

IPX MMA10G-IPX v3.3

Security Administrative Guide Addendum for Common Criteria

Version 1.2, February 03, 2023

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:  @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 MAGNUM-HW 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.....	6
1.3 Operational Environment.....	7
2. Secure Installation	9
2.1 Obtaining and installing the CC Certified Firmware.....	9
2.1.1 Secure Delivery Verification.....	9
2.1.2 Device Registration.....	9
2.1.3 Physical security Requirements.....	9
2.1.4 Installing the unit.....	9
2.2 Physical Installation.....	10
2.3 Initial Configuration	10
2.3.1 Accessing the IPXS	10
2.3.2 Configure System Date and Time	11
2.3.3 Configure Network Profile	12
2.4 Secure Configuration.....	12
2.4.1 Configure Secure Mode	12
2.4.2 Verify Power-On Self-Tests	13
2.4.3 Verify Secure Mode Banners.....	15
2.4.4 Fips Mode	16
2.4.5 Self-Test	16
2.4.6 Cipher Suites	17
2.4.7 Key Parameters	17
2.4.8 Hash and Keyed-Hash Algorithms	17
2.4.9 Configure Access Controls.....	17
2.4.10 Configure TLS Server.....	22
2.4.11 Configure TLS Client	28
3. Secure Management.....	30
3.1 User Management	30
3.2 Certificate Management	33
3.3 Key/Cipher Management	34
3.3.1 Zeroing Crypto Material.....	34
4. Performing Secure Upgrade	36
4.1 Upgrade.....	36
4.2 Verify Current Installed Image.....	37
4.3 Switch an Inactive Image to Active Image.....	39
4.4 Upgrade Errors.....	39
4.4.1 Upgrade Errors: Without a Signature	39
4.4.2 Upgrade Errors: Corrupted Image	40
4.4.3 Upgrade Errors: Bad Signature	40
5. Audit Events.....	41



- 5.1 Viewing Audit Events via Web Interface 41
- 5.2 Offloading Audit Logs 42
- 5.3 Audit Events Table 43
- 6. Appendix.....48
 - 6.1 Communication of Magnum with IPX (Supplementary) 48
 - 6.2 Reboot IPX 48

Table of Figures

Figure 1 TOE Overview	8
Figure 2: Enabling Secure Mode	13
Figure 3: Signature Image Verification	14
Figure 4: Self-Test Verification	14
Figure 5: Self-Test during critical operation	15
Figure 6: Verify Secure Banner	15
Figure 7: Verify Secure Access Banner	16
Figure 8: Secure Passwords	18
Figure 9: Set Session Timeout	19
Figure 10: Strict Session Handling	20
Figure 11: Set Max Attempts	21
Figure 12: Configure Access Banner	21
Figure 13: Disable REST API	22
Figure 14: Generating a CSR	23
Figure 15: Download CSR	24
Figure 16: Magnum Reset TLS	25
Figure 17: Magnum Enable Encryption	25
Figure 18: Transfer CSR file to Magnum via WinSCP	26
Figure 19: OpenSSL command output for CSR signing	26
Figure 20: Upload Cert Chain	27
Figure 21: Upload SSL Certificate	28
Figure 22: Secure Log Service	29
Figure 23: User Management	30
Figure 24: New User Creation	31
Figure 25: New User Confirmation	31
Figure 26: New Role Creation	32
Figure 27: Roles Overview	33
Figure 28: Selecting the image file to Upgrade	36
Figure 29: Image details	37
Figure 30: Boot Image Selection	37
Figure 31: Verify Active Boot Image	38
Figure 32: Verify Active Boot Image Settings	38
Figure 33: Selecting next boot image	39
Figure 34: Error upgrading to an image with no signature	39
Figure 35: Error upgrading a corrupted image	40
Figure 36: Error upgrading with an image with mismatched signature	40
Figure 37: Download Audit Events	41

1. Introduction

1.1 Audience

This document is targeted to administrators configuring the TOE, specifically for the following Evertz supplied IPX hardware devices,

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

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

1.2 Objective

Objective of this document is to provide preparative and administrative measures for setting up the **IPX system in common criteria evaluated state**. It highlights the measures and administrative steps that are necessary to be undertaken to **configure and maintain** the IPX TOE 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 of 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]	Evertz IPX User Manual	Supplied after product purchase
[2]	RFC 5424 : Syslog Protocol	https://tools.ietf.org/html/rfc5424
[3]	RFC 5425 : Transport Layer Security	https://tools.ietf.org/html/rfc5425
[4]	RFC 5280: X509 PKI Cert and CRL Profile	https://tools.ietf.org/html/rfc5280

1.3 Operational Environment

Component	Required	Usage/Purpose Description for TOE Performance
Syslog Server	Yes	<ul style="list-style-type: none"> • Conformant to [2] • Conformant to [3] • Acts as a TLSv1.2 server • Supports client certificate authentication • Supports at least one of the following cipher suits (IANA) <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	Yes	<ul style="list-style-type: none"> • Internet Explorer/Google Chrome or Firefox • Supports TLSv1.2 protocol • Supports at least one of the following cipher suits <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	Yes	<ul style="list-style-type: none"> • Conformant to [4]

Magnum	Yes	<ul style="list-style-type: none"> • Video switching controller used for management of the TOE
Media Gateway	No	<ul style="list-style-type: none"> • Component which converts media streams • Not in scope
Video Destination Devices	No	<ul style="list-style-type: none"> • Component which is used for viewing video streams output by the TOE • Not in scope
Video Source Devices	No	<ul style="list-style-type: none"> • Component which feeds the video streams in to the network • Not in scope

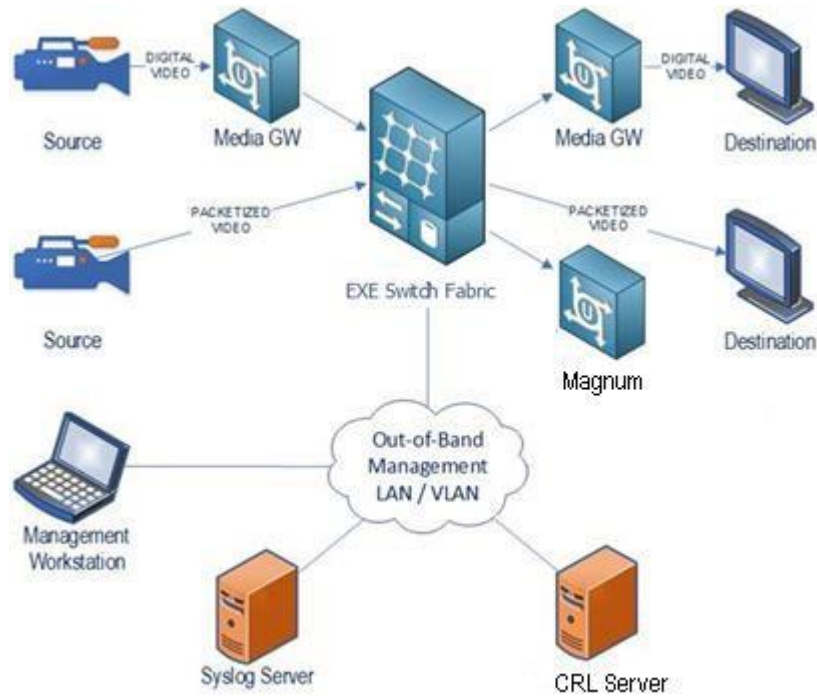


Figure 1 TOE Overview

2. Secure Installation

2.1 Obtaining and installing the CC Certified Firmware

2.1.1 Secure Delivery Verification

Before installing the Evertz IPX 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 you identify any concerns while verifying the integrity of the unit, contact your 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 IPX Server 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 IPX Server is installed in a secure physical location.
2. Physical access to the IPX Server 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 CC certified firmware

The validated firmware version is 3.3.

The IPX server 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 File Transfer Protocol Secure (FTPS) using signed and hashed code.

2.2 Physical Installation

For physical installation steps related to IPX, refer to EXE User Manual [1]. Preparation of the physical site and network are not in the scope of this document.

2.3 Initial Configuration

The IPX 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 TOE 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 IPX operational in a target TOE network environment:

- Configure System Date and Time
- Configure Network Profile

2.3.1 Accessing the IPXS

Login via Local Serial Connection

Prerequisites

- Administrator is equipped with tools capable of making a serial connection to IPX:
 - o Serial Cable
 - o Workstation (Windows)
 - o Serial Connection Program (Putty etc.)

Steps

1. Obtain the serial connection port (COM) in workstation
2. Run your serial connection program (Ex: Putty)
3. Set the parameters of serial connection
 - o COM Port
 - o Bits Per Second:
115200
 - o Data Bits: 8
 - o Stop
Bits: 2
 - o Flow Control: None

4. Confirm successful serial connection
5. Login to the CLI with administrator username and password.

Terminating Serial Console Connection

Prerequisites

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

Steps

1. Use the following to terminate the serial console connection

```
# logout
```

Note:

exit command can also be used instead of **logout** command to terminate serial console connection

Login via Web GUI

Prerequisites

- The steps in the 'Configure Network Profile' are complete and the IPX has network access via the configured IP address.

Steps

1. Using a web browser login to the IPX by entering `https://<ip address of the IPX>`
- 3) Log in with username of the administrative user and the password

Terminating Web Session

Prerequisites

- User already signed in to the web session

Steps

1. Click "**Logout**" button on top right corner

2.3.2 Configure System Date and Time

Prerequisites

- Successful local serial console connection to IPX

Steps

1. Log in to the IPX using administrative credentials
2. Use the following to set the date of system

```
# date -s "DD MONTH YEAR HH:MM:SS"
```

Example: If you want to set the date to 2022-May-01 and time to 16:06:00 type as below,

```
# date -s "1 MAY 2022 16:06:00"
```

3. Reboot the IPX
4. Confirm/Verify the date change by executing the following command in console `# date`

2.3.3 Configure Network Profile

Prerequisites

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

Steps

1. Login to the IPX using administrative credentials
2. Use the following to set the network parameters

```
# ncs_config ctrl_net set <ip_address> <netmask> <gateway>
```

Example: To set the IPX ip address to 172.16.227.52, netmask 255.255.0.0 and gateway to 172.16.1.1

```
# ncs_config ctrl_net set 172.16.227.52 255.255.0.0 172.16.1.1
```

3. Reboot IPX

2.4 Secure Configuration

2.4.1 Configure Secure Mode

Prerequisites

- Completion of prior steps

Steps

1. Login to the IPX **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

- Click **“Apply”** button at the top of the displayed page*

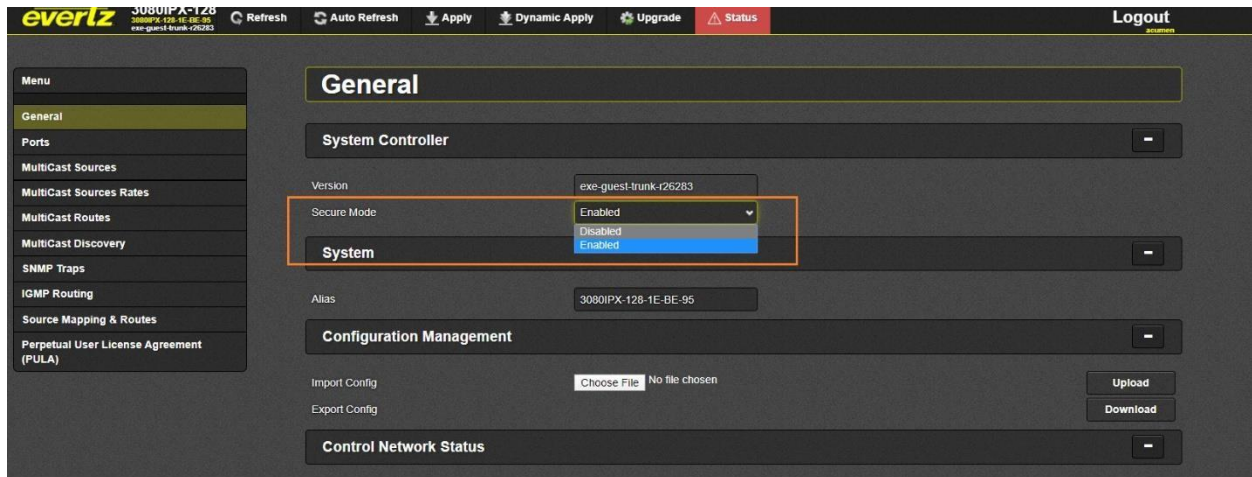


Figure 2: Enabling Secure Mode

Note:

Once **“Apply”** button is clicked some systems may reboot to boot in to secure-mode while others may require a manual reboot. Please refer you IPX user manual for details on the behavior.

2.4.2 Verify Power-On Self-Tests

IPX performs FIPS power-up self-test to ensure all applications are in compliance with FIPS 140-2 Security Policy. If self-test is failed, IPX will continue to perform securely but stays non-compliant to FIPS.

Prerequisites

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

Steps

1. Reboot IPX
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).

Successful Signature Image Verification

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

```

notice: configuring ctrl_net eth0 was successful
[ 48.210381] 8021q: adding VLAN 0 to HW filter on device eth1
[ 48.216367] ip (781) used greatest stack depth: 12880 bytes left
[ 48.394534] 8021q: adding VLAN 0 to HW filter on device eth1
[ 48.527401] 8021q: adding VLAN 0 to HW filter on device eth1
Notice: only main table catch all traffic
OK
Starting logging: OK
[ 48.913659] Run check for /etc/init.d/S024mlnx_fw_update_ncs
[ 48.959605] Run check for /etc/init.d/S025scrub_boot_images
[ 48.992871] Running /etc/init.d/S025scrub_boot_images
Starting power-on image sha256 checksum self-test: [ 49.409548] e1000e: eth0 NIC Link is Up 100 Mbps Full Duplex, Flow Control: None
[ 49.417127] e1000e 0000:00:19:0 eth0: 10/100 speed: disabling TSO
OK
Starting scrub_boot_images : OK
[ 52.956378] Run check for /etc/init.d/S026sensors_config_ncs
[ 53.020756] Run check for /etc/init.d/S027smartd
[ 53.072766] Running /etc/init.d/S027smartd

```

Figure 3: Signature Image Verification

Unsuccessful Signature Image Verification

Instead of **“OK”** the output would be **“FAILED”**. If the image verification failed, the system will not boot up beyond this point and administrator is required to contact Evertz product support for further resolution.

Successful Self-Test Verification

IPX 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

```

[ 16.880611] EXT4-fs (zram0): mounted filesystem without journal. Opts: (null)
[ 18.629669] S036orphan_code (1014): drop_caches: 3
Starting syslog compression: OK
Enabling fipscheck: OK
Generating 2048-bit rsa key... OK
[ 25.102422] EXT4-fs (dm-0): recovery complete
[ 25.109672] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Opts: (null)
Waiting for /mnt/enclave to mount...OK
Preparing /mnt/enclave...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

“Enabling fipscheck: Failed”

The system is allowed 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

If self-test verification failed during any critical operation, following output is produced in console “**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 IPX

Steps

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

```

[ 158.397283] hrtimer: interrupt took 8427 ns

You are accessing a U.S Government (USG) Information System (IS) that is provide
By using this IS (which includes any device attached to this IS), you consent to
-The USG routinely intercepts and monitors communications on the IS for purposes
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 subje
-This IS includes security measures (e.g. authentication and access controls) to
-Notwithstanding the above, this IS does not constitute consent to PM, LE or CI
ys, psychotherapists, or clergy, and their assistants. Such communications and w

3080IPX-128-1E-BE-95 login:
You are accessing a U.S Government (USG) Information System (IS) that is provide
By using this IS (which includes any device attached to this IS), you consent to
-The USG routinely intercepts and monitors communications on the IS for purposes
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 subje
-This IS includes security measures (e.g. authentication and access controls) to
-Notwithstanding the above, this IS does not constitute consent to PM, LE or CI
ys, psychotherapists, or clergy, and their assistants. Such communications and w

3080IPX-128-1E-BE-95 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.

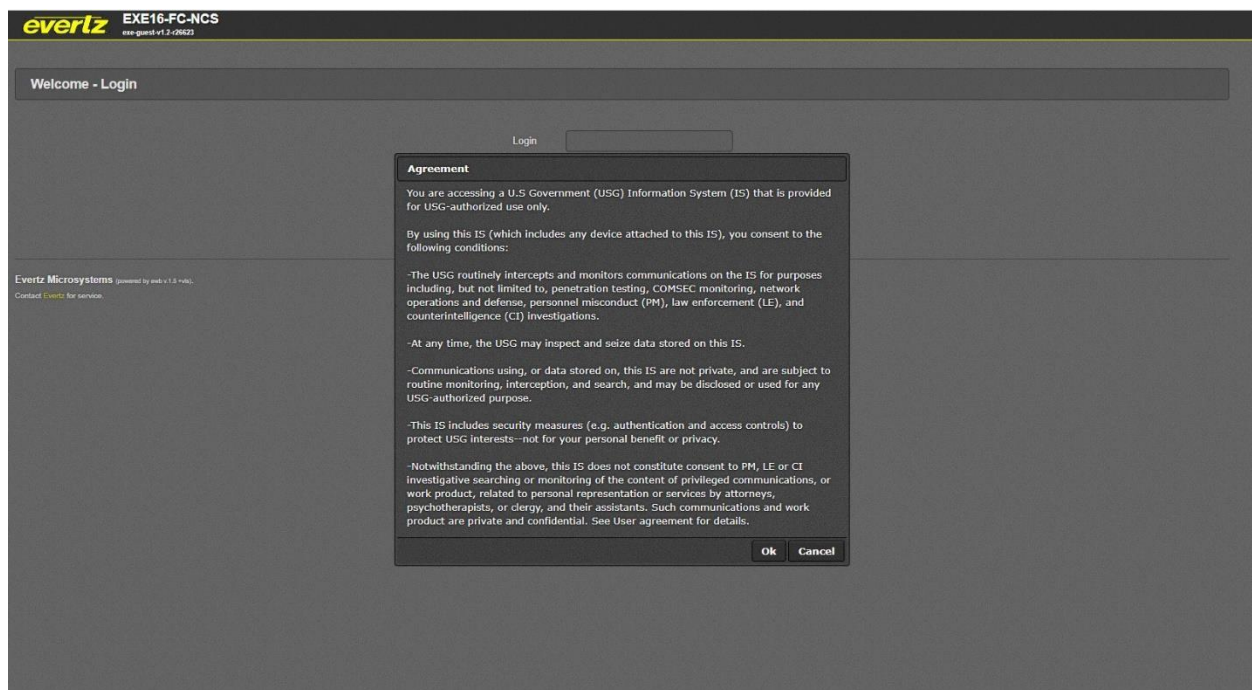


Figure 7: Verify Secure Access Banner

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

2.4.4 Fips Mode

IPX does not allow or provide interfaces for 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

IPX 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 Cipher Suites

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

2.4.7 Key Parameters

IPX does not allow or provide interfaces for the administrator to configure key generation parameters; Parameters are configured implicitly as in accordance with the CC evaluation criteria. IPX only supports generation of RSA keys.

2.4.8 Hash and Keyed-Hash Algorithms

IPX does not allow or provide interfaces for the administrator to configure Hash or Keyed Hash algorithm parameters; Parameters are configured implicitly as in accordance with the CC evaluation criteria. By default, IPX 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.

2.4.9 Configure Access Controls

The IPX class of switches 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, IPX class of switches supports unauthorized access prevention through the use of username/password combinations. The administrator is able to access and configure the IPX 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 IPX class of switches 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 IPX **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

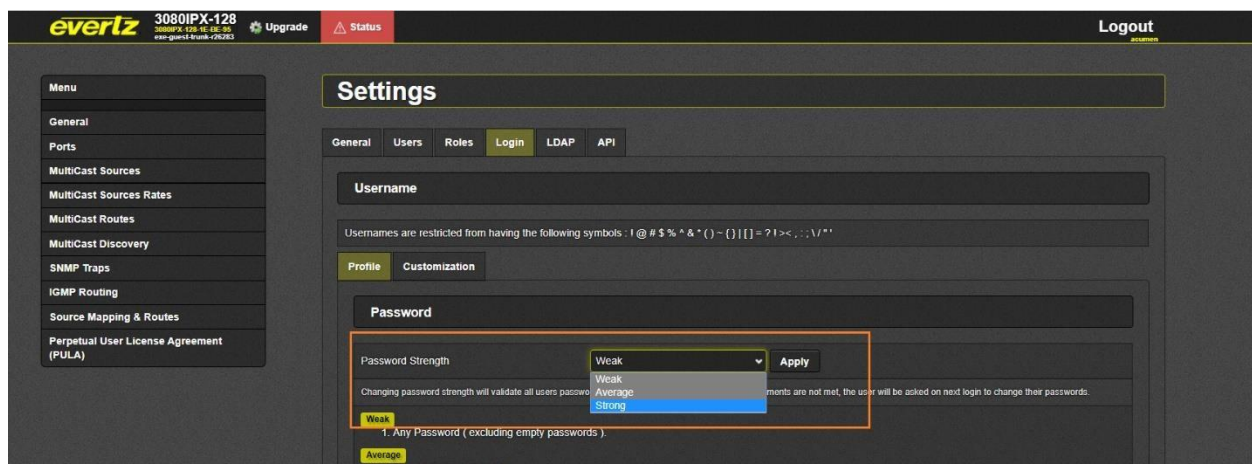


Figure 8: Secure Passwords

Once the above choice is made, IPX 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: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, “;”];
- b) Minimum password length shall be configurable to between [15] and [20] characters.

Set Session Timeout

Prerequisites

- Completion of prior steps

Steps

1. Login to the IPX **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

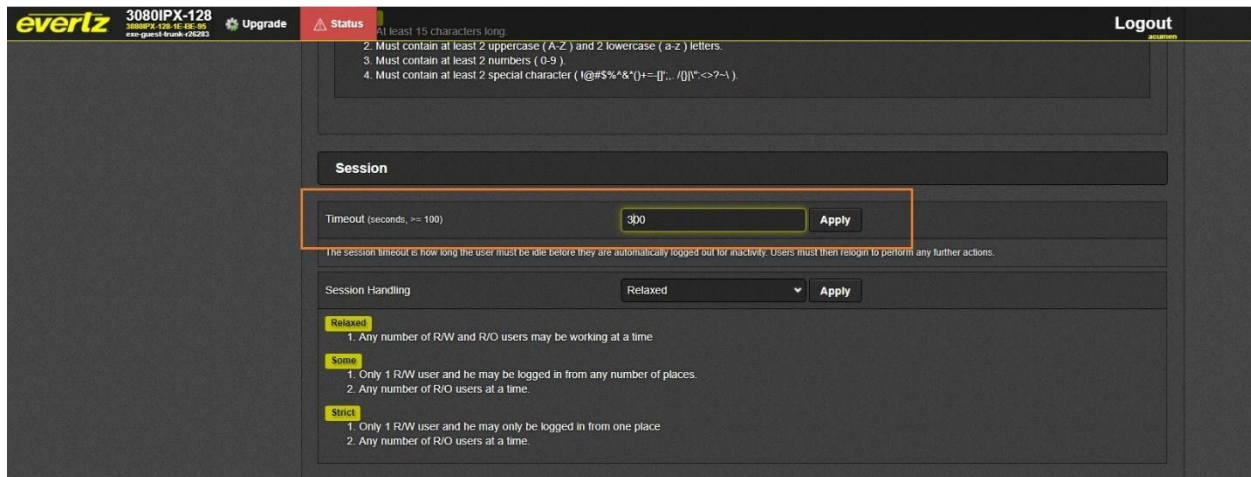


Figure 9: Set Session Timeout

Configure Session Handling

Prerequisites

- Completion of prior steps

Steps

1. Login to the IPX **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

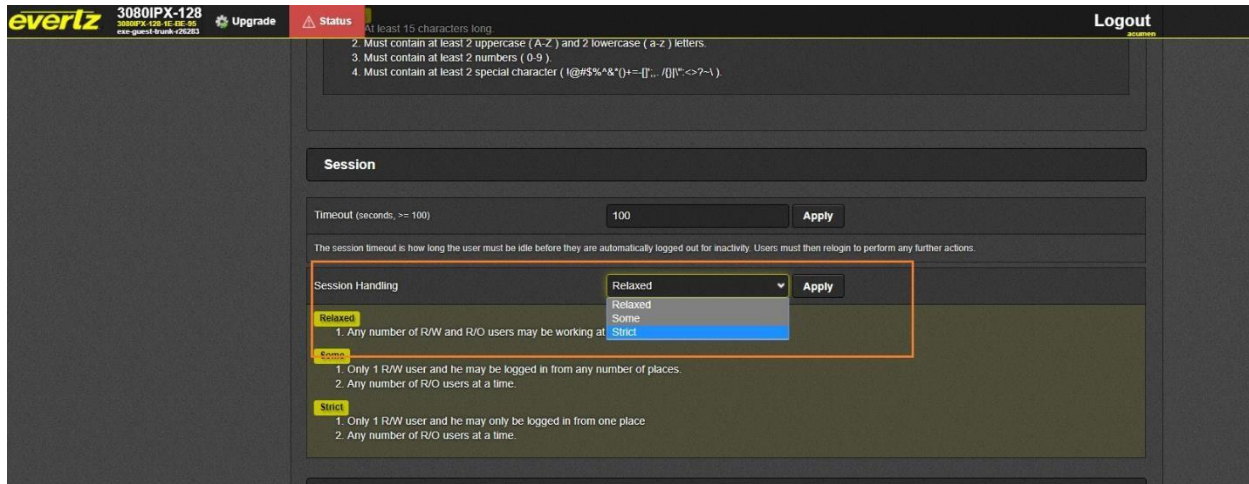


Figure 10: Strict Session Handling

Limit Login Attempts

Prerequisites

- Completion of prior steps

Steps

1. Login to the IPX **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 ONLY for web console-based sessions. It is not applicable for local console sessions.

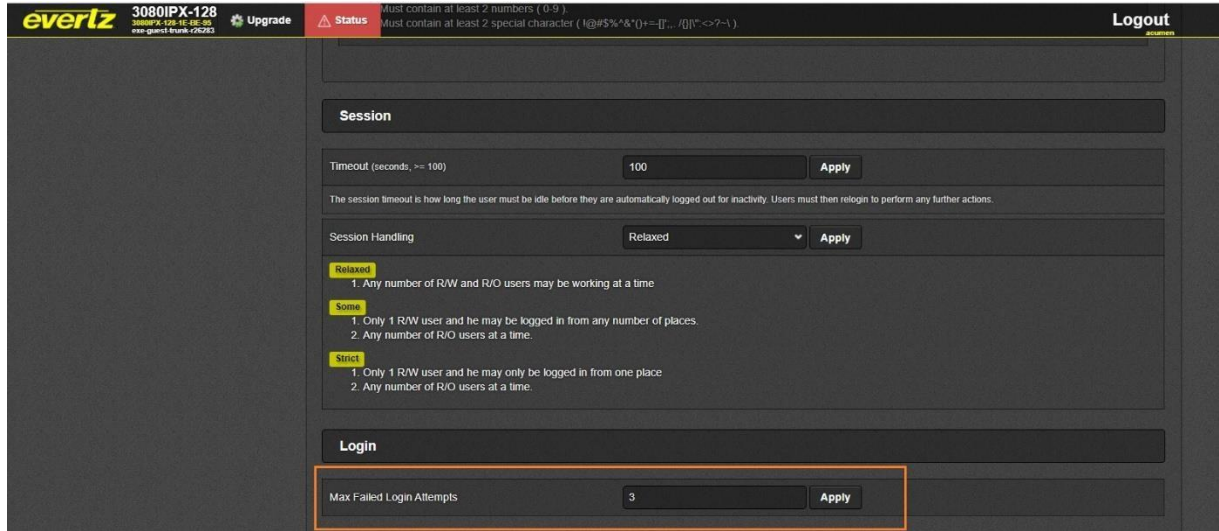


Figure 11: Set Max Attempts

Configure Secure Access Banner

Prerequisites

- Completion of prior steps

Steps

1. Login to the IPX **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

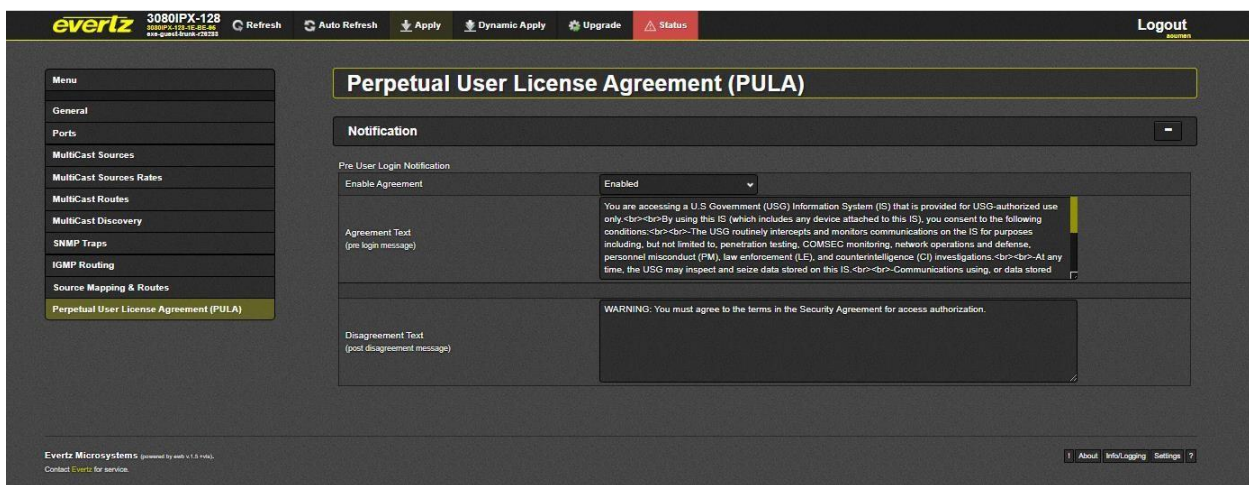


Figure 12: Configure Access Banner

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

Disable REST API

Prerequisites

- Completion of prior steps

Steps

1. Login to the **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”**

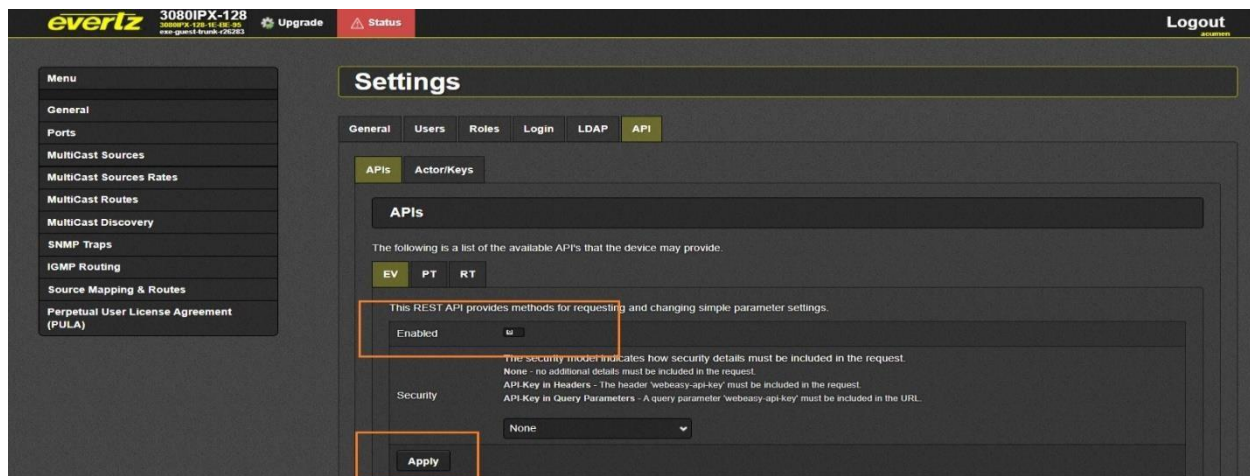


Figure 13: Disable REST API

2.4.10 Configure TLS Server

In IPX both HTTP and Synergy Server (Magnum) use TLS Server capabilities to provide secure form of 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

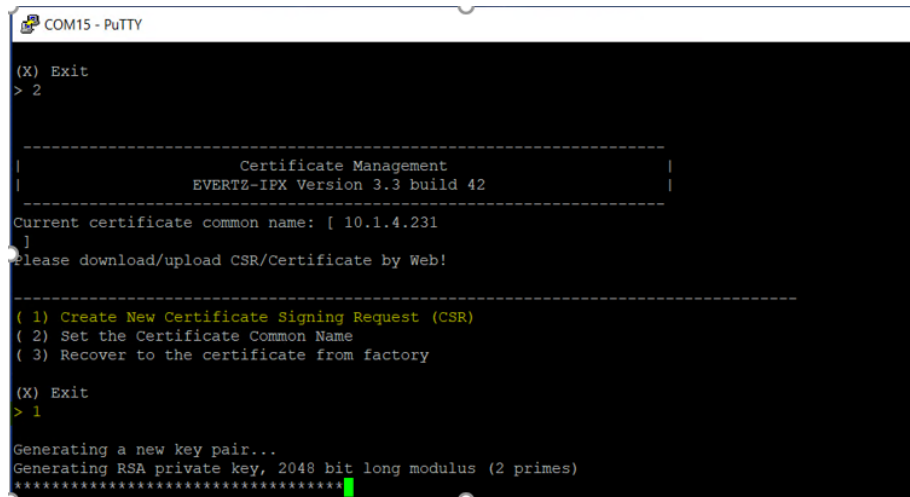
Create Certificate Signing Request

Prerequisites

- None

Steps

1. Login to the IPX **Serial Console**
2. Go to '**Certificate Management**' and select the option **(1) Create New Certificate Signing Request (CSR)**
3. Enter the following fields.
 - Common Name
 - Organization
 - Organizational Unit
 - Country
4. Generate the CSR.



```
COM15 - PuTTY
(X) Exit
> 2

-----
|                               |
|           Certificate Management           |
|           EVERTZ-IPX Version 3.3 build 42   |
|-----|
Current certificate common name: [ 10.1.4.231
]
Please download/upload CSR/Certificate by Web!

-----
( 1) Create New Certificate Signing Request (CSR)
( 2) Set the Certificate Common Name
( 3) Recover to the certificate from factory

(X) Exit
> 1

Generating a new key pair...
Generating RSA private key, 2048 bit long modulus (2 primes)
*****
```

Figure 14: Generating a CSR

Download Certificate Signing Request

Prerequisites

- Completion of prior steps

Steps

1. Login to the IPX **Management Web Application**
2. Click "**General**" menu from Menus listed on left of the displayed index page
3. Scroll down to "**Credentials**" section
4. Click "**Download**" button from "**CSR Regenerate and Download**" segment

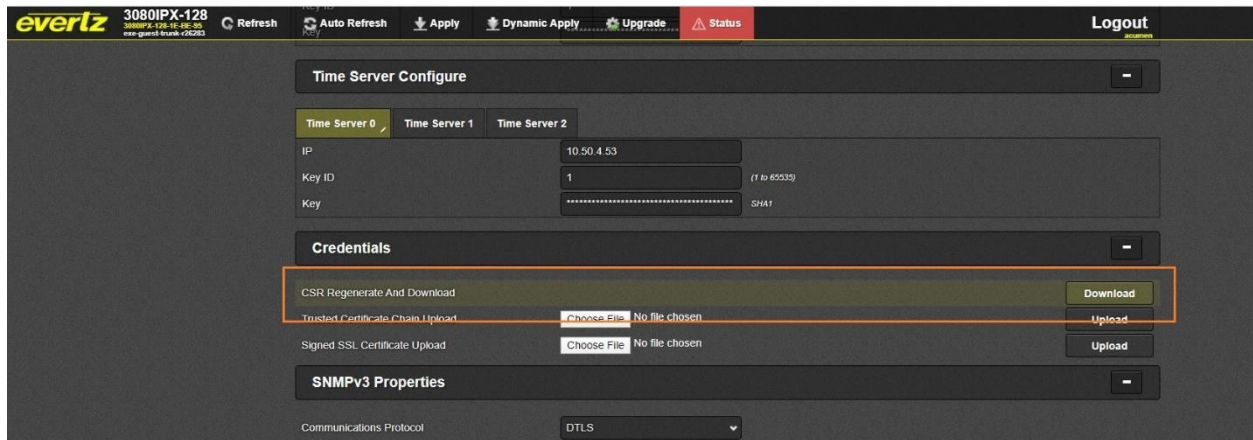


Figure 15: Download CSR

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 IPX 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

Signing the CSR using Evertz Magnum as CA

Note:

Please refer to latest "Magnum User Manual" for detailed steps on using Magnum as CA

Setting Evertz Magnum to Secure Mode

1. Obtain latest security build for magnum and upgrade it
2. Open an SSH connection to SDVN's IP address.
3. Login with admin/admin credentials.
4. Navigate to Security
5. Select Reset TLS key

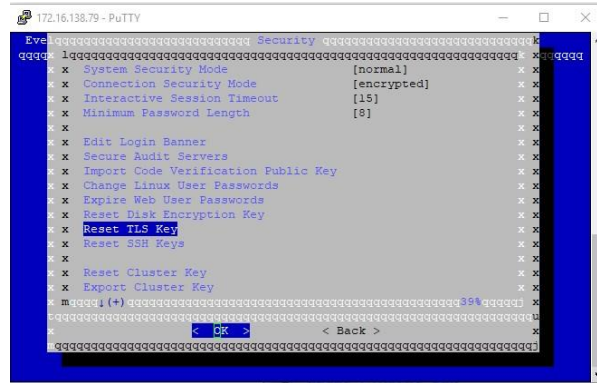


Figure 16: Magnum Reset TLS

6. Set “connection security mode” to “encrypted”

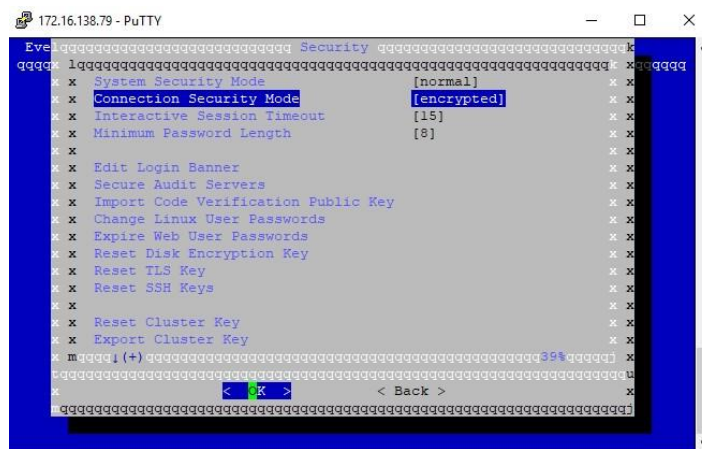


Figure 17: Magnum Enable Encryption

Sign Certificate (Using Magnum as Certificate Authority)

1. Set Magnum to Secure-Mode (Ref Appendix → Setting Magnum to Secure Mode)
2. Use the downloaded CSR file from IPX. Using WinSCP, login in Magnum at etdev, transfer the downloaded “csr.pem” file to Magnum’s /etdev/ folder

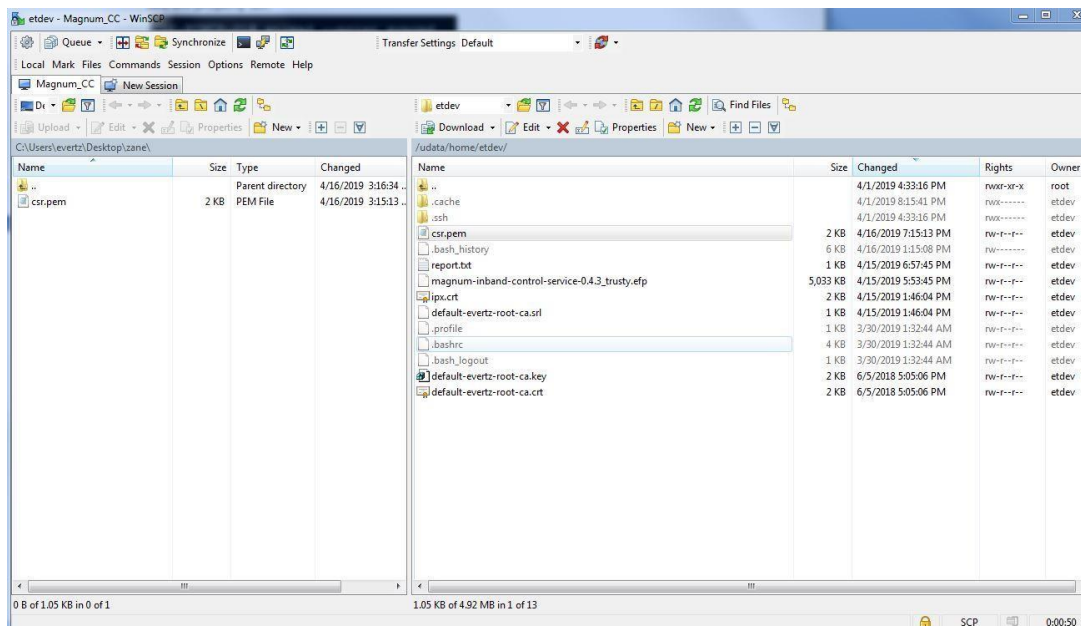


Figure 18: Transfer CSR file to Magnum via WinSCP

- Open SSH session to secure Magnum with etdev user and sign the csr file using the following command:

```
openssl x509 -req -in csr.pem -CA default-evertz-root-ca.crt -CAkey default-evertz-rootca.key -CAcreateserial -out exe.crt -days 365
```

```
etdev@magnum:~$ openssl x509 -req -in csr.pem -CA default-evertz-root-ca.crt -CA
key default-evertz-root-ca.key -CAcreateserial -out exe.crt -days 365
Signature ok
subject=/C=CA/ST=Ontario/L=Burlington/O=Evertz Microsystems Ltd./OU=EXE/CN=172.1
6.138.78/emailAddress=support@evertz.com
Getting CA Private Key
```

Figure 19: OpenSSL command output for CSR signing

Transfer “exe.crt” signed by Magnum and trusted certificate chain (default-evertz-root-ca.crt) file back to IPX. Use WinSCP to transfer these two files from Magnum.

Upload Certificate Chain

Prerequisites

- Completion of prior steps
- Equipped with certificate chain applicable to the TOE 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

- Log in to the IPX **Management Web Application**
- Click “**General**” menu from Menus listed on left of the displayed index page
- Scroll down to “**Credentials**” section

4. Click **“Choose File”** button of **“Trusted 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

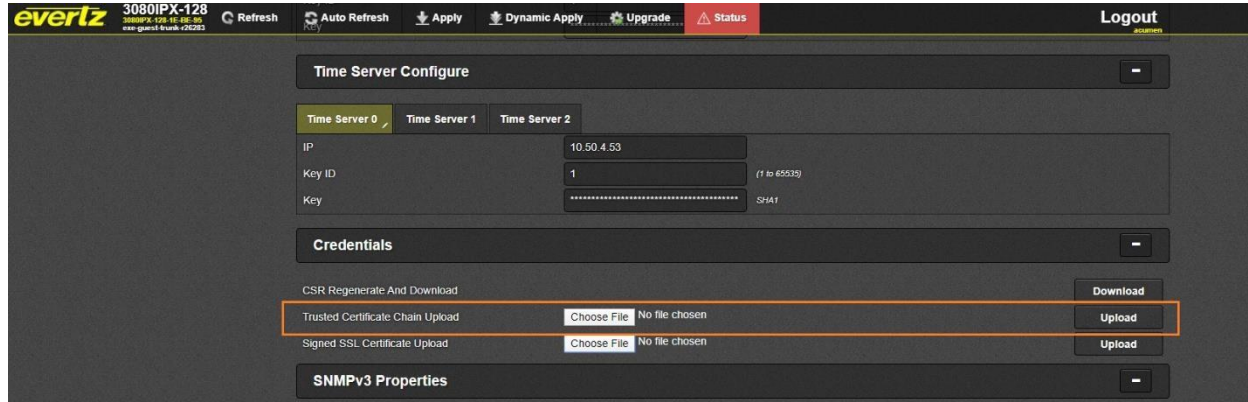


Figure 20: Upload Cert Chain

Note:

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

IPX 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 IPX

Upload SSL Certificate

Prerequisites

- Completion of prior steps
- Equipped with signed certificate obtained from TOE Certificate Authority

Steps

1. Login to the IPX **Management Web Application**
2. Click **“General”** menu from Menus listed on left of the page
3. Scroll down to **“Credentials”** section
4. Click **“Choose File”** button of **“Signed SSL 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 IPX

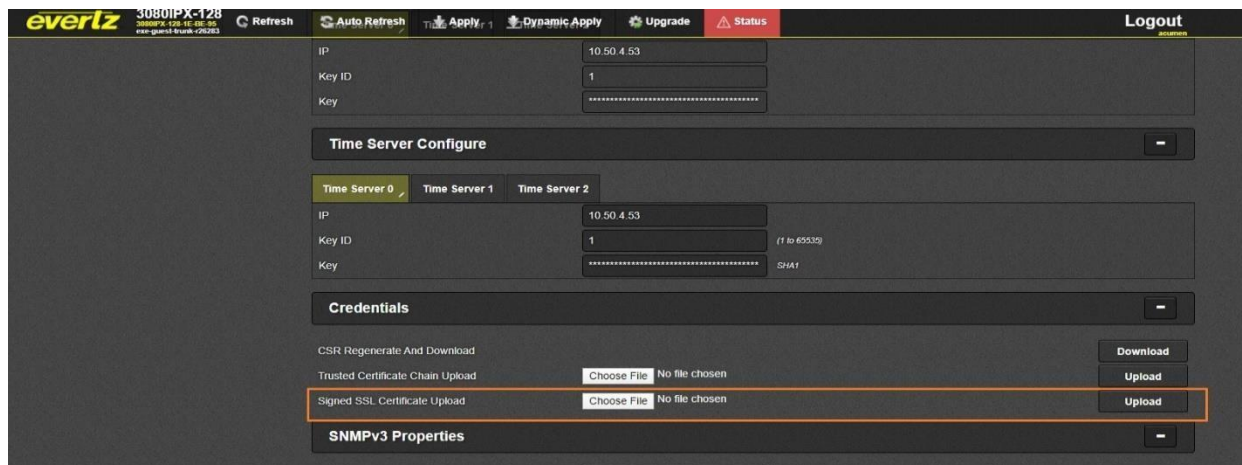


Figure 21: Upload SSL Certificate

Note:

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

For all the TLS client and server connections, if the certificate verification fails for any reason (including a failure to establish a connection), the connection attempt fails, and the trusted channel is not established. There are no fallback authentication functions for failed certificate authentication. The administrators must refer to the audit logs to identify what causes the failure. The detailed audit log description can be found in the 'Audit Events' section below.

2.4.11 Configure TLS Client

IPX supports secure TLS client configuration in compliance with the CC evaluation criteria. The rsyslog service client acts as a TLS client in the IPX 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 TOE syslog server Certificate Authority

Steps

1. Login to the **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 TOE syslog server Certificate Authority
10. Click “**Upload**” button
11. Click “**Apply**” button at the top of the page

The screenshot displays the Evertz IPX web interface for configuring the Secure Log Service. The interface is dark-themed and includes a top navigation bar with buttons for 'Refresh', 'Auto Refresh', 'Apply', 'Dynamic Apply', 'Upgrade', and 'Status'. A 'Logout' button is in the top right corner. On the left, there is a 'Menu' sidebar with options like 'General', 'Ports', 'MultiCast Sources', etc. The main content area is titled 'Product' and contains several sections: 'Software' (Revision Major: 1, Revision Minor: 1, Build Number: 26283), 'Board' (Serial Number: -, Name: EXE-VSRA, Revision: 2, Build Number: 1), and 'Log Streaming'. The 'Log Streaming' section is expanded to show 'Sys Log' configuration for 'LLDP'. The 'Sys Log' section includes: 'Enable' (Enabled), 'Reference ID' (SYSLOG), 'Destination IP Address' (10.50.4.33), 'Destination Port' (81514), 'Level' (Debug), and 'Import CA Certificate' (Choose File: ica_1_chain.pem). An 'Upload' button is located at the bottom right of the Sys Log configuration area.

Figure 22: Secure Log Service

Once 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. IPX 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 IPX certificate store.

For all the TLS client and server connections, if the certificate verification fails for any reason (including a failure to establish a connection), the connection attempt fails, and the trusted channel is not established. There are no fallback authentication functions for failed certificate authentication. The administrators must refer to the audit logs to identify what causes the failure. The detailed audit log description can be found in the 'Audit Events' section below.

3. Secure Management

3.1 User Management

IPX 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. Details of user management can be found at IPX general user manual.

Prerequisites

- Completion of prior steps

Steps

1. Login to the “**Management Web Application**”
2. Click “**Settings**” displayed at the bottom of the displayed page
3. Select “**Users**” tab
4. Following screen will be displayed

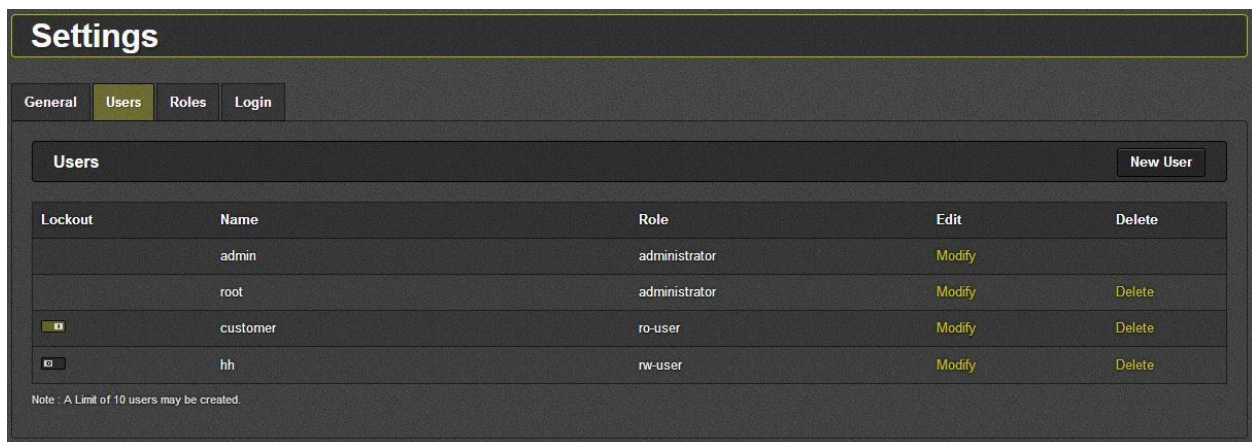


Figure 23: User Management

Following segment provide abstract description on user-management within the IPX

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.



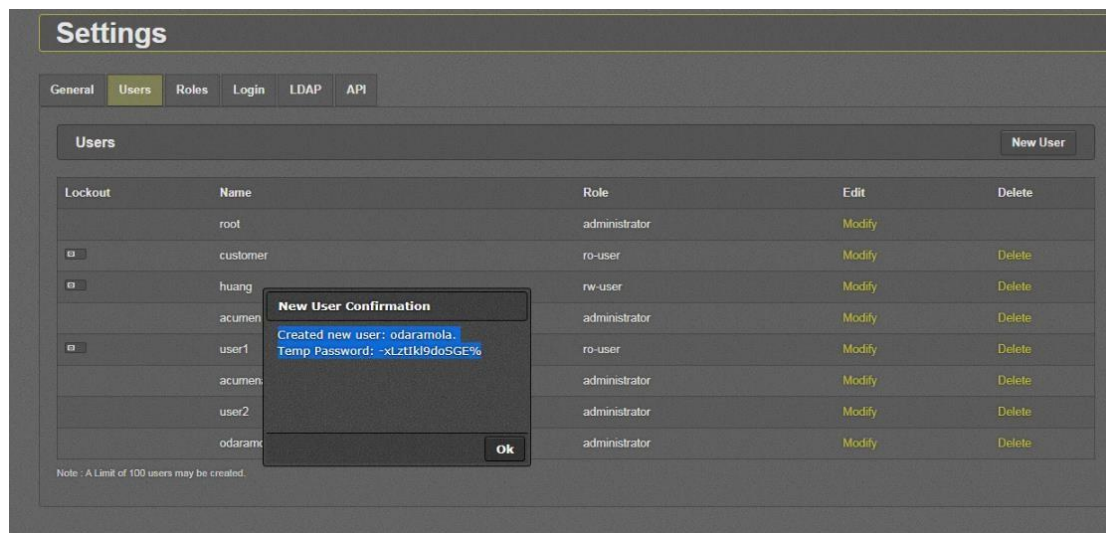
The 'New User' dialog box contains the following fields and controls:

- Name:** A text input field.
- Password Reset:** A checkbox with a label 'Password Reset' and a small icon to its right.
- User will be prompted on next login to reset password.** A text label below the checkbox.
- Role:** A dropdown menu currently showing 'administrator'.
- Buttons:** 'Ok' and 'Cancel' buttons at the bottom right.

Figure 24: 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. It is recommended that a new administrative account be created and used for day to day administration of the TOE. 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



The 'Settings' page shows a 'Users' table with the following data:

Lockout	Name	Role	Edit	Delete
	root	administrator	Modify	
<input type="checkbox"/>	customer	ro-user	Modify	Delete
<input type="checkbox"/>	huang	rw-user	Modify	Delete
	acumen	administrator	Modify	Delete
<input type="checkbox"/>	user1	ro-user	Modify	Delete
	acumen	administrator	Modify	Delete
	user2	administrator	Modify	Delete
	odaramx	administrator	Modify	Delete

The 'New User Confirmation' dialog box displays the following information:

- Created new user:** odaramola
- Temp Password:** -xLztki9dosGE%
- Buttons:** 'Ok' button.

Note: A Limit of 100 users may be created.

Figure 25: New User Confirmation

Roles: By default, there are three roles on the system, administrator, rw-user, and ro-user. The Security Administrator is the only account that should be used. This account has the Administrator role. The rw-user and ro-user should not be used in the evaluated configuration.

1. **Administrator:** There are no limitation/restriction for administrator role.
2. **rw-user:** Users with this role can change the configuration of IPX, 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 IPX configuration settings, nor can they change any user settings. This role can only view IPX and user settings, view the event log and upgrade firmware.

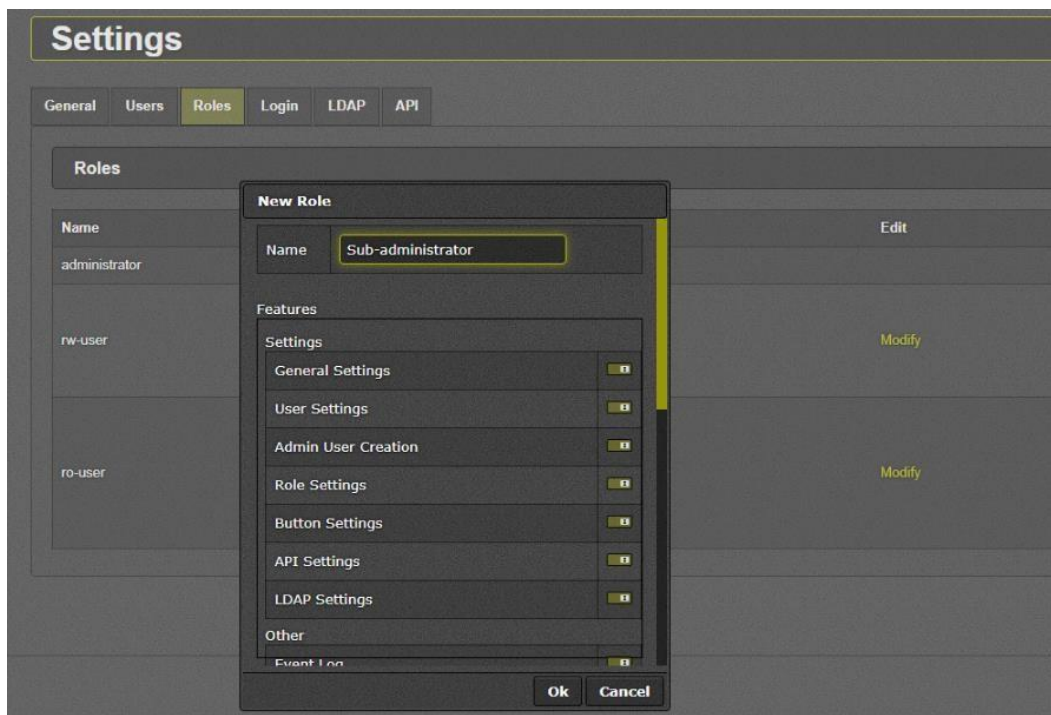


Figure 26: New Role Creation

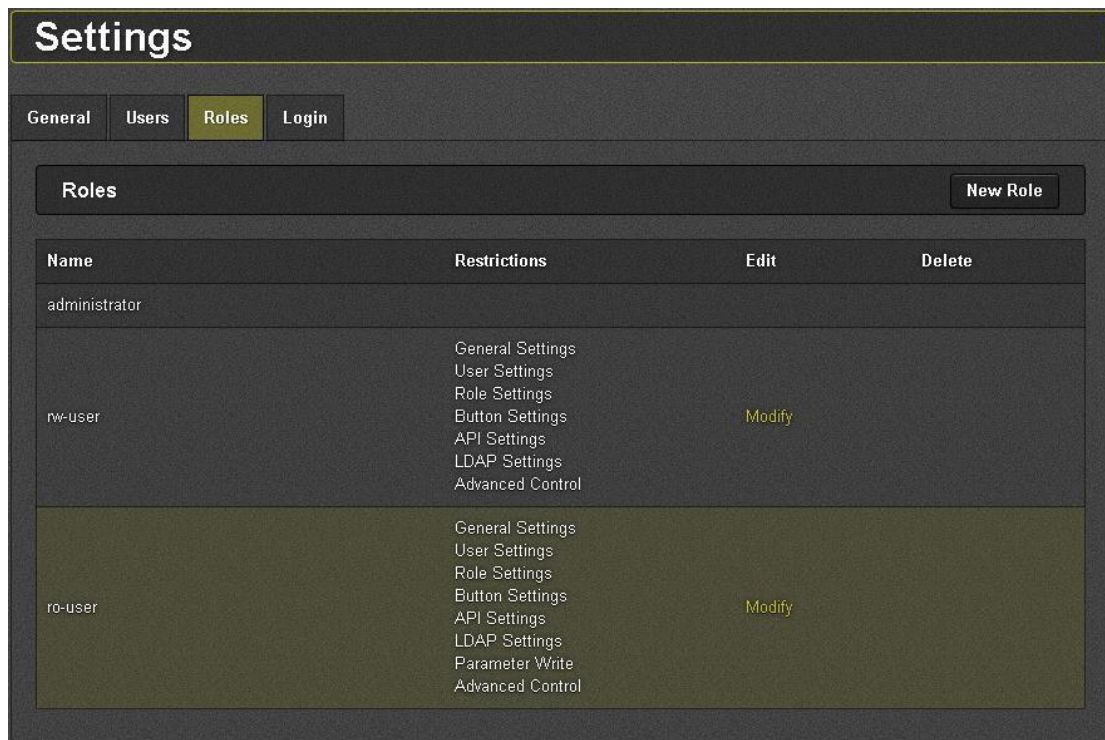


Figure 27: Roles Overview

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 given to that role.

Delete: This control is used to permanently delete a user. The user will no longer be able to access the system.

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 removing 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 TOE. Each certificate (other than the first certificate) in the certificate chain has the Subject Type=CA flag set.
- Certificates are not used for any purposes other than establishing TLS sessions.
- If certificates are uploaded to IPX for its own use those certificates are checked upon upload. When the TOE acts as a server it does not perform verification of its own server certificate. The TOE's client certificate is validated prior to use for authentication as well as upon upload. The certificate presented by remote TLS clients using mutual authentication is validated during the establishment of a TLS connection.
- For an expired certificate, IPX will deny the connection.
- IPX also uses CRL to verify whether the leaf certificate or intermediate CA certificate has been revoked. During session establishment with IPX, any byte modification in the certificate will lead to the failure of connection. The 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 TOE is unable to reach the CRL DP it will not accept the certificate and the session associated with the certificate will be denied.

3.3 Key/Cipher Management

Key Management within the IPX is transparent to the system user during secure-mode activation/deactivation. All actions related to key management are done implicitly without the user's knowledge or involvement.

3.3.1 Zeroing Crypto Material

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

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

Prerequisites

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

Steps

1. Login with Administrative credentials
2. Use following to set shred crypto key materials permanently **# zeroize**

Note:

The steps presented here will permanently disable IPX secure-mode operational functionality and the command should be used with care.

Once Zeroize command is executed successfully all sensitive key material and crypto specific data will be disposed PERMANENTLY WITHOUT DELAY and IPX becomes non-operational in secure-mode. To recover IPX in to operational mode, the user needs to perform an Upgrade procedure. Please not that STILL old sensitive information is lost permanently and nonrecoverable

4. Performing Secure Upgrade

IPX class of switches support 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. IPX supports the following features during any secure upgrade:

- Multiple firmware version support simultaneously and simplified switch process between firmware versions
- Upgrade rollback capability o If the integrity or authenticity of the Image is faulted the switch rolls back to the last stable operational image
- Image Authenticity Verification
- Image Integrity validation by the use of o Signature verification o File corruption analysis

4.1 Upgrade

Prerequisites

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

Steps

1. Login to the **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

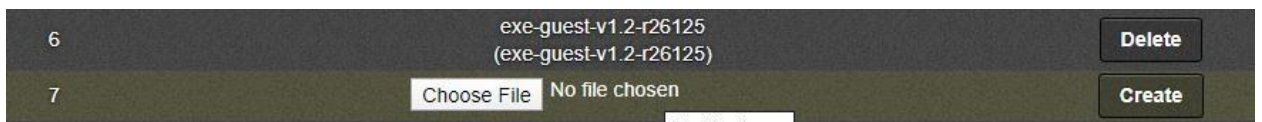


Figure 28: Selecting the image file to Upgrade

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>”

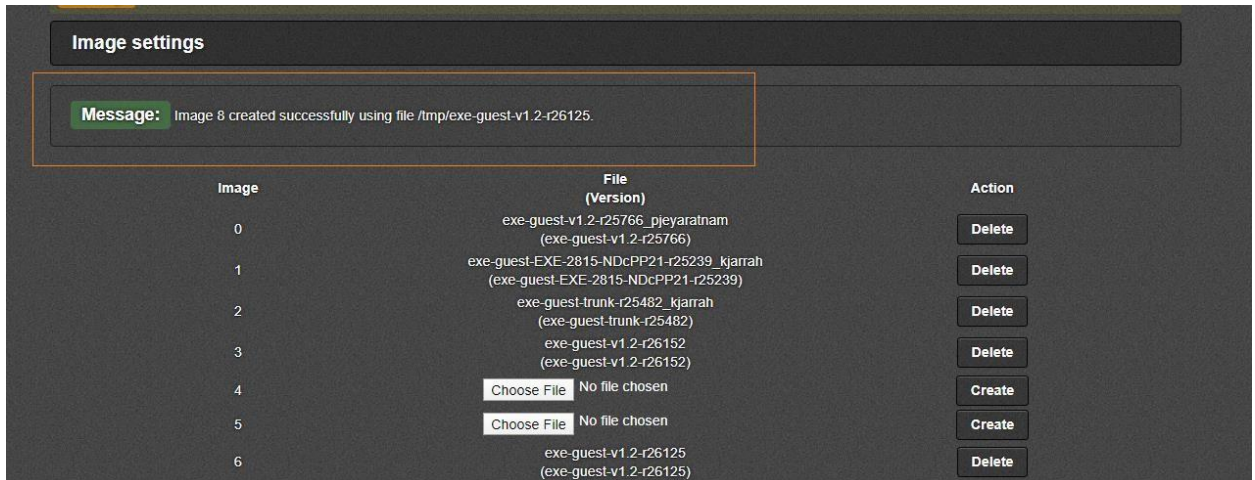


Figure 29: Image details

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

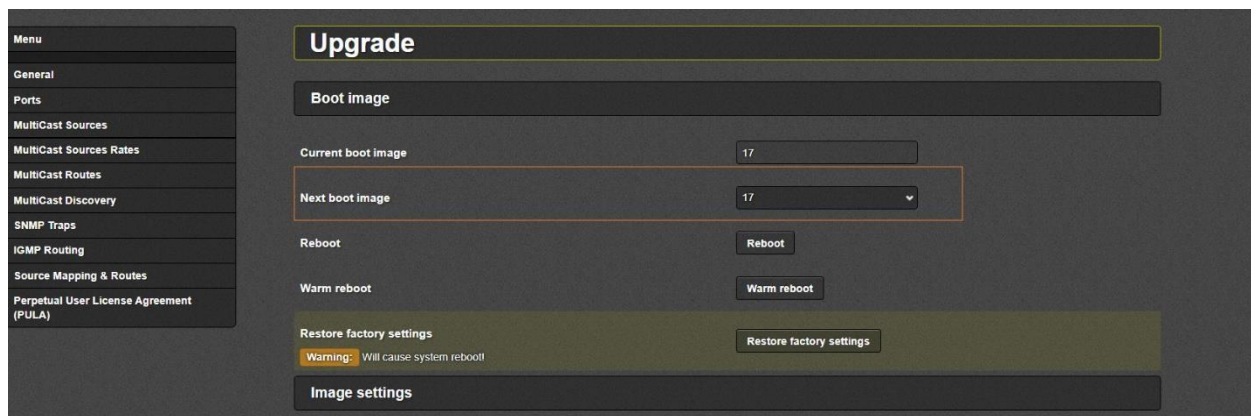


Figure 30: Boot Image Selection

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

4.2 Verify Current Installed Image

Prerequisites

- None

Steps

1. Login to the **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

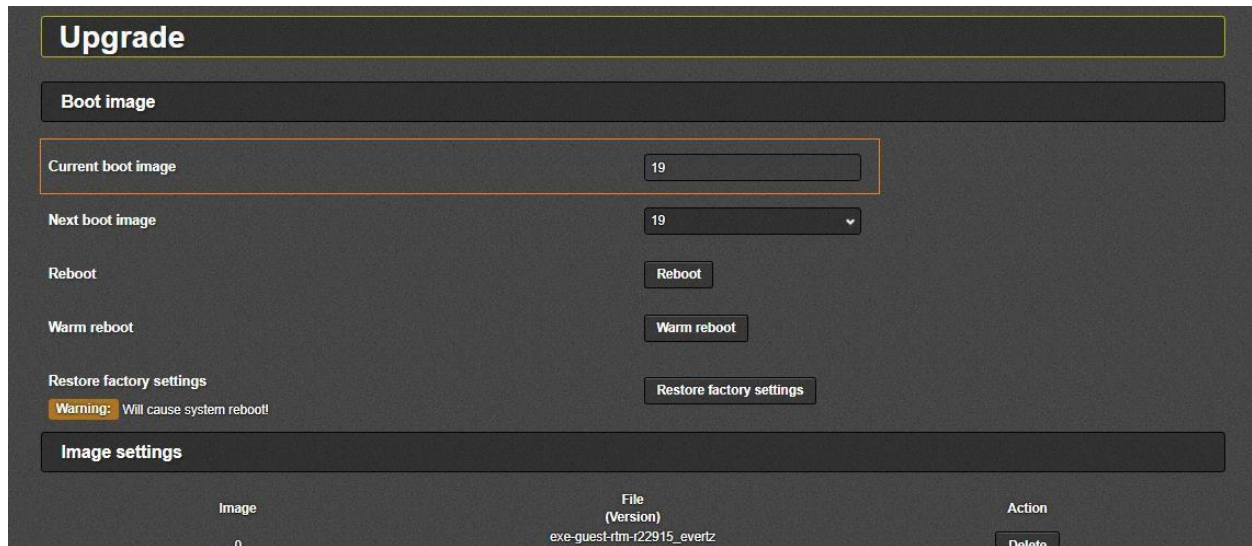


Figure 31: Verify Active Boot Image

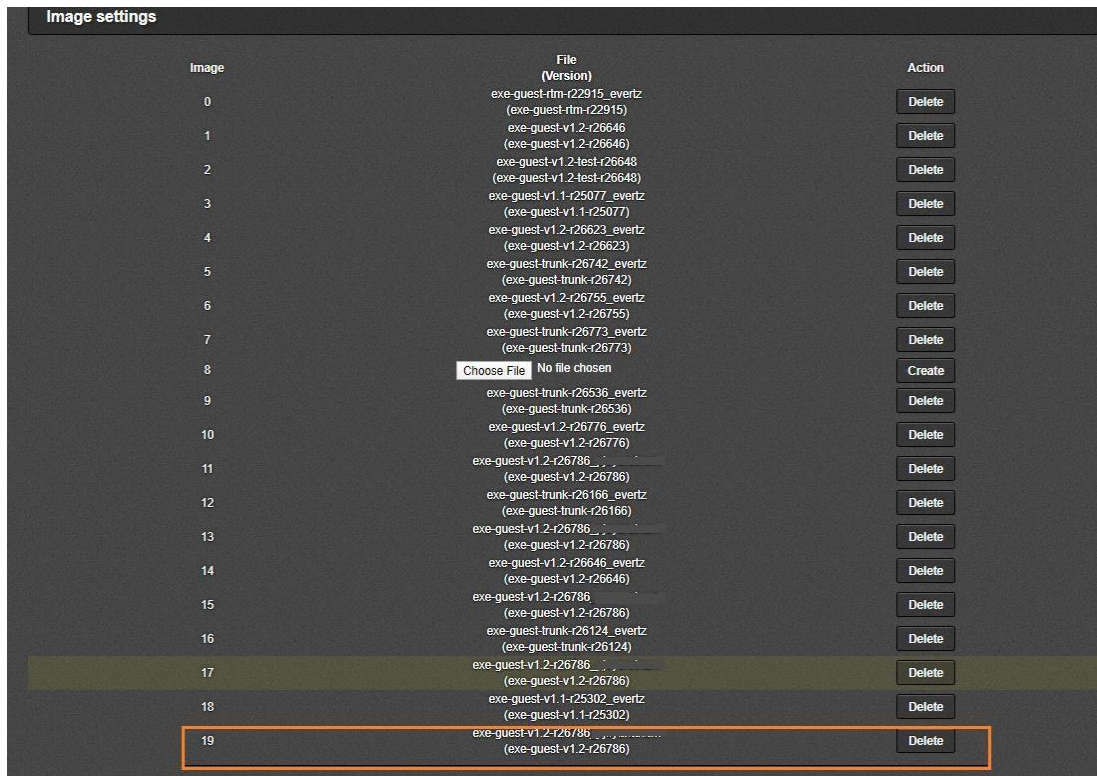


Figure 32: Verify Active Boot Image Settings

4.3 Switch an Inactive Image to Active Image

Prerequisites

- None

Steps

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

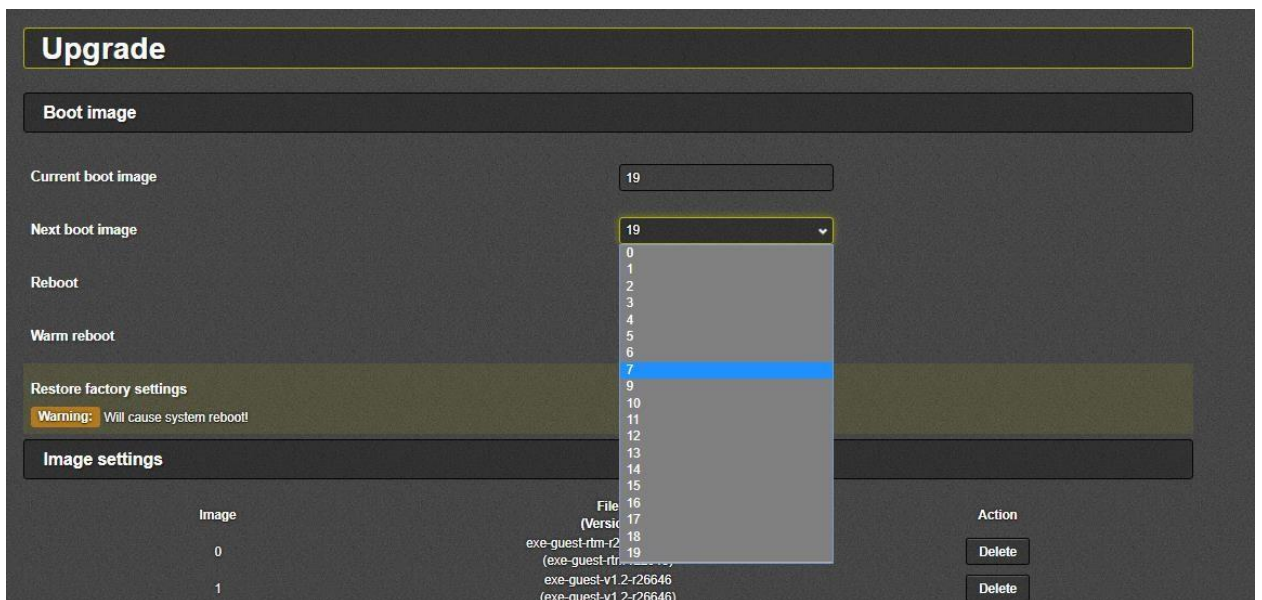


Figure 33: Selecting next boot image

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.

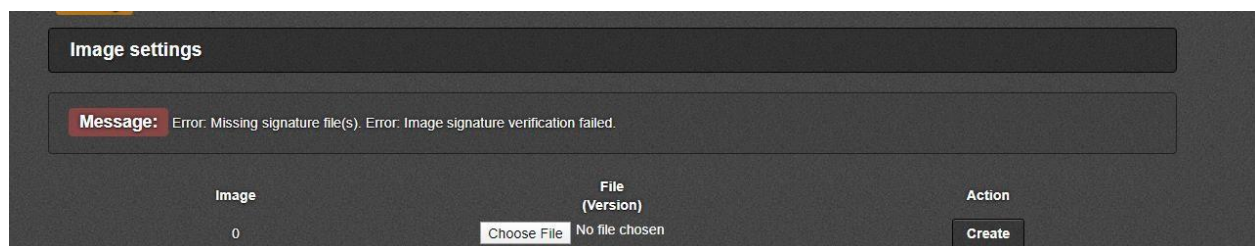


Figure 34: Error upgrading to an image with no signature

4.4.2 Upgrade Errors: Corrupted Image

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

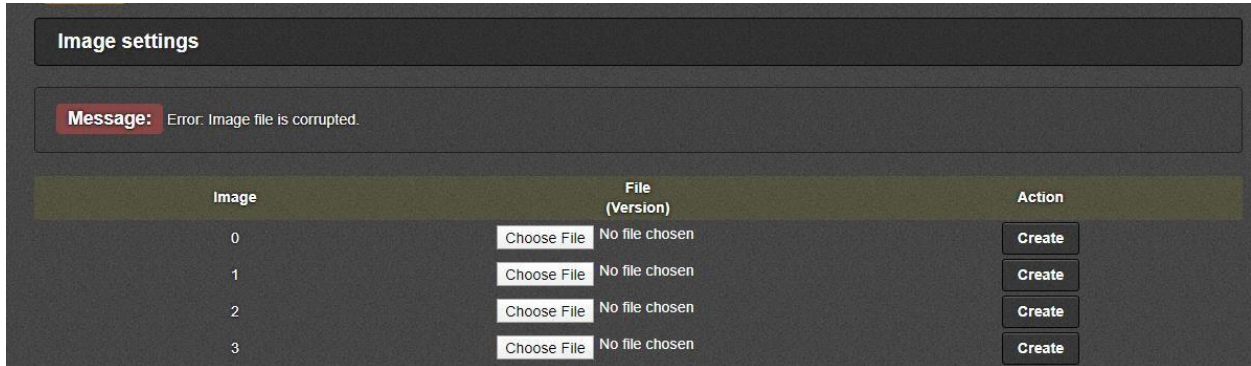


Figure 35: Error upgrading a corrupted image

4.4.3 Upgrade Errors: Bad Signature

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

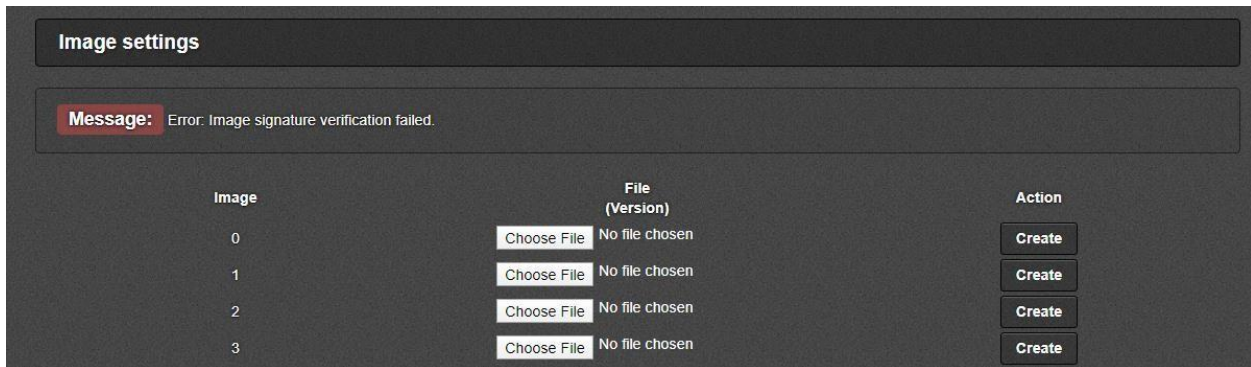


Figure 36: Error upgrading with an image with mismatched signature

For details regarding the Upgrade Menu and internals, please refer to the IPX User Manual.

5. Audit Events

The IPX is able to generate audit records which are stored internally within the IPX whenever a relevant event occurs. IPX 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. IPX 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

IPX provides functionalities to view audit events through the web-interface

Prerequisites

- None

Steps

1. Login to the **Management Web Application**
2. Click “**General**” menu option
3. Scroll to “**Make Logs**” section in the displayed page and click “**Download**” button
4. Immediate audit events are stored in location (“/var/log”) of the downloaded makelogs file. Previous audit events are stored in (“/ssd/syslog/current”)

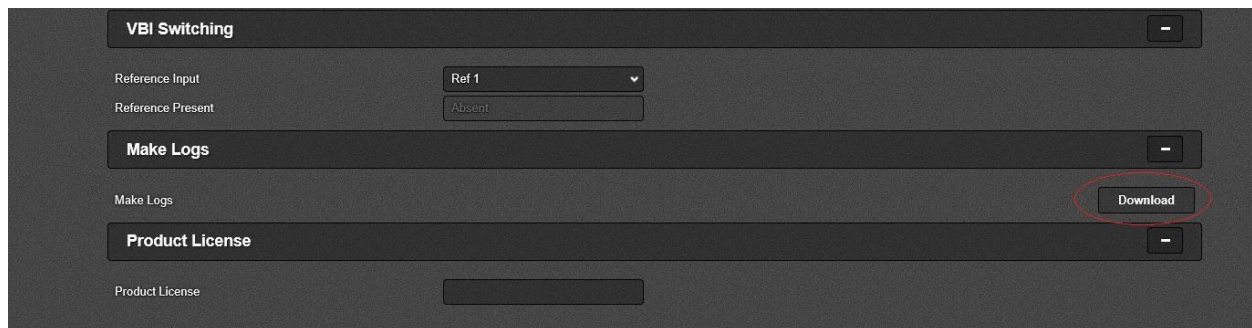


Figure 37: Download Audit Events

Note:

The TOE is a standalone TOE. IPX stores audit logs internally in real-time. The internal logs are stored unencrypted, but they are only accessible (and then read-only) via the web browser, which can only be used by Administrators. IPX stores all audit data locally in a secure location; it is accessible to administrators using the “Syslog” tab on the web interface.

For local audit log storage, two log files are used, each with a maximum capacity of 900 KB. Initially both files are empty, and entries are added to file 1. Once file 1 is full, newer entries will be added to file 2 until it becomes full, at which time content of file 1 will be cleared and entries added to file 1 again. The audit logs will keep getting forwarded to the secure syslog server in the event of an audit space is full.

5.2 Offloading Audit Logs

System log messages can be sent to a remote audit server. The remote audit server must listen on port 6514 for TLS connections, and its certificate chain must be trusted by IPX when the Secure Mode is enabled. All audit events are simultaneously sent to the remote server and the local store. If this or any outgoing client connection is unintentionally broken, IPX 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 ciphersuites listed in the section 2.4.6 above.

Steps

1. Login to the **Management Web Application**
2. Click “**General**” menu on top the displayed page
3. Under ‘**Syslog Configuration**’ section, enter the following information:
 - Reference Identifier
 - Syslog Server IP
 - Syslog Server Port

The screenshot displays the Syslog Configuration page in the Evertz IPX management web application. The page has a dark theme and includes a navigation bar at the top with the Evertz logo, device information (3080IPX-16GE), and various action buttons like Refresh, Auto Refresh, Apply, Dynamic Apply, Upgrade, and Logout. The main content area is divided into several sections:

- Reference Identifier:** rsyslog.acumen.com
- Syslog Server IP:** 10.1.5.183
- Syslog Server Port:** 6,514 (with a note: (0 to 65535))
- Certificate Section:**
 - Certificate Upload: Choose File (No file chosen) with an Upload button.
 - Certificate Status: MD5:cebff9ad5fff9963a55859fa052f
 - Signing CA Upload: Choose File (No file chosen) with an Upload button.
 - Signing CA Status: Updated, need system reboot
 - CSR Download: Download button
 - CSR Status: Available
- Trusted Certificate Section:**
 - CA Upload: Choose File (No file chosen) with an Upload button.
 - CA Status: MD5:bae4aa5e144ff3d902e9cbe8af
- CRL Section:**
 - CRL Upload: Choose File (No file chosen) with an Upload button.
 - CRL Status: MD5:47dccc15d502a93f2f047f3cf00
 - Clear Cached CRL button

Note:

Ensure that the IPX has the same CA certificates used in the Syslog Server.

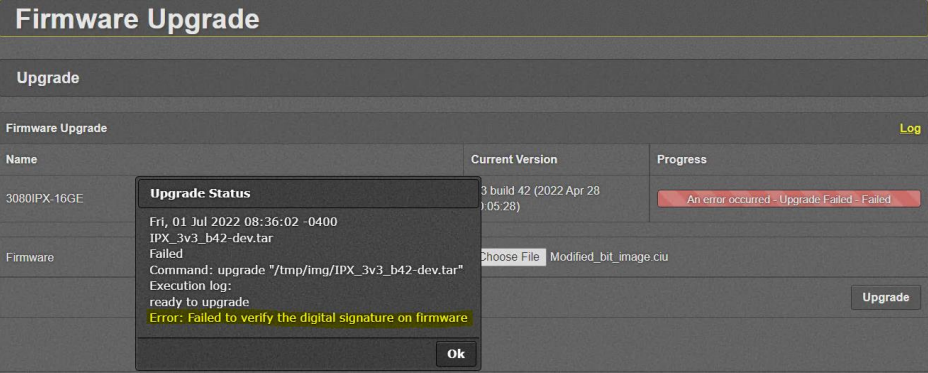
5.3 Audit Events Table

Below table describes the IPX 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 (name of user account shall be logged if individual user accounts are required for Administrators).	<pre> Mar 31 09:45:55 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.79) login. Mar 31 09:51:06 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.79) logout. Dec 7 12:32:29 2022 Evertz-IPX authpriv.info login[23274]: pam_unix(login:session): session opened for user root by LOGIN(uid=0) Dec 7 12:32:29 2022 Evertz-IPX auth.info login[23365]: root login on 'console' </pre>
Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).	<pre> Dec 7 11:06:44 2022 Evertz-IPX user.notice IPX: New CSR has been generated from the console. </pre>
Resetting passwords (name of related user account shall be logged).	<pre> Dec 12 06:57:09 2022 Evertz-IPX authpriv.info WebEasy: Password has been changed for user (user1). Dec 12 06:57:09 2022 Evertz-IPX authpriv.info WebEasy: User user1 (192.168.254.45) login. </pre>
Failure to establish a HTTPS Session	<pre> Mar 24 10:21:18 2022 Evertz-IPX authpriv.notice login[3107]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=console ruser=rhost= user=customer Mar 24 10:21:21 2022 Evertz-IPX auth.warn login[3107]: pam_authenticate call failed: Authentication failure (7) </pre>

Auditable Events	Sample Logs
<p>Failure to establish a TLS Session with a TLS Server</p>	<pre>May 10 12:49:39 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='SSL routines:set_client_ciphersuite.wrong cipher returned', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 12:49:39 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p> <p>Server certificate which doesn't match cipher suite</p> <pre>Sep 19 11:11:56 2022 Evertz-IPX user.warn syslog Syslog connection established; fd='21', server='AF_INET(10.1.5.183:6514)', local='AF_INET(0.0.0.0:0)'</pre> <pre>Sep 19 11:11:56 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Success (0)'</pre> <pre>Sep 19 11:11:56 2022 Evertz-IPX user.warn syslog Syslog connection broken; fd='21', server='AF_INET(10.1.5.183:6514)', time_reopen='5'</pre> <p>Server Hello using unsupported cipher suite.</p> <pre>May 10 12:49:39 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='SSL routines:set_client_ciphersuite.wrong cipher returned', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 12:49:39 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p> <p>ECDHE key exchange using unsupported curve.</p> <pre>May 10 12:56:14 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='SSL routines:tls_process_ske_ecdhe.wrong curve', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 12:56:14 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p> <p>Server Hello using unsupported TLS version.</p> <pre>May 10 13:17:05 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='SSL routines:ssl_choose_client_version:unsupported protocol', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 13:17:05 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p> <p>Modify signature in the server key exchange.</p> <pre>May 10 13:34:20 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='rsa routines:RSA_padding_check_PKCS1_type_1:invalid padding', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 13:34:20 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p> <p>Modify byte in the server finish message.</p> <pre>May 10 13:48:46 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='SSL routines:tls_process_finished:digest check failed', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 13:48:46 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p> <p>Send a garbled message after Change Cipher Spec message.</p> <pre>May 10 14:04:52 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error='SSL routines:ss3_read_bytes:data between ccs and finished', location='/tmp/syslog_network.conf:2.75'</pre> <p>May 10 14:04:52 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd='21', error='Broken pipe (32)'</p>
<p>Failure to establish a TLS Session with a TLS Client</p>	<pre>May 24 10:05:39 2022 Evertz-IPX daemon.err lighttpd[1155]: (connections.c.750) invalid request-line -> sending Status 400</pre> <pre>May 24 12:25:23 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre> <pre>May 24 12:35:45 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre> <p>Client hello unsupported cipher suite.</p> <pre>May 24 10:05:39 2022 Evertz-IPX daemon.err lighttpd[1155]: (connections.c.750) invalid request-line -> sending Status 400</pre> <pre>May 24 12:25:23 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre> <pre>May 24 12:35:45 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre> <p>Modify byte in client finish message.</p> <pre>May 24 10:05:39 2022 Evertz-IPX daemon.err lighttpd[1155]: (connections.c.750) invalid request-line -> sending Status 400</pre> <pre>May 24 12:25:23 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre> <pre>May 24 12:35:45 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre> <p>Initiate connection to the TOE using secp224r1.</p> <pre>May 25 12:50:05 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher</pre>

Auditable Events	Sample Logs
<p>Failure to authenticate the TLS client</p>	<pre>Aug 29 14:59:54 2022 Evertz-IPX user.notice IPX: SYNERGY: Loading CRL file. Aug 29 14:59:54 2022 Evertz-IPX user.err IPX: X509 [Certificate Verify Fail]: Error with certificate at depth (0) Aug 29 14:59:54 2022 Evertz-IPX user.err IPX: X509 [Certificate Verify Fail]: Issuer = /C=US/O=Acumen/OU=CC/CN=AcumenCA Aug 29 14:59:54 2022 Evertz-IPX user.err IPX: X509 [Certificate Verify Fail]: Subject = /C=US/ST=Maryland/O=Acumen/OU=CC/CN=VM-Client-New Aug 29 14:59:54 2022 Evertz-IPX user.err IPX: X509 [Certificate Verify Fail]: Error (26 unsupported certificate purpose) Aug 29 14:59:54 2022 Evertz-IPX user.err IPX: SYNERGY: TLS handshaking failed for client [10.1.5.183]!</pre> <p>Client hello unsupported cipher suite.</p> <pre>May 24 10:05:39 2022 Evertz-IPX daemon.err lighttpd[1155]: (connections.c.750) invalid request-line -> sending Status 400 May 24 12:25:23 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello.no shared cipher May 24 12:35:45 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello.no shared cipher</pre> <p>Modify byte in client finish message.</p> <pre>May 24 10:05:39 2022 Evertz-IPX daemon.err lighttpd[1155]: (connections.c.750) invalid request-line -> sending Status 400 May 24 12:25:23 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello.no shared cipher May 24 12:35:45 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello.no shared cipher</pre> <p>Initiate connection to the TOE using secp224r1.</p> <pre>May 25 12:50:05 2022 Evertz-IPX daemon.err lighttpd[1155]: (mod_openssl.c.3095) SSL: 1 error:1417A0C1:SSL routines:tls_post_process_client_hello.no shared cipher</pre>
<p>Unsuccessful login attempts limit is met or exceeded</p>	<pre>Mar 21 07:29:32 2022 Evertz-IPX authpriv.warn WebEasy: User acumen (192.168.254.79) authentication failure. Mar 21 07:29:45 2022 Evertz-IPX authpriv.warn WebEasy: User acumen (192.168.254.79) authentication failure. Mar 21 07:30:03 2022 Evertz-IPX authpriv.warn WebEasy: User acumen (192.168.254.79) authentication failure. Mar 21 07:30:03 2022 Evertz-IPX authpriv.info WebEasy: User acumen has been locked out because of reaching the authentication maximum attempts!</pre>
<p>Use of identification and authentication mechanism</p>	<p>Console</p> <pre>Mar 24 10:21:18 2022 Evertz-IPX authpriv.notice login[3107]: pam_unix(login.auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=console ruser=rhost= user=customer Mar 24 10:21:21 2022 Evertz-IPX auth.warn login[3107]: pam_authenticate call failed: Authentication failure (7)</pre> <pre>Mar 24 10:27:32 2022 Evertz-IPX authpriv.info login[12905]: pam_unix(login.session): session opened for user customer by LOGIN(uid=0)</pre> <p>Web-GUI</p> <pre>Mar 24 10:34:37 2022 Evertz-IPX authpriv.warn WebEasy: User root (192.168.254.79) authentication failure. Mar 24 10:40:55 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.79) login.</pre>
<p>Use of identification and authentication mechanism</p>	<pre>Mar 24 10:21:18 2022 Evertz-IPX authpriv.notice login[3107]: pam_unix(login.auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=console ruser=rhost= user=customer Mar 24 10:21:21 2022 Evertz-IPX auth.warn login[3107]: pam_authenticate call failed: Authentication failure (7)</pre> <pre>Mar 24 10:27:32 2022 Evertz-IPX authpriv.info login[12905]: pam_unix(login.session): session opened for user customer by LOGIN(uid=0)</pre>
<p>Ability to import X.509v3 certificates to the TOE's trust store</p>	<pre>Sep 9 13:29:29 2022 Evertz-IPX user.notice IPX: Successfully uploaded signing CA certificate Sep 9 13:29:39 2022 Evertz-IPX user.notice IPX: Successfully uploaded CA certificate</pre>
<p>Generating Certificate Signing Requests</p>	<pre>Dec 7 11:06:44 2022 Evertz-IPX user.notice IPX: New CSR has been generated from the console.</pre>
<p>Unsuccessful attempt to validate a x509 certificate</p>	<pre>Jun 1 14:17:18 2022 Evertz-IPX user.warn syslog Syslog connection established; fd=24; server=AF_INET(10.1.5.183:6514); local=AF_INET(0.0.0.0) Jun 1 14:17:18 2022 Evertz-IPX user.warn syslog Certificate validation failed; subject=CN=server_vm, OU=CC, O=Acumen, C=US; issuer=CN=AcumenCA, OU=CC, O=Acumen, C=US; error='unable to get local issuer certificate'; depth=0 Jun 1 14:17:18 2022 Evertz-IPX user.warn syslog SSL error while writing stream; tls_error=SSL routines:tls_process_server_certificate.certificate verify failed; location=/tmp/syslog_network.conf:2:75 Jun 1 14:17:18 2022 Evertz-IPX user.warn syslog I/O error occurred while writing; fd=24; error=Broken pipe (32)</pre>
<p>replacement or removal of trust anchors in the TOE's trust store</p>	<pre>Sep 9 13:29:29 2022 Evertz-IPX user.notice IPX: Successfully uploaded signing CA certificate Sep 9 13:29:39 2022 Evertz-IPX user.notice IPX: Successfully uploaded CA certificate</pre> <p>No option to delete certificate on TOE. Although, it's been replacing with newly uploaded certificate with existing one.</p>
<p>CRL server unreachable to validate a certificate</p>	<pre>Dec 9 07:11:10 2022 Evertz-IPX user.err SYSLOG [Client]: X509 [Certificate Verify Fail]: Error with certificate at depth (0) Dec 9 07:11:10 2022 Evertz-IPX user.err SYSLOG [Client]: X509 [Certificate Verify Fail]: Issuer = /C=US/ST=Maryland/O=Acumen/OU=CC/CN=ICA Dec 9 07:11:10 2022 Evertz-IPX user.err SYSLOG [Client]: X509 [Certificate Verify Fail]: Subject = /C=US/ST=Maryland/O=Acumen/OU=CC/CN=rsyslog.acumen.com Dec 9 07:11:10 2022 Evertz-IPX user.err SYSLOG [Client]: X509 [Certificate Verify Fail]: Error (3 unable to get certificate CRL) Dec 9 07:11:10 2022 Evertz-IPX user.err SYSLOG [Client]: Failed connecting to syslog server (10.1.5.183)</pre> <p>The TOE is unable to reach the CRL server, and it is failing to validate the certificate and rejecting the connection.</p>

Auditable Events	Sample Logs
Clearing CRL Cache	<pre>Dec 7 11:10:08 2022 Evertz-IPX user.info sys_app: Ctrl Name: clearCachedCRL, Type: Set, from user: root Dec 7 11:10:08 2022 Evertz-IPX user.notice IPX: The cached CRL has been deleted.</pre>
Ability to configure the access banner.	<pre>Mar 31 10:13:11 2022 Evertz-IPX user.info sys_app: Ctrl Name: WarningBanner, Type: Set, from user: root</pre>
Discontinuous changes to time - either Administrator actuated or changed via an automated process.	<p>Time can only be set via console access of device.</p> <pre>Apr 12 20:26:52 2022 Evertz-IPX user.info sys_app: Ctrl Name: setDate, Type: Set, from user: customer Jan 1 12:00:00 2023 Evertz-IPX user.notice IPX: Date changed to Sun Jan 1 12:00:00 GMT-4 2023 from Tue Apr 12 20:26:52 GMT-4 2022 manually from serial menu.</pre> <pre>Dec 7 03:26:56 2022 Evertz-IPX user.info sys_app: Ctrl Name: TimezoneOffset, Type: Set, from user: root Dec 7 08:26:56 2022 Evertz-IPX user.notice sys_app: Time zone has changed!</pre> <pre>Dec 7 07:05:00 2022 Evertz-IPX user.notice IPX: Date changed to Wed Dec 7 07:05:00 GMT+5 2022 from Wed Dec 7 12:53:11 GMT+5 2022 manually from serial menu. Dec 7 07:05:14 2022 Evertz-IPX daemon.info : process '/sbin/getty -L console 0 vt100 ' (pid 23606) exited. Scheduling for restart. Dec 7 07:05:14 2022 Evertz-IPX daemon.info : starting pid 24576, tty '/dev/console': '/sbin/getty -L console 0 vt100 '</pre>
Initiating manual updates	<p>Verify the updates using digital signature capability prior to installing those updates, and successful upgrade of firmware:</p> <pre>Sep 1 14:06:31 2022 Evertz-IPX authpriv.info root: Firmware was upgraded to ver: 3.3 build 57 from ver: 3.3 build 42 Sep 1 14:06:47 2022 Evertz-IPX authpriv.info root: POWER-ON-SELF-TEST (POST) passed. Sep 1 14:12:08 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.45) login.</pre> <p>Failed upgradation due to failed to verify digital signature:</p>  <pre>Jul 1 07:33:02 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.128.237) login. Jul 1 07:36:02 2022 Evertz-IPX authpriv.crit daemon: Unsuccessful upgrade attempt: Invalid signature</pre> <p>Failed upgradation due to the use of a modified version (e.g., using a hex editor) of a legitimately signed update:</p> <pre>Jul 1 07:33:02 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.128.237) login. Jul 1 07:36:02 2022 Evertz-IPX authpriv.crit daemon: Unsuccessful upgrade attempt: Invalid signature</pre> <p>Failed upgradation due to the use of an image that has not been signed:</p> <pre>Jul 1 08:14:44 2022 Evertz-IPX authpriv.crit daemon: Unsuccessful upgrade attempt</pre> <p>Failed upgradation due to the use of an image signed with an invalid signature.</p> <pre>Jul 1 08:31:10 2022 Evertz-IPX authpriv.crit daemon: Unsuccessful upgrade attempt: Invalid signature</pre>
Ability to configure the authentication failure parameters	<pre>Dec 13 12:45:33 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.228.42) login. Dec 13 12:48:11 2022 Evertz-IPX authpriv.info WebEasy: The max-attempts to login has been changed to 4 by user (root).</pre>

Auditable Events	Sample Logs
Ability to re-enable an Administrator account	<p>Mar 21 07:35:18 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.79) login.</p> <p>Mar 21 07:44:22 2022 Evertz-IPX authpriv.info WebEasy: User acumen has been unlocked.</p> <p>Mar 21 07:47:01 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.79) logout.</p> <p>Mar 21 07:47:25 2022 Evertz-IPX authpriv.info WebEasy: User acumen (192.168.254.79) login.</p>
The termination of a remote session by the session locking mechanism	<p>Apr 26 12:09:10 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.128.237) login.</p> <p>Apr 26 12:12:13 2022 Evertz-IPX authpriv.info WebEasy: Idle session timeout (user: root, session: 17817ab76844845285d7faa25d31b759)!</p> <p>Apr 26 12:12:13 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.128.237) logout.</p> <p>Apr 26 12:13:39 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.128.237) login.</p>
Ability to configure the session inactivity time before session termination or locking.	<p>Dec 13 12:50:04 2022 Evertz-IPX authpriv.info WebEasy: The session-timeout has been changed to 120 seconds by user (root).</p>
The termination of an interactive session	<p>Sep 15 10:05:58 2022 Evertz-IPX authpriv.info login[19897]: pam_unix(login:session): session opened for user customer by LOGIN(uid=0)</p> <p>Sep 15 10:07:09 2022 Evertz-IPX authpriv.info login[19897]: pam_unix(login:session): session closed for user customer</p>
The termination of a local session by the session locking mechanism	<p>Apr 29 02:16:11 2022 Evertz-IPX authpriv.info login[3734]: pam_unix(login:session): session opened for user customer by LOGIN(uid=0)</p> <p>Apr 29 02:17:11 2022 Evertz-IPX authpriv.info Login: Idle session timeout for console menu!</p> <p>Apr 29 02:17:12 2022 Evertz-IPX authpriv.info login[3734]: pam_unix(login:session): session closed for user customer</p> <p>Apr 29 02:19:08 2022 Evertz-IPX authpriv.info WebEasy: User root (192.168.254.79) login.</p>
Connections with Trusted Channels	<p>Initiation of the trusted channel.</p> <p>May 11 11:23:40 2022 Evertz-IPX user.warn syslog Syslog connection established; fd=25, server=AF_INET(10.1.5.183:6514), local=AF_INET(0.0.0.0:0)</p> <p>May 11 11:25:45 2022 Evertz-IPX user.warn syslog Syslog connection broken; fd=25, server=AF_INET(10.1.5.183:6514), time_reopen=5'</p> <p>Aug 29 15:13:48 2022 Evertz-IPX user.notice IPX: SYNERGY: Loading CRL file.</p> <p>Aug 29 15:13:49 2022 Evertz-IPX user.info IPX: SYNERGY: TLS handshaking succeeded for client [10.1.5.183].</p> <p>Aug 29 15:13:49 2022 Evertz-IPX user.info IPX: SYNERGY: Connected to 10.1.5.183:36778</p> <p>Aug 29 15:14:16 2022 Evertz-IPX user.warn IPX: SYNERGY: Inactivity disconnect from 10.1.5.183:36778</p> <p>Aug 29 15:14:16 2022 Evertz-IPX user.info IPX: SYNERGY: Disconnected from 10.1.5.183:36778</p> <p>Termination of the trusted channel.</p> <p>Dec 7 10:58:15 2022 Evertz-IPX user.warn syslog Syslog connection established; fd=25, server=AF_INET(10.1.5.183:6514), local=AF_INET(0.0.0.0:0)</p> <p>Dec 7 11:00:37 2022 Evertz-IPX user.warn syslog Syslog connection broken; fd=25, server=AF_INET(10.1.5.183:6514), time_reopen=5'</p> <p>Dec 7 11:00:42 2022 Evertz-IPX user.warn syslog Syslog connection failed; fd=25, server=AF_INET(10.1.5.183:6514), error=Connection refused (111), time_reopen=5'</p> <p>Failure of the trusted channel.</p> <p>Dec 13 13:11:06 2022 Evertz-IPX user.warn syslog Syslog connection broken; fd=25, server=AF_INET(10.1.5.183:6514), time_reopen=5'</p> <p>Dec 13 13:11:11 2022 Evertz-IPX user.warn syslog Syslog connection failed; fd=25, server=AF_INET(10.1.5.183:6514), error=Connection refused (111), time_reopen=5'</p>

Table 1: Audit Events

6. Appendix

6.1 Communication of Magnum with IPX (Supplementary)

IPX can be controlled by MAGNUM. The connection between IPX 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. The IPX can maintain all functionality without the connection to the video control system. If the connection is unintentionally broken, the IPX will wait for the MAGNUM server to reestablish the connection

6.2 Reboot IPX

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