

MMA10G-EXE SERIES

Security Administrative Guide Addendum for Common Criteria

Version 1.2, March 19, 2024

EVERTZ MICROSYSTEMS LTD.

5292 John Lucas Drive
Burlington, Ontario
Canada L7L5Z9

Phone: +1 905-335-3700

Sales: sales@evertz.com

Tech Support: service@evertz.com

Web Page: www.evertz.com

Fax: +1 905-335-3573

Fax: +1 905-335-7571

Twitter: @EvertzTV

The material contained in this manual consists of information that is the property of Evertz Microsystems and is intended solely for the use of purchasers of EXE series products. Evertz Microsystems expressly prohibits the use of this manual for any purpose other than the operation of the device.

All rights reserved. No part of this publication may be reproduced without the express written permission of Evertz Microsystems Ltd. Copies of this manual can be ordered from your Evertz dealer or from Evertz Microsystems.

This page left intentionally blank !

Table of Contents

1.	Introduction	6
1.1	Audience.....	6
1.2	Objective.....	7
1.3	Operational Environment.....	7
2.	9
3.	Secure Installation	10
3.1	Obtaining and installing the CC Certified Firmware.....	10
3.1.1	Secure Delivery Verification.....	10
3.1.2	Device Registration.....	10
3.1.3	Physical security Requirements	10
3.1.4	Installing the unit	10
3.2	Physical Installation.....	11
3.3	Initial Configuration	11
3.3.1	Accessing the EXE.....	11
3.3.2	Configuring the 'recovery' user for local console.....	12
3.3.3	Configure System Date and Time	13
3.3.4	Network Configuration	14
3.4	Secure Configuration.....	17
3.4.1	Configure Secure Mode.....	17
3.4.2	Verify Power-On Self-Tests	17
3.4.3	Verify Secure Mode Banners.....	19
3.4.4	FIPS Mode.....	21
3.4.5	Self-Test.....	21
3.4.6	Cipher Suites.....	21
3.4.7	Key Parameters.....	22
3.4.8	Hash and Keyed-Hash Algorithms	22
3.4.9	Configure Access Controls	22
3.4.10	Configure TLS Server.....	30
3.4.11	Configure TLS Client	34
4.	Secure Management.....	36
4.1	User Management	36
4.2	Certificate Management	39
4.3	Key/Cipher Management	40
4.3.1	Zeroing Crypto Material.....	40
5.	Performing Secure Upgrade	42
5.1	Upgrade.....	42
5.2	Verify Current Installed Image.....	43
5.3	Switch an Inactive Image to Active Image.....	45
5.4	Upgrade Errors.....	45
5.4.1	Upgrade Errors: Without a Signature	45
5.4.2	Upgrade Errors: Corrupted Image.....	46



- 5.4.3 Upgrade Errors: Bad Signature..... 46
- 6. Audit Events.....47
 - 6.1 Viewing Audit Events via Web Interface 47
 - 6.2 Offloading Audit Logs 48
 - 6.3 Audit Events Table 49
- 7. Appendix.....58
 - 7.1 Communication of Magnum with EXE (Supplementary)..... 58
 - 7.2 Reboot EXE 58

Table of Figures

Figure 1 Typical EXE Network Topology Overview	8
Figure 2: Enabling Secure Mode	17
Figure 3: Signature Image Verification	18
Figure 4: Self-Test Verification	18
Figure 5: Self-Test during critical operation	19
Figure 6: Verify Secure Banner	20
Figure 7: Verify Secure Access Banner	21
Figure 8: Secure Passwords	23
Figure 9: Set Session Timeout	25
Figure 10: Strict Session Handling	26
Figure 11: Set Max Attempts	27
Figure 12: Configure Access Banner	28
Figure 13: Disable REST API	29
Figure 14: Generating and Downloading a CSR	31
Figure 15: Upload Cert Chain	32
Figure 16: Upload SSL Certificate	33
Figure 17: Secure Log Service	35
Figure 18: User Management	36
Figure 19: New User Creation	37
Figure 20: New User Confirmation	37
Figure 21: New Role Creation	38
Figure 22: Roles Overview	39
Figure 23: Selecting the image file to Upgrade	42
Figure 24: Image details	43
Figure 25: Boot Image Selection	43
Figure 26: Verify Active Boot Image	44
Figure 27: Reviewing the list of active and inactive Images	44
Figure 28: Selecting next boot image	45
Figure 29: Error upgrading to an image with no signature	45
Figure 30: Error upgrading a corrupted image	46
Figure 31: Error upgrading with an image with mismatched signature	46
Figure 32: Download Audit Events	47

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	<p>A Syslog Server is required to offload audit logs. The syslog server shall meet the following:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> 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	<p>The management workstation which is to be used for the management of the EXE device must be capable of supporting the following:</p> <ul style="list-style-type: none"> • Use to manage Supporting TLSv1.2. • Supporting at least one of the following ciphersuites: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Conformant with RFC 5280.
Evertz Magnum Server	<p>Evertz Magnum Server provides remote management of the EXE’s routing and switching of video signals. The communication channel between the EXE and the Magnum Server must be secured with following parameters:</p> <ul style="list-style-type: none"> 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, communication channels that are used for the communication with these devices were not tested.

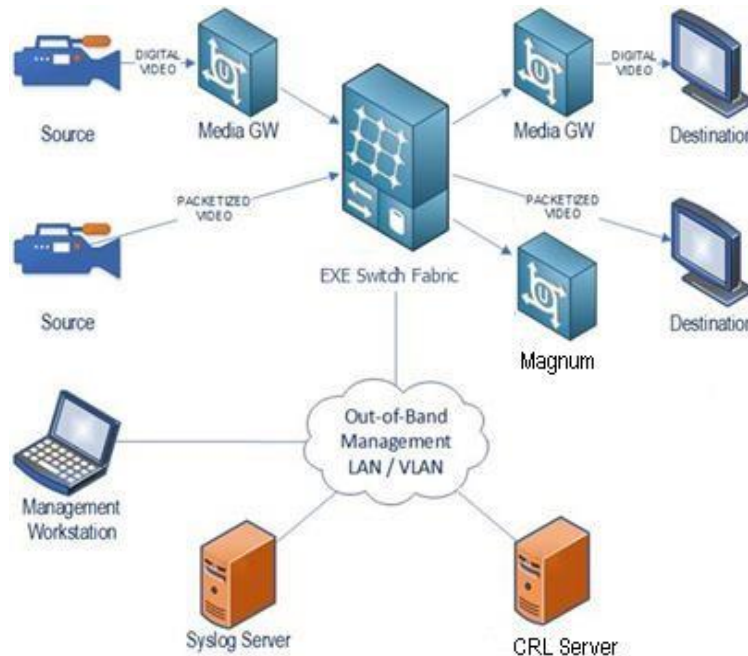


Figure 1 Typical EXE Network Topology Overview

2.

3. Secure Installation

3.1 Obtaining and installing the CC Certified Firmware

3.1.1 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.

3.1.2 Device Registration

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

3.1.3 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.

3.1.4 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.

3.2 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.

3.3 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

3.3.1 Accessing the EXE

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

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.

3.3.2 Configuring the ‘recovery’ user for local console

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.

3.3.3 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.

```

-----
(1) Network Configuration
(2) System Utilities

(X) Exit
> 2
-----
|                               |
|           System Utilities     |
| EXE16-FC-NCS 1.5 build 38382  |
|                               |
-----

(1) Set time
(2) Set Password
(3) Reboot
(4) Factory Restore
(5) Factory Reset

(X) Exit
> 1
Current time: Thu Aug 31 10:22:02 UTC 2023

Set time (format:[date -u +%Y-%m-%d %H:%M:%S])> 2023-08-31 10:23:00
LOCAL: Stopping etimed: OK
LOCAL: Thu Aug 31 10:23:00 UTC 2023
PEER: Error: Stopping etimed or setting sys/hw time on peer(169.254.18.21) failed
PEER: Error: Starting etimed on peer(169.254.18.21) failed
PEER: Error: Stopping etimed or setting sys/hw time on peer(169.254.11.21) failed
PEER: Error: Starting etimed on peer(169.254.11.21) failed
PEER: Error: Stopping etimed or setting sys/hw time on peer(169.254.10.21) failed
PEER: Error: Starting etimed on peer(169.254.10.21) failed
LOCAL: Starting etimed: OK
LOCAL: Setting time was successful
New time: Thu Aug 31 10:23:08 UTC 2023

-----
|                               |
|           System Utilities     |
| EXE16-FC-NCS 1.5 build 38382  |
|                               |
-----

(1) Set time
(2) Set Password
(3) Reboot
(4) Factory Restore
(5) Factory Reset

(X) Exit
> █

```

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

YYYY-MM-DD hours:minutes:seconds

Press ENTER to apply the settings.

3.3.4 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.

```

-----
|                               Main menu                               |
|                               EXE16-FC-NCS 1.5 build 38456           |
|-----|
(1) Network Configuration
(2) System Utilities

(X) Exit
> 1

```

Choose option 1 'Network Configuration' > Enter.

```

-----
|                               Network Configuration                   |
|                               EXE16-FC-NCS 1.5 build 38456           |
|-----|
(1) Network 1
(2) Network 2
(3) Network 3

(X) Exit
> 2

```

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 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.

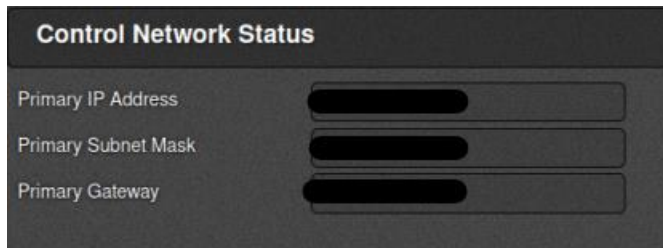
Steps using Web Access.

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.



3.4 Secure Configuration

3.4.1 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*

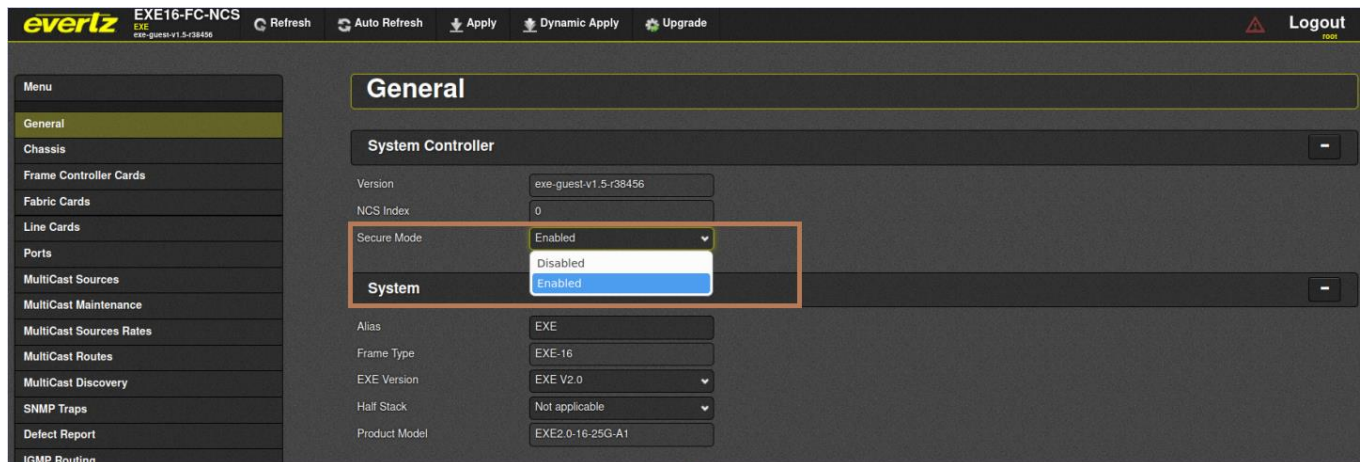


Figure 2: Enabling Secure Mode

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

3.4.2 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. This few minutes will allow the image to be recovered from a redundant image. If the system 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

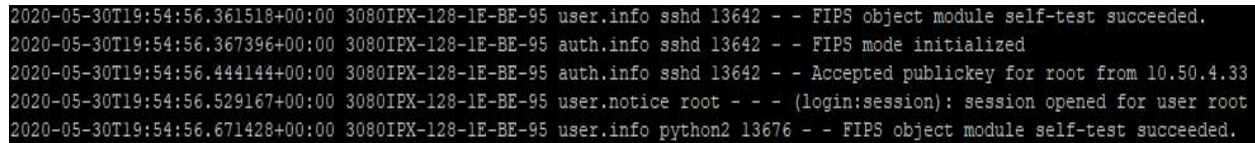
If fips self-test verification during boot failed following output is produced in console or syslog

“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 failed during any critical operation, following output is produced in console or syslog, and applications that requires FIPS support will fail to start.

“FIPS object module self-test failed.”

Please contact Evertz product support for further assistance and resolution.

3.4.3 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.

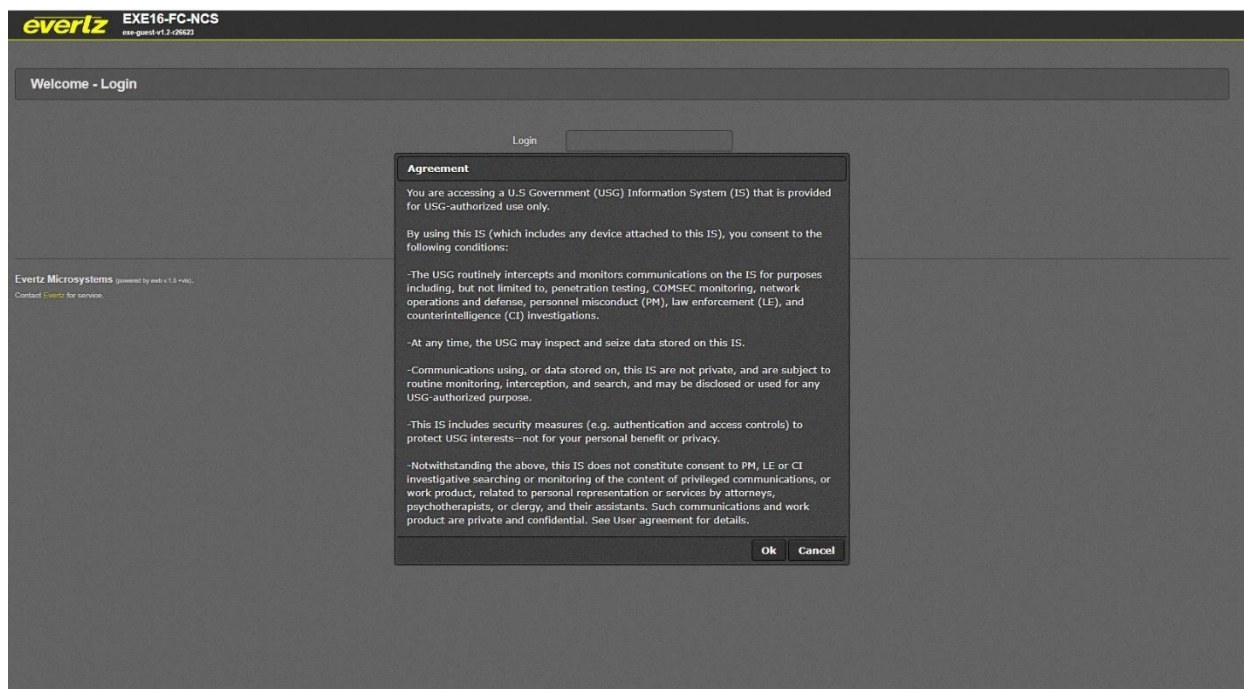


Figure 7: Verify Secure Access Banner

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.

3.4.4 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.

3.4.5 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

3.4.6 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

3.4.7 Key Parameters

EXE only supports generation of 2048-bit RSA keys that are generated only 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.

3.4.8 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.

3.4.9 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 through the use of username/password combinations. The administrator is able to 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 through the use of 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

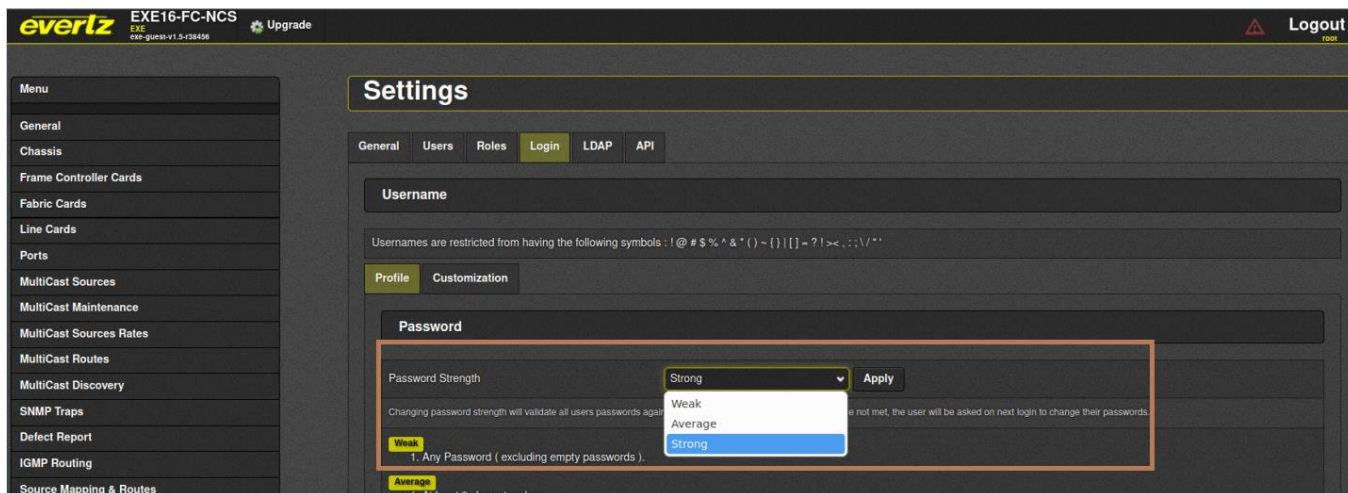


Figure 8: Secure Passwords

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:

The screenshot shows the administrative interface with the following elements:

- Navigation tabs: General, Users, Roles, **Login**, LDAP, API
- Section: Username
- Text: Usernames are restricted from having the following symbols : ! @ # \$ % ^ & * () ~ { } | [] = ? ! > < , ; \ / " ' *
 - Profile: **Customization**
 - Section: Password Customization
 - Text: You can customize the password profile to your liking as long as the minimums do not go below the set profiles minimums.
 - Form fields for Password Customization:

Minimum length	15
Maximum length(<=32)	20
Minimum uppercase letters to include (A-Z).	2
Minimum lowercase letters to include (a-z).	2
Minimum numbers to include (0-9).	2
Minimum special characters to include (!@#\$%^&*()+=~-[]";'./{} '":<>?~\).	2
 - Apply button

- 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

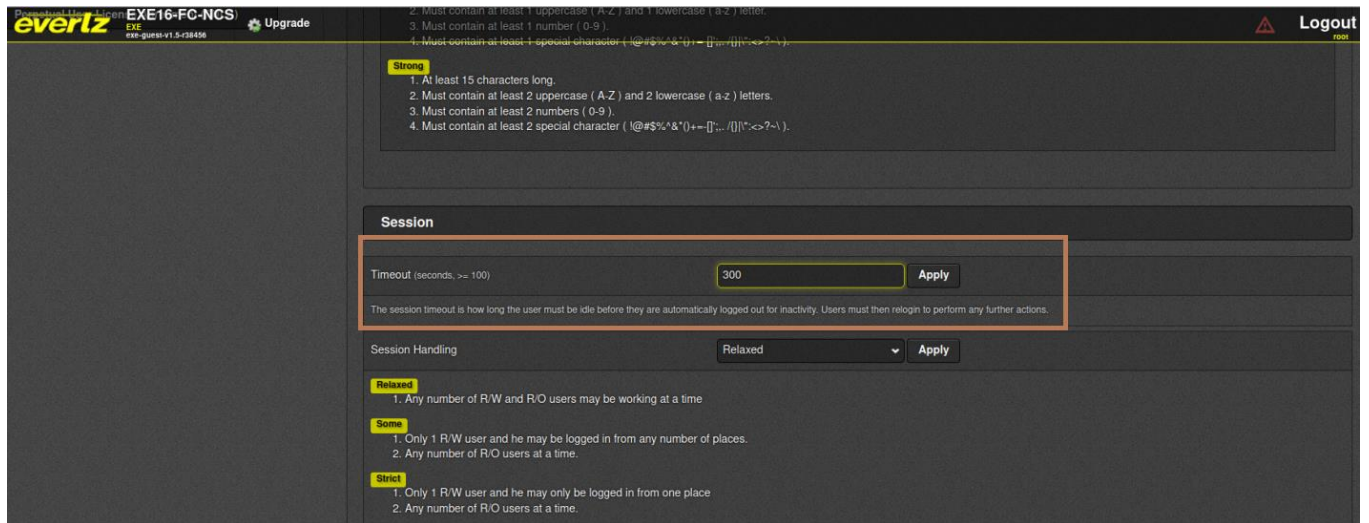


Figure 9: Set Session Timeout

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

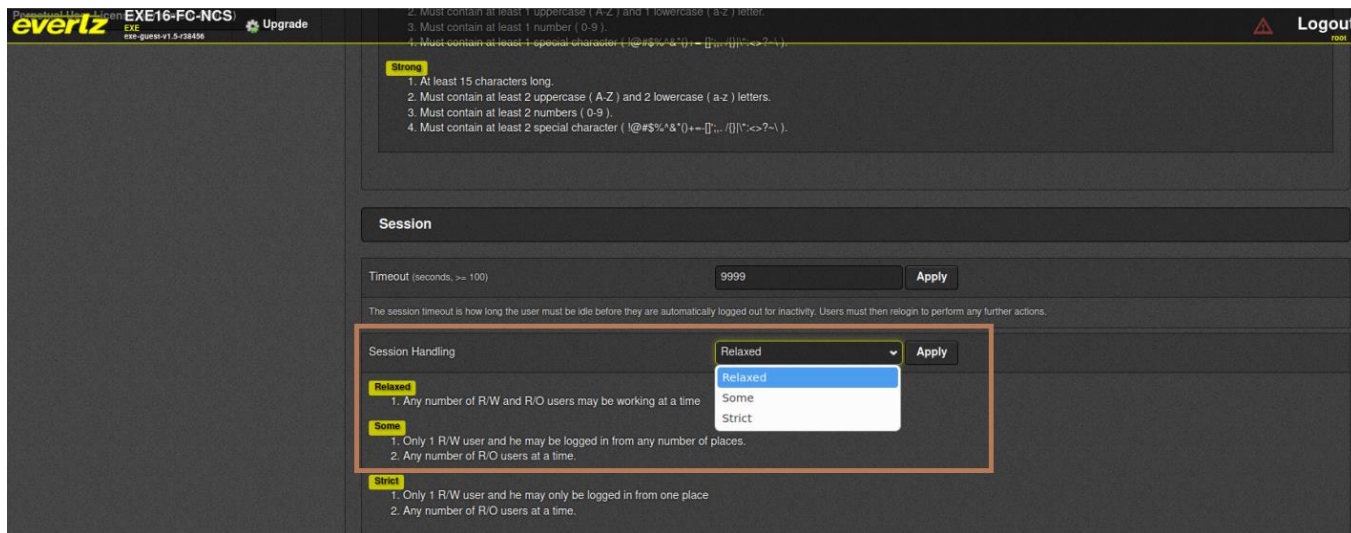


Figure 10: Strict Session Handling

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.

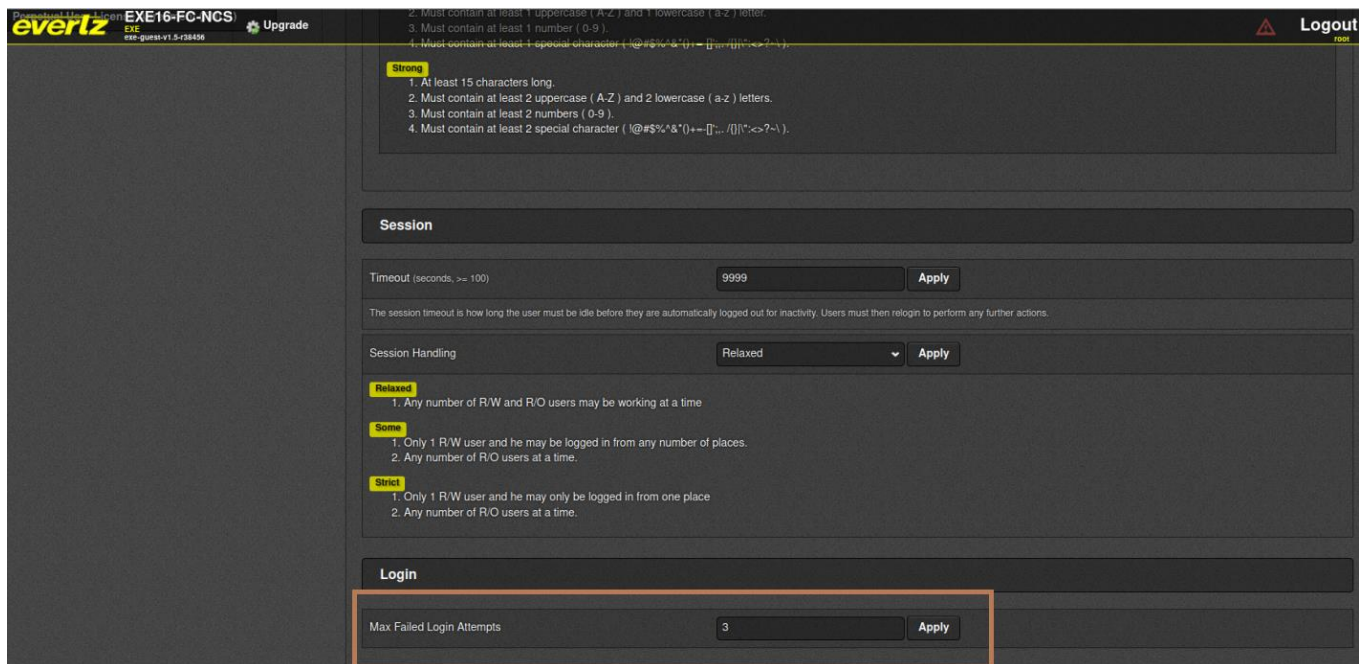


Figure 11: Set Max Attempts

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

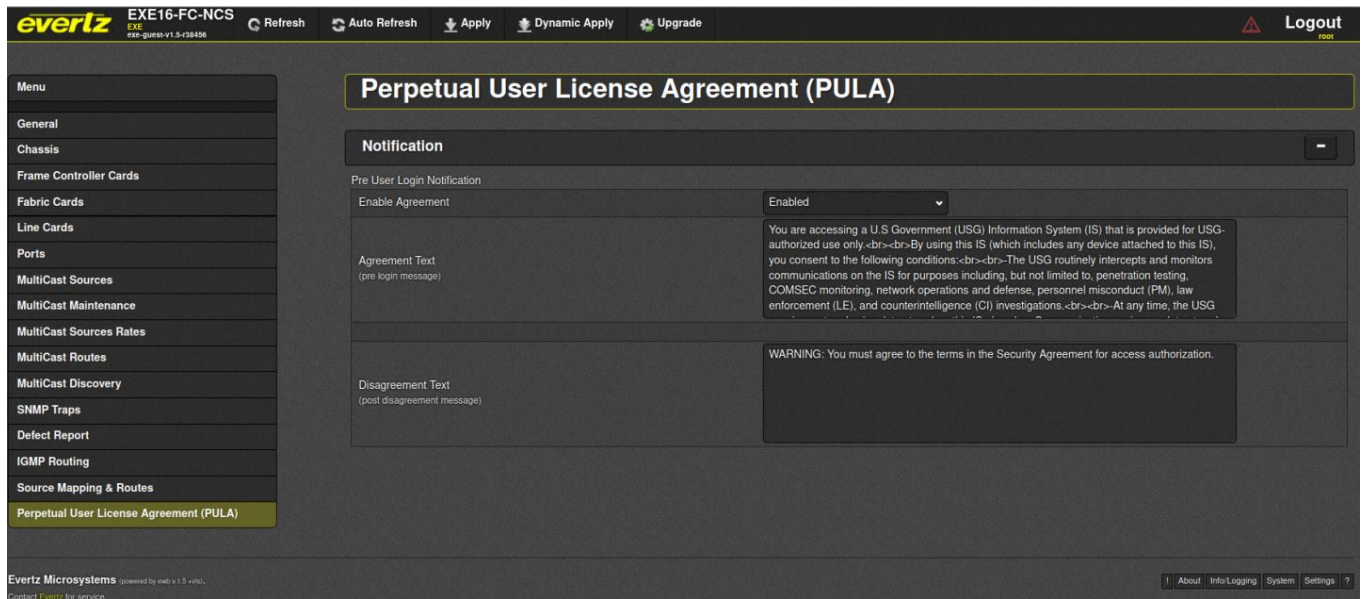


Figure 12: Configure Access Banner

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**”

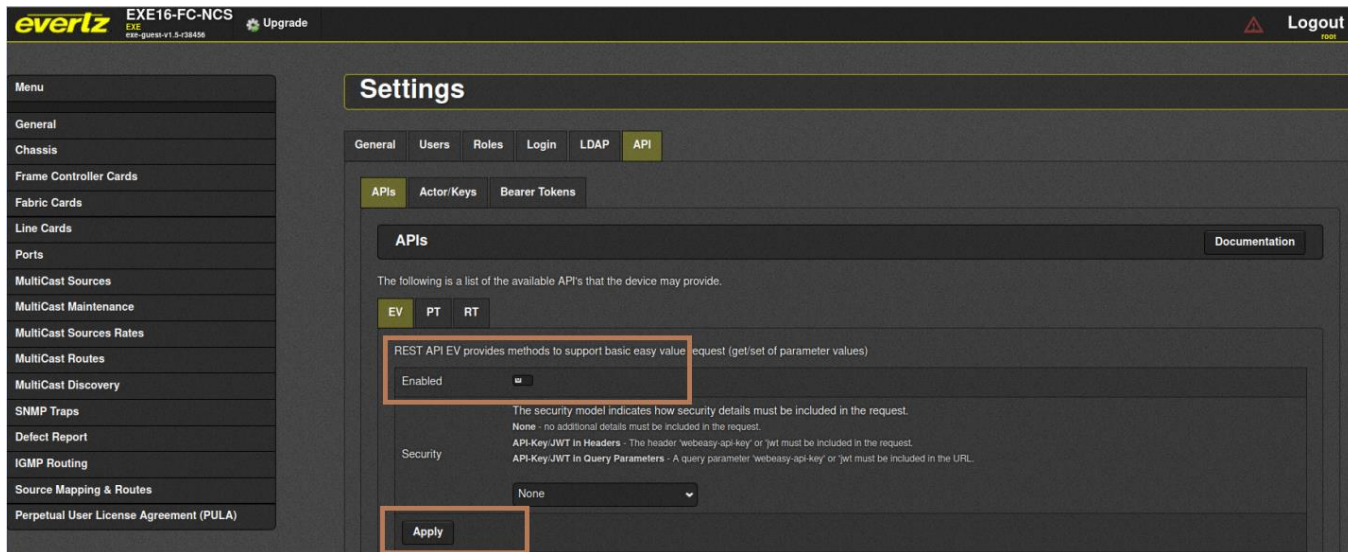
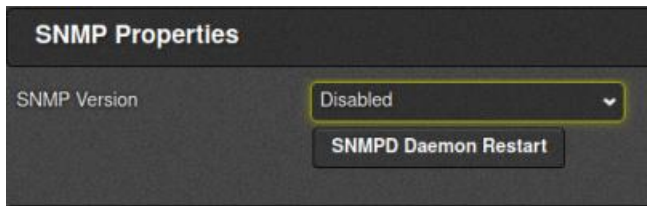


Figure 13: Disable REST API

Disable SNMP:

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



Disable NTP:

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



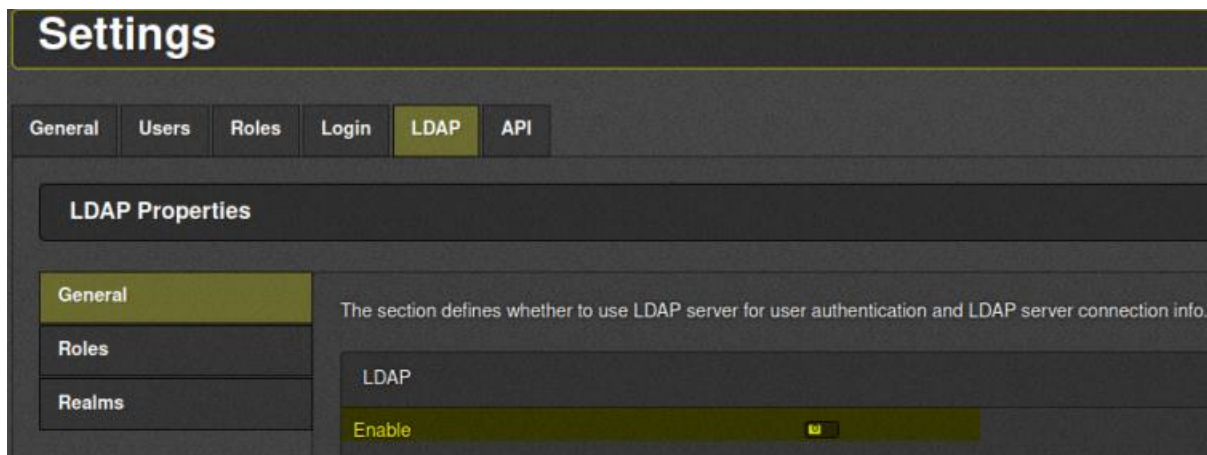
Disable LLDP streaming:

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



Disable LDAP:

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



3.4.10 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.

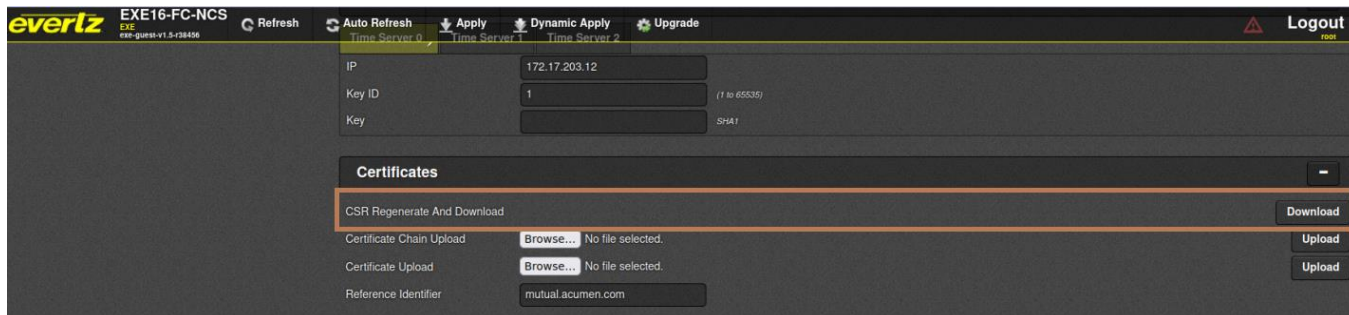


Figure 14: Generating and Downloading a CSR

Note: Reference-Identifier

Only host names are used for reference identifiers, the product does not support IPV4 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.

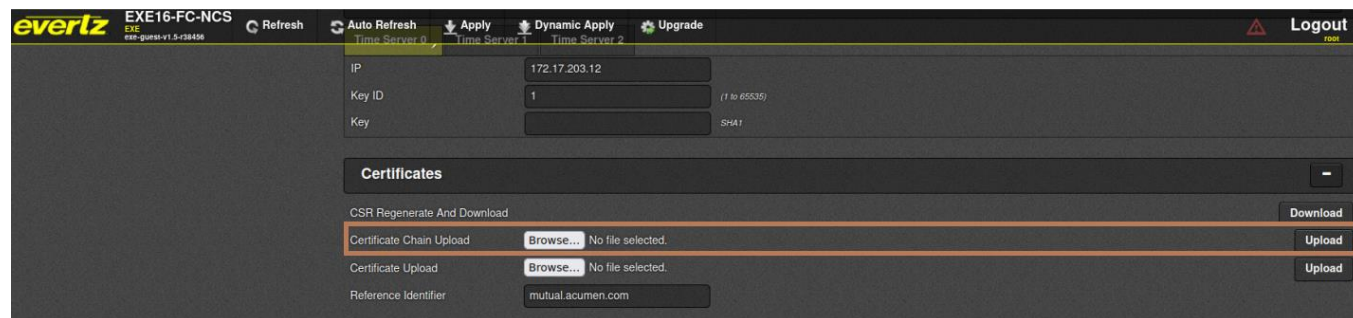


Figure 15: Upload Cert Chain

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

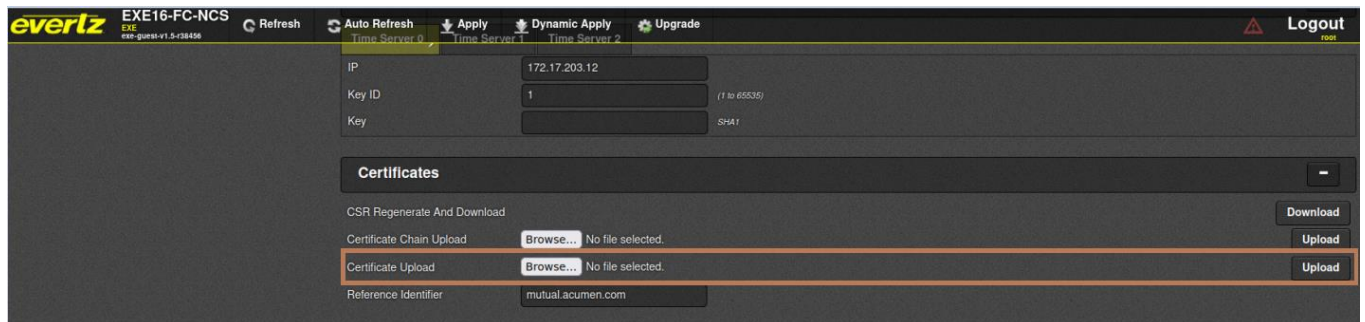


Figure 16: Upload SSL Certificate

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.

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.

3.4.11 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.

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.

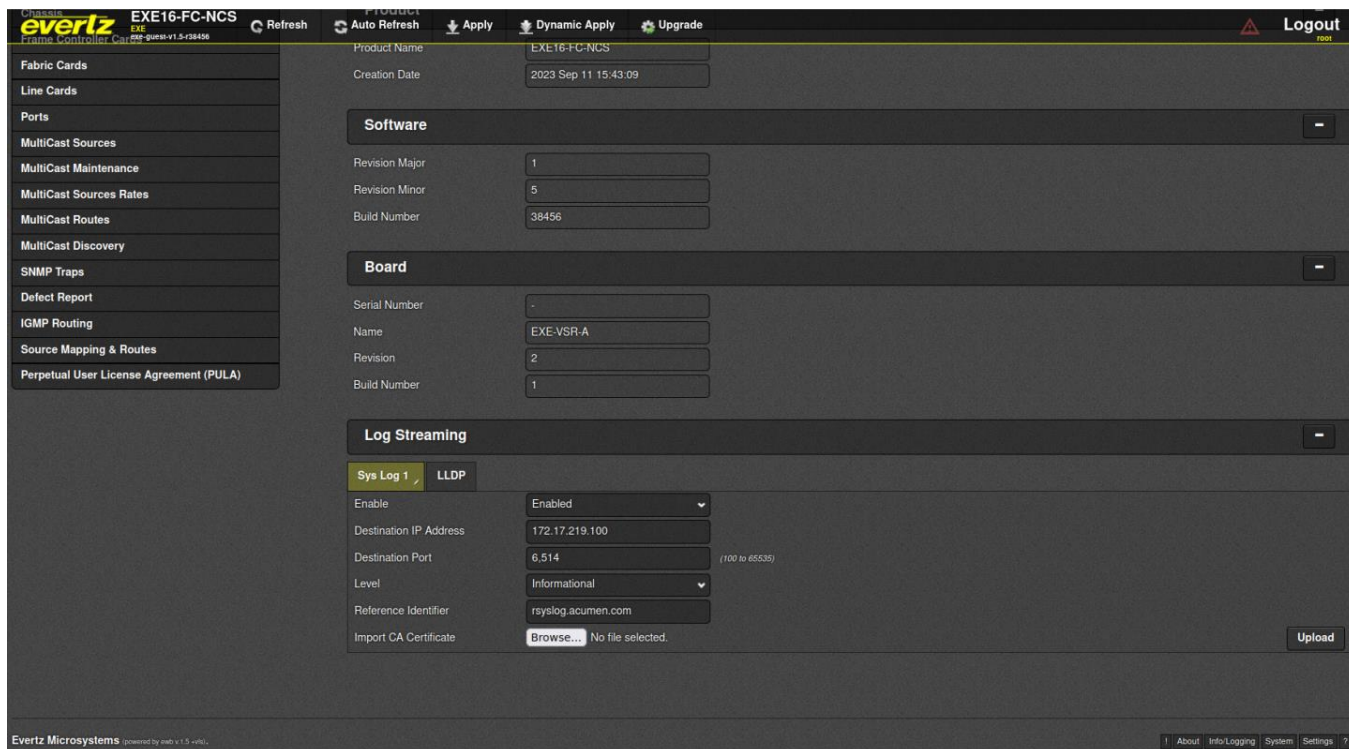


Figure 17: Secure Log Service

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

Note: Reference-Identifier*

*Note Only host names are used for reference identifiers we do not support IPV4 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.

4. Secure Management

4.1 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. Following screen will be displayed

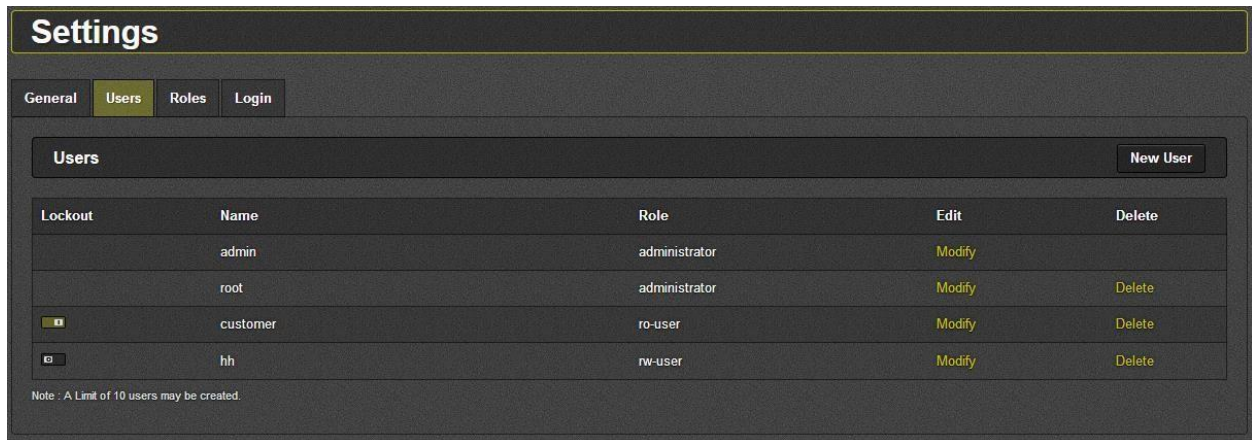


Figure 18: User Management

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 Security Administrator accounts.

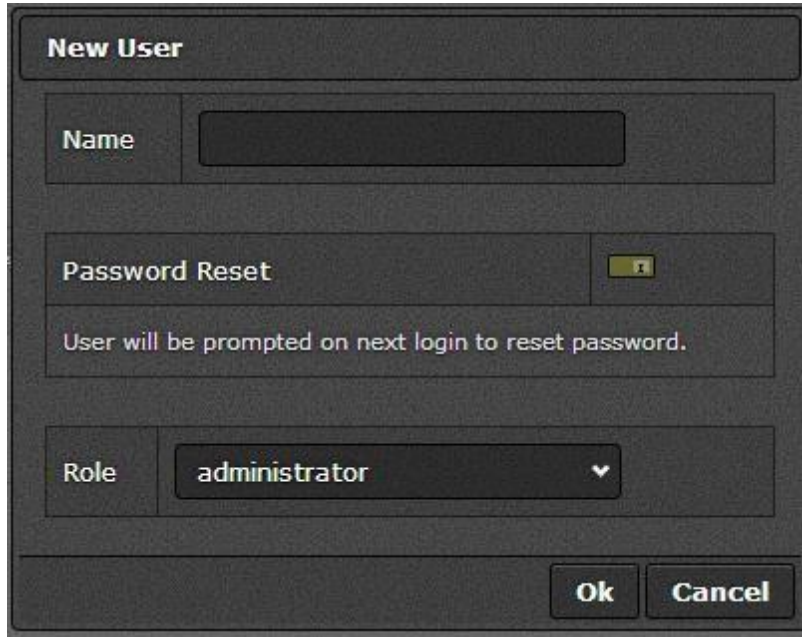


Figure 19: New User Creation

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

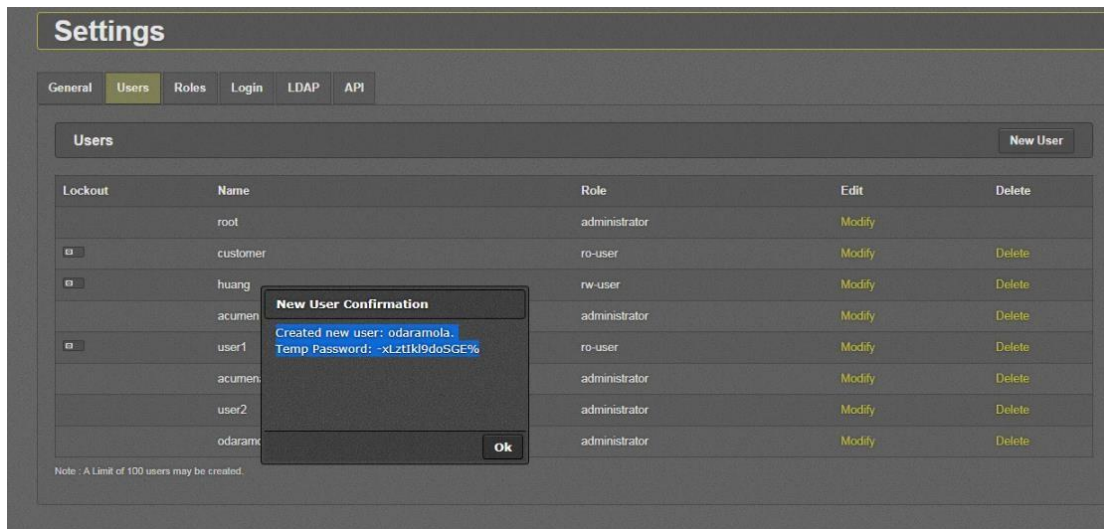


Figure 20: New User Confirmation

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.

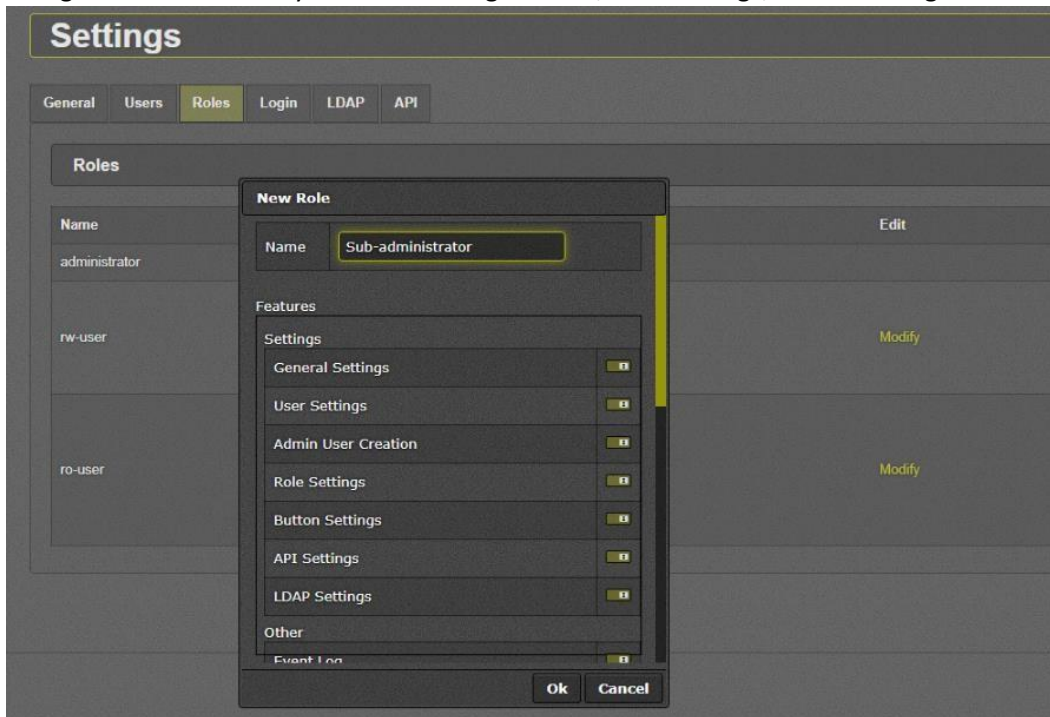


Figure 21: New Role Creation

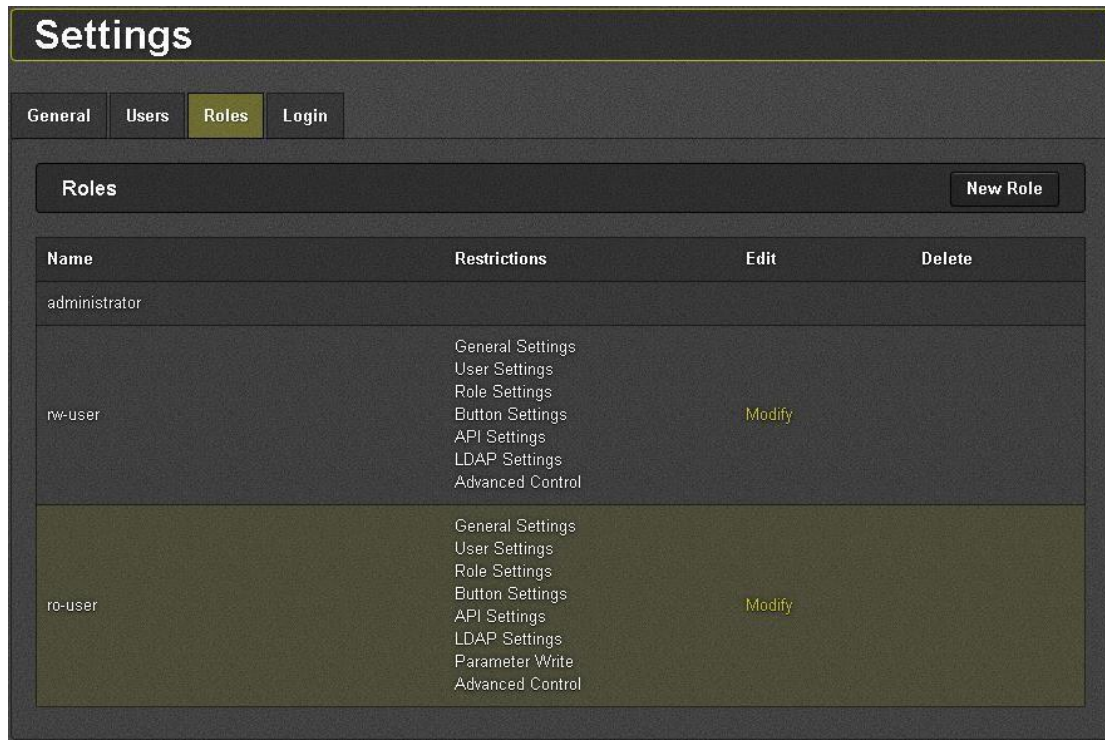


Figure 22: Roles Overview

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.

4.2 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.

4.3 Key/Cipher Management

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

4.3.1 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.

```
-----  
(1) Network Configuration  
(2) System Utilities  
(X) Exit  
> 2  
  
-----  
|                               System Utilities                               |  
|                               EXE16-FC-NCS 1.5 build 38382                   |  
|-----|  
(1) Set time  
(2) Set Password  
(3) Reboot  
(4) Factory Restore  
(5) Factory Reset
```

Note: Once Factory Reset command is executed successfully all sensitive key material and crypto specific data will be disposed PERMANANTLY during the reboot.

5. 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.

5.1 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 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

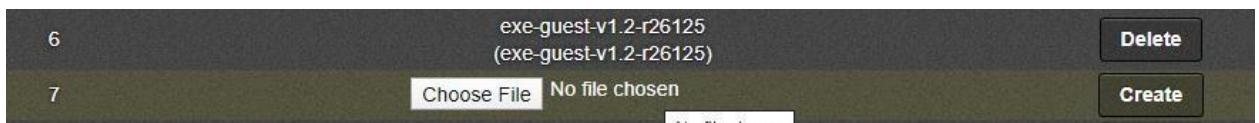


Figure 23: Selecting the image file to Upgrade

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>”

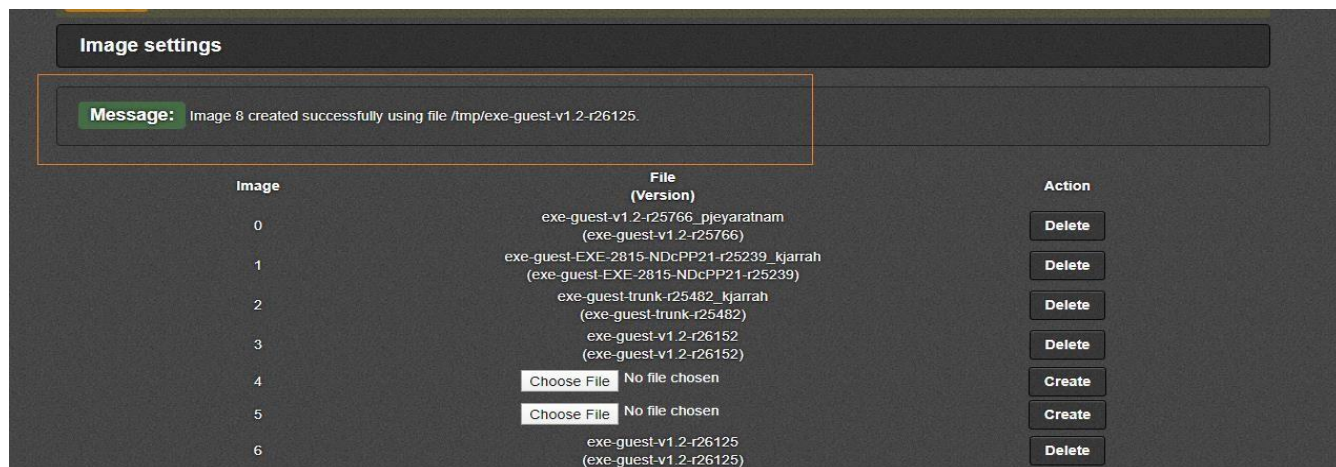


Figure 24: Image details

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

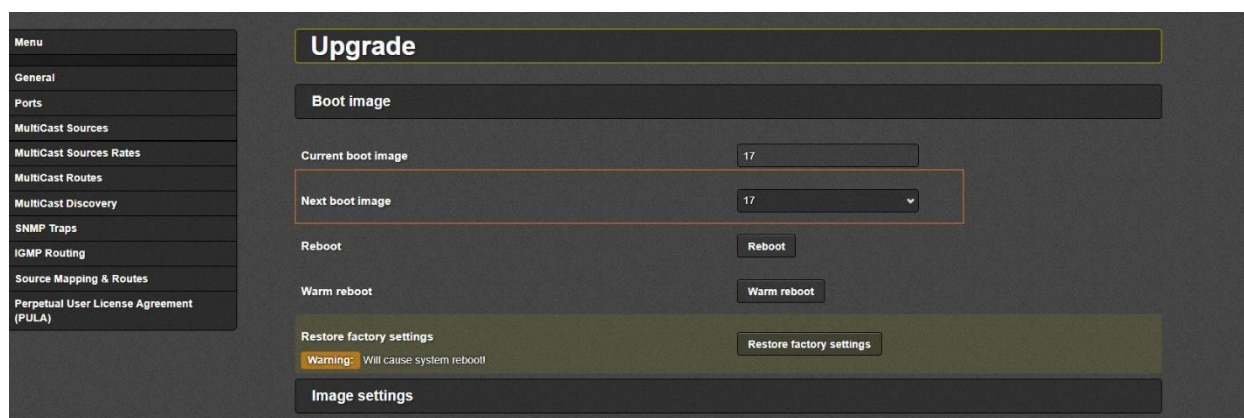


Figure 25: Boot Image Selection

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

5.2 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.

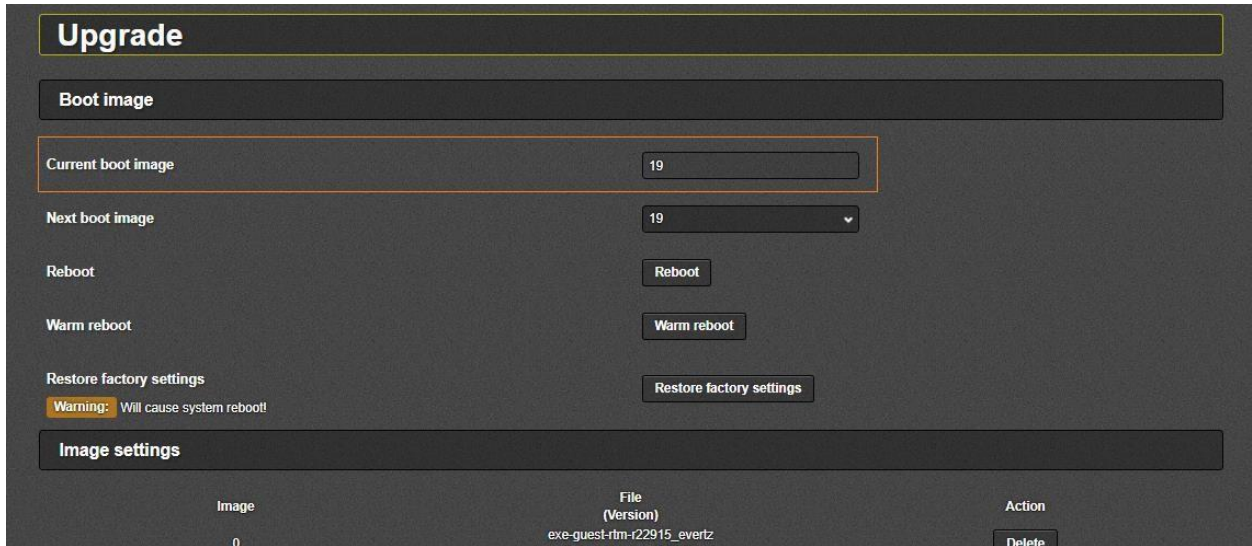


Figure 26: Verify Active Boot Image

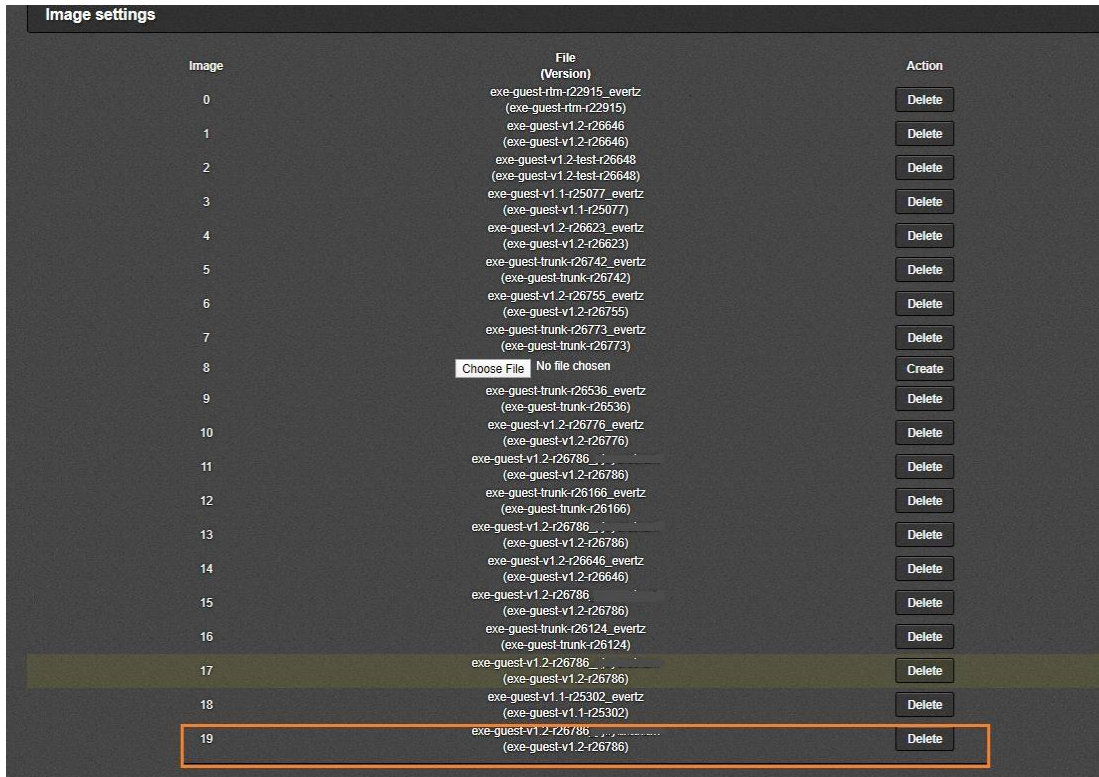


Figure 27: Reviewing the list of active and inactive Images.

Note:

The ‘Image Settings’ section shows all the image files (active and inactive) that are loaded onto the TOE.

5.3 Switch an Inactive Image to Active Image

Prerequisites

- None

Steps

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

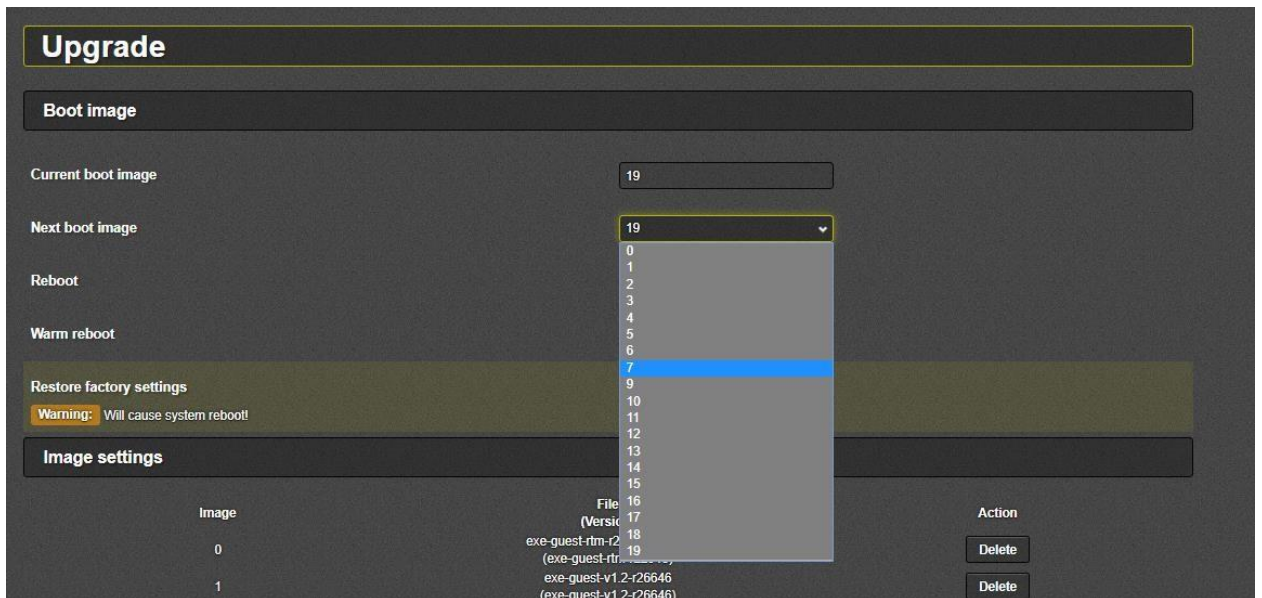


Figure 28: Selecting next boot image

4. Click “Reboot” button for the image to be booted as the new active firmware image

5.4 Upgrade Errors

5.4.1 Upgrade Errors: Without a Signature

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

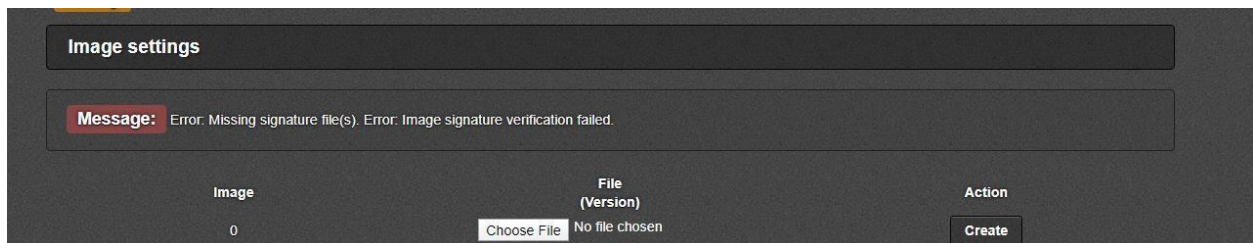


Figure 29: Error upgrading to an image with no signature

5.4.2 Upgrade Errors: Corrupted Image

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

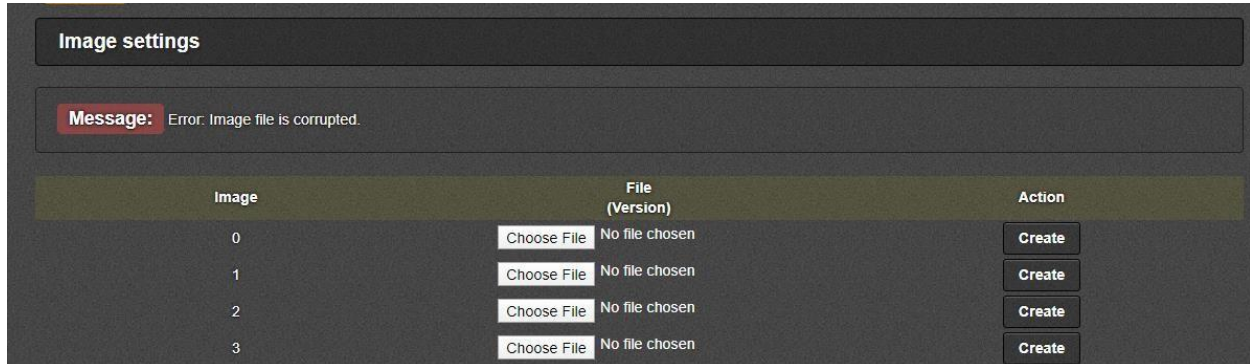


Figure 30: Error upgrading a corrupted image

5.4.3 Upgrade Errors: Bad Signature

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

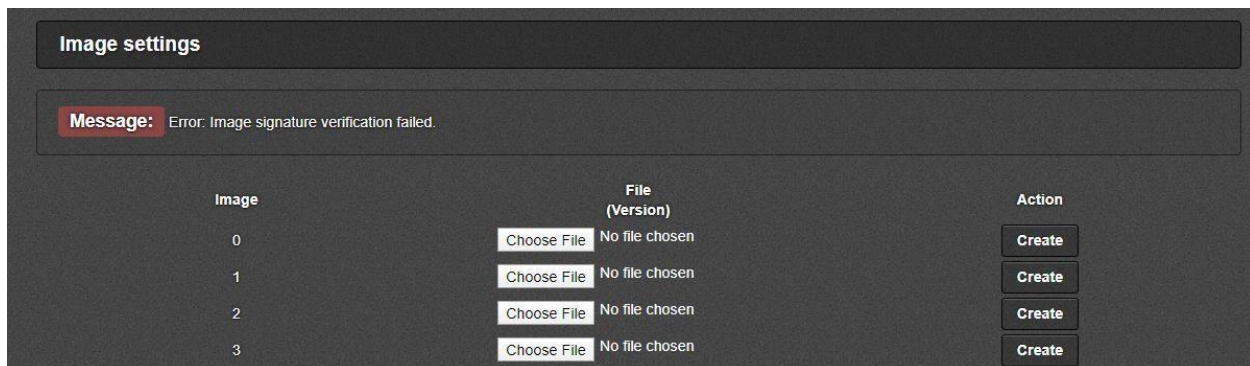


Figure 31: Error upgrading with an image with mismatched signature

6. Audit Events

EXE is able to 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.

6.1 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.

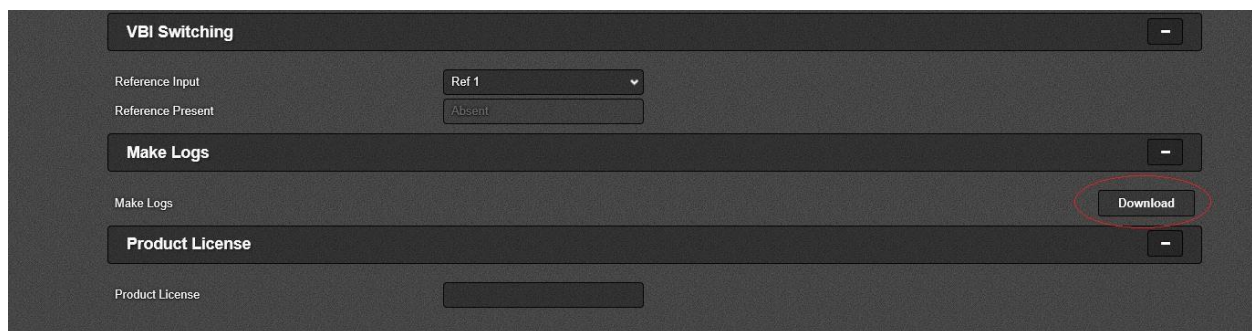


Figure 32: Download Audit Events

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 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 . *In the CC evaluated configuration, the audit log path cannot be accessed by the recovery user through the console.*

6.2 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

The screenshot displays the EXE Management Web Application interface. The left sidebar contains a navigation menu with items like Fabric Cards, Line Cards, Ports, MultiCast Sources, MultiCast Maintenance, MultiCast Sources Rates, MultiCast Routes, MultiCast Discovery, SNMP Traps, Defect Report, IGMP Routing, Source Mapping & Routes, and Perpetual User License Agreement (PULA). The main content area shows configuration for a device named EXE16-FC-NCS. The 'Software' section includes Revision Major (1), Revision Minor (5), and Build Number (38456). The 'Board' section includes Serial Number (-), Name (EXE-VSR-A), Revision (2), and Build Number (1). The 'Log Streaming' section is highlighted with an orange border and contains the following configuration for 'Sys Log 1':

Field	Value
Enable	Enabled
Destination IP Address	172.17.219.100
Destination Port	6,514 (100 to 65535)
Level	Informational
Reference Identifier	rsyslog.acumen.com
Import CA Certificate	Browse... No file selected.

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

6.3 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
Administrative login and logout	<p>WebGUI Login:</p> <pre>2023-04-13T07:09:11.271017+00:00 EXE-FCNCS-01 local0.notice user_action 17612 - - Webeasy: User "root:172.17.219.99" logged in. 2023-04-13T07:09:11.273287+00:00 EXE-FCNCS-01 user.notice lighttpd - - - Access log: User "root:172.17.219.99" logged in.</pre> <p>WebGUI Logout:</p> <pre>2023-04-13T07:11:24.359917+00:00 EXE-FCNCS-01 local0.notice user_action 25456 - - Webeasy: User "root:172.17.219.99" logged out. 2023-04-13T07:11:24.362188+00:00 EXE-FCNCS-01 user.notice lighttpd - - - Access log: User "root:172.17.219.99" logged out.</pre> <p>Console Login:</p> <pre>2023-08-31T09:53:30.851580+00:00 EXE-FCNCS-01 authpriv.info login 21841 - - DIALUP AT ttyS0 BY recovery 2023-08-31T09:53:30.851585+00:00 EXE-FCNCS-01 authpriv.info login 21841 - - LOGIN ON ttyS0 BY recovery EXE-FCNCS-01#</pre> <p>Console Logout:</p>
Generating/import of, changing, or deleting of cryptographic keys	<pre>2023-04-10T09:48:17.253359+00:00 EXE-FCNCS-01 local0.notice regenerate_export_csr 9070 - - CSR Regeneration and export succeeded 2023-04-10T09:48:17.261281+00:00 EXE-FCNCS-01 local0.notice user_action 9330 - - Webeasy: User "root:172.17.219.99" regenerated csr successfully.</pre>
Resetting passwords	<pre>2023-09-15T09:07:06.273613+00:00 EXE-FCNCS-01 local0.notice user_update 9614 - - Webeasy: User "good1:172.17.219.99" updated password. 2023-09-15T09:07:06.280397+00:00 EXE-FCNCS-01 local0.notice user_action 9617 - - Webeasy: User "good1:172.17.219.99" logged i n.</pre>
Failure to establish a HTTPS Session	Please refer to "Failure of the trusted path functions (WebGUI)" below for related audit logs.
Failure to establish a TLS Session when the EXE acting as a TLS Client	Server using unsupported cipher suite: -

Auditable Events	Sample Logs
	<p>2023-03-23T10:17:11.221038+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 15901 - - SSL_connect: 0:error:1421C105:SSL routines:set_client_ciphersuite:wrong cipher returned:ssl/statem/statem_clnt.c:1342:</p> <p>Server using ECDHE key exchange with an unsupported Elliptic Curve: -</p> <p>2023-03-23T10:23:01.490617+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 29582 - - SSL_connect: 0:error:141A417A:SSL routines:tls_process_ske_ecdhe:wrong curve:ssl/statem/statem_clnt.c:2210:</p> <p>Server using unsupported TLS version: -</p> <p>2023-03-23T10:32:16.885820+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 19059 - - SSL_connect: 0:error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol:ssl/statem/statem_lib.c:1957:</p> <p>Modify signature in the server key exchange: -</p> <p>2023-03-23T10:38:02.137856+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 32501 - - SSL_connect: 0:error:0407008A:rsa routines:RSA_padding_check_PKCS1_type_1:invalid padding:crypto/rsa/rsa_pkl.c:66:</p> <p>2023-03-23T10:38:02.137862+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 32501 - - SSL_connect: 0:error:04067072:rsa routines:rsa_ossl_public_decrypt:padding check failed:crypto/rsa/rsa_ossl.c:662:</p> <p>Modify byte in the server finish message: -</p> <p>2023-03-23T10:46:52.531938+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 21255 - - SSL_connect: 0:error:1416C095:SSL routines:tls_process_finished:digest check failed:ssl/statem/statem_lib.c:811:</p> <p>Receiving a garbled message after Change Cipher Spec message: -</p>

Auditable Events	Sample Logs
	<p>2023-03-23T10:53:27.834477+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 4239 - - SSL_connect: 0:error:14094091:SSL routines:ssl3_read_bytes:data between ccs and finished:ssl/record/rec_layer_s3.c:1347:</p>
<p>Failure to establish a TLS Session when the TOE acts as a TLS Server for WebGUI</p>	<p>Receiving a Client hello with unsupported cipher suites: -</p> <p>2023-03-29T09:29:55.006362+00:00 EXE-FCNCS-01 daemon.info lighttpd 6570 - - SSL_read: 0:error:1417A0C1:SSL routines:tls_post_process_client_hello: no shared cipher:ssl/statem/statem_srvr.c:2283:</p> <p>2023-03-29T09:29:55.006372+00:00 EXE-FCNCS-01 daemon.err lighttpd 6570 - - connection_read_cq_ssl: Connection to 172.17.219.99:46470 failed!</p> <p>Receiving a client finish message with modified Bytes: -</p> <p>2023-03-29T10:17:08.966384+00:00 EXE-FCNCS-01 daemon.info lighttpd 6570 - - SSL_read: 0:error:1416C095:SSL routines:tls_process_finished: digest check failed:ssl/statem/statem_lib.c:811:</p> <p>2023-03-29T10:17:08.966392+00:00 EXE-FCNCS-01 daemon.err lighttpd 6570 - - connection_read_cq_ssl: Connection to 172.17.219.99:41748 failed!</p> <p>Receiving a Client Hello with an unsupported Elliptic Curve:-</p> <p>2023-03-30T08:02:43.084913+00:00 EXE-FCNCS-01 daemon.info lighttpd 6570 - - SSL_read: 0:error:1417A0C1:SSL routines:tls_post_process_client_hello: no shared cipher:ssl/statem/statem_srvr.c:2283:</p> <p>2023-03-30T08:02:43.084923+00:00 EXE-FCNCS-01 daemon.err lighttpd 6570 - - connection_read_cq_ssl: Connection to 172.17.219.99:42766 failed!</p>
<p>Failure to authenticate the client when the EXE acts as the TLS Server for Magnum Connections (Synergy)</p>	<p>Client using unsupported cipher-suites: -</p> <p>2023-03-29T09:29:55.006362+00:00 EXE-FCNCS-01 daemon.info lighttpd 6570 - - SSL_read: 0:error:1417A0C1:SSL routines:tls_post_process_client_hello: no shared cipher:ssl/statem/statem_srvr.c:2283:</p> <p>2023-03-29T09:29:55.006372+00:00 EXE-FCNCS-01 daemon.err lighttpd 6570 - - connection_read_cq_ssl: Connection to 172.17.219.99:46470 failed!</p> <p>Client using unsupported Signature Algorithm: -</p>

Auditable Events	Sample Logs
	<pre> 2023-08-03T12:44:05.749534+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - Certificate verification failed: depth=0 s ubject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=mutual.acumen.com errmsg=certificate signature failure 2023-08-03T12:44:05.749592+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - SSL_accept: return=-1 ssl_error=5 err_msg= 'Success' 2023-08-03T12:44:05.749593+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - SYNERGY: accept() on ssl client failed 2023-08-03T12:44:05.749593+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - SYNERGY: Closing connection to 172.17.219. 100:53056 2023-08-03T12:44:05.749594+00:00 EXE-FCNCS-01 user.info synergy_server 5900 - - SYNERGY: closing 0x55ef6c3c83e0 Receiving a Client Certificate Verify handshake message with an modified byte in the signature block: - 2023-10-27T08:05:40.551746+00:00 EXE-FCNCS-01 user.info synergy_server 5913 - - SSL_accept: 0:error:0407E086:rsa routines:RSA_ver ify_PKCS1_PSS_mgf1:last octet invalid:crypto/rsa/rsa_pss.c:88: 2023-10-27T08:05:40.551754+00:00 EXE-FCNCS-01 user.info synergy_server 5913 - - SSL_accept: 0:error:1417B07B:SSL routines:tls_pro cess_cert_verify:bad signature:ssl/statem/statem_lib.c:504: Receiving a client certificate that is signed by an CA that is not in the EXE's trust store: - 2023-08-03T13:29:39.349278+00:00 EXE-FCNCS-01 user.info synergy_server 5900 - - SYNERGY: Connection accepted 2023-08-03T13:29:39.349281+00:00 EXE-FCNCS-01 user.info synergy_server 5900 - - SYNERGY: Accepted inet connection from 17 2.17.219.100:36920 2023-08-03T13:29:39.350235+00:00 EXE-FCNCS-01 user.notice synergy_server 5900 - - Using non-blocking socket (10). 2023-08-03T13:29:39.360980+00:00 EXE-FCNCS-01 user.notice synergy_server 5900 - - SSL_accept: SSL_ERROR_WANT_READ 2023-08-03T13:29:39.383431+00:00 EXE-FCNCS-01 user.info synergy_server 5900 - - SSL_accept: 0:error:1417C086:SSL routine s:tls_process_client_certificate:certificate verify failed:ssl/statem/statem_srvr.c:3760: 2023-08-03T13:29:39.383403+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - Certificate verification failed: depth=0 s ubject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=mutual.acumen.com errmsg=unable to get local issuer certificate 2023-08-03T13:29:39.383435+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - SSL_accept: return=-1 ssl_error=5 err_msg= 'Success' 2023-08-03T13:29:39.383436+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - SYNERGY: accept() on ssl client failed 2023-08-03T13:29:39.383436+00:00 EXE-FCNCS-01 user.err synergy_server 5900 - - SYNERGY: Closing connection to 172.17.219. 100:36920 </pre>
<p>Unsuccessful login attempts limit is met or exceeded</p>	<pre> 2023-04-10T05:34:07.235042+00:00 EXE-FCNCS-01 local0.notice user_action 15287 - - Webeasy: User "acumen:172.17.219.99" was permanently locked out (max failed login attempts reached). </pre>
<p>Failure of identification and authentication mechanism</p>	<pre> Console: - 2023-08-31T09:50:13.873598+00:00 EXE-FCNCS-01 authpriv.notice login 6241 - - pam_unix(login:auth): authentication failure; logname=recovery uid=0 euid=0 tty=/dev/ttyS0 ruser= rhost= user=recovery 2023-08-31T09:50:15.684620+00:00 EXE-FCNCS-01 authpriv.notice login 6241 - - FAILED LOGIN SESSION FROM ttyS0 FOR recovery, Authentication failure EXE-FCNCS-01# WebGUI: - 2023-04-10T07:22:32.868734+00:00 EXE-FCNCS-01 local0.notice user_action 15115 - - Webeasy: User "root:172.17.219.99" login failed. 2023-04-10T07:22:32.870978+00:00 EXE-FCNCS-01 user.notice lighttpd - - - Access log: User "root:172.17.219.99" login failed. </pre>

Auditable Events	Sample Logs
Successful identification and authentication mechanism	<i>Please refer to "Administrative login and logout" above for the related audit logs.</i>
Unsuccessful attempt to validate a certificate	<p>When the issuer certificate is not found:</p> <pre> 2023-08-09T12:44:07.456931+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 14642 - - LOG5[22]: s_connect: connected 172.17.219.100:6514 2023-08-09T12:44:07.456945+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 14642 - - LOG5[22]: Service [rsyslog] co nected remote server from 172.17.219.170:35328 2023-08-09T12:44:07.462144+00:00 EXE-FCNCS-01 daemon.warning stunnel-rsyslog 14642 - - LOG4[22]: CERT: Pre-verificat ion error at dept=0: unable to get local issuer certificate. 2023-08-09T12:44:07.462166+00:00 EXE-FCNCS-01 daemon.warning stunnel-rsyslog 14642 - - LOG4[22]: Rejected by CERT at depth=0: C=US, ST=Maryland, O=Acumen, OU=CC, CN=rsyslog.acumen.com 2023-08-09T12:44:07.462218+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 14642 - - SSL_connect: 0:error:1416F086:SS L routines:tls_process_server_certificate:certificate verify failed:ssl/statem/statem_clnt.c:1913: 2023-08-09T12:44:07.462240+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 14642 - - LOG3[22]: SSL_connect: Peer sudde nly disconnected 2023-07-05T07:22:45.968227+00:00 EXE-FCNCS-01 daemon.warning stunnel-rsyslog 26909 - - LOG4[13117]: CERT: Pre-verificat ion error at dept=0: certificate has expired. EXE-FCNCS-01# 2023-08-25T05:46:09.155563+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 7574 - - LOG5[96]: CRL verification successful: dep th=2 issuer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA errmsg=ok. 2023-08-25T05:46:09.155748+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 7574 - - LOG5[96]: CRL verification successful: dep th=1 issuer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA errmsg=ok. 2023-08-25T05:46:09.162191+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 7574 - - LOG3[96]: CRL verification failed: depth=0 is suer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=rsyslog.acumen.com errmsg=certificate r evoked. 2023-08-25T05:46:09.162238+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 7574 - - SSL_connect: 0:error:1416F086:SSL routines:t ls_process_server_certificate:certificate verify failed:ssl/statem/statem_clnt.c:1913: 2023-08-25T05:46:09.162252+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 7574 - - LOG3[96]: SSL_connect: Peer suddenly disconne cted </pre>
Any addition, replacement or removal of trust anchors in the EXE's trust store	<pre> 2023-08-29T18:28:42.704452+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - /tmp/img/AcumenCAICA_EXE16_29082023.pem is a valid CA chain. 2023-08-29T18:28:42.705371+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - Found 2 CA certs in /tmp/img/AcumenCAICA_EXE16_2908202 3.pem. 2023-08-29T18:28:42.708653+00:00 EXE-FCNCS-01 user.notice root - - openssl crl2pkcs7 -nocrl -certfile /tmp/img/AcumenCAICA_EXE16_29082023 .pem 2023-08-29T18:28:42.708700+00:00 EXE-FCNCS-01 user.notice root - - openssl pkcs7 -print_certs -text -noout 2023-08-29T18:28:42.757016+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - Found CRL Sign bit set on all CA certs in /tmp/img/Acu menCAICA_EXE16_29082023.pem. 2023-08-29T18:28:42.764671+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - copying /tmp/img/AcumenCAICA_EXE16_29082023.pem to /mnt /enclave/uploaded_certs/client-ca-chain-cert.incoming.pem: OK 2023-08-29T18:28:42.773744+00:00 EXE-FCNCS-01 local0.notice import_client_ca 896 - - security file "/tmp/img/AcumenCAICA_EXE16_29082023.pem " was deleted. 2023-08-29T18:28:42.775839+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - Importing CA chain certificate succeeded. 2023-08-29T18:28:42.789468+00:00 EXE-FCNCS-01 local0.notice import_client_ca 907 - - security file "/mnt/enclave/uploaded_certs.old/cert.pe m" was deleted. </pre> <p>Note: Removal of certificates is not an option. Certificates can only be added and replaced.</p>

Auditable Events	Sample Logs
<p>The EXE is unable to reach the CRL server, and it is failing to validate the certificate and rejecting the connection.</p>	<pre>2023-08-29T17:08:33.278809+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 9773 - - LOG5[4062]: s_connect: connected 172.17.219.100:6514 2023-08-29T17:08:33.278823+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 9773 - - LOG5[4062]: Service [rsyslog] connected remote server from 172.17.219.170:60670 2023-08-29T17:08:33.284089+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 9773 - - LOG5[4062]: CRL verification successful: depth=2 issu er=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA errmsg=ok. 2023-08-29T17:08:33.284272+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 9773 - - LOG5[4062]: CRL verification successful: depth=1 issu er=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA errmsg=ok. 2023-08-29T17:08:36.372086+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 9773 - - LOG3[4062]: CRL download failed (URI: http://172.17.219. 9/AcumenICA-New1.cr1)</pre>
<p>All management activities that changes EXE's configuration data.</p>	<ul style="list-style-type: none"> • Administering the EXE locally and remotely; <pre>2023-08-31T10:23:08.324976+00:00 EXE-FCNCS-01 local0.info recoverysh 29020 - - User "recovery:console" set time to "Thu Aug 31 10:23:08 UTC 2023" successfully. EXE-FCNCS-01#</pre> • Configuring the access banner; <pre>2023-04-13T07:31:16.141885+00:00 EXE-FCNCS-01 user.info cfgjsonrpc 29009 - - [195 process] Login banner was modified 2023-04-13T07:31:16.151701+00:00 EXE-FCNCS-01 user.info cfgjsonrpc 29009 - - [050 onReceive] [root:172.17.219.99] PULA update was successful.</pre> • Configuring the session inactivity time before session termination or locking; <pre>2023-08-31T08:14:41.225092+00:00 EXE-FCNCS-01 local0.notice user_action 12800 - - Webeasy: User "root:172.17.219.99" set se ssion timeout to "120".</pre> • Updating the EXE, and to verify the updates using [digital signature] capability prior to installing those updates; <p>Please refer to "Initiation of Secure updates" below for the related audit logs.</p> • Configuring the authentication failure parameters. <pre>2023-04-10T05:25:46.370566+00:00 EXE-FCNCS-01 local0.notice /bin/user_action 27769 - - Webeasy: User "root:172.17.219.99" set max failed login attempts to "3".</pre> • Managing cryptographic keys. <p>Please refer to "Generating/import of, changing, or deleting of cryptographic keys" above for related audit logs.</p> • Ability to import X.509v3 certificates to the EXE's trust store.

Auditable Events	Sample Logs
	<pre> 2023-08-29T18:28:42.704452+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - /tmp/img/AcumenCAICA_EXE16_29082023.pem is a valid CA chain. 2023-08-29T18:28:42.705371+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - Found 2 CA certs in /tmp/img/AcumenCAICA_EXE16_29082023.pem. 2023-08-29T18:28:42.708653+00:00 EXE-FCNCS-01 user.notice root - - openssl crl2pkcs7 -nocrl -certfile /tmp/img/AcumenCAICA_EXE16_29082023.pem 2023-08-29T18:28:42.708700+00:00 EXE-FCNCS-01 user.notice root - - openssl pkcs7 -print_certs -text -noout 2023-08-29T18:28:42.757016+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - Found CRL Sign bit set on all CA certs in /tmp/img/AcumenCAICA_EXE16_29082023.pem. 2023-08-29T18:28:42.764671+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - copying /tmp/img/AcumenCAICA_EXE16_29082023.pem to /mnt/enclave/uploaded_certs/client-ca-chain-cert.incoming.pem: OK 2023-08-29T18:28:42.773744+00:00 EXE-FCNCS-01 local0.notice import_client_ca 896 - - security file "/tmp/img/AcumenCAICA_EXE16_29082023.pem" was deleted. 2023-08-29T18:28:42.775839+00:00 EXE-FCNCS-01 local0.notice import_client_ca 817 - - Importing CA chain certificate succeeded. </pre> <ul style="list-style-type: none"> • Ability to re-enable an Administrator account. <i>2023-04-10T06:23:18.990486+00:00 EXE-FCNCS-01 local0.notice user_action 2921 - - Webeasy: User "root:172.17.219.99" unlocked user "acumen".</i> • Ability to set the time which is used for timestamps. <pre> 2023-08-31T10:23:08.324976+00:00 EXE-FCNCS-01 local0.info recoverysh 29020 - - User "recovery:console" set time to "Thu Aug 31 10:23:08 UTC 2023" successfully. EXE-FCNCS-01# </pre>
<p>Discontinuous changes to time - either Administrator actuated or changed via an automated process</p>	<pre> 2023-08-31T10:23:08.324976+00:00 EXE-FCNCS-01 local0.info recoverysh 29020 - - User "recovery:console" set time to "Thu Aug 31 10:23:08 UTC 2023" successfully. EXE-FCNCS-01# </pre>
<p>Initiation of Secure updates</p>	<ul style="list-style-type: none"> • Successful attempt to initiate an update. <pre> 2023-09-25T13:17:26.976629+00:00 EXE-FCNCS-01 user.info image_config 32059 - - Creating image 5 using file /tmp/exe-guest-v1.5-r38456 ... 2023-09-25T13:17:28.416014+00:00 EXE-FCNCS-01 user.info image_config 32059 - - Image support for feature FCNCS detected 2023-09-25T13:17:30.604069+00:00 EXE-FCNCS-01 user.info image_config 32059 - - Image 5 created successfully using file /tmp/exe-guest-v1.5-r38456 EXE-FCNCS-01# 2023-09-25T13:22:14.824047+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Scrubbing boot images ... 2023-09-25T13:22:17.549388+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Setting next boot image to image 5 ... 2023-09-25T13:22:19.278216+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Image support for feature FCNCS detected 2023-09-25T13:22:23.981617+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Stopping app ... 2023-09-25T13:22:41.306052+00:00 EXE-FCNCS-01 user.info image_config 16729 - - App stopped successfully 2023-09-25T13:22:41.306355+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Image 5 set to be the next boot image successfully 2023-09-25T13:22:41.306365+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Image version upgraded from exe-guest-v1.5-r38382 to exe-guest-v1.5-r38456 successfully 2023-09-25T13:22:41.306371+00:00 EXE-FCNCS-01 user.info image_config 16729 - - Please reboot to use the next boot image EXE-FCNCS-01# </pre>

Auditable Events	Sample Logs
	<pre>2023-09-04T13:17:50.229134+00:00 EXE-FCNCS-01 user.notice cardedged 2976 - - Message Received: 1: EXE16-FC-NCS 1.5 build 38382 172.17.219.170 SECURE 2023-09-04T13:17:50.313713+00:00 EXE-FCNCS-01 user.notice auto_start - - Welcome to Version 1.5 build 38382 built on 2023 Aug 30 05:51:43 2023-09-04T13:18:10.910643+00:00 EXE-FCNCS-01 user.notice sc 5608 - - SETTINGS: Upgrading from build exe-guest-v1.5-r38360 2023-09-04T13:18:13.137553+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 6255 - - LOG5[ui]: stunnel 5.58 on x86_64-buildroot-linux-gnu platform 2023-09-04T13:18:50.280704+00:00 EXE-FCNCS-01 user.notice cardedged 2976 - - Message Received: 1: EXE16-FC-NCS 1.5 build 38382 172.17.219.170 SECURE EXE-FCNCS-01#</pre> <ul style="list-style-type: none"> • Unsuccessful attempt to initiate an update with a Modified image file. <pre>2023-05-04T15:31:17.699629+00:00 EXE-FCNCS-01 user.info image_config 18134 - - Creating image 11 using file /tmp/exe-guest-v1.5-r37421.is_corrupted ... 2023-05-04T15:31:17.713293+00:00 EXE-FCNCS-01 user.err image_config 18134 - - Image file is corrupted EXE-FCNCS-01#</pre> <ul style="list-style-type: none"> • Unsuccessful attempt to initiate an update with an image that has not been signed. <pre>2023-05-05T04:19:14.652386+00:00 EXE-FCNCS-01 user.err image_config 7569 - - Missing signatures 2023-05-05T04:19:14.652425+00:00 EXE-FCNCS-01 user.err image_config 7569 - - Image signature verification failed EXE-FCNCS-01#</pre> <ul style="list-style-type: none"> • Unsuccessful attempt to initiate an update with an image signed with invalid signature. <pre>2023-05-05T04:33:12.871561+00:00 EXE-FCNCS-01 user.err image_config 23064 - - Image signature verification failed EXE-FCNCS-01#</pre>
<p>The termination of a remote session by the session locking mechanism (exceeding the maximum number of login attempts)</p>	<pre>2023-04-10T05:34:07.235042+00:00 EXE-FCNCS-01 local0.notice /bin/user_action 15287 - - Webeasy: User "acumen:172.17.219.99" was permanently locked out (max failed login attempts reached).</pre>
<p>The termination of an interactive session (User initiated logout)</p>	<p><i>Please refer to "Administrative login and logout" above for the related audit logs.</i></p>
<p>The termination of a local session by the session locking mechanism</p>	<p><i>Note: Session locking mechanisms are not applied to the local Console user 'Recovery'.</i></p>

Auditable Events	Sample Logs
(exceeding the maximum number of login attempts)	
Initiation of the trusted channel (Syslog)	<pre> 2023-09-15T08:40:51.648411+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 18055 - - LOG5[125]: s_connect: connected 172.17.219.100:6514 2023-09-15T08:40:51.648433+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 18055 - - LOG5[125]: Service [rsyslog] connected remote server from 172.17.219.170:50120 2023-09-15T08:40:51.653704+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 18055 - - LOG5[125]: CRL verification successful: depth=2 issuer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA errmsg=ok. 2023-09-15T08:40:51.653895+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 18055 - - LOG5[125]: CRL verification successful: depth=1 issuer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=CA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA errmsg=ok. 2023-09-15T08:40:51.654564+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 18055 - - LOG3[125]: CRL download failed (URI: http://172.17.219.99/AcumenCA-New1.crl) 2023-09-15T08:40:51.654824+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 18055 - - LOG3[125]: CRL download failed (URI: http://172.17.219.99/AcumenICA-New1.crl) 2023-09-15T08:40:51.654861+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 18055 - - LOG5[125]: CRL verification successful: depth=0 issuer=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA subject=/C=US/ST=Maryland/O=Acumen/OU=CC/CN=rsyslog.acumen.com errmsg=ok. 2023-09-15T08:40:51.661471+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 18055 - - SSL_connect: Negotiated TLSv1.2 cipher suite: ECDHE-RSA-AES256-GCM-SHA384 (256-bit encryption) </pre>
Termination of the trusted channel (Syslog)	<pre> 2023-09-15T08:44:14.101791+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 30472 - - SSL_connect: Negotiated TLSv1.2 cipher suite: ECDHE-RSA-AES256-GCM-SHA384 (256-bit encryption) 2023-09-15T08:44:19.017196+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 30472 - - LOG5[164]: Connection closed: 8984 byte(s) sent to TLS, 0 byte(s) sent to socket 2023-09-15T08:44:19.017285+00:00 EXE-FCNCS-01 syslog.info rsyslogd 9885 - - Connection broken, socket fd = 13 [v8.2010.0] </pre>
Failure of the trusted channel functions (Syslog)	<pre> 2023-09-15T08:47:09.155098+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 8768 - - LOG5[198]: s_connect: connected 172.17.219.100:6514 2023-09-15T08:47:09.155112+00:00 EXE-FCNCS-01 daemon.notice stunnel-rsyslog 8768 - - LOG5[198]: Service [rsyslog] connected remote server from 172.17.219.170:50422 2023-09-15T08:47:09.156259+00:00 EXE-FCNCS-01 daemon.info stunnel-rsyslog 8768 - - SSL_connect: 0:error:1425F102:SSL routine:ssl_choose_client_version:unsupported protocol:ssl/statem/statem_lib.c:1957: 2023-09-15T08:47:09.156286+00:00 EXE-FCNCS-01 daemon.err stunnel-rsyslog 8768 - - LOG3[198]: SSL_connect: Peer suddenly disconnected </pre>
Initiation of the trusted path (WebGUI)	<p><i>Please refer to "Administrative login and logout" above for the related audit logs.</i></p>
Termination of the trusted path (WebGUI)	<p><i>Please refer to "Administrative login and logout" above for the related audit logs.</i></p>
Failure of the trusted path functions (WebGUI)	<pre> 2023-03-29T10:17:08.966384+00:00 EXE-FCNCS-01 daemon.info lighttpd 6570 - - SSL_read: 0:error:1416C095:SSL routines:tls_process_finished:digest check failed:ssl/statem/statem_lib.c:811: 2023-03-29T10:17:08.966392+00:00 EXE-FCNCS-01 daemon.err lighttpd 6570 - - connection_read_cq_ssl: Connection to 172.17.219.99:41748 failed! </pre>

Table 1: Audit Events

7. Appendix

7.1 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.

7.2 Reboot EXE

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