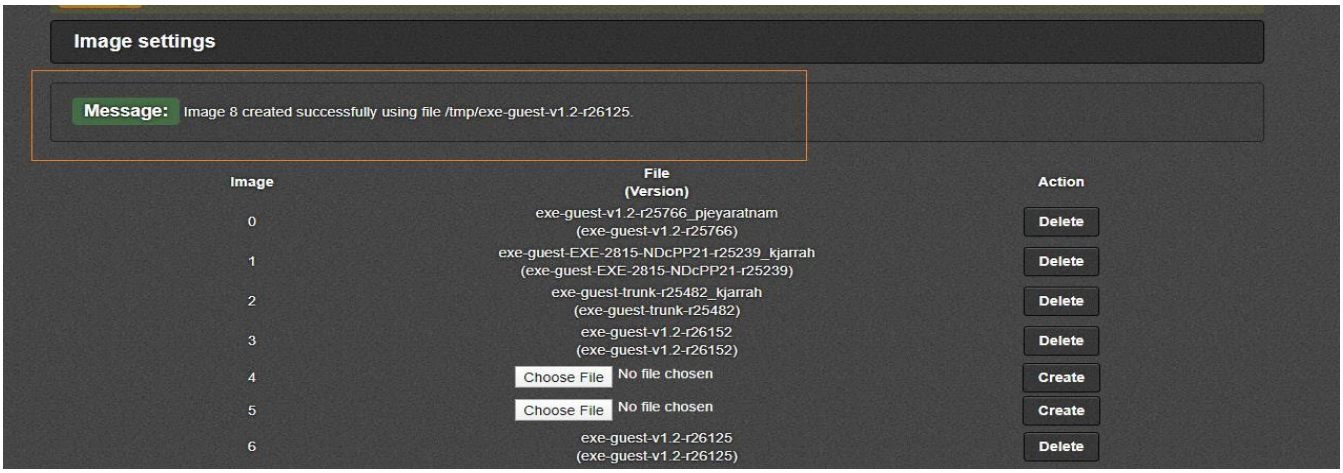


Figure 24: Image details.

9. Image has been successfully upgraded into the slot location.
10. Scroll up to "**Boot Image**" section and Select "**Next boot Image**" to the newly uploaded image slot.

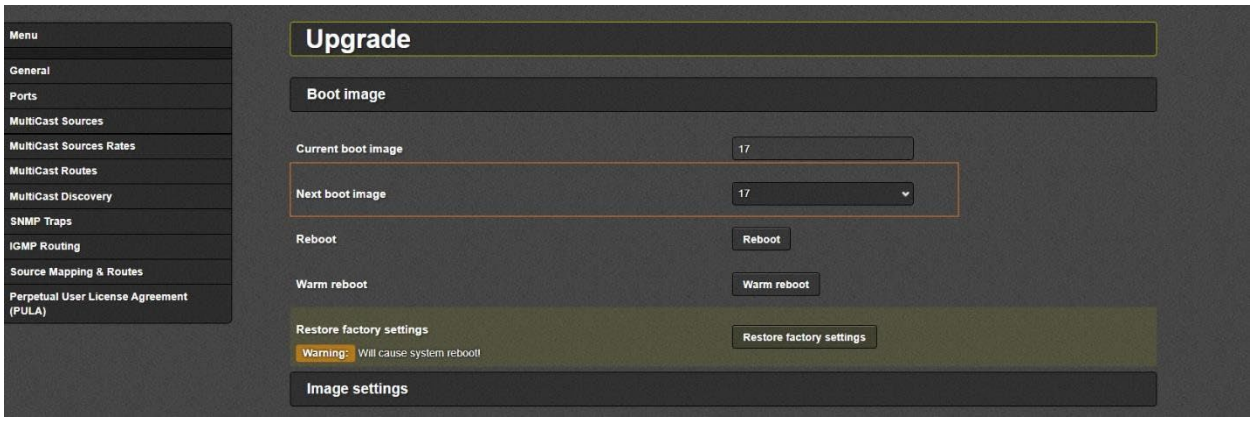


Figure 25: Boot Image Selection

11. Click "**Reboot** button", wait for system to reboot into the newly uploaded image.

4.2 Verify Current Installed Image

Prerequisites

- None

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Upgrade**" menu on top the displayed page.
3. Current active firmware image-slot will be displayed by "**Current Boot Image**" field under "**Boot Image**" section.

4. Check the firmware version by going to "**Image setting**" section and confirming the file against image-slot displayed in step 3.

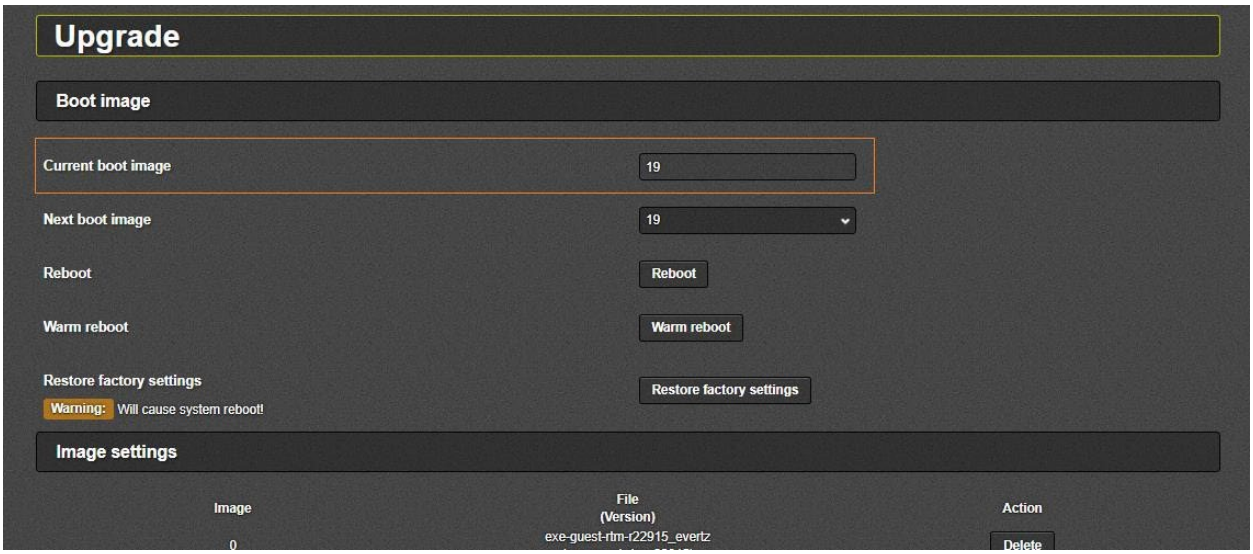


Figure 26: Verify Active Boot Image

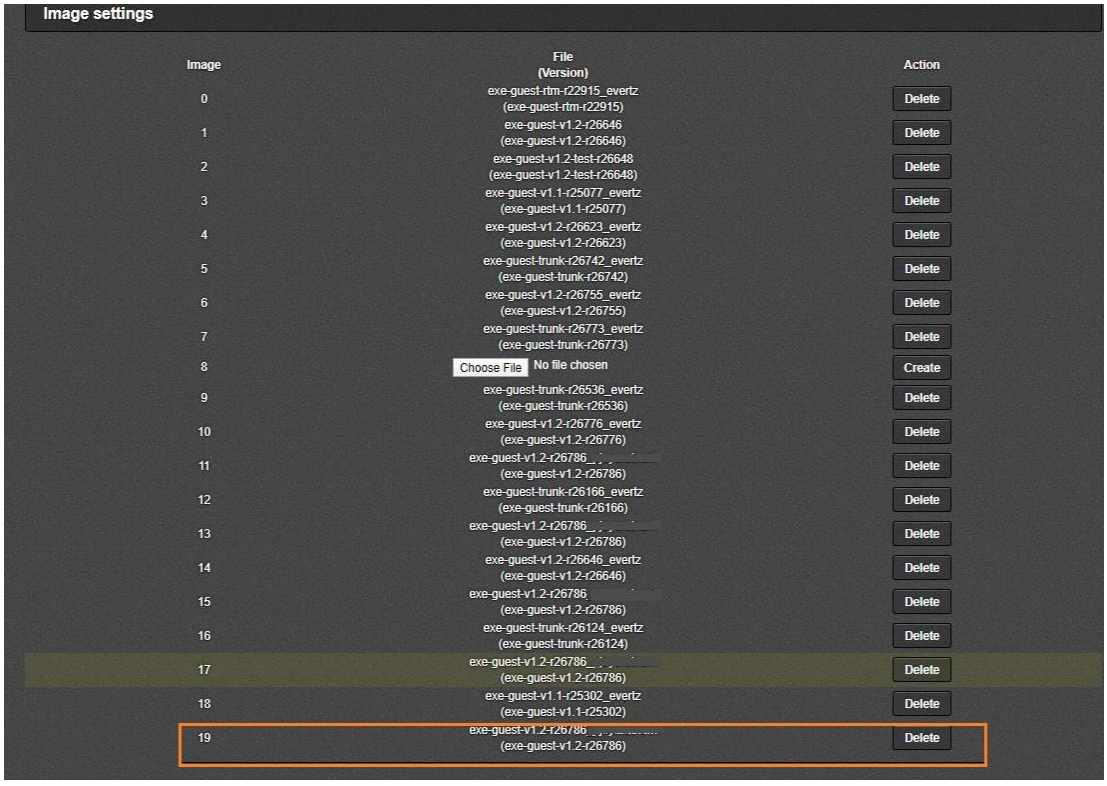


Figure 27: Reviewing the list of active and inactive Images.

Note:

The 'Image Settings' section shows all the image files (active and inactive) that are loaded onto the EXE.

4.3 Switch an Inactive Image to Active Image

Prerequisites

- None

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**Upgrade**" menu on top of the displayed page.
3. Choose "**Next boot image**" from "**Boot image**" section and select a suitable slot containing the next boot image.

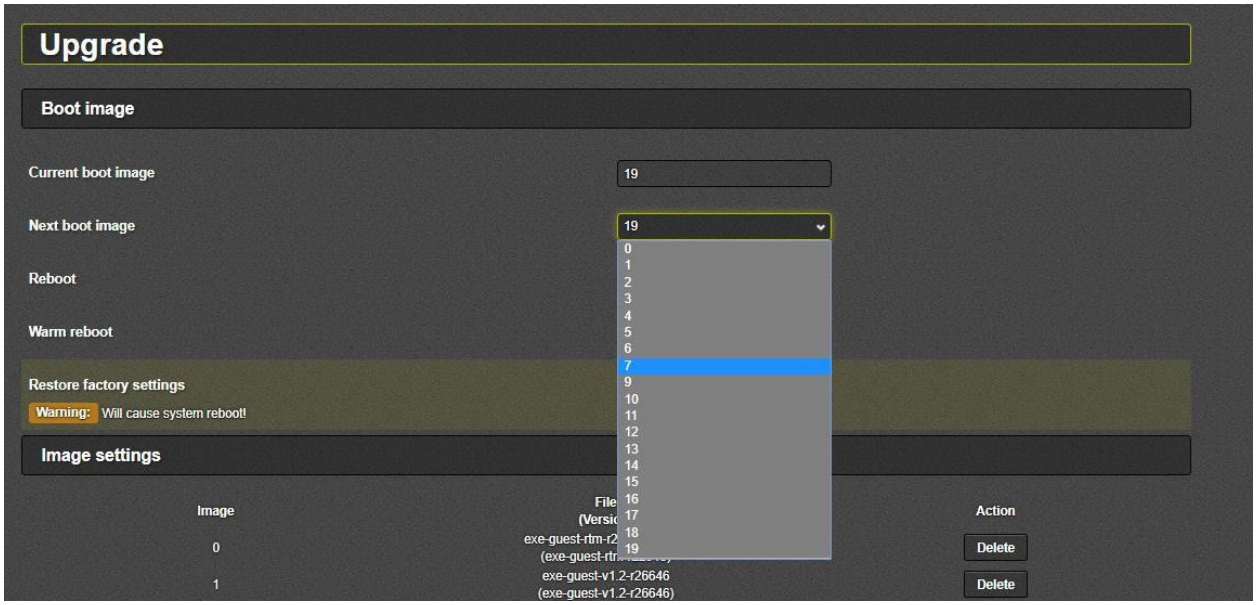


Figure 28: Selecting next boot image

4. Click "**Reboot**" button for the image to be booted as the new active firmware image.

4.4 Upgrade Errors

4.4.1 Upgrade Errors: Without a Signature

Upgrade will fail with the following "**Message**" when upgrading to an image without a signature file.

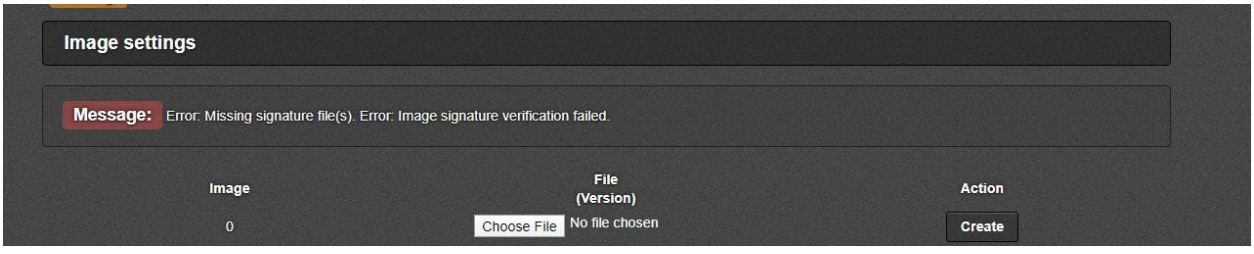


Figure 29: Error upgrading to an image with no signature.

4.4.2 Upgrade Errors: Corrupted Image

Upgrade will fail with the following "**Message**" when upgrading to an image which has been corrupted.

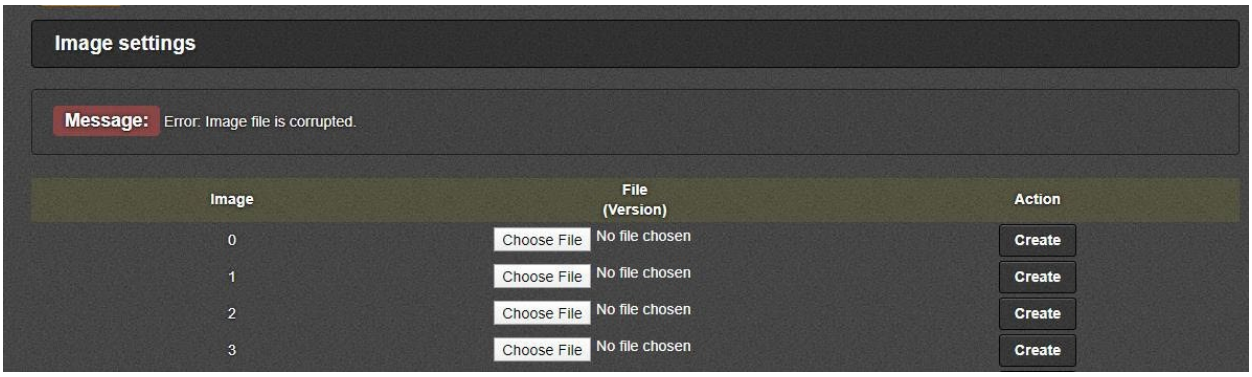


Figure 30: Error upgrading a corrupted image.

4.4.3 Upgrade Errors: Bad Signature

Upgrade will fail with the following "**Message**" when upgrading to an image with a mismatched signature file.

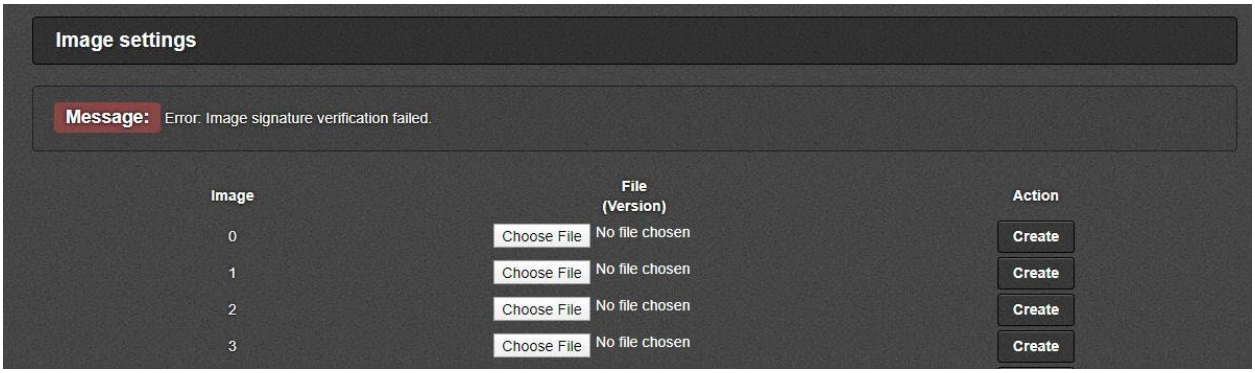


Figure 31: Error upgrading with an image with mismatched signature.

5. Audit Events

EXE can generate audit records which are stored internally within the EXE whenever a relevant event occurs. EXE also provides a facility to offload the audited events to an external syslog server in a secure manner in compliance with CC criteria. The internal logs are stored unencrypted; they are accessible through the web-interface for authorized users only. EXE provides functionality to configure and send audit logs through an encrypted channel to an external Syslog server. No configuration is required for audit event generation. When used with a remote syslog server the audit events are transferred in real-time to the remote syslog server.

5.1 Viewing Audit Events via Web Interface

EXE provides functionalities to view audit events through the web-interface.

Prerequisites

- None

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**General**" menu option.
3. Scroll to "**Make Logs**" section in the displayed page and click "**Download**" button.

Figure 32: Download Audit Events

Note:

The EXE can be operated as a standalone Network Device. EXE stores audit logs internally in real-time. The internal logs are stored unencrypted, but they are only accessible as a downloadable tar file.

For local audit log storage, multiple log files are generated, each with a maximum capacity of approx. 60 MB. Once the current log file is full under "/var/log" path it is log-rotated., and simultaneously the old log-rotated logs are compressed and saved under a long-term storage location "/ssd/syslog/current" path. Compressed old log-rotated log files under the long-term storage are cleared based on a first-in-first-out basis with approximate maximum compressed logs of number 100. The

audit logs will keep getting overwritten(log-rotated) with new files and audit log storage will never become full*. This is the default behaviour and this cannot be modified by the administrators. In the CC evaluated configuration, the audit log path cannot be accessed by the recovery user through the console.*

5.2 Offloading Audit Logs

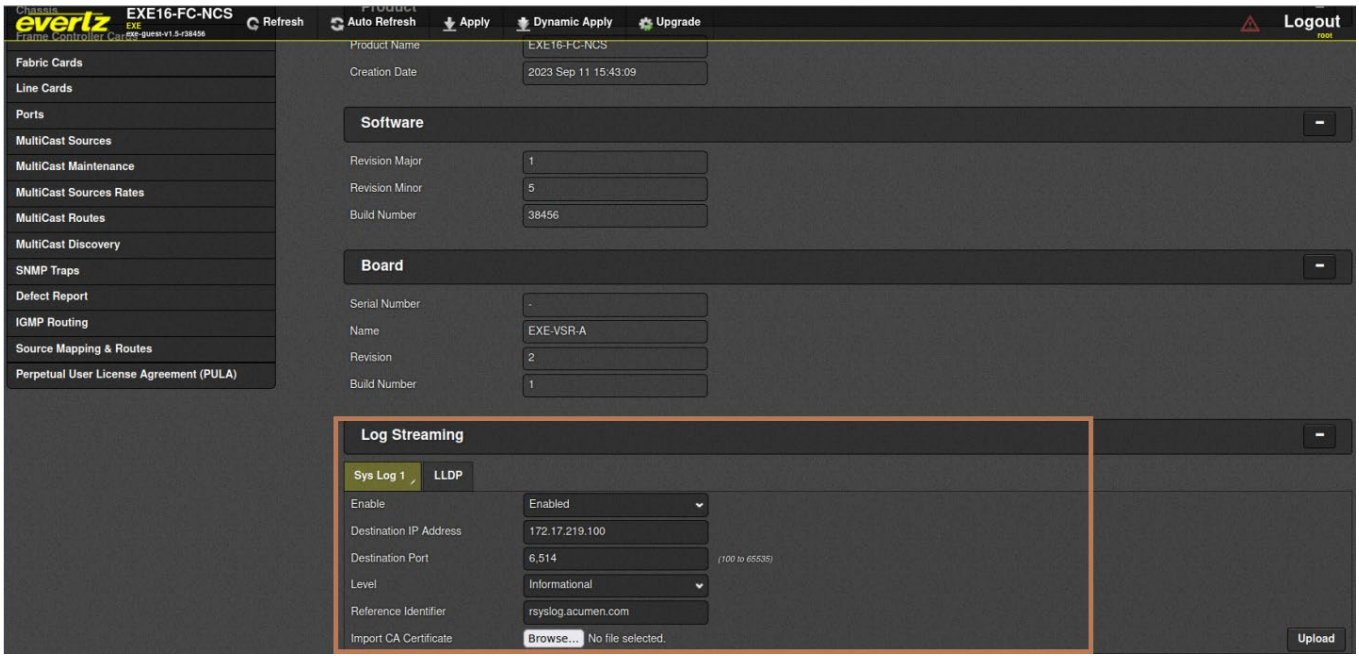
System log messages can be sent to a remote audit server. The remote audit server must listen on TCP port 6514(port number is user configurable, default value for port number is 6514) for TLS connections. All audit events are simultaneously sent to the remote server and the local store. If this or any outgoing client connection is unintentionally broken, EXE will automatically reconnect within seconds.

Prerequisites

- A syslog server which supports secure TLS communication is up and running listening on TCP port 6514.
- The syslog server supports TLS protocol version 1.2 and supports the cipher suites listed in the section 2.4.6 above.

Steps

1. Login to the EXE **Management Web Application.**
2. Click "**General**" menu on top of the displayed page.
3. Click on "**Info/Logging**" Tab at bottom of right-hand side of the page.
4. Under "**Sys Log 1**" of "**Log Streaming"** section, enter the following information:
    - Destination IP Address
    - Destination Port
    - Level
    - Reference Identifier



***Note:** Ensure that the EXE has the same CA chain used in the Syslog Server.*

5.3 Audit Events Table

Below table describes the EXE audited events along with the requirements for administrative review. Each event generates multiple audit entries. The yellow highlighted portions of the audit entries below are to guide administrators to help understand the audit behavior.

Auditable Events	Sample Logs
Start-up and shut-down of the audit functions	2024-07-04T08:06:47.959880+00:00 IPX128 syslog.info earlysyslog 146 - - starting 2024-07-04T08:06:47.960253+00:00 IPX128 syslog.info earlysyslog 146 - - terminating
Administrative login and logout via WebGUI	**Successful Login Attempt via GUI** 2024-03-22T06:16:07.934178+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 21399 - - Webeasy: User "root:192.168.254.157" logged in. **Unsuccessful Login Attempt via GUI** 2024-03-22T06:13:40.055252+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 20532 - - Webeasy: User "root:192.168.254.157" login failed. **Logout from GUI** 2024-03-28T09:28:39.581177+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 12441 - - Webeasy: User "root:192.168.254.157" logged out.
Administrative login and logout via Local Console	**Successful Login Attempt from Console** 2024-03-22T06:08:16.710161+00:00 MMA10G-IPX-128-3C-E6-7E authpriv.info login 18296 - - LOGIN ON ttyS0 BY recovery 2024-03-22T06:08:16.732668+00:00 MMA10G-IPX-128-3C-E6-7E user.notice root - - - (login:session): session opened for user recovery **Unsuccessful Login Attempt from Console** 2024-03-22T06:03:27.993059+00:00 MMA10G-IPX-128-3C-E6-7E authpriv.notice login 16633 - - FAILED LOGIN SESSION FROM ttyS0 FOR recovery, Authentication failure **Logout from Console** 2024-03-22T08:10:53.988934+00:00 MMA10G-IPX-128-3C-E6-7E user.notice root - - - (login:session): session closed for user recovery
Unsuccessful login attempts limit is met or exceeded for a user	2024-03-21T10:07:41.209060+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 16660 - - Webeasy: User "admin:192.168.228.19" was permanently locked out (max failed login attempts reached).
User forced logout from webGUI due to inactivity	2024-03-22T07:49:49.323838+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 25285 - - Webeasy: User "root:192.168.254.157" session timedout

Auditable Events	Sample Logs
User force logout from the local console due to inactivity	2024-03-26T10:05:07.238486+00:00 MMA10G-IPX-128-3C-E6-7E local0.err recoverysh 22582 - - User "recovery:console" session timedout.
Management activities	**Configure the access banner;** 2024-03-26T10:30:55.972359+00:00 MMA10G-IPX-128-3C-E6-7E user.info cfgjsonrpc 563 - - [069|onReceive] [root:192.168.228.28] PULA update was successful. **Configure the session inactivity time before session termination or locking;** 2024-03-26T10:00:15.146133+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 21480 - - Webeasy: User "root:192.168.228.28" set session timeout to "120". **Configure the authentication failure parameters;** 2024-03-21T09:52:18.818290+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 10745 - - Webeasy: User "root:192.168.228.19" set max failed login attempts to "3". **Import X.509v3 certificates to the local trust store.** 2024-03-14T13:18:46.662162+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice import_client_ca 22183 - - copying /tmp/img/AcumenCAICA-New.pem to /mnt/enclave/uploaded_certs/client-ca-chain-cert.incoming.pem: OK 2024-03-14T13:18:47.212225+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 22306 - - Webeasy: User "root:192.168.254.157" imported client CA successfully. **Generating CSR.** 2024-03-22T07:32:23.200955+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice regenerate_export_csr 18454 - - CSR Regeneration and export succeeded. 2024-03-22T07:32:23.217372+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 18541 - - Webeasy: User "root:192.168.254.157" regenerated csr successfully. **Note:-** Administrator are not allowed to import and delete cryptographic keys and only generation of cryptographic keys is allowed. **Re-enable an Administrator account.** 2024-03-21T10:31:12.503061+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_action 25352 - - Webeasy: User "root:192.168.228.19" unlocked user "admin". **Resetting Passwords.** 2024-03-21T13:10:32.741273+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice user_update 18674 - - Webeasy: User "good_user1:192.168.228.19" updated password. **Changing the time.**

Auditable Events	Sample Logs
	2024-07-03T14:28:20.000026+00:00 MMA10G-IPX-128-3C-E6-7E user.notice date 8806 - - User root change system time from [2024/07/03 14:55:54] to new value [2024/07/03 14:28:20]: Success 2024-07-03T14:28:22.453670+00:00 MMA10G-IPX-128-3C-E6-7E local0.info recoverysh 8625 - - User "recovery:console" set time to "Wed Jul 3 14:28:22 UTC 2024" successfully. **Note:** Time can only change via console access.
Successfully upgrading the device firmware	2024-03-13T14:49:28.778125+00:00 IPX128 user.notice auto_start - - - Welcome to Version 1.5 build 40017 built on 2024 Mar 02 00:13:14
Unsuccessful attempts to upgrade the device firmware	**Modified image file:** 2024-03-19T11:44:46.603121+00:00 MMA10G-IPX-128-3C-E6-7E user.info image_config 5306 - - Creating image 3 using file /tmp/exe-guest-v1.5-r37421.is_corrupted ... 2024-03-19T11:44:46.619396+00:00 MMA10G-IPX-128-3C-E6-7E user.err image_config 5306 - - Image file is corrupted **An image that no has been signed:** 2024-03-19T12:11:42.682511+00:00 MMA10G-IPX-128-3C-E6-7E user.err image_config 15307 - - Missing signatures 2024-03-19T12:11:42.682581+00:00 MMA10G-IPX-128-3C-E6-7E user.err image_config 15307 - - Image signature verification failed **An image signed with invalid signature:** 2024-03-19T12:11:42.682511+00:00 MMA10G-IPX-128-3C-E6-7E user.err image_config 15307 - - Missing signatures 2024-03-19T12:11:42.682581+00:00 MMA10G-IPX-128-3C-E6-7E user.err image_config 15307 - - Image signature verification failed
Successfully connecting to a syslog server	2024-04-12T14:09:27.472530+00:00 MMA10G-IPX-128-3C-E6-7E daemon.notice stunnel-rsyslog 1805 - - LOG5[508]: s_connect: connected 10.1.5.44:6514
Successfully connecting with a Magnum Server (Synergy Channel)	2024-04-12T13:42:40.399405+00:00 MMA10G-IPX-128-3C-E6-7E user.info synergy_server 5091 - - SYNERGY: Connected to 10.1.5.44:59416
Terminating the connection with a syslog server	2024-04-12T14:10:03.033570+00:00 MMA10G-IPX-128-3C-E6-7E daemon.notice stunnel-rsyslog 1805 - - LOG5[508]: Connection closed: 34155 byte(s) sent to TLS, 0 byte(s) sent to socket
Terminating the connection with a Magnum Server (Synergy Channel)	2024-04-12T13:07:58.605806+00:00 MMA10G-IPX-128-3C-E6-7E user.info synergy_server 5091 - - SYNERGY: Disconnected from 10.1.5.44:60874
Failures to establish a TLS Session when the EXE is acting as a TLS Client (for the Syslog Server Communication)	**Server certificate which doesn't match cipher suite: -** 2024-02-05T10:00:38.504653+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 30832 - - SSL_connect: 0:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:ssl/record/rec_layer_s3.c:1543:SSL alert number 40 **Server Hello using unsupported cipher suite: -**

Auditable Events	Sample Logs
	2024-02-05T14:35:04.988252+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 28980 - - SSL_connect: 0:error:1421C105:SSL routines:set_client_ciphersuite:wrong cipher returned:ssl/statem/statem_clnt.c:1342: **ECDHE key exchange using unsupported curve: -** 2024-02-05T14:55:53.225535+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 3732 - - SSL_connect: 0:error:141A417A:SSL routines:tls_process_ske_ecdhe:wrong curve:ssl/statem/statem_clnt.c:2210: **Server Hello using unsupported TLS version: -** 2024-02-05T15:13:49.390467+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 10220 - - SSL_connect: 0:error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol:ssl/statem/statem_lib.c:1957: **Modify signature in the server key exchange: -** 2024-02-05T15:27:44.009919+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 14889 - - SSL_connect: 0:error:1416D07B:SSL routines:tls_process_key_exchange:bad signature:ssl/statem/statem_clnt.c:2406: **Modify byte in the server finish message: -** 2024-03-01T14:56:41.530100+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 28052 - - SSL_connect: 0:error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac:ssl/record/ssl3_record.c:676: **Send a garbled message after Change Cipher Spec message: -** 2024-03-01T15:10:54.011048+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info stunnel-rsyslog 931 - - SSL_connect: 0:error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac:ssl/record/ssl3_record.c:676:
Failures to establish a TLS Session when the EXE is acting as a TLS Server (for the WebGUI (HTTPS) Management and for communication with Magnum)	**Client hello unsupported cipher suite: -** 2024-02-22T14:33:25.776164+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info lighttpd 5646 - - SSL_read: 0:error:14209102:SSL routines:tls_early_post_process_client_hello:unsupported protocol:ssl/statem/statem_srvr.c:1685: **Modify byte in client finish message: -** 2024-02-22T13:37:49.020074+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info lighttpd 5646 - - SSL_read: 0:error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac:ssl/record/ssl3_record.c:676: **Initiate connection to the EXE using secp224r1:-** 2024-02-22T11:27:13.028972+00:00 MMA10G-IPX-128-3C-E6-7E daemon.info lighttpd 5662 - - SSL_read: 0:error:140940F4:SSL routines:ssl3_read_bytes:unexpected message:ssl/record/rec_layer_s3.c:1476:

Auditable Events	Sample Logs
Failures to establish a TLS Session when the EXE is acting as a TLS Server with mutual authentication (for the communication with Magnum)	**Send an empty certificate list: -** 2024-02-28T10:52:57.072649+00:00 MMA10G-IPX-128-3C-E6-7E user.info synergy_server 5114 - - SSL_accept: 0:error:1417C0C7:SSL routines:tls_process_client_certificate:peer did not return a certificate:ssl/statem/statem_srvr.c:3734: **Unsupported Signature Algorithm: -** 2024-03-27T06:02:51.339411+00:00 MMA10G-IPX-128-3C-E6-7E user.err synergy_server 5123 - - Certificate verification failed: depth=0 subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=mutual.acumen.com errmsg=certificate signature failure **Modify a byte in the signature block of the client's Certificate Verify handshake message: -** 2024-02-29T08:58:53.870495+00:00 MMA10G-IPX-128-3C-E6-7E user.info synergy_server 5359 - - SSL_accept: 0:error:0407E086:rsa routines:RSA_verify_PKCS1_PSS_mgf1:last octet invalid:crypto/rsa/rsa_pss.c:88: 2024-02-29T08:58:53.870513+00:00 MMA10G-IPX-128-3C-E6-7E user.info synergy_server 5359 - - SSL_accept: 0:error:1417B07B:SSL routines:tls_process_cert_verify:bad signature:ssl/statem/statem_lib.c:504: **Client identity certificate that is signed by an impostor CA: -** 2024-02-29T07:36:06.447571+00:00 MMA10G-IPX-128-3C-E6-7E user.err synergy_server 5359 - - Certificate verification failed: depth=0 subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=mutual.acumen.com errmsg=unable to get local issuer certificate
Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the local certificate trust store	**Incomplete chain of certificates:** 2024-03-07T07:44:57.348315+00:00 MMA10G-IPX-128-3C-E6-7E daemon.warning stunnel-rsyslog 8063 - - LOG4[61]: CERT: Pre-verification error at dept=0: unable to get local issuer certificate. **Expired Certificate:** 2024-03-12T11:28:49.558647+00:00 MMA10G-IPX-128-3C-E6-7E daemon.warning stunnel-rsyslog 26714 - - LOG4[648]: CERT: Pre-verification error at dept=0: certificate has expired. **Revoked certificate:** 2024-03-11T10:13:22.773996+00:00 MMA10G-IPX-128-3C-E6-7E daemon.err stunnel-rsyslog 12106 - - LOG3[957]: CRL verification failed: depth=0 issuer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA2 subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=rsyslog.acumen.com errmsg=certificate revoked. **When a CRL download fails:** 2024-03-13T11:47:26.071568+00:00 MMA10G-IPX-128-3C-E6-7E daemon.err stunnel-rsyslog 6520 - - LOG3[14]: CRL download failed (URI: http://10.1.5.4/AcumenICA-New2.crl) **Addition/Replacement/Removal of Trust Anchors**

Auditable Events	Sample Logs
	2024-03-06T13:25:02.055519+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice import_syslog_ca 12257 - - /tmp/img/CA-ICA.pem certificate format is supported. 2024-03-06T13:25:02.452565+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice import_syslog_ca 12257 - - /tmp/img/CA-ICA.pem is a valid CA chain. 2024-03-06T13:25:02.968161+00:00 MMA10G-IPX-128-3C-E6-7E local0.notice import_syslog_ca 12257 - - Importing rsyslog certificate succeeded. **Note:-** Only one CA-Chain is allowed in the device at a time, hence, when a new CA-Chain is added, the old chain gets deleted/replaced. Hence, an additional audit log for deletion is not required.

Table 1: Audit Events

6. Appendix

6.1 Communication of Magnum with EXE (Supplementary)

EXE can be controlled by MAGNUM. The connection between EXE server and MAGNUM client is done with TLS. To enable this connection, TLS Server Connection specified previously in the documentation above needs to be followed. EXE can maintain all functionality without connection to the video control system. If the connection is unintentionally broken, the EXE will wait for the MAGNUM server to reestablish the connection.

6.2 Reboot EXE

Refer to specific board EXE user manual for steps on rebooting.