IPX MMA10G-IPX Security Administration Manual

Revision 1b: Aug 16, 2019

Contents

1. OVERVIEW 3
   1.1. TOE IT ENVIRONMENT 3
2. INSTALLATION 6
3. SERIAL PORT INTERFACE 7
   3.1. BOARD POWER ON 7
   3.2. SERIAL PORT INTERFACE AUTHENTICATION 8
   3.3. SERIAL MENU SYSTEM 9
4. WEB INTERFACE 18
   4.1. INITIAL LOGIN AND PASSWORD CONFIGURATIONS 18
   4.2. TOP MENU BAR DESCRIPTIONS 20
   4.3. BOTTOM MENU BAR DESCRIPTIONS 20
   4.4. SYSTEM TAB 35
   4.5. SYSLOG TAB 39
5. FIRMWARE UPGRADE 45

1. OVERVIEW

The TOE is a network-based audio video distribution system and is classified as a network device (a generic infrastructure device that can be connected to a network). The TOE hardware devices are the Evertz MMA10G-IPX-16 (1 RU) running MMA10G-IPX-16-CC v3.2, MMA10G-IPX-32 (3RU) running MMA10G-IPX-16-CC v3.2, and MMA10G-IPX-64 (6 RU) running MMA10G-IPX-16-CC v3.2 and will be referred to as IPX throughout this document. The IPX appliances are Ethernet switches optimized for video content.

The Internet Protocol Crosspoint (IPX) switch is a 10 Gigabit (Gb) Internet Protocol (IP) switch optimized for video-over-IP traffic (compressed or uncompressed). The IPX features (16), (32) or (64) 10 Gigabit per second (Gbps) IP ports (depending on the capacity of the IPX card). Each IPX card occupies two (2) slots (16- and 32-port IPX cards) or four (4) slots (64-port IPX cards) in an Evertz Modular Crosspoint (EMX) frame. All IPX-compatible cards may be inserted into any IPX frame configuration provided there are sufficient contiguous free slots available.

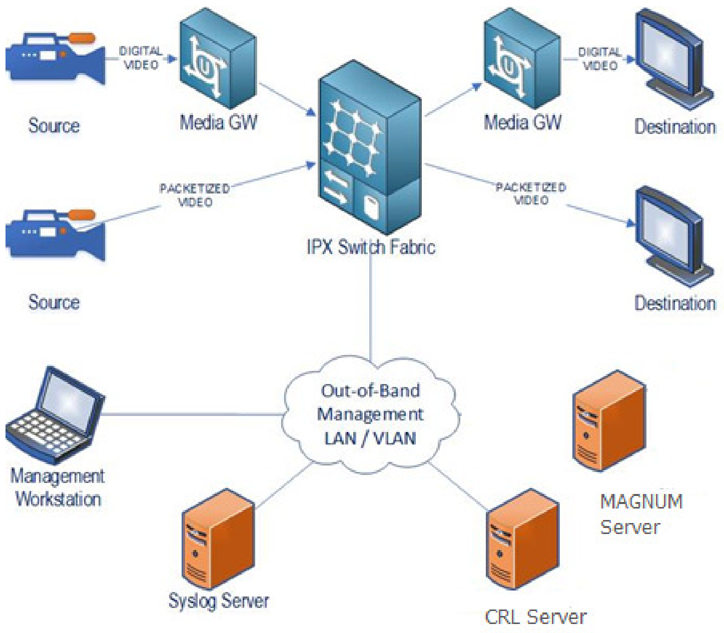


Figure 1-1 : TOE Topology

1.1. TOE IT ENVIRONMENT

The TOE's operational environment must provide the following services to support the secure operation of the TOE:

Table 1 : IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Syslog server	Yes	• **Conformant with RFC 5424 (Syslog Protocol)** • **Supporting Syslog over TLS (RFC 5425)** • **Acting as a TLSv1.2 server** • **Supporting Client Certificate authentication** • **Supporting at least one of the following cipher suites:** ○ **TLS_RSA_WITH_AES_128_CBC_SHA** ○ **TLS_RSA_WITH_AES_256_CBC_SHA** ○ **TLS_RSA_WITH_AES_128_CBC_SHA256** ○ **TLS_RSA_WITH_AES_256_CBC_SHA256** ○ **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** ○ **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
Management Workstation with web browser	Yes	• **Internet Explorer 11, Google Chrome 50, or Firefox 38** • **Supporting TLSv1.2** • **Supporting Client Certificate authentication** • **Supporting at least one of the following ciphersuites:** ○ **TLS_RSA_WITH_AES_128_CBC_SHA** ○ **TLS_RSA_WITH_AES_256_CBC_SHA** ○ **TLS_RSA_WITH_AES_128_CBC_SHA256** ○ **TLS_RSA_WITH_AES_256_CBC_SHA256** **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** ○ **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
CRL Server	Yes	• **Conformant with RFC 5280**
MAGNUM Server	Yes	• **Provides remote management of the TOE's routing and switching of video signals** • **Supporting TLSv1.2 with at least one of the following ciphersuites:** ○ **TLS_RSA_WITH_AES_128_CBC_SHA** ○ **TLS_RSA_WITH_AES_256_CBC_SHA** ○ **TLS_RSA_WITH_AES_128_CBC_SHA256** ○ **TLS_RSA_WITH_AES_256_CBC_SHA256** ○ **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** ○ **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
Media Gateway	No	• **Optional component for converting media streams. Not required for TOE operation.**
Video Source devices	No	• **Optional component for creating video streams that are sent to the TOE. Not required for TOE operation.** • **Supporting packetized or digital video**
Video Destination devices	No	• **Optional component for viewing video streams output by the TOE. Not required for TOE operation.** • **Supporting packetized or digital video**

Each IPX model includes an EMX chassis, one or more IPX card with TOE software, and SFP module. The TOE is shipped with all components, including TOE software pre-installed on the TOE. The TOE software can also be downloaded from the Evertz website. The TOE's user guidance, described in section 1.4.8, is also included with the shipped appliance.

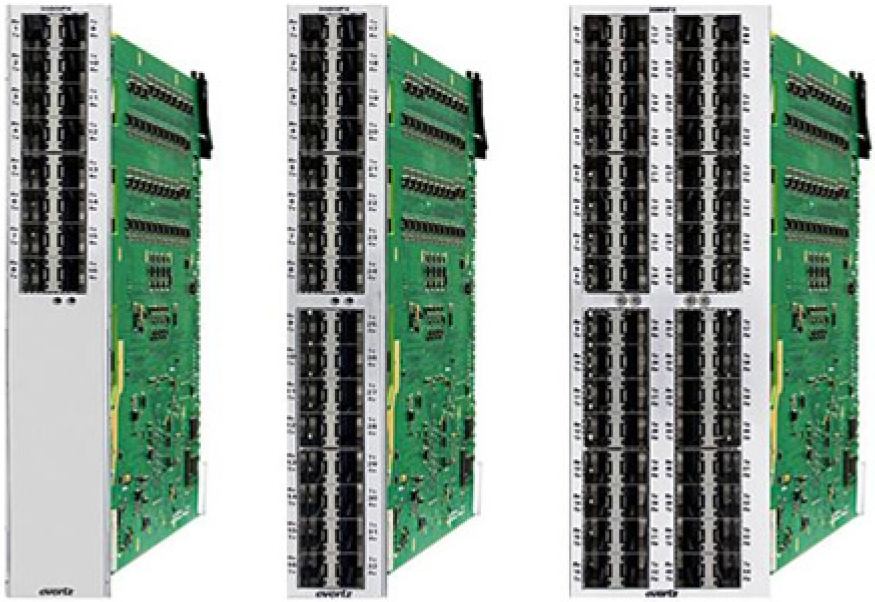
IPX supports three (3) available chassis (frames). Each chassis includes a single standard power supply, and each can support dual redundant power supplies. Each chassis has front panels with fans, and there are also fans on the power supplies.

1. ***EMX1-FR***

2. ***EMX3-FR***
3. ***EMX6-FR***

These chasses serve only to enclose the IPX cards and provide power distribution. Each chassis must also include an EMX Frame Controller Card.

The IPX cards with MMA10G-IPX firmware, associated SFPs, their mounting frames and the frames' controllers and power supplies make up an IPX installation. Figure 1-2 shows images of the IPX cards and Table 2 describes the differences between the cards.



MMA10G-IPX-16-CC **MMA10G-IPX-32-CC** **MMA10G-IPX-64-CC**

Figure 1-2 : 10Gb Interface Cards for the IPX Family

The EMX frames are the chassis in which the IP cards are installed. Figure 1-3shows images of the EMX frames and Table 2 describes the differences between the frames.

Table 2 : IPX Card Types

IPX Card	Contiguous Slots	SFP Ports	CPU	EMX1-FR	EMX3-FR	EMX6-FR
MMA10G-IPX-16-CC	2	16	PowerQUICC® II Pro MPC8377E	✓	✓	✓
MMA10G-IPX-32-CC	2	32	PowerQUICC® II Pro MPC8377E	✓	✓	✓
MMA10G-IPX-64-CC	4	64	PowerQUICC® II Pro MPC8377E		✓	✓

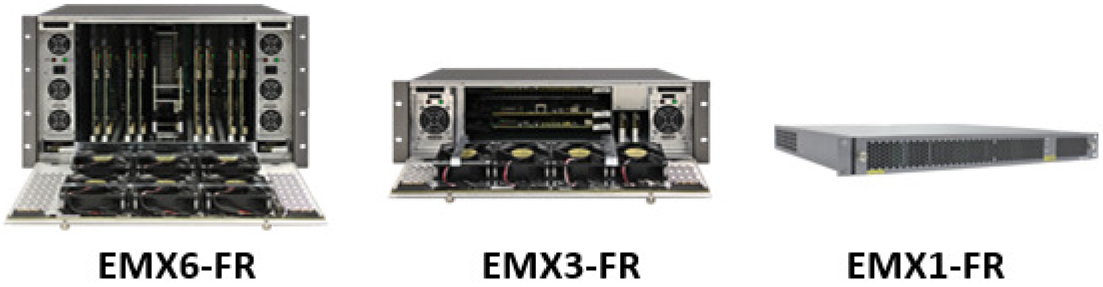


Figure 1-3 EMX Frame Options for the IPX Family

The EMX frames are passive (except for the door-mounted fans, which are the only powered equipment permanently attached to the frame). The frames mount power supplies, frame controllers and IPX cards. The frame controllers serve as a passthrough proxy to distribute Ethernet-based control connections to the individual IPX cards within the EMX frame chassis.

Table 3 : EMX Frames

Frame	Main Power	Redundant Power	Frame Controller	Controller Slots	Equipment Slots	RUs
EMX1-FR	EMX1-PS	Empty slot	EMX-FC	1	2	1
EMX1-FR+PS	EMX1-PS	EMX1-PS	EMX-FC	1	2	1
EMX3-FR	EMX3-PS	Empty slot	EMX-FC	2	5	3
EMX3-FR+3PS	EMX3-PS	EMX3-PS	EMX-FC	2	5	3
EMX6-FR	EMX6-PS	Empty slot	EMX-FC	2	15	6
EMX6FR-6PS	EMX6-PS	EMX6-PS	EMX-FC	2	15	6

Instructions for the physical installation of IPX can be found in the IPX User Manual v1.9. Evertz service provides a copy of this document to customers after they have purchased IPX.

2. INSTALLATION

The TOE arrives, shipped from the factory with all cards installed. Administrators must connect to the serial port interface and configure the network settings (see Section 3). On first connection, the administrator will open a terminal session and configure the port configurations:

- Bits Per Second: 115200
- Data Bits: 8
- Parity: None
- Stop Bits: 2
- Flow Control: None

Click OK to apply the settings and the Main Menu will appear. See Section 3.2 to reset the default password and Section 3.3 for initial network configurations.

Once network configurations are complete, the web interface will be accessible (see Section 4). Once the web administrators password has been reset, the TOE is configured.

The TOE only support the below set of ciphersuites and no configuration of these ciphersuites or the TOE’s RNG functionality is required or possible to put the TOE into the evaluated configuration.

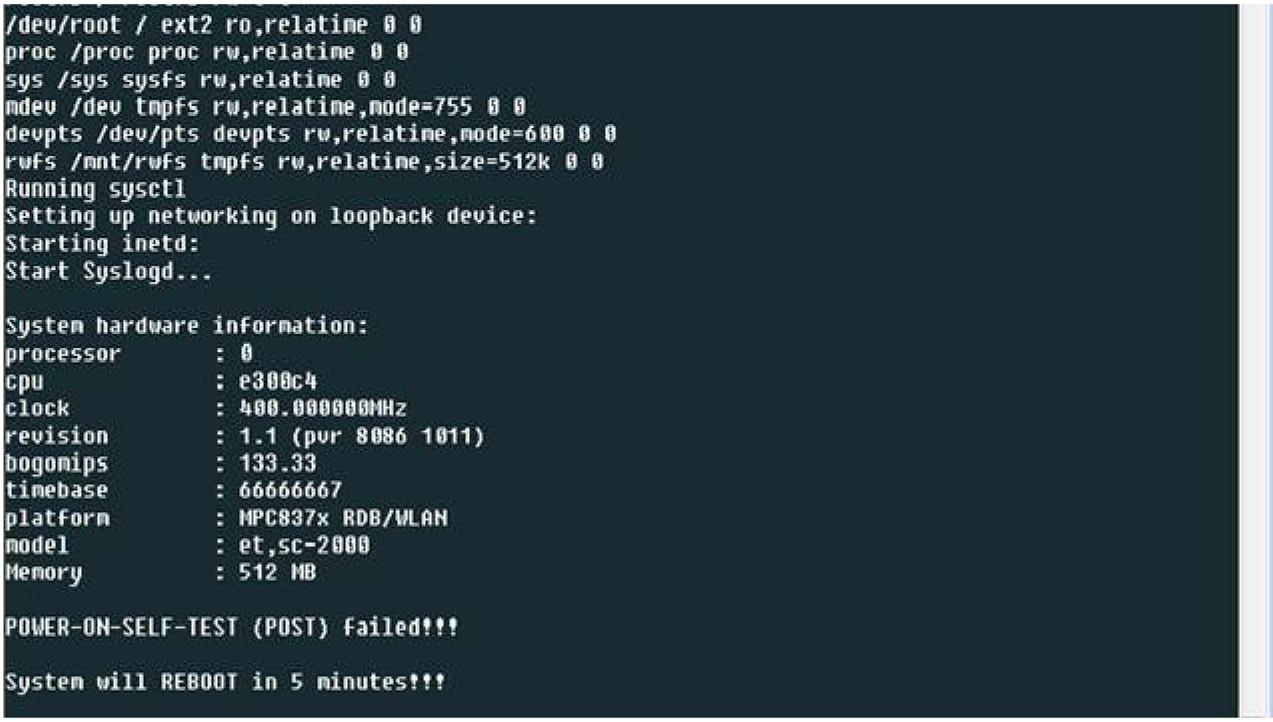
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

3. SERIAL PORT INTERFACE

Serial port interface is an interactive menu system, which is mainly used to set up a new IPX from factory. To access the serial port interface, physical serial cable connection from PC to IPX is needed. Please refer to the general IPX manual for serial cable connection.

3.1. BOARD POWER ON

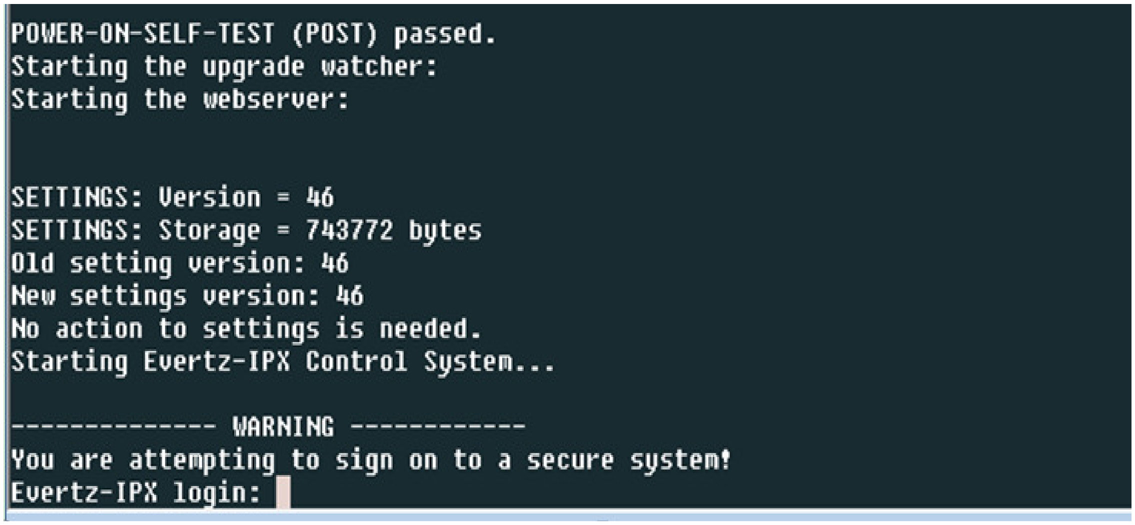
After power on, IPX will enter the system bootup process. During system bootup, the self-test will be excuted. If it fails, bootup will stop, and IPX will wait 5 minutes, then reboot. The reboots will continue until self-test pass. If issues persist contact the Evertz service department for repair or replacment



```
/dev/root / ext2 ro,relatime 0 0
proc /proc proc rw,relatime 0 0
sys /sys sysfs rw,relatime 0 0
mdev /dev tmpfs rw,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
rwfs /mnt/rwfs tmpfs rw,relatime,size=512k 0 0
Running sysctl
Setting up networking on loopback device:
Starting inetd:
Start Syslogd...

System hardware information:
processor       : 0
cpu             : e300c4
clock           : 400.000000MHz
revision        : 1.1 (pvr 8086 1011)
bogomips        : 133.33
timebase        : 66666667
platform        : MPC837x RDB/WLAN
model           : et,sc-2000
Memory          : 512 MB

POWER-ON-SELF-TEST (POST) failed!!!

System will REBOOT in 5 minutes!!!
```

Figure 3-1 : Self-Test Failure

After the successful system bootup and passage of the self-tests, login will prompt for authentication.



```
POWER-ON-SELF-TEST (POST) passed.
Starting the upgrade watcher:
Starting the webserver:


SETTINGS: Version = 46
SETTINGS: Storage = 743772 bytes
Old setting version: 46
New settings version: 46
No action to settings is needed.
Starting Evertz-IPX Control System...

------------- WARNING ------------
You are attempting to sign on to a secure system!
Evertz-IPX login:
```

Figure 3-2 : Serial Port - Login Prompt

3.2. SERIAL PORT INTERFACE AUTHENTICATION

First time configuration requires the user to enter in the factory default login and password.

- "***customer***" for both Login and Password as seen in Figure 3-3.

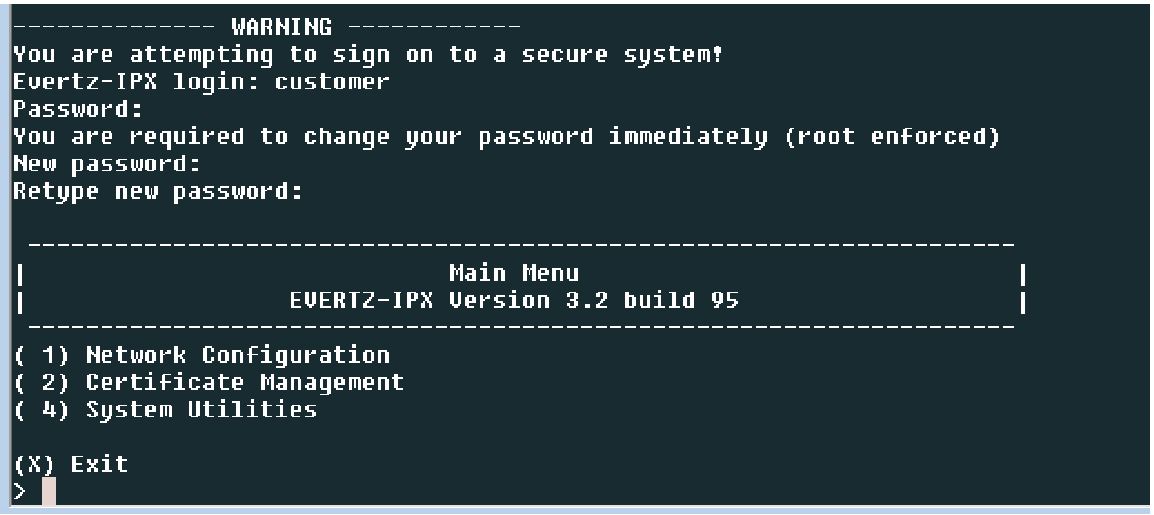
First time initialization requires the user to enter a new password and reconfirm it by entering for a second time. See Figure 3-3.

Password requirements:

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 shall be configurable to between [15] and [20] characters.

Example: **XyzAbc#4321@evertz**



```
-------------- WARNING ------------
You are attempting to sign on to a secure system!
Evertz-IPX login: customer
Password:
You are required to change your password immediately (root enforced)
New password:
Retype new password:

 ------------------------------------------------------------------
|                             Main Menu                            |
|                  EVERTZ-IPX Version 3.2 build 95                 |
 ------------------------------------------------------------------
( 1) Network Configuration
( 2) Certificate Management
( 4) System Utilities

(X) Exit
>
```

Figure 3-3 : Serial Port - New Password Configurations

Note: Once password is created, login name will still be "customer".

3.3. SERIAL MENU SYSTEM

Serial menu system consists of three categories,

- Network Configuration
  This sub-menu includes items to configure IP addresses of Ethernet controllers, either with pre-assigned IP or by DHCP.
- Certificate Management
  This sub-menu includes items to generate a Certificate Signing Request (CSR), and do TLS certificate factory reset. The CSR file can be downloaded from web interface and signed by a Certificate Authority to obtain a valid certificate which can be uploaded back to MMA10G-IPX via web (see section 3.4).
- System Utilities
  This sub-menu includes system-related functionalities.

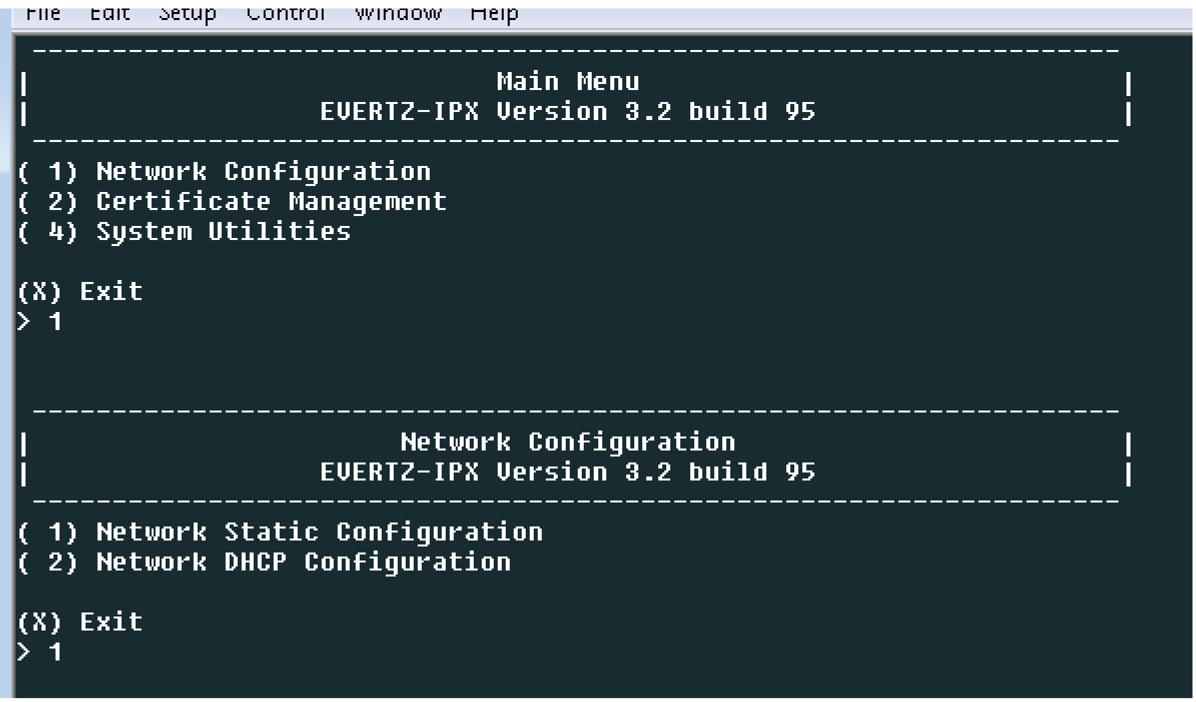
For a new IPX from factory, initial setup is needed after first system bootup. Initial setup includes,

- Set IP addresses for Ethernet controllers;
- Generate TLS certificate CSR;
- Generate SHA256 MAC;
- Set system date;

All these can be done through the serial menu system which is described with details in this section.

3.3.1. Network Configurations

IPX has two Ethernet controllers to provide control network with redundancy. Ethernet controller 1 connects the left most (facing the frame) Frame Controller, while Ethernet controller 2 connects the right most (facing the frame) Frame Controller. The IP addresses of Ethernet controllers can be set manually or assigned by DHCP. DHCP takes precedence over manual configuration.

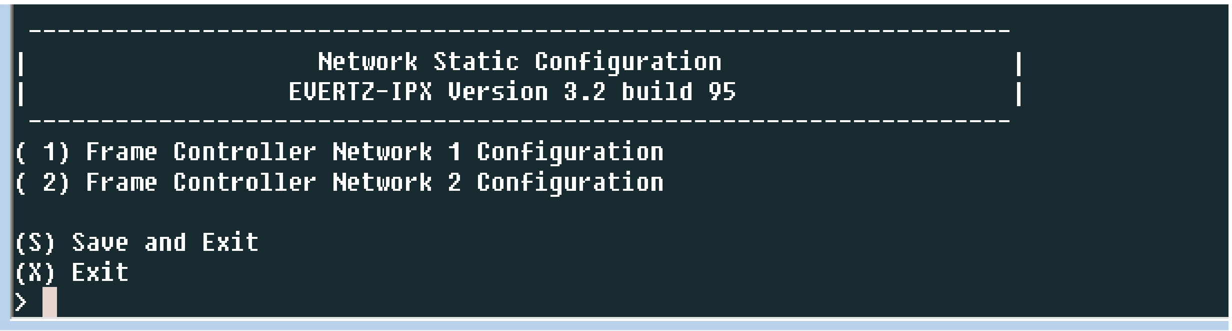


```
 ------------------------------------------------------------------
|                              Main Menu                           |
|                   EVERTZ-IPX Version 3.2 build 95                |
 ------------------------------------------------------------------
( 1) Network Configuration
( 2) Certificate Management
( 4) System Utilities

(X) Exit
> 1


 ------------------------------------------------------------------
|                        Network Configuration                     |
|                   EVERTZ-IPX Version 3.2 build 95                |
 ------------------------------------------------------------------
( 1) Network Static Configuration
( 2) Network DHCP Configuration

(X) Exit
> 1
```

Figure 3-4 : TeraTerminal Main Menu

3.3.1.1. Network Static Configuration

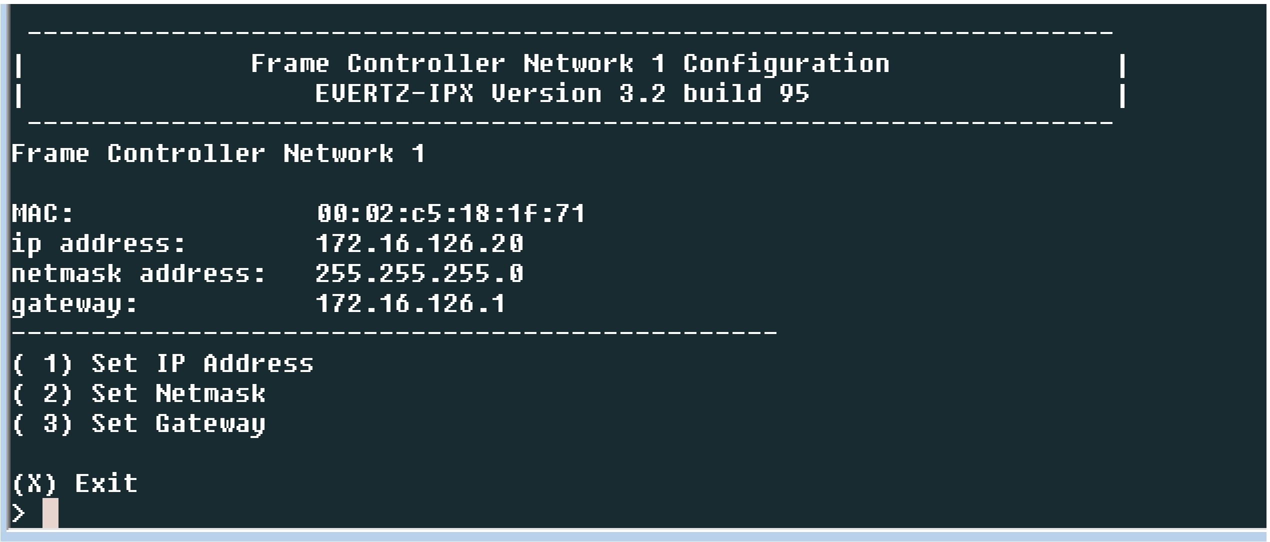
Two menu items are available for Frame Controller 1 and Frame Controller 2, respectively. (See Figure 3-5)



```
 ------------------------------------------------------------
|                  Network Static Configuration               |
|                 EVERTZ-IPX Version 3.2 build 95             |
 ------------------------------------------------------------
( 1) Frame Controller Network 1 Configuration
( 2) Frame Controller Network 2 Configuration

(S) Save and Exit
(X) Exit
>
```

Figure 3-5 : Network Configuration Main Menu

Each item includes three sub-items to configure IP address, netmaks, and gateway. (See Figure 3-6)



```
 -------------------------------------------------------------------
|              Frame Controller Network 1 Configuration              |
|                  EVERTZ-IPX Version 3.2 build 95                    |
 -------------------------------------------------------------------
Frame Controller Network 1

MAC:                 00:02:c5:18:1f:71
ip address:          172.16.126.20
netmask address:     255.255.255.0
gateway:             172.16.126.1
------------------------------------------------
( 1) Set IP Address
( 2) Set Netmask
( 3) Set Gateway

(X) Exit
>
```

Figure 3-6 : Network Configuration Sub-Menu

To choose one of the menu options, enter the number shown on the left and then press <Enter>. You will be prompted to enter the required parameter value. When you are done configuring the Network Setup menu items press (X) to return to the main menu.

(1)	This control sets the IP address.
(2)	This control sets the “subnet mask”.
(3)	This control sets the “Gateway”.

1. Select option (1) *Set IP Address* and configure the IP address for the IPX ensuring that the IP address is not already in use on the network.

2. Now select option (2) *Set Netmask* and configure the correct subnet mask for your network.

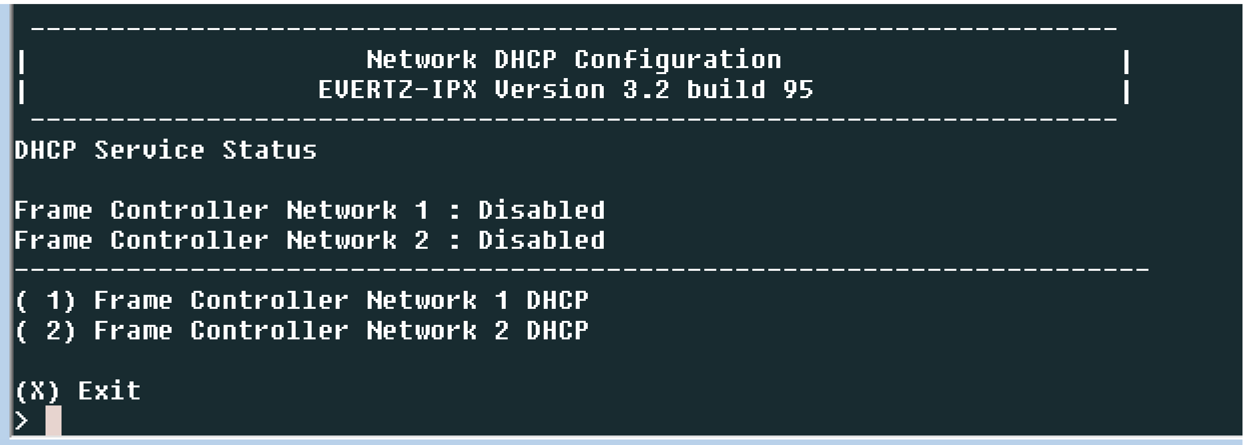
3. If required also configure the Default Gateway.

4. Exit from the Network Configuration menu using (s) *Save and Exit*, NOT (x) *Exit*.

Entering (X) Exit or (S) Save and Exit on any menu will take the administrator to the higher menu. Entering (X) Exit on the Main Menu will log out the administrator.

3.3.1.2. Network DHCP Configuration

This menu is used to enable IP configuration on Ethernet controllers via DHCP. For any change of DHCP configuration, system needs to reboot.

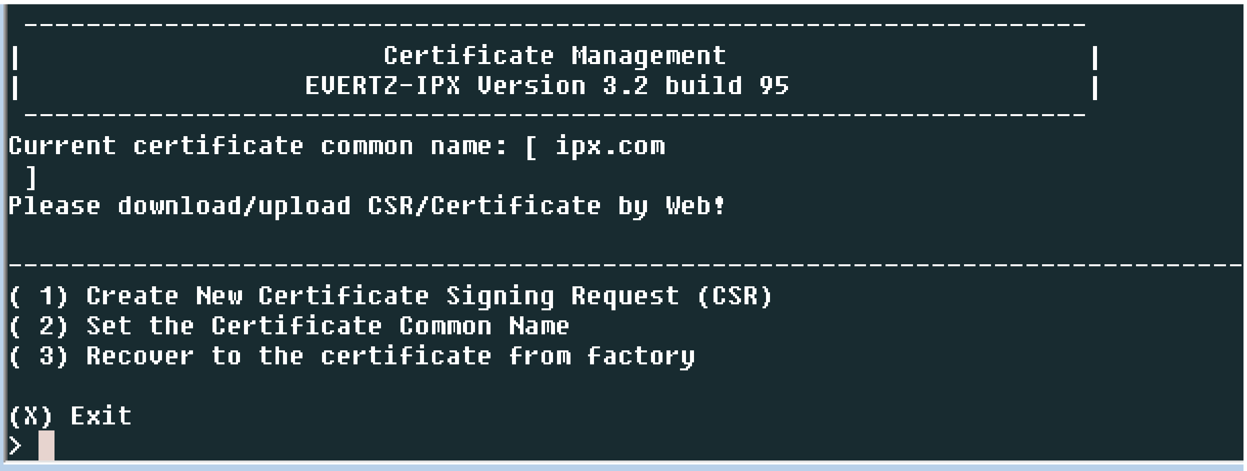


```
 -------------------------------------------------------------------
|                     Network DHCP Configuration                   |
|                  EVERTZ-IPX Version 3.2 build 95                 |
 -------------------------------------------------------------------
DHCP Service Status

Frame Controller Network 1 : Disabled
Frame Controller Network 2 : Disabled
----------------------------------------------------------------------
( 1) Frame Controller Network 1 DHCP
( 2) Frame Controller Network 2 DHCP

(X) Exit
>
```

Figure 3-7 : Network DHCP Configuration Menu

3.3.2. Certificate Management

By default IPX uses the self-signed TLS certificate for all services which are carried over TLS. To update certificate, user needs to generate certificate signing request (CSR) first via serial menu.

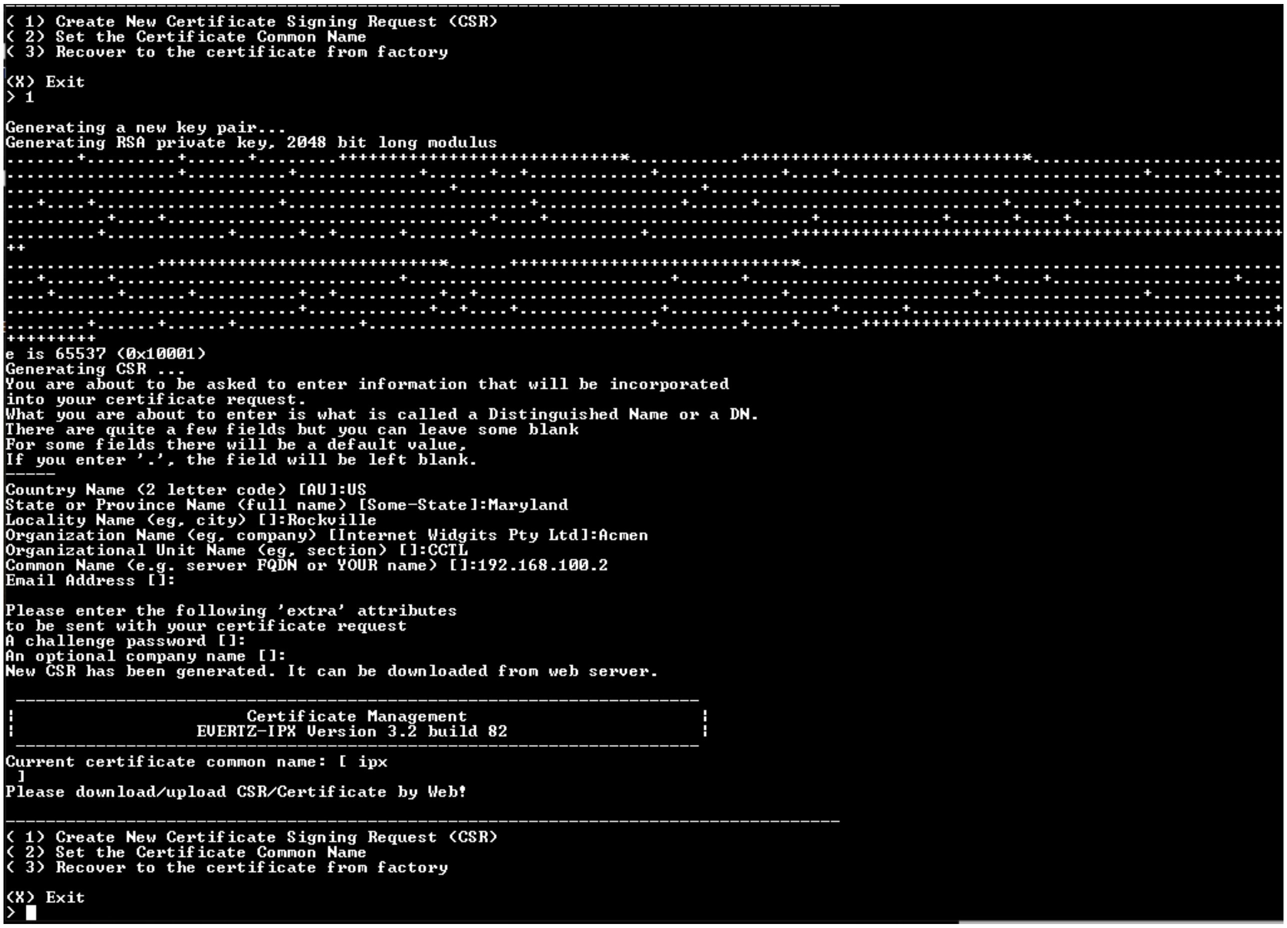


```
 -------------------------------------------------------------------
|                      Certificate Management                      |
|                  EVERTZ-IPX Version 3.2 build 95                 |
 -------------------------------------------------------------------
Current certificate common name: [ ipx.com
 ]
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
>
```

Figure 3-8 : Certificate Management Menu

Select option (1): From console access, Create New Certificate Signing Certificate. As can be seen in the Figure below, the following options are defined:

- **Country Name:** a 2 letter code for the country is entered.
- **State or Providence:** not required
- **Locality Name:** not required
- **Organization Name:** name of company using the TOE
- **Organizational Unit:** unit within the company using the TOE
- **Common Name:** can be IP address or name of Administrator

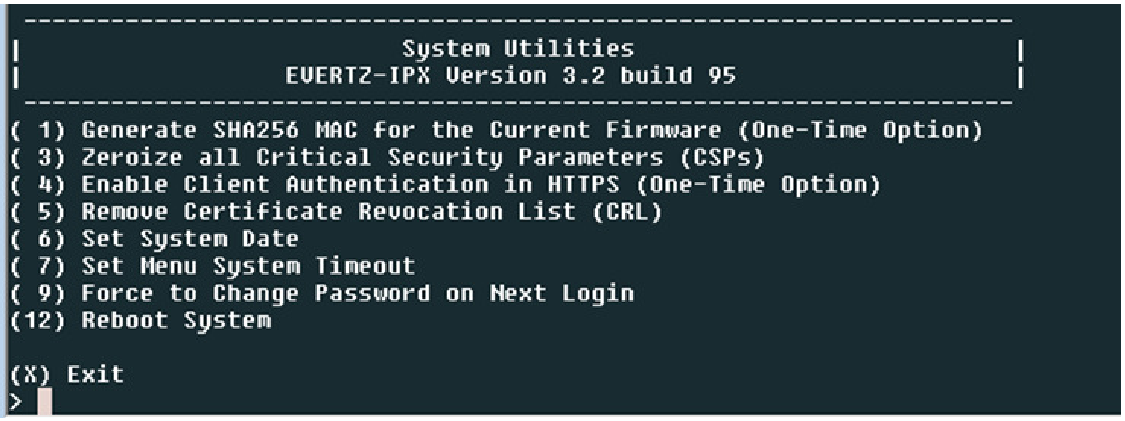


```
--------------------------------------------------------------------------------
( 1) Create New Certificate Signing Request (CSR)
( 2) Set the Certificate Common Name
( 3) Recover to the certificate from factory

(X) Exit
> 1

Generating a new key pair...
Generating RSA private key, 2048 bit long modulus
.......+.........+.........+.....+++++++++++++++++++++++++++++*..........++++++++++++++++++++++++++++*.........................
.................+..........+.............+.....+..+.............+...........+....+...............................+.....+......
.............................................+.......................+.........................................................
...+.....+.................+........................+..............+.......+.......................+.......+...................
..........+....+................................+....+..........................+............+......+....+.....................
.........+............+......+...+......+......+................+..............+++++++++++++++++++++++++++++++++++++++++++++++
++
...............+++++++++++++++++++++++++++++*.....+++++++++++++++++++++++++++++*...............................................
...+......+.............................+.........................+.......+........................+....+..................+...
....+......+......+..........+...+.........+..+..............................+...................+................+............
.............................+............+...+....+.............+.................+......+...................................+
.........+.....+......+.............+............................+........+....+.....+++++++++++++++++++++++++++++++++++++++++
+++++++++
e is 65537 (0x10001)
Generating CSR ...
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Rockville
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Acmen
Organizational Unit Name (eg, section) []:CCTL
Common Name (e.g. server FQDN or YOUR name) []:192.168.100.2
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
New CSR has been generated. It can be downloaded from web server.

 ---------------------------------------------------------------------
¦                         Certificate Management                      ¦
¦                   EVERTZ-IPX Version 3.2 build 82                   ¦
 ---------------------------------------------------------------------
Current certificate common name: [ ipx
 ]
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
> 
```

Figure 3-9 : New Certificate Creation

The ‘Certificate Management’ item also includes two items to set the certificate common name and do factory reset for certificate. Note that system reboot is needed for certificate factory reset.

3.3.3. System Utilities



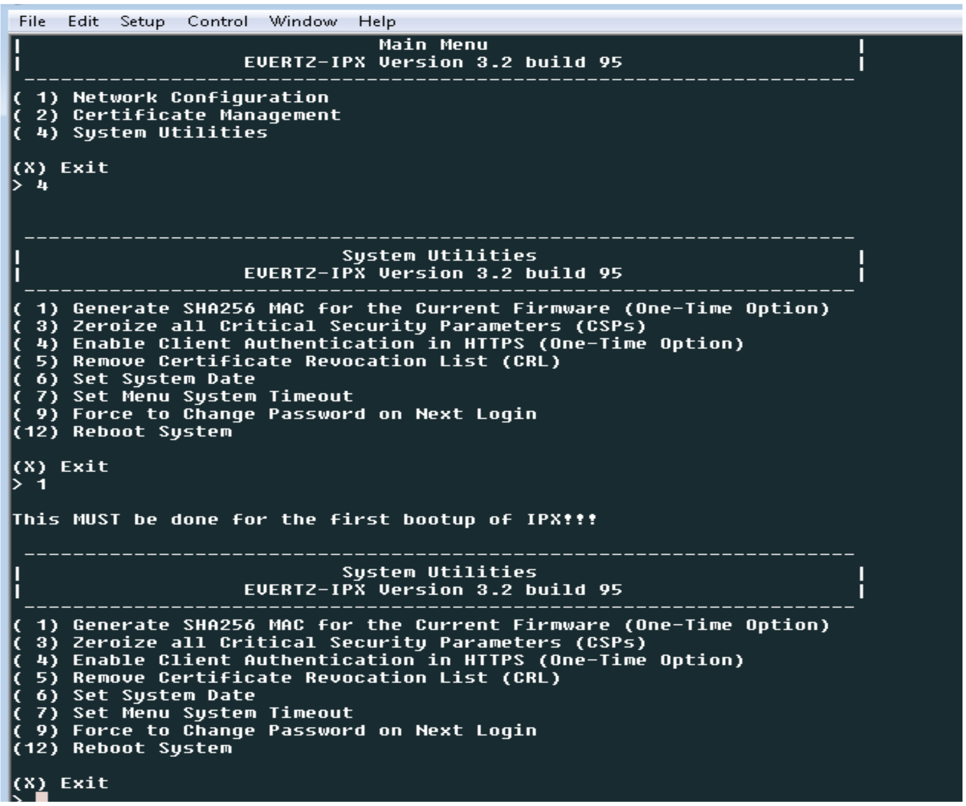
```
 ---------------------------------------------------------------
|                       System Utilities                        |
|                 EVERTZ-IPX Version 3.2 build 95               |
 ---------------------------------------------------------------
( 1) Generate SHA256 MAC for the Current Firmware (One-Time Option)
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
>
```

Figure 3-10 : System Utilities Menu

3.3.3.1. Generate SHA256 MAC for the Current Firmware (One-Time Option)

For new IPX from factory, SHA256 MAC on loaded firmware needs to be generated. This is a one time option. See Figure 3-11.

- Select <**4**> for *System Utilities*
- Select <**1**> to *Generate SHA256 MAC*
- Select <**12**> to *Reboot System*



```
|                           Main Menu                            |
|                 EVERTZ-IPX Version 3.2 build 95                |
 ----------------------------------------------------------------
( 1) Network Configuration
( 2) Certificate Management
( 4) System Utilities

(X) Exit
> 4


 ----------------------------------------------------------------
|                        System Utilities                        |
|                 EVERTZ-IPX Version 3.2 build 95                |
 ----------------------------------------------------------------
( 1) Generate SHA256 MAC for the Current Firmware (One-Time Option)
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
> 1

This MUST be done for the first bootup of IPX!!!

 ----------------------------------------------------------------
|                        System Utilities                        |
|                 EVERTZ-IPX Version 3.2 build 95                |
 ----------------------------------------------------------------
( 1) Generate SHA256 MAC for the Current Firmware (One-Time Option)
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
>
```

Figure 3-11 : Serial Port - Generating SHA256 MAC

3.3.3.2. Zeroize all Critical Security Parameters (CSPs)

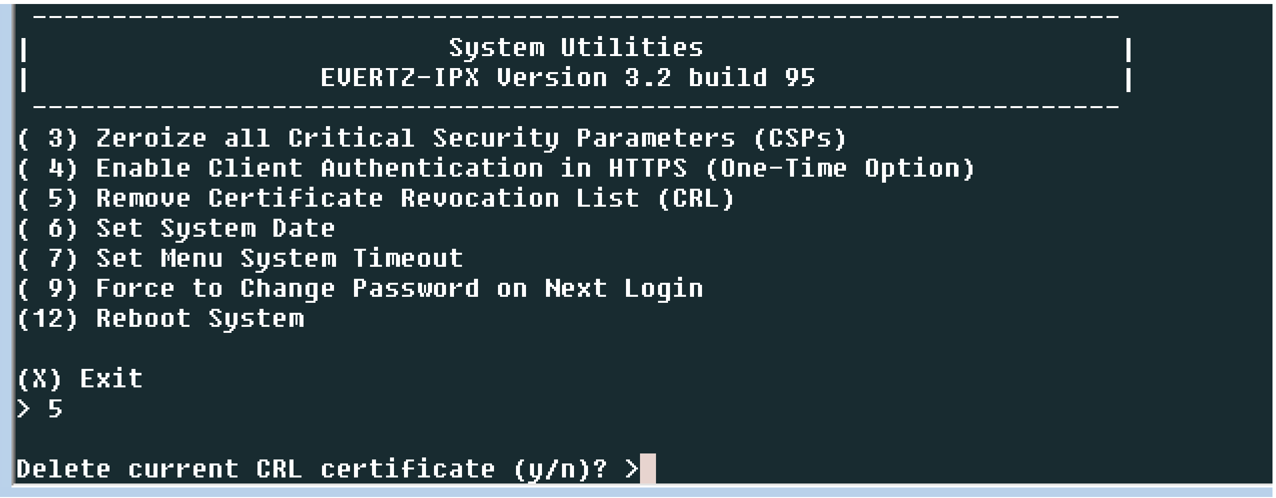
By selecting #3, administrator can use this menu item to delete all certificate-related files and keys.

3.3.3.3. Enable Client Authentication in HTTPS (One-Time Option)

By selecting #4, administrator can enable client certificate authentication for HTTPS service with this menu item. Need to reboot IPX for this change.

3.3.3.4. Remove Certificate Revocation List (CRL)

By selecting #5, administrator can upload CRL file to IPX via web interface. This menu item provides option to delete it.

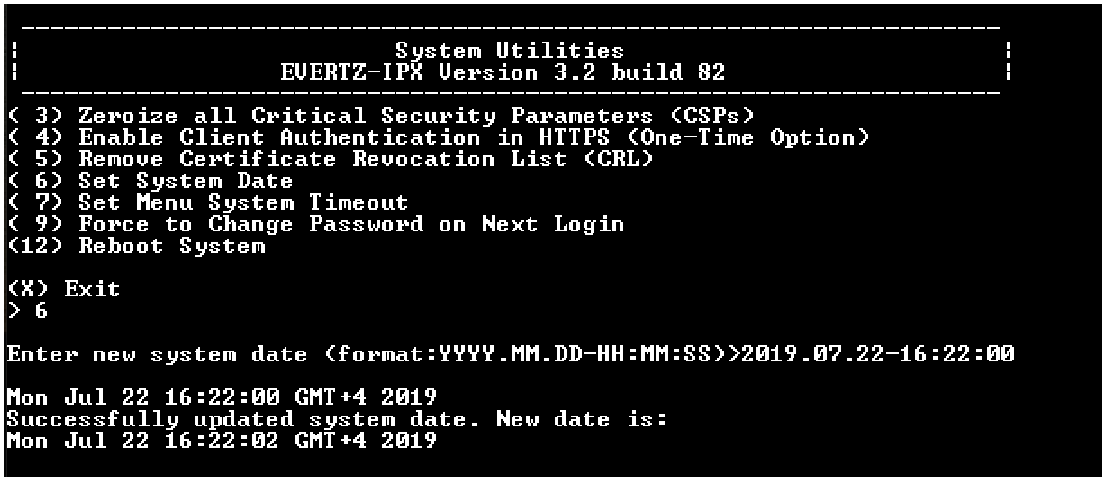


```
 -------------------------------------------------------------------
|                          System Utilities                         |
|                  EVERTZ-IPX Version 3.2 build 95                  |
 -------------------------------------------------------------------
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
> 5

Delete current CRL certificate (y/n)? >
```

Figure 3-12 : Certificate Deletion

3.3.3.5. Set System Date

Selecting #6 Set System Date will take you to the following menu:



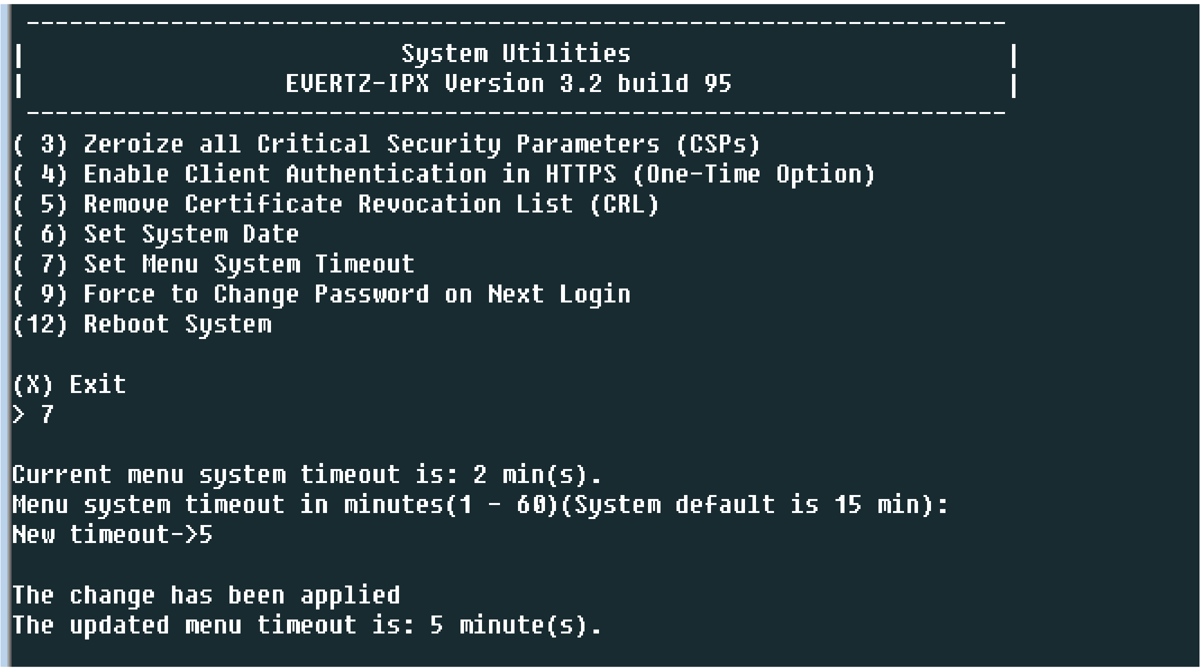
```
 -------------------------------------------------------------------
|                          System Utilities                         |
|                  EVERTZ-IPX Version 3.2 build 82                  |
 -------------------------------------------------------------------
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
> 6

Enter new system date (format:YYYY.MM.DD-HH:MM:SS)>2019.07.22-16:22:00

Mon Jul 22 16:22:00 GMT+4 2019
Successfully updated system date. New date is:
Mon Jul 22 16:22:02 GMT+4 2019
```

Figure 3-13 : Serial Port – System Date

The administrator is asked to enter the new system date. Once the date and time are entered and the administrator hits return, the date and time are updated.

3.3.3.6. Set Menu System Timeout

Selecting #7 Set Menu System Timeout will take you to the system timeout menu shown below.



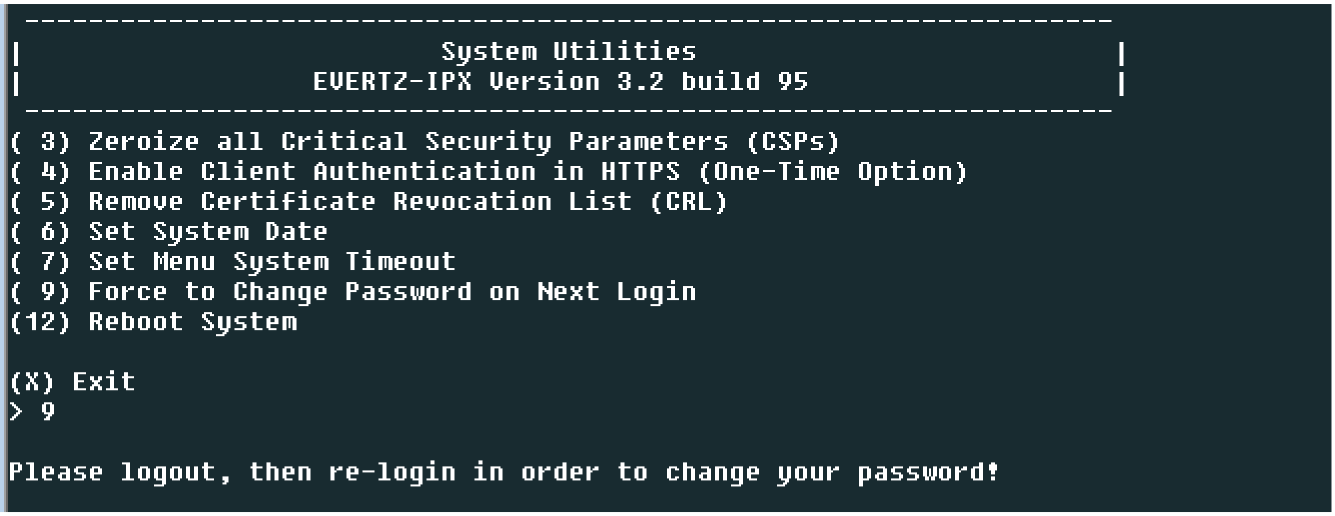
```
 --------------------------------------------------------------------
|                          System Utilities                           |
|                  EVERTZ-IPX Version 3.2 build 95                    |
 --------------------------------------------------------------------
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
> 7

Current menu system timeout is: 2 min(s).
Menu system timeout in minutes(1 - 60)(System default is 15 min):
New timeout->5

The change has been applied
The updated menu timeout is: 5 minute(s).
```

Figure 3-14 : Serial Port – System Timeout

The administrator can enter a value of 1 – 60 minutes. Once the configuration is entered and the administrator hits return, the timeout value is set.

3.3.3.7. Force to Change Password on Next Login

Selecting #9, the administrator is forced to change password for ‘customer’ account on next login.

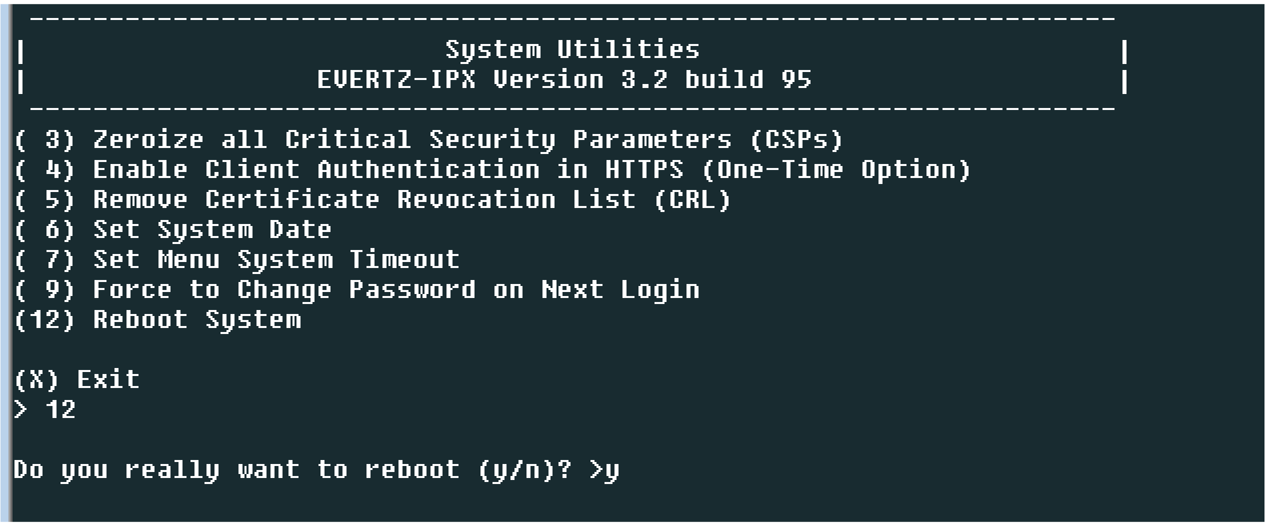


```
 --------------------------------------------------------------------
|                          System Utilities                           |
|                  EVERTZ-IPX Version 3.2 build 95                    |
 --------------------------------------------------------------------
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
> 9

Please logout, then re-login in order to change your password!
```

Figure 3-15 : Force Password Change

3.3.3.8. Reboot System

Administrator can use Item (12) to reboot IPX.



```
 ---------------------------------------------------------------------
|                          System Utilities                           |
|                  EVERTZ-IPX Version 3.2 build 95                    |
 ---------------------------------------------------------------------
( 3) Zeroize all Critical Security Parameters (CSPs)
( 4) Enable Client Authentication in HTTPS (One-Time Option)
( 5) Remove Certificate Revocation List (CRL)
( 6) Set System Date
( 7) Set Menu System Timeout
( 9) Force to Change Password on Next Login
(12) Reboot System

(X) Exit
> 12

Do you really want to reboot (y/n)? >y
```

Figure 3-16 : Reboot System

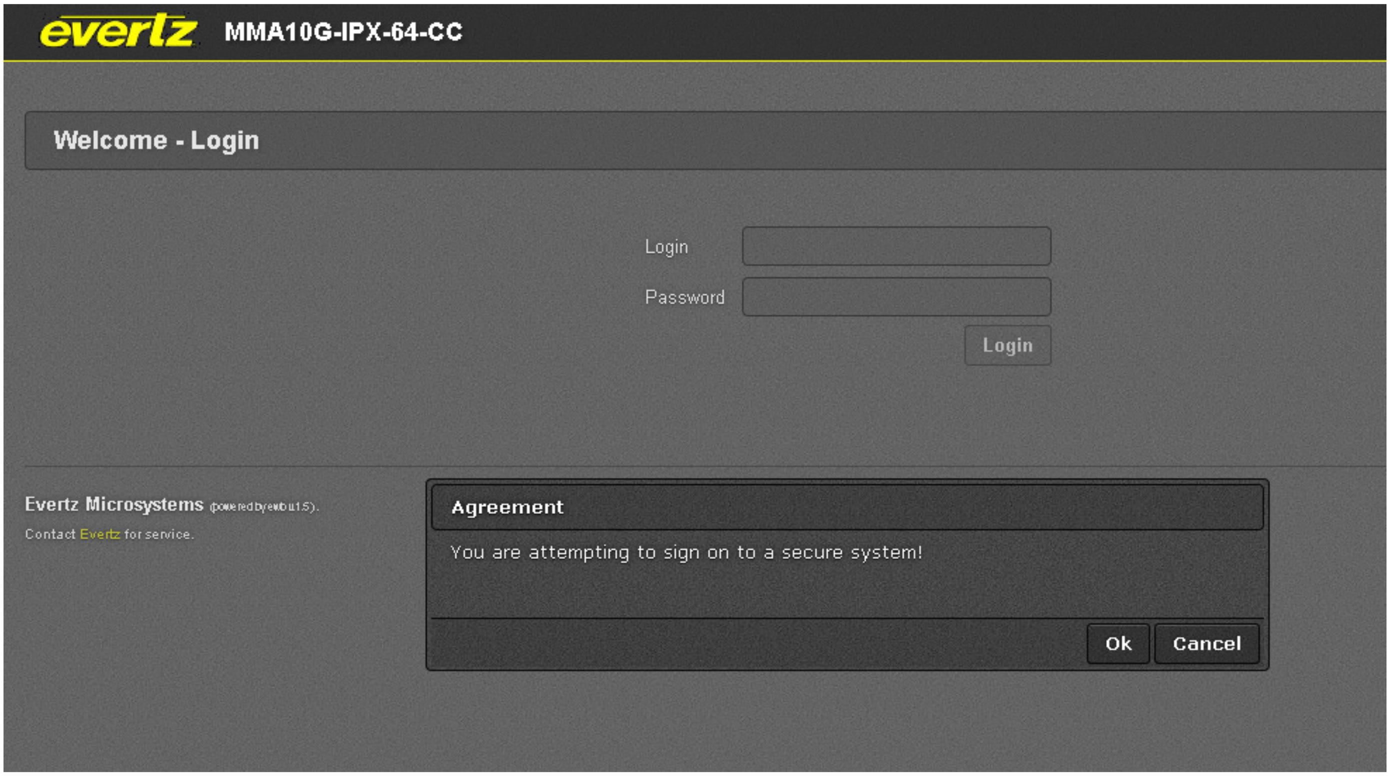
4. WEB INTERFACE

Login

Connect to the MMA10G-IPX by entering in the IP address for the EMX frame controller created in section 3.3.3.6 into a web browser such as FireFox or Chrome.

Make sure to use a secured HTTPS URL, i.e. "https://172.21.1.236"

Whenever logging in, the user must agree to sign on to a secure system. See Figure 4-1.
Click "***OK***" to agree the terms for entering a secured system.



Evertz Microsystems (powered by ewbu1.5).

Contact Evertz for service.

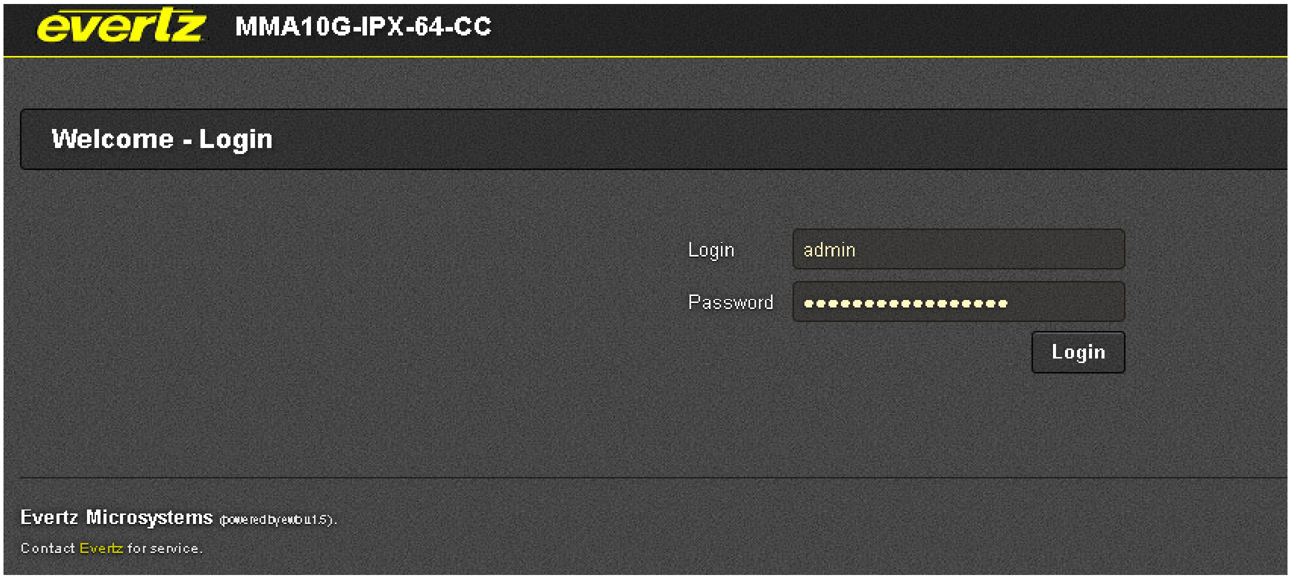
You are attempting to sign on to a secure system!

Figure 4-1 : WebEASY® - Entering Secured System Prompt

4.1. INITIAL LOGIN AND PASSWORD CONFIGURATIONS

First time configuration requires the administrator to enter in the factory default login and password, see Figure 4-2.

For login enter "***admin***" and keep password blank for first time, system will prompt the user to update a new password.



MMA10G-IPX-64-CC

Welcome - Login

Login: admin

Password: ●●●●●●●●●●●●●●●●●

Evertz Microsystems (powered by ewb u1.5).

Contact Evertz for service.

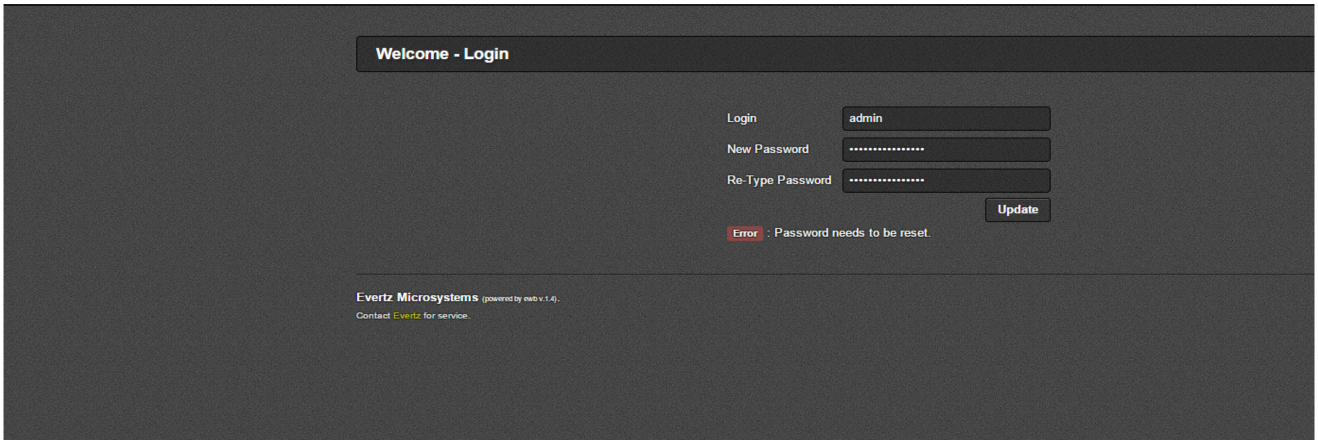
Figure 4-2 : WebEASY® - Default Login Prompt

First time initialization requires the user to enter a new password and confirm it by entering it again for second time. See Figure 4-3.

Password requirements:

- At least 15 characters long
- Must contain at least two upper case (A-Z) and two lower case (a-z) letters
- Must contain at least two number (0-9)
- Must contain at least two special characters (~!@#$%^&*()-)

Example: ***XyzAbc1234@evert&***



Welcome - Login

Login: admin

New Password: ••••••••••••••••

Re-Type Password: ••••••••••••••••

Error : Password needs to be reset.

Evertz Microsystems (powered by ewb v.1.4).

Contact Evertz for service.

Figure 4-3 : WebEASY® - New Password Configuration

Click "***Update***" button to access module and enter the secured system.

4.2. TOP MENU BAR DESCRIPTIONS

The features on the top menu bar are dependant on the privileges set for the user. Some of these features will be used often by the user when making changes or updates to the system. Figure 4-4 displays the top menu bar for a user with full privileges.

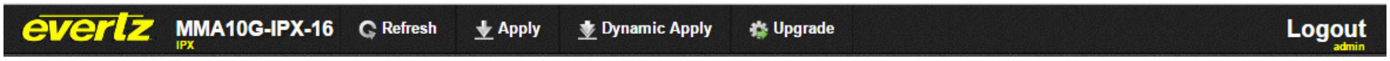


Figure 4-4 : WebEASY® - Top Menu

Refresh: The MMA10G-IPX requires the user to click the Refresh button when changes are made and applied. Also monitoring windows are not dynamically updated and requires the user to refresh the screen to get new updates.

Apply: When changes are made to the system, the Apply button needs to be clicked in order for changes to take effect. Also it may be required to reboot the system after applying some changes.

Dynamic Apply: This feature automatically applies changes as they are being made. This mode requires the user to be familiar and experienced with using the product.

> **Note:** *Any previous changes that were made and not applied before entering the Dynamic Apply Mode will not be saved.*

Upgrade: From time to time, new features and improvements are added to the system. The Upgrade button is used to upload the new firmware.

Logout: This button is used for logging out the user.

> **Note:** *This is also a feature added that mandates the user to re-login after a specified idle time under the users tab in the bottom menu bar.*

4.3. BOTTOM MENU BAR DESCRIPTIONS

The features on the bottom menu bar are used for checking the login reports, adding and modifying users, roles and adding information to be displayed when the user scrolls over different menu items.

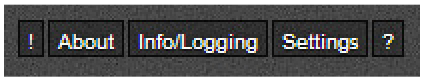
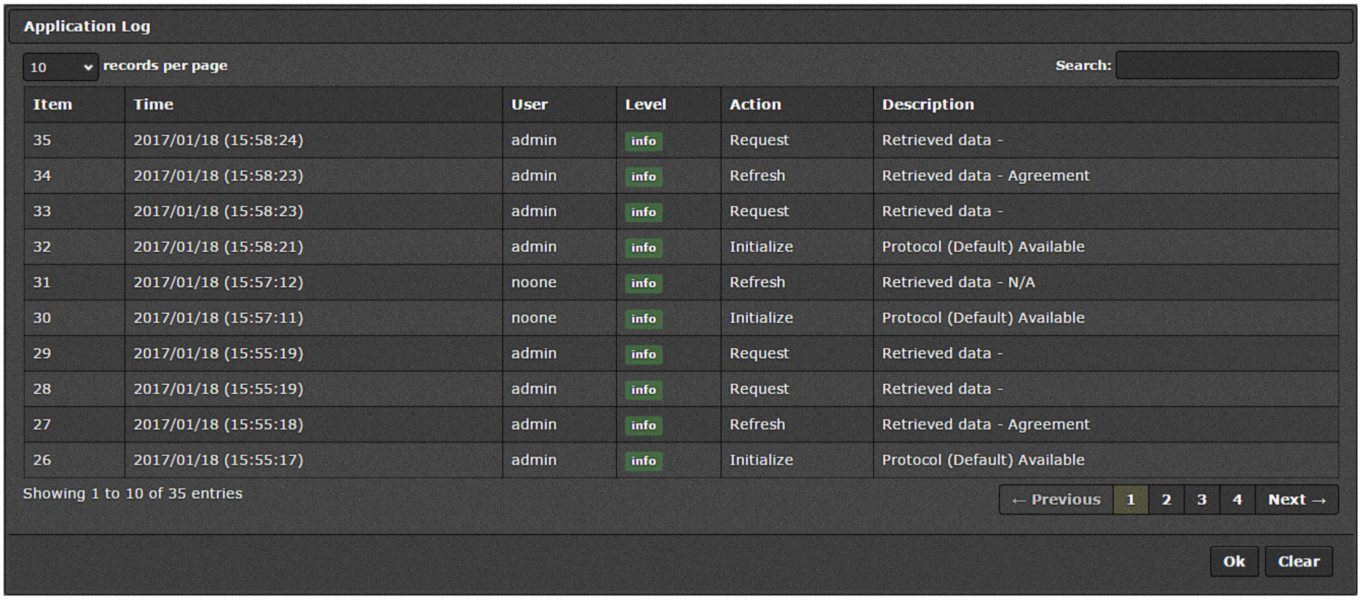


Figure 4-5 : WebEASY® - Bottom Menu

4.3.1. Exclamation Mark Button (!)

The Exclamation Mark button brings up an Application Log report that lists all the active users (with recent activities) on the system. (Figure 4-6).



Application Log

10 records per page

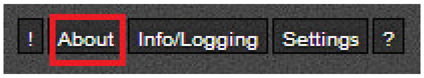
Search:

Item	Time	User	Level	Action	Description
35	2017/01/18 (15:58:24)	admin	info	Request	Retrieved data -
34	2017/01/18 (15:58:23)	admin	info	Refresh	Retrieved data - Agreement
33	2017/01/18 (15:58:23)	admin	info	Request	Retrieved data -
32	2017/01/18 (15:58:21)	admin	info	Initialize	Protocol (Default) Available
31	2017/01/18 (15:57:12)	noone	info	Refresh	Retrieved data - N/A
30	2017/01/18 (15:57:11)	noone	info	Initialize	Protocol (Default) Available
29	2017/01/18 (15:55:19)	admin	info	Request	Retrieved data -
28	2017/01/18 (15:55:19)	admin	info	Request	Retrieved data -
27	2017/01/18 (15:55:18)	admin	info	Refresh	Retrieved data - Agreement
26	2017/01/18 (15:55:17)	admin	info	Initialize	Protocol (Default) Available

Showing 1 to 10 of 35 entries

Figure 4-6 : WebEASY® - Exclamation Button Menu / Application Log

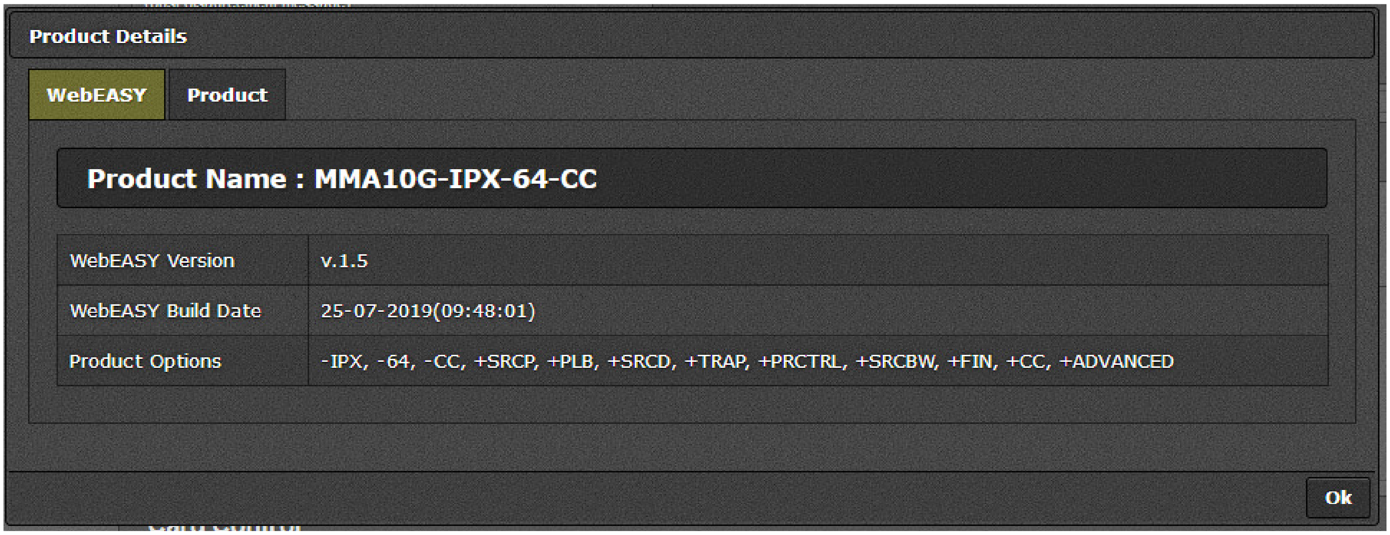
4.3.2. About



The about button brings up product details including information about the WebEASY® build and information about the MMA10G-IPX-64 product.

4.3.2.1. WebEASY®

This tab contains information about WebEASY® including installed WebEASY® version, build date of this version and product options.



Product Details

Product Name : MMA10G-IPX-64-CC

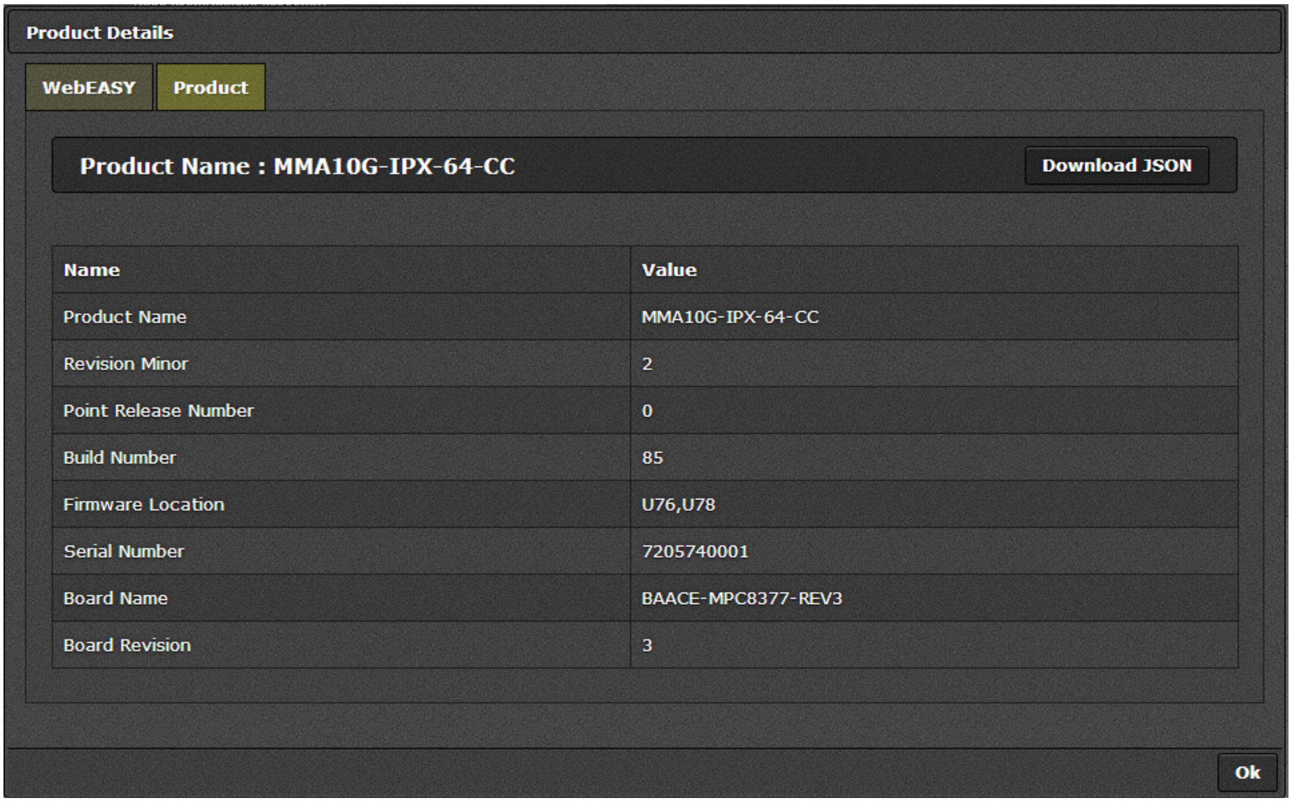
WebEASY Version	v.1.5
WebEASY Build Date	25-07-2019(09:48:01)
Product Options	-IPX, -64, -CC, +SRCP, +PLB, +SRCD, +TRAP, +PRCTRL, +SRCBW, +FIN, +CC, +ADVANCED

Figure 4-7 WebEASY® - About / WebEASY

4.3.2.2. Product:

This tab contains information about the MMA10G-IPX-64 product.

Download JSON: This tab allows the user to download JSON.

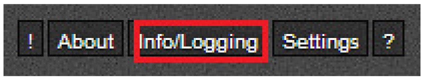


Product Name : MMA10G-IPX-64-CC

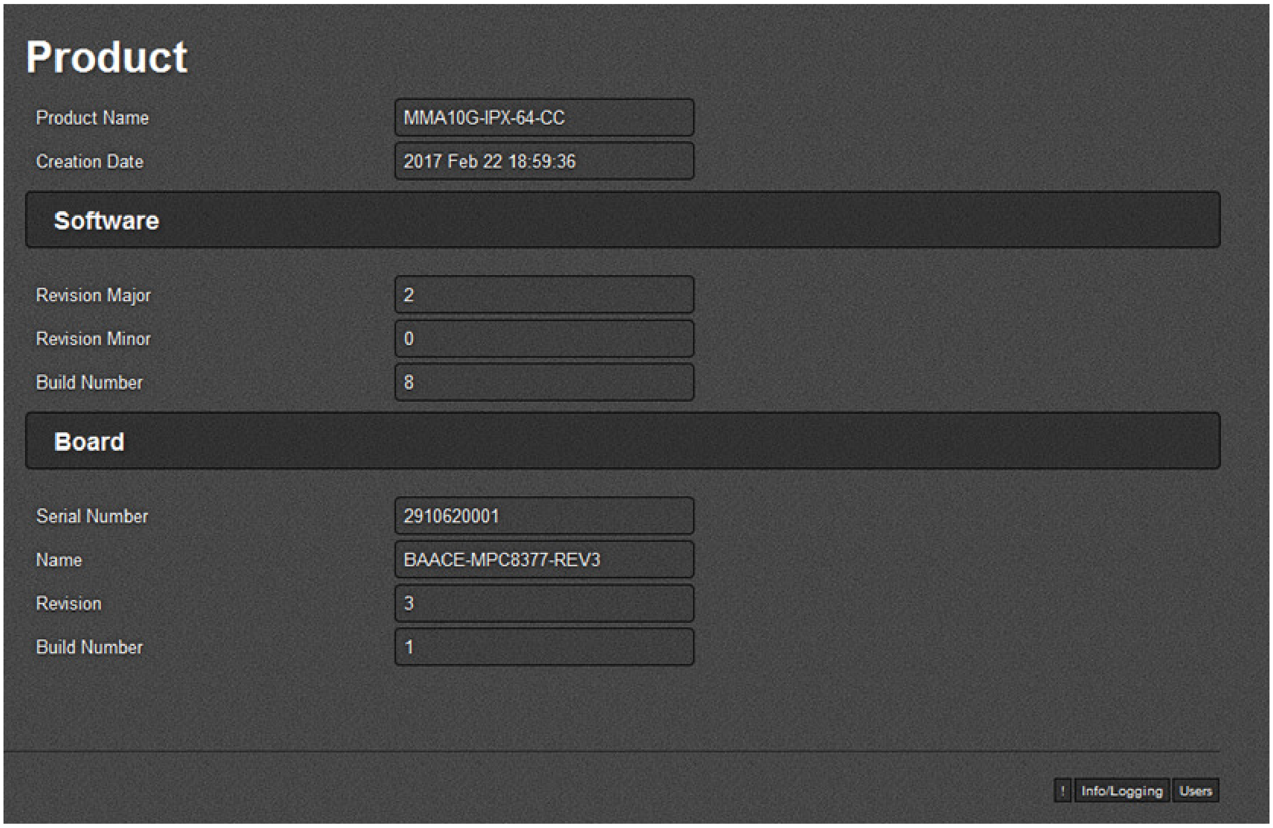
Name	Value
Product Name	MMA10G-IPX-64-CC
Revision Minor	2
Point Release Number	0
Build Number	85
Firmware Location	U76,U78
Serial Number	7205740001
Board Name	BAACE-MPC8377-REV3
Board Revision	3

Figure 4-8 : WebEASY® - About / Product Tab

4.3.3. Info/Logging



By clicking Info/Logging button on the bottom bar, a window will appear as is shown in Figure 4-9. In this section the user can find some information about product, software and board.



Product

Product Name: MMA10G-IPX-64-CC

Creation Date: 2017 Feb 22 18:59:36

Software

Revision Major: 2

Revision Minor: 0

Build Number: 8

Board

Serial Number: 2910620001

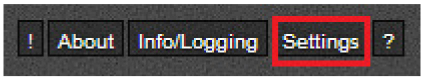
Name: BAACE-MPC8377-REV3

Revision: 3

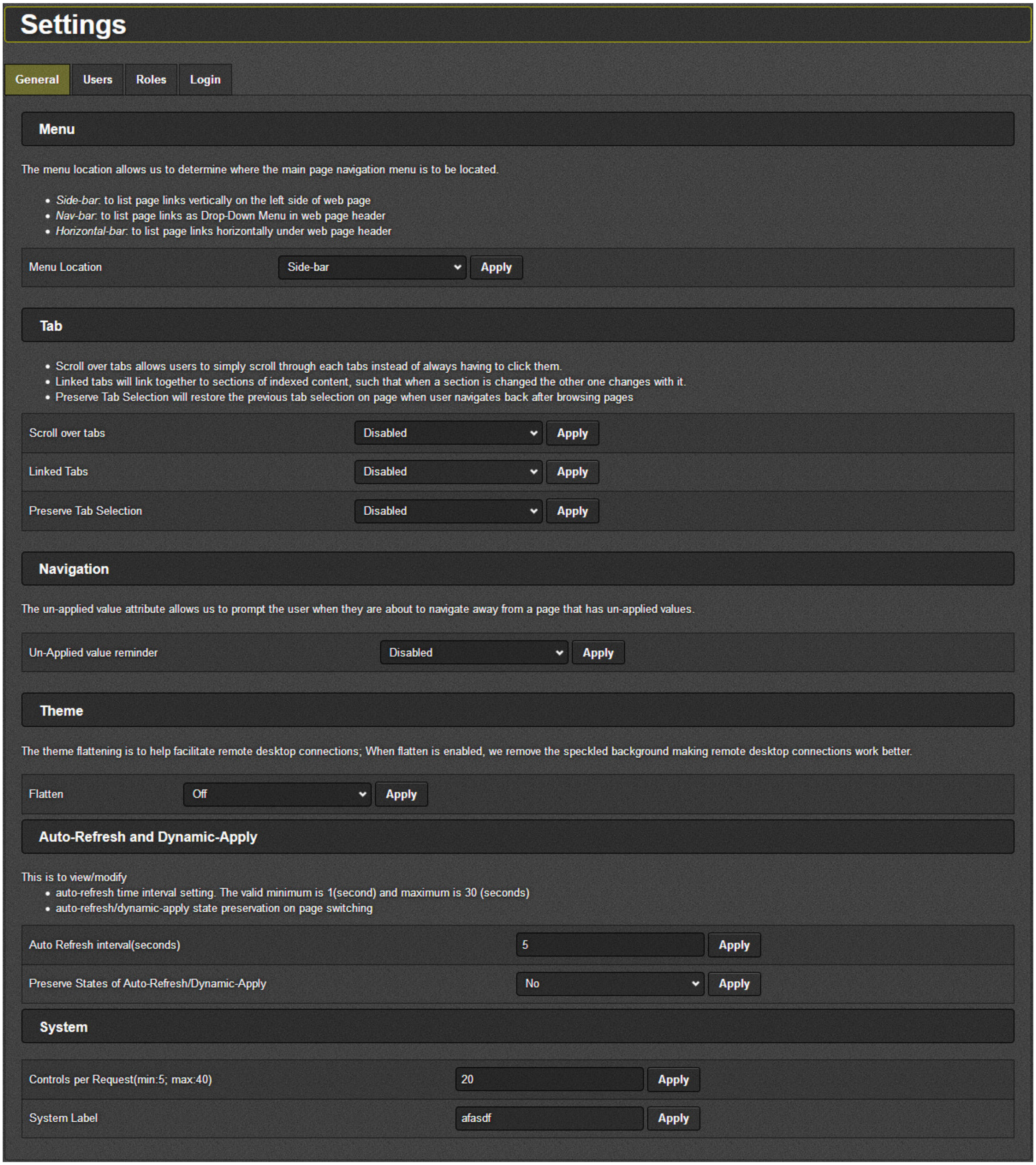
Build Number: 1

Figure 4-9 : WebEASY® - Info / Logging Button

4.3.4. Settings



The Settings button will be managed and accessed only by privileged users.



Menu

The menu location allows us to determine where the main page navigation menu is to be located.

- *Side-bar*: to list page links vertically on the left side of web page
- *Nav-bar*: to list page links as Drop-Down Menu in web page header
- *Horizontal-bar*: to list page links horizontally under web page header

Menu Location: Side-bar — Apply

Tab

- Scroll over tabs allows users to simply scroll through each tabs instead of always having to click them.
- Linked tabs will link together to sections of indexed content, such that when a section is changed the other one changes with it.
- Preserve Tab Selection will restore the previous tab selection on page when user navigates back after browsing pages

Scroll over tabs: Disabled — Apply

Linked Tabs: Disabled — Apply

Preserve Tab Selection: Disabled — Apply

Navigation

The un-applied value attribute allows us to prompt the user when they are about to navigate away from a page that has un-applied values.

Un-Applied value reminder: Disabled — Apply

Theme

The theme flattening is to help facilitate remote desktop connections; When flatten is enabled, we remove the speckled background making remote desktop connections work better.

Flatten: Off — Apply

Auto-Refresh and Dynamic-Apply

This is to view/modify

- auto-refresh time interval setting. The valid minimum is 1(second) and maximum is 30 (seconds)
- auto-refresh/dynamic-apply state preservation on page switching

Auto Refresh interval(seconds): 5 — Apply

Preserve States of Auto-Refresh/Dynamic-Apply: No — Apply

System

Controls per Request(min:5; max:40): 20 — Apply

System Label: afasdf — Apply

Figure 4-10 : WebEASY® - Settings / General

4.3.4.1. General

Menu

Menu Location: The menu location allows us to determine where the main page navigation menu is to be located. Click apply to set menu location after selecting.

- *Side-bar:* List page links vertically on the left side of web page.
- *Nav-bar*: List page links as drop-down menu in web page header
- *Horizontal-bar:* List page links horizontally under web page header

Tab:

Tab: Allows user to enable/disable tab functionality.

- *Scroll-Over Tabs*: Scroll over tabs allow users to simply scroll through each tab instead of always having to click them.
- *Linked Tabs* Linked tabs will link together to sections of indexed content, such that when a section is changed the other one changes with it.
- *Preserve Tab Selection:* will restore the previous tab selection on page when user navigates back after browsing pages.

Navigation:

Un-Applied Value Reminder: The un-applied value attribute allows a prompt to be generated when the user is about to navigate away from a page that has un-applied values.

Theme:

Flatten: Theme flattening will remove speckled background, this will make remote desktop connections work better.

Auto-Refresh and Dynamic-Apply:

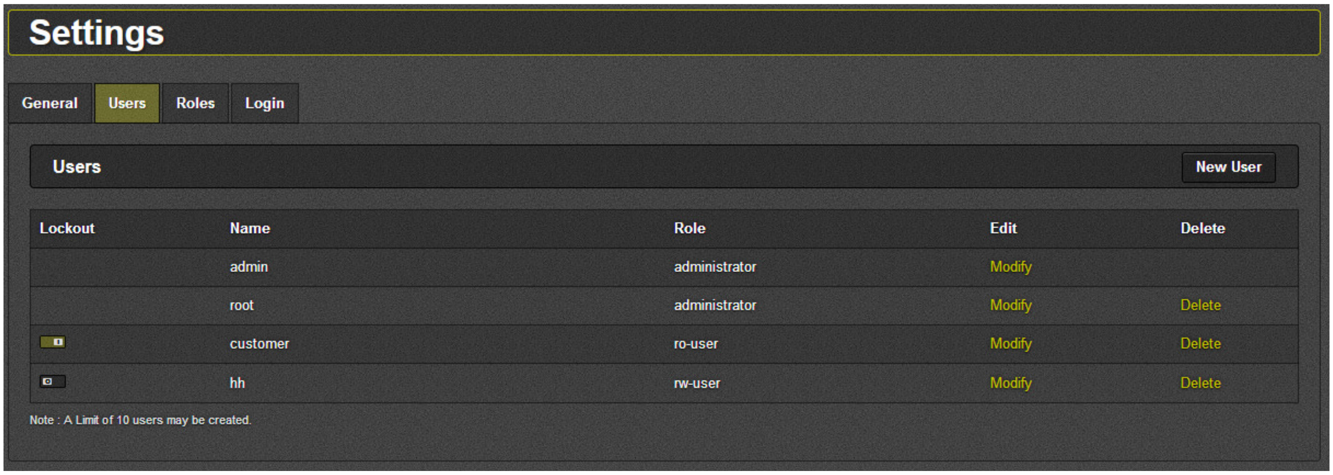
Allows automatic page refresh and dynamic-apply to be set.

- *Auto Refresh Interval:* Page auto-refresh can be set between 1sec and 30sec.
- *Preserve States of Auto-Refresh/Dynamic-Apply:* Preserves state of auto-refresh and dynamic apply when switching pages.

System:

The TOE is classified as a network device (a generic infrastructure device that can be connected to a network). The TOE hardware devices are the Evertz MMA10G-IPX-16 (1 RU), MMA10G-IPX-32 (3RU), MMA10G-IPX-64 (6 RU) running IPX v3.2 and will be referred to as IPX throughout this document. The IPX appliances are Ethernet switches optimized for video content.

4.3.4.2. Users



Settings

General | **Users** | Roles | Login

Users — New User

Lockout	Name	Role	Edit	Delete
	admin	administrator	Modify	
	root	administrator	Modify	Delete
■	customer	ro-user	Modify	Delete
□	hh	rw-user	Modify	Delete

Note : A Limit of 10 users may be created.

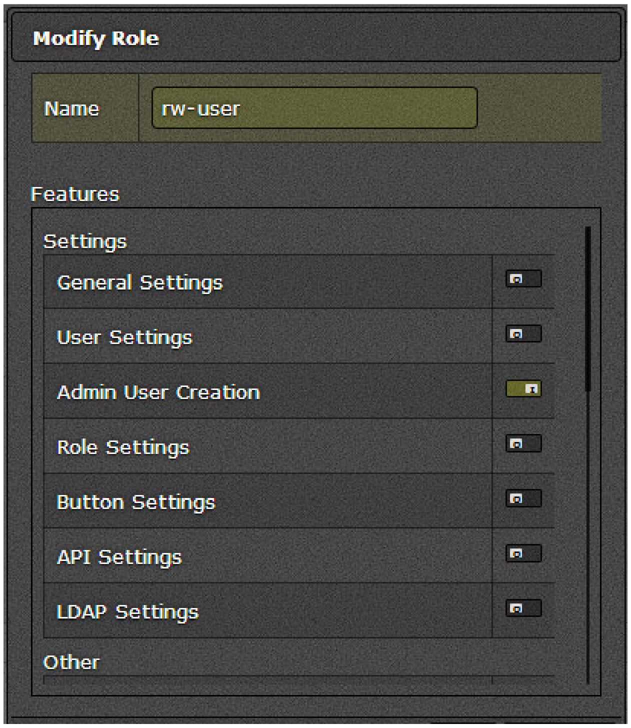
Figure 4-11 : WebEASY® - Settings / Users

Lockout: This button shows if the user is locked out for meet the maximum failed authentication attempts. If the button is to the left (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 can 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.



Modify Role

Name: rw-user

Features

Settings

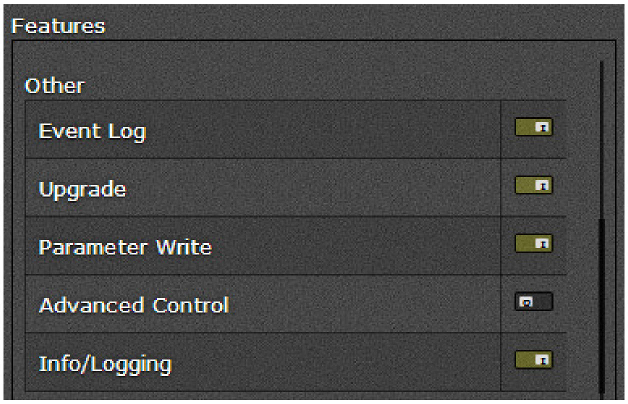
General Settings	□
User Settings	□
Admin User Creation	■
Role Settings	□
Button Settings	□
API Settings	□
LDAP Settings	□

Other

Figure 4-12 : - Settings / Users / Modify User (1) / Settings

The modify users allows for the following features to be enabled or disabled:

- **Settings:**
  - *General Settings:* Whether the user can view and modify settings in the general menu.
  - *User Settings:* Whether the user configure user permissions
  - *Admin User Creation:* Whether the user can create new admin user accounts.
  - *Role Settings:* Whether the user can configure roles.
  - *Whether the user can configure protected buttons permissions.*
  - *API Settings:* Whether the user can configure the LDAP settings.



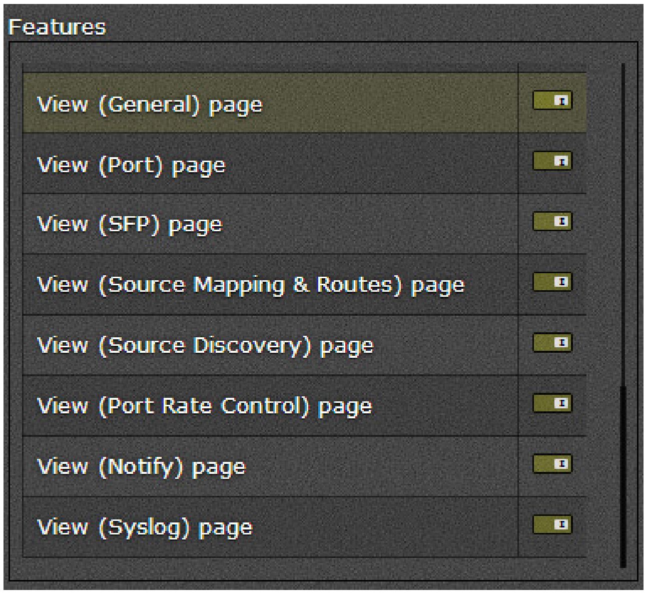
Features

Other

Event Log	☑
Upgrade	☑
Parameter Write	☑
Advanced Control	☐
Info/Logging	☑

Figure 4-13 : Settings / Users / Modify User (2) / Other

- **Other**
  - *Event Log:* Whether user can display the event log.
  - *Upgrade:* Whether user can perform firmware upgrades
  - *Parameter Write:* Whether the user can change the value of controls
  - *Advanced Control:* Whether the user can get access to Advanced-Control parameters.
  - *Info/Logging:* Whether the user can access Mini-agent or Card Info/Logging.



Features

View (General) page

View (Port) page

View (SFP) page

View (Source Mapping & Routes) page

View (Source Discovery) page

View (Port Rate Control) page

View (Notify) page

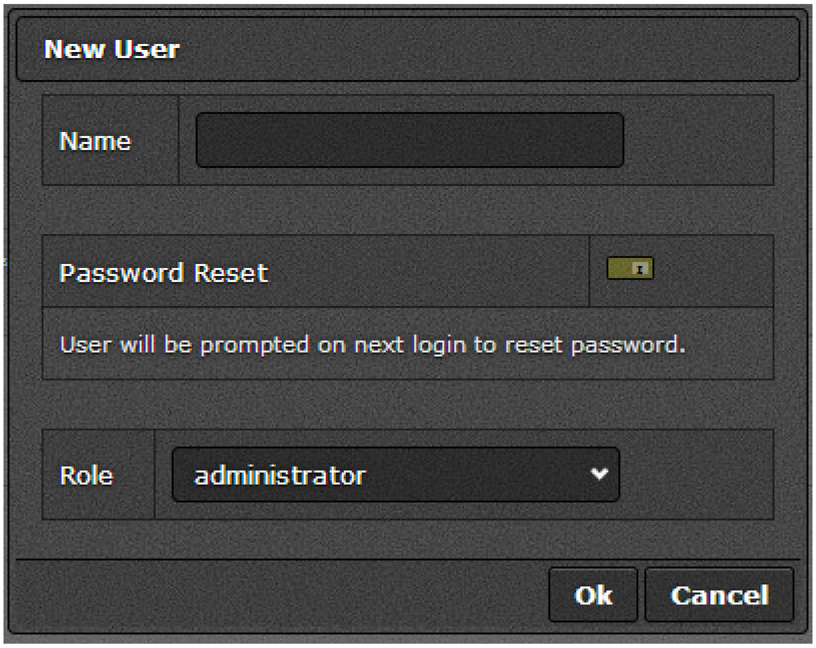
View (Syslog) page

Figure 4-14 : Settings / Users / Modify User (2) / Page

- **Page:** These options all determine if the user has permission to view the page listed within the brackets.
  - *View (System) page*
  - *View (General) page*
  - *View (Port) page*
  - *View (SFP) page*
  - *View (Source Mapping & Routes) page*
  - *View (Source Discovery) page*
  - *View (Port Rate Control) page:*
  - *View (Notify) page*
  - *View (Syslog) page*

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

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. The only accounts that should be established are Security Administrator accounts. CO/Administrators are identified and authenticated via username and password prior to performing any operations other than acknowledging the warning banner. The IPX CO/Administrators user accounts module maintains Security Administrator credentials. Since the only role that accesses the IPX directly is that of Security Administrator there is no assignment of roles required.



New User

Name

Password Reset

User will be prompted on next login to reset password.

Role: administrator

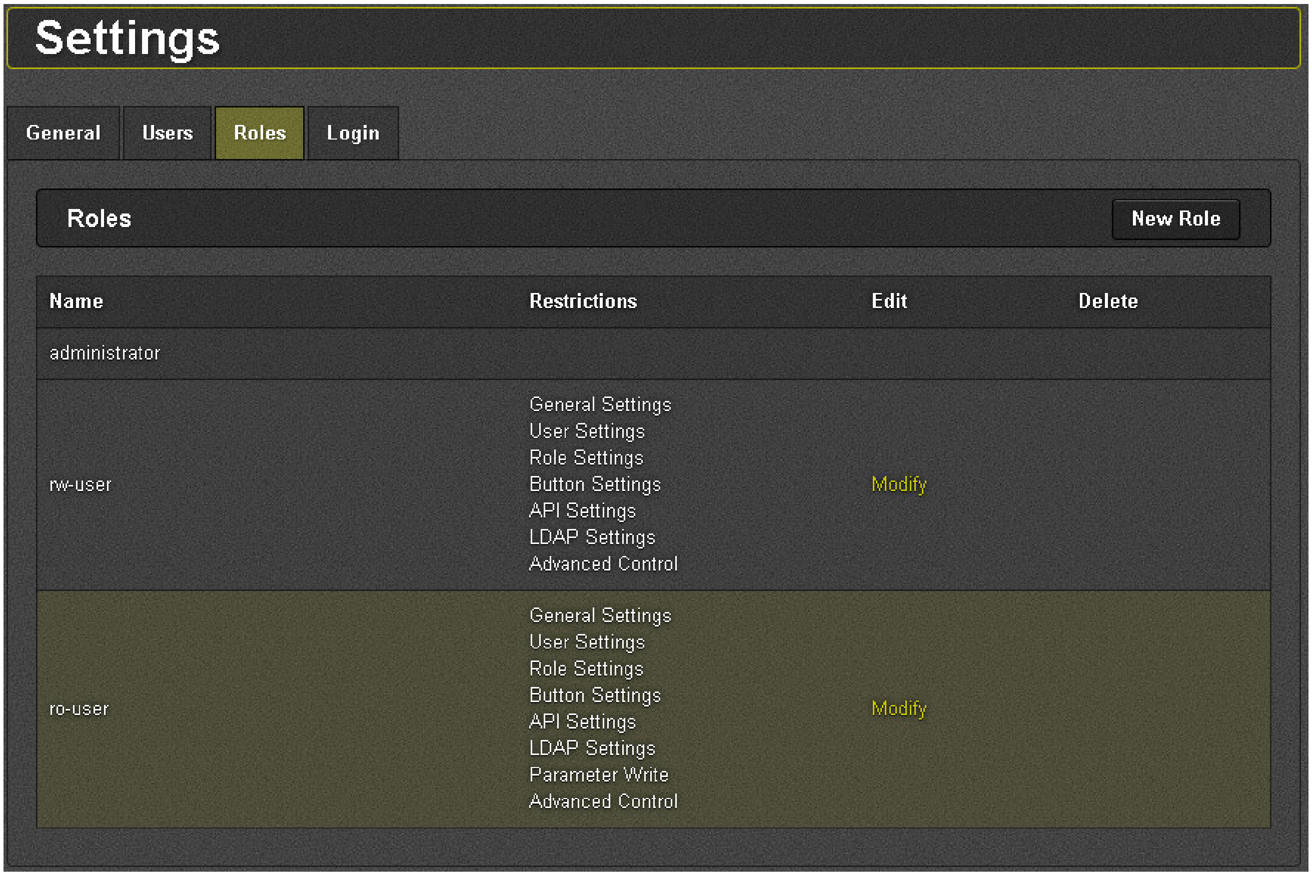
Figure 4-15 : WebEASY® - Settings / Users / New User

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.

4.3.4.3. 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, canot 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.



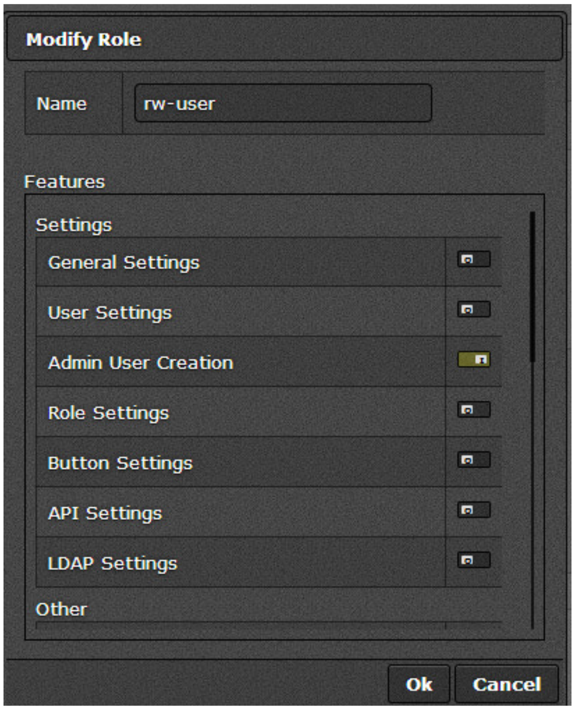
Name	Restrictions	Edit	Delete
administrator			
rw-user	General Settings User Settings Role Settings Button Settings API Settings LDAP Settings Advanced Control	Modify	
ro-user	General Settings User Settings Role Settings Button Settings API Settings LDAP Settings Parameter Write Advanced Control	Modify	

Figure 4-16 : WebEASY® - Settings / Roles

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

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

Edit: The *modify* button is used to enable or disable restrictions given to each role.



Modify Role

Name: rw-user

Features

Settings

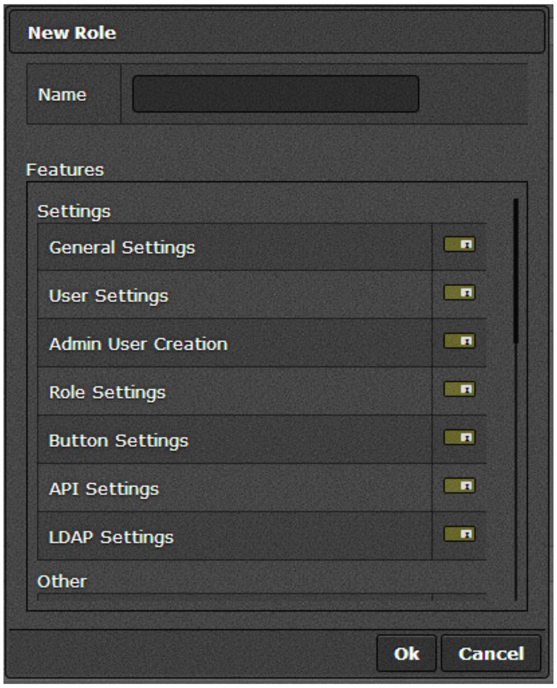
General Settings	☐
User Settings	☐
Admin User Creation	☑
Role Settings	☐
Button Settings	☐
API Settings	☐
LDAP Settings	☐

Other

Figure 4-17 : WebEASY® - Settings / Roles / Modify Role

Delete: This button allows the user to delete any created roles. The default roles can not be selected for deletion.

New Role: This control is used for creating new role. A name is given to that new role and restrictions are selected. The new roles can then be given to the users.



New Role

Name:

Features

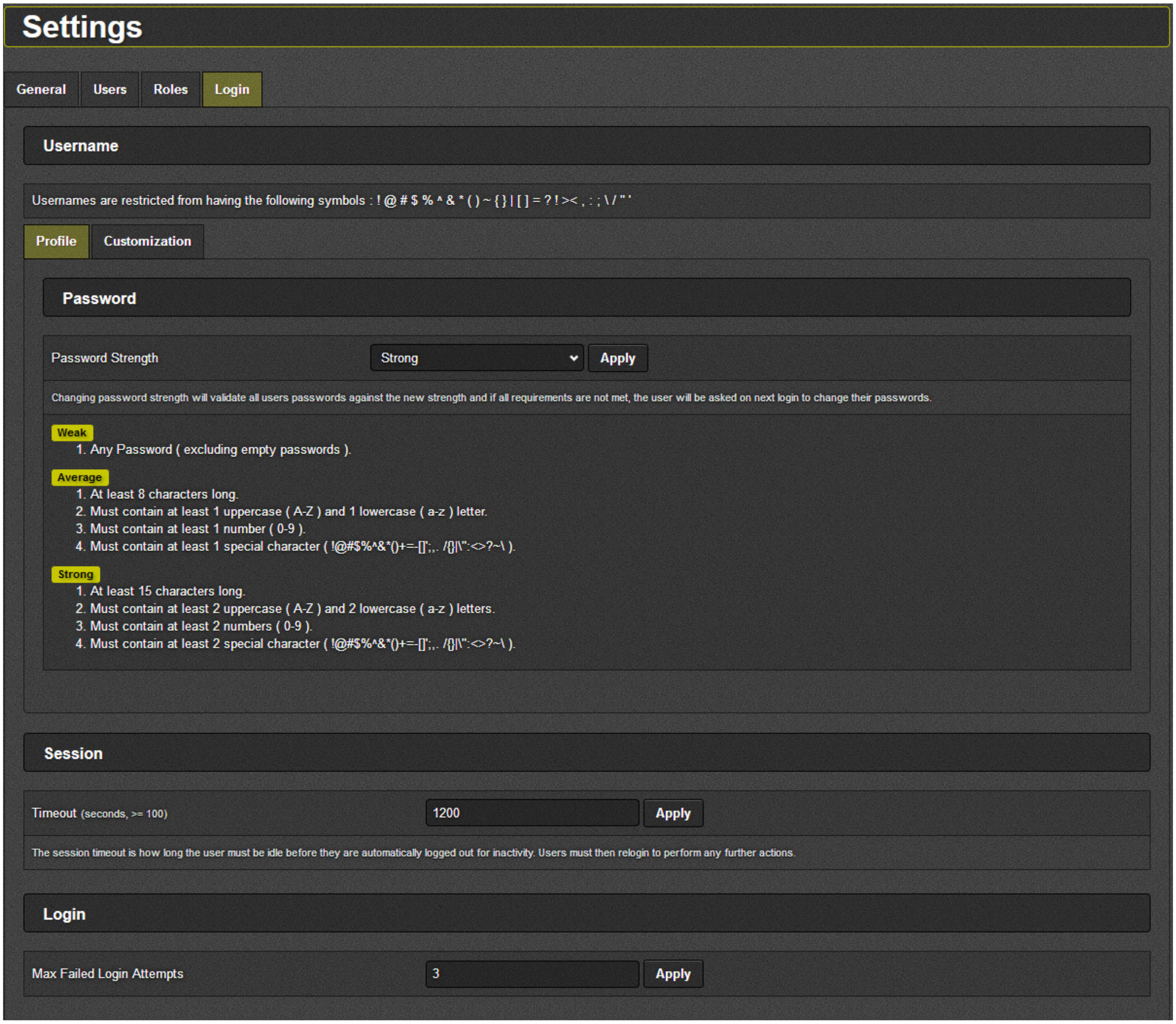
Settings

General Settings	☑
User Settings	☑
Admin User Creation	☑
Role Settings	☑
Button Settings	☑
API Settings	☑
LDAP Settings	☑

Other

Figure 4-18 : WebEASY® - Settings / Roles / New Role

4.3.4.4. Login



Username

Usernames are restricted from having the following symbols : ! @ # $ % ^ & * ( ) ~ { } | [ ] = ? ! >< , : ; \ / " '

Password

Password Strength: Strong

Changing password strength will validate all users passwords against the new strength and if all requirements are not met, the user will be asked on next login to change their passwords.

Weak

1. Any Password (excluding empty passwords).

Average

1. At least 8 characters long.
2. Must contain at least 1 uppercase (A-Z) and 1 lowercase (a-z) letter.
3. Must contain at least 1 number (0-9).
4. Must contain at least 1 special character (!@#$%^&*()+=-[]';,. /{}|\":<>?~\ ).

Strong

1. At least 15 characters long.
2. Must contain at least 2 uppercase (A-Z) and 2 lowercase (a-z) letters.
3. Must contain at least 2 numbers (0-9).
4. Must contain at least 2 special character (!@#$%^&*()+=-[]';,. /{}|\":<>?~\ ).

Session

Timeout (seconds, >= 100): 1200

The session timeout is how long the user must be idle before they are automatically logged out for inactivity. Users must then relogin to perform any further actions.

Login

Max Failed Login Attempts: 3

Figure 4-19 : WebEASY® - User Settings / Login

<u>Profile</u>

Password Strength: This drop down menu allows the user to define the strength level of the passwords. An explanation is given below the menu item.

<u>Session</u>

Timeout: This field allows the user to specify the amount of idle time, in seconds, of inactivity before the system logs out automatically. A re-login will be required if system times out.

<u>Login</u>

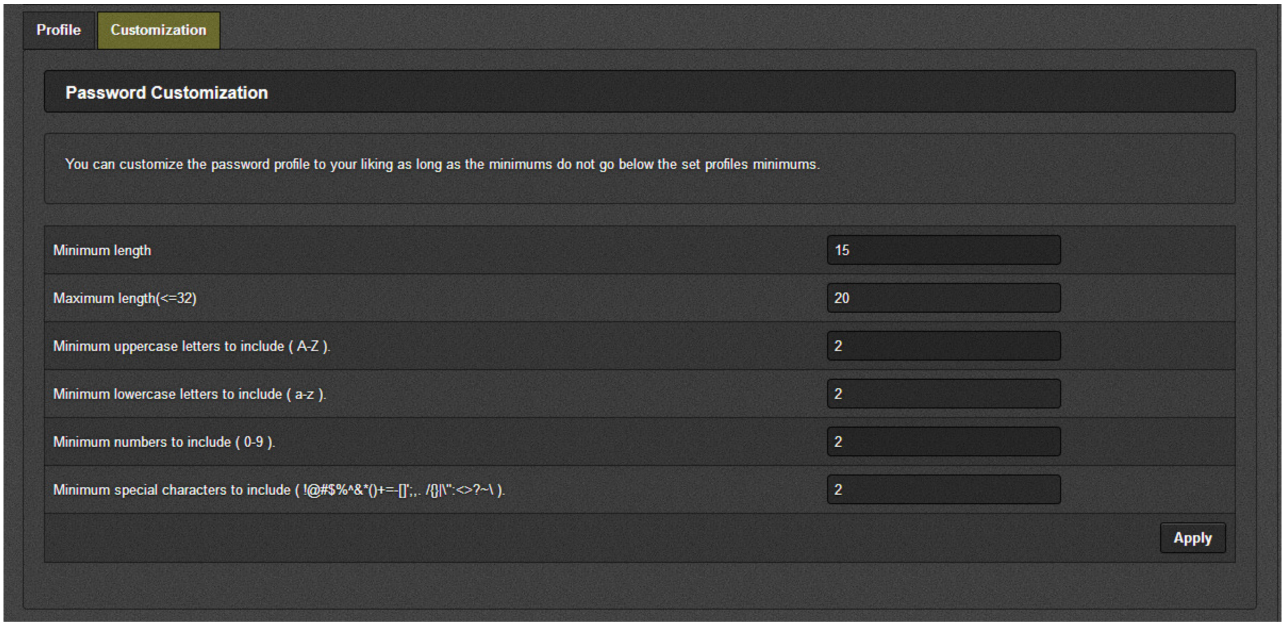
Max Failed Login Attempts: This field sets the maximum number of incorrect logins that are allowed before a user is locked out. The user is locked out for 12 hours or until an Administrator unlocks the user.

Customization:

Password Customization: Password customization allows administrators to customize the password profile to their liking, with options for specific password requirements.

In the evaluated configuration, passwords must be set to:

- **Minimum length**: 15
- **Maximum length:** 20
- **Minimum uppercase letters to include (A-Z)**: any number greater than 0
- **Minimum lowercase letters to include (a-z)**: any number greater than 0
- **Minimum numbers to include (0-9)**: any number greater than 0
- **Minimum special characters to include (!@#$%^&*()_-+=[]{}**\/**”,,.<>?)**: any number greater than 0



Password Customization

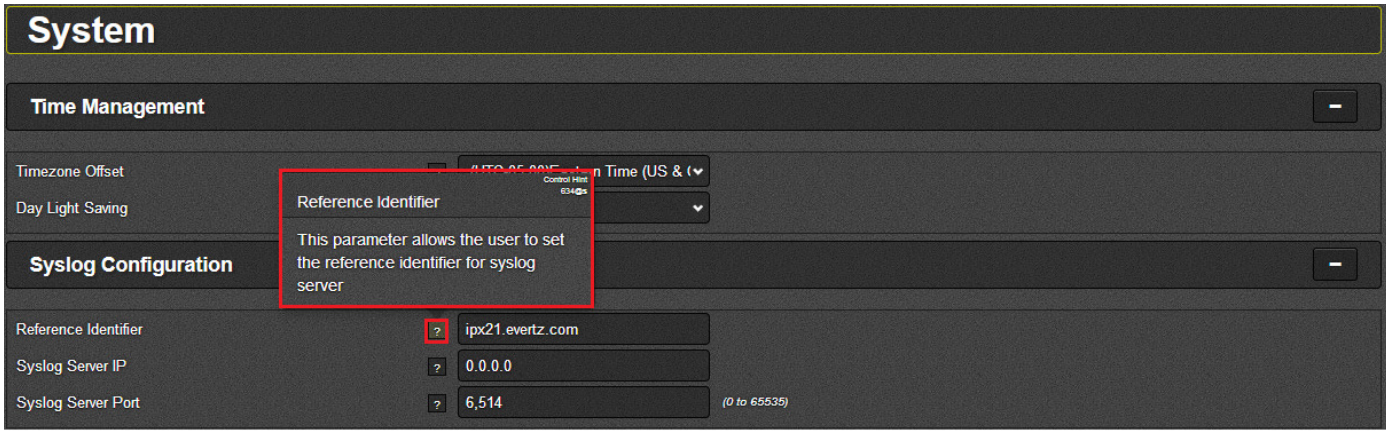
You can customize the password profile to your liking as long as the minimums do not go below the set profiles minimums.

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

Figure 4-20: WebEASY® - Settings / Login / Customization

4.3.5. Question Mark Button (?)

By clicking the Question Mark button from the bottom menu, the “?” sign will appear beside each field and provides information about the functionality of each field when the mouse button is scrolled over the question marks.



Timezone Offset (UTC-05:00)Eastern Time (US & (

Day Light Saving

Reference Identifier

This parameter allows the user to set the reference identifier for syslog server

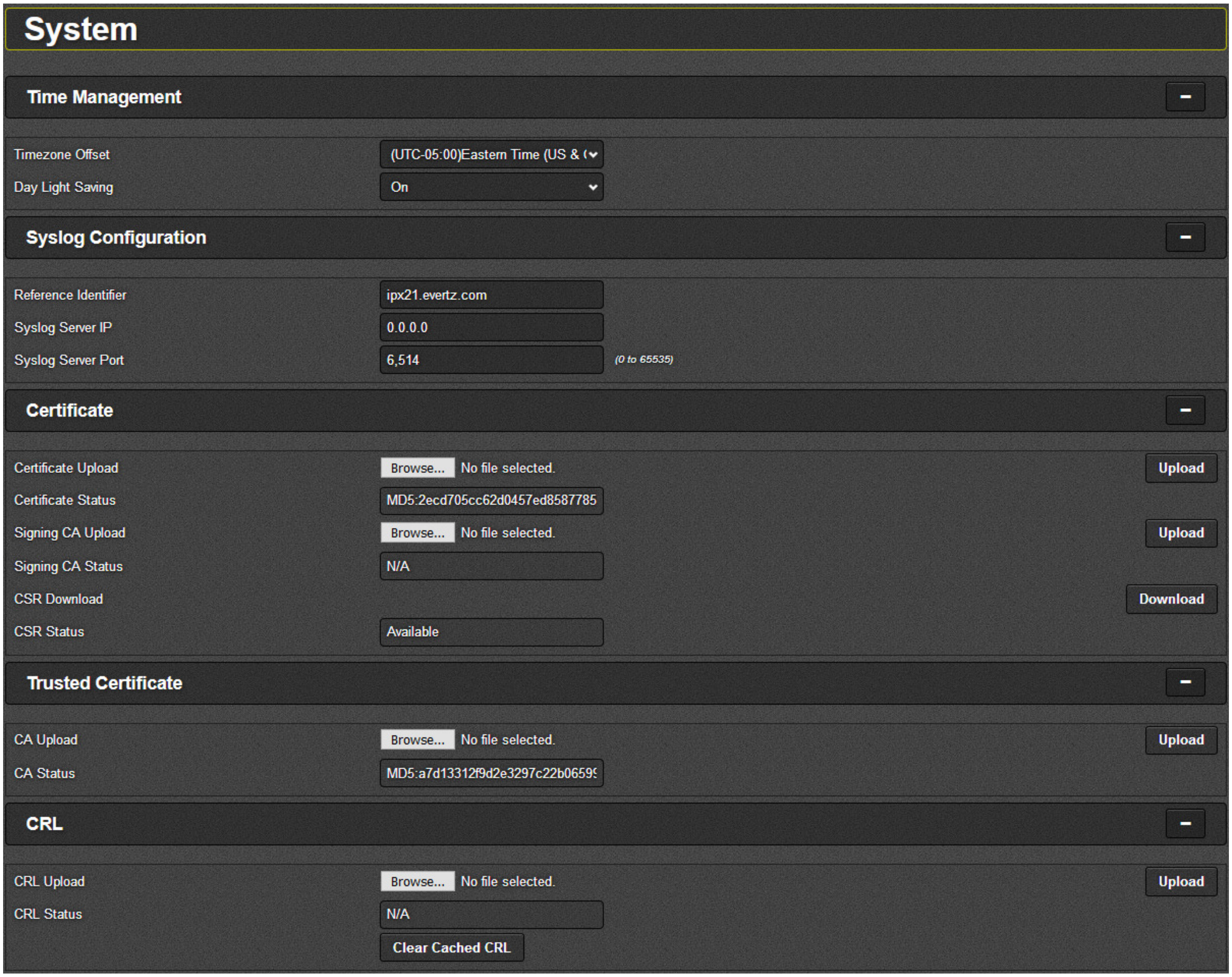
Reference Identifier ? ipx21.evertz.com

Syslog Server IP ? 0.0.0.0

Syslog Server Port ? 6,514 *(0 to 65535)*

Figure 4-21 : WebEASY® - Question Button Feature Illustration

4.4. SYSTEM TAB



System

Time Management

Timezone Offset	(UTC-05:00)Eastern Time (US & (
Day Light Saving	On

Syslog Configuration

Reference Identifier	ipx21.evertz.com	
Syslog Server IP	0.0.0.0	
Syslog Server Port	6,514	(0 to 65535)

Certificate

Certificate Upload	No file selected.
Certificate Status	MD5:2ecd705cc62d0457ed8587785
Signing CA Upload	No file selected.
Signing CA Status	N/A
CSR Download	
CSR Status	Available

Trusted Certificate

CA Upload	No file selected.
CA Status	MD5:a7d13312f9d2e3297c22b0659

CRL

CRL Upload	No file selected.
CRL Status	N/A

Figure 4-22 : WebEASY® - System Tab (part 1)

Time Management

Timezone Offset (-12 to 14): This control allows the user to set the timezone offset in hours.

Day Light Saving: This control allows the user to On/Off day light saving possibility.

Syslog Configuration

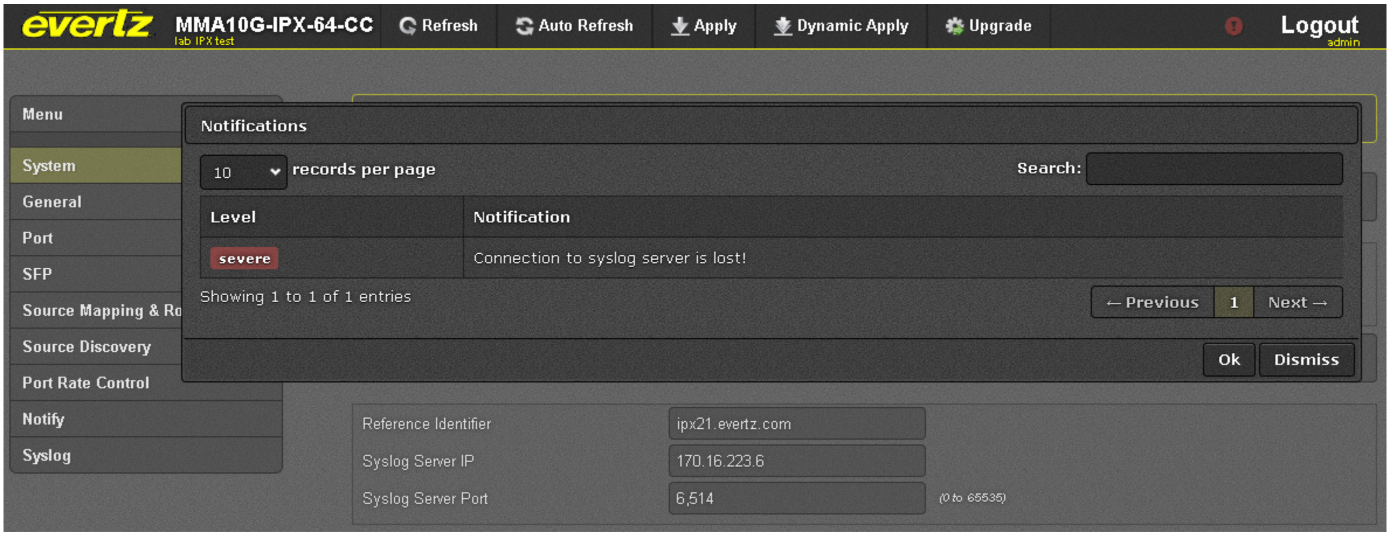
Reference Identifier: Allows the user to set the reference identifier for the syslog server. IPX allows configuration of reference identifier from a peer it expects to connect with before connection is made. The reference identifier can be any string up to 64 bytes that is present in the peer certificate’s DN/SAN field. The verification against DN/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.

Syslog Server IP: This field allows the user to define external syslog server IP address.

Syslog Server Port: This field allows the user to define external syslog server port address.

The connection to the Sylog server will be made using TLS.

There is a flashing icon on the top right of screen when the connection to syslog server is lost, either syslog server is down or there’s no physical connection between IPX and syslog server. By clicking on the flashing icon, a Notification page will appear as is shown in Figure 4-23. If the connection to the syslog server is lost, IPX will attempt to reestablish the connection. If the connection cannot be reestablished, the Security Administrator shall reset the reference ID and click Apply.



Notifications

10 records per page Search:

Level	Notification
severe	Connection to syslog server is lost!

Showing 1 to 1 of 1 entries

Reference Identifier	ipx21.evertz.com	
Syslog Server IP	170.16.223.6	
Syslog Server Port	6,514	(0 to 65535)

Figure 4-23 : WebEASY® - Syslog Server Lost Notification

Certificate

Certificate Upload: This field allows the user to load a certificate file. A certificate chain must include Root CA, Intermediate CA, and end-entity certificate.

Certificate Status: This field shows current certificate status.

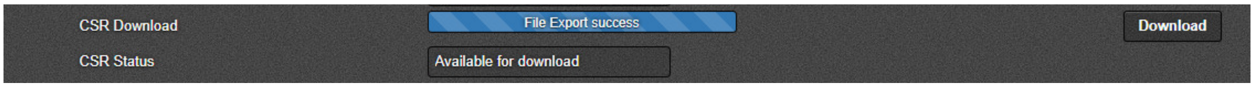
Signing CA Upload: This field allows the user to load a signing CA file.

Signing CA Status: This field shows the current signing CA status.

CSR Download: This field allows the user to download a CSR file.

To download the CSR file, you have the option to either:

#1 Generate CSR via serial menu interface (refer to section 3.3.2)#2 Download the newly generated CSR from Web interface



CSR Download	File Export success
CSR Status	Available for download

CSR Status: This field shows the current CSR status.

Trusted Certificate

CA Upload: This field allows the user to upload the signing CA and client certificates that have been signed by same CA will be trusted by TOE. The changes are reflected after the device is rebooted.

CA Status: This field shows the current CA status.

CRL

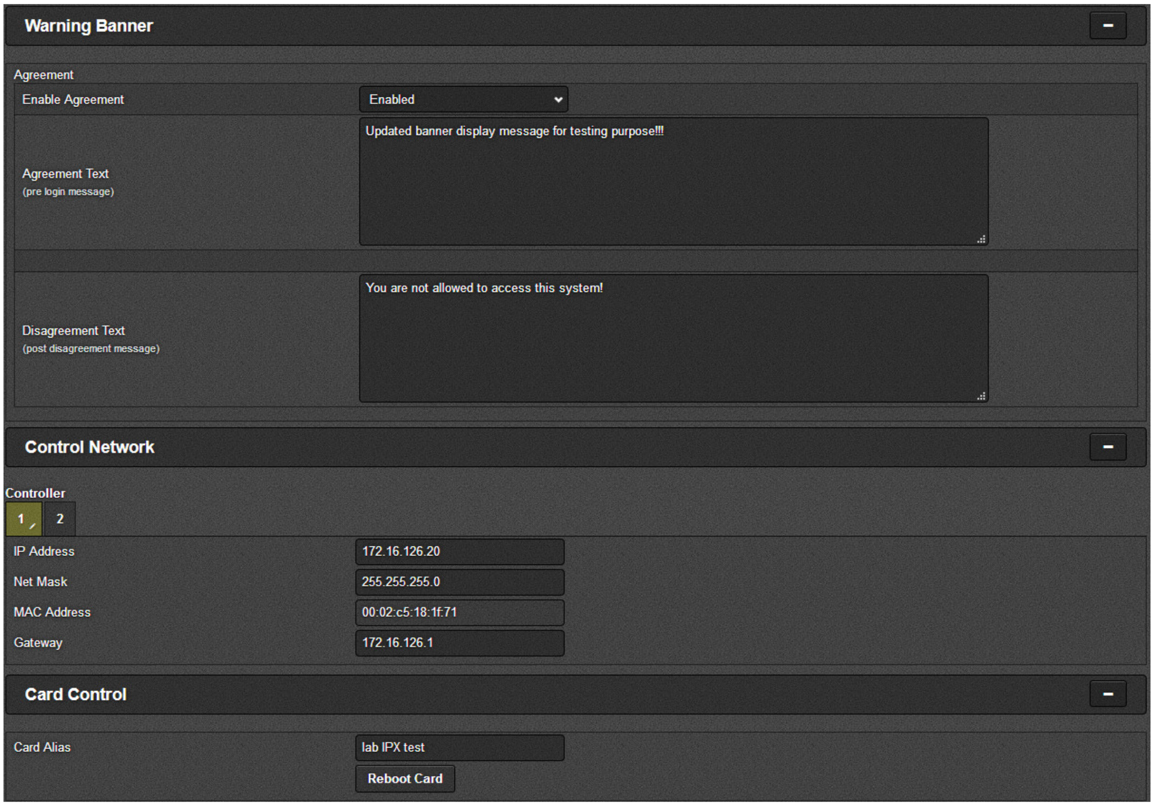
CRL Upload: This field allows the user to upload a CRL file. The CRL can fail to be validated by the TOE if the CRL that is being uploaded is not signed by the currently uploaded (signing) CA.

CRL Status: This field shows the current CRL status.

Clear Cached CRL: This button will clear CRL files stored in the cache.

Note on Communication with MAGNUM

IPX can be controlled by MAGNUM. The connection between IPX server and MAGNUM client is done with TLS. Mutual authentication is enforced. To enable this connection the CA for the MAGNUM certificate must be loaded onto IPX as described above. The uploaded CA and CRL certificates on IPX are used to verify against MAGNUM's certificate. CRL can be either uploaded to IPX or downloaded with the CRL distribution point extension in certificate.



Warning Banner

Agreement

Enable Agreement	Enabled
Agreement Text (pre login message)	Updated banner display message for testing purpose!!!
Disagreement Text (post disagreement message)	You are not allowed to access this system!

Control Network

Controller

1 2

IP Address	172.16.126.20
Net Mask	255.255.255.0
MAC Address	00:02:c5:18:1f:71
Gateway	172.16.126.1

Card Control

Card Alias	lab IPX test

Figure 4-24 : WebEASY® - System Tab (Part 2)

Warning banner

Enable Agreement: This dropdown allows the user to enable/disable the warning banner to be displayed.

Agreement Text (pre login message): This text window allows the user to write a message agreement for the warning banner. The warning banner is placed at beginning when accessing the module. The user will need to agree to these terms.

Disagreement Text: Upon a disagreement to the warning banner, this text window allows the user to write a message to be displayed when a disagreement is made.

Control Network

This panel displays the settings of both of the control Ethernet interfaces of the IPX.

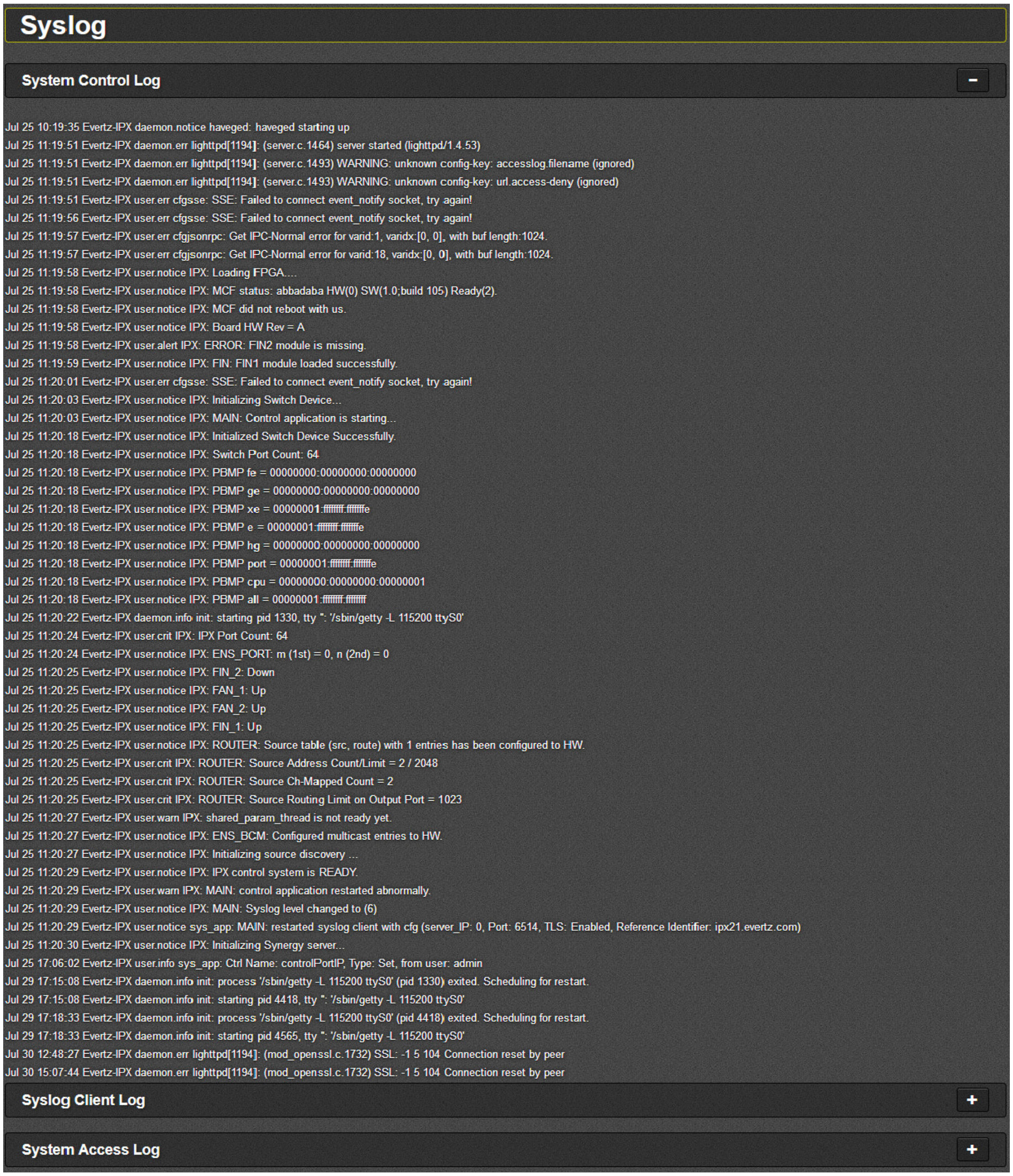
IP Address: This field is used to display the IP address for the IPX controller.

Net Mask: This monitor is used to display the subnet mask associated with the controller IP address.

MAC Address: This monitor is used to display the MAC address of the controller.

Gateway: This monitor is used to display the gateway address for the control network.

4.5. SYSLOG TAB



```
Jul 25 10:19:35 Evertz-IPX daemon.notice haveged: haveged starting up
Jul 25 11:19:51 Evertz-IPX daemon.err lighttpd[1194]: (server.c.1464) server started (lighttpd/1.4.53)
Jul 25 11:19:51 Evertz-IPX daemon.err lighttpd[1194]: (server.c.1493) WARNING: unknown config-key: accesslog.filename (ignored)
Jul 25 11:19:51 Evertz-IPX daemon.err lighttpd[1194]: (server.c.1493) WARNING: unknown config-key: url.access-deny (ignored)
Jul 25 11:19:51 Evertz-IPX user.err cfgsse: SSE: Failed to connect event_notify socket, try again!
Jul 25 11:19:56 Evertz-IPX user.err cfgsse: SSE: Failed to connect event_notify socket, try again!
Jul 25 11:19:57 Evertz-IPX user.err cfgjsonrpc: Get IPC-Normal error for varid:1, varidx:[0, 0], with buf length:1024.
Jul 25 11:19:57 Evertz-IPX user.err cfgjsonrpc: Get IPC-Normal error for varid:18, varidx:[0, 0], with buf length:1024.
Jul 25 11:19:58 Evertz-IPX user.notice IPX: Loading FPGA....
Jul 25 11:19:58 Evertz-IPX user.notice IPX: MCF status: abbadaba HW(0) SW(1.0;build 105) Ready(2).
Jul 25 11:19:58 Evertz-IPX user.notice IPX: MCF did not reboot with us.
Jul 25 11:19:58 Evertz-IPX user.notice IPX: Board HW Rev = A
Jul 25 11:19:58 Evertz-IPX user.alert IPX: ERROR: FIN2 module is missing.
Jul 25 11:19:59 Evertz-IPX user.notice IPX: FIN: FIN1 module loaded successfully.
Jul 25 11:20:01 Evertz-IPX user.err cfgsse: SSE: Failed to connect event_notify socket, try again!
Jul 25 11:20:03 Evertz-IPX user.notice IPX: Initializing Switch Device...
Jul 25 11:20:03 Evertz-IPX user.notice IPX: MAIN: Control application is starting...
Jul 25 11:20:18 Evertz-IPX user.notice IPX: Initialized Switch Device Successfully.
Jul 25 11:20:18 Evertz-IPX user.notice IPX: Switch Port Count: 64
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP fe = 00000000:00000000:00000000
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP ge = 00000000:00000000:00000000
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP xe = 00000001:ffffffff:fffffffe
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP e = 00000001:ffffffff:fffffffe
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP hg = 00000000:00000000:00000000
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP port = 00000001:ffffffff:fffffffe
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP cpu = 00000000:00000000:00000001
Jul 25 11:20:18 Evertz-IPX user.notice IPX: PBMP all = 00000001:ffffffff:ffffffff
Jul 25 11:20:22 Evertz-IPX daemon.info init: starting pid 1330, tty '': '/sbin/getty -L 115200 ttyS0'
Jul 25 11:20:24 Evertz-IPX user.crit IPX: IPX Port Count: 64
Jul 25 11:20:24 Evertz-IPX user.notice IPX: ENS_PORT: m (1st) = 0, n (2nd) = 0
Jul 25 11:20:25 Evertz-IPX user.notice IPX: FIN_2: Down
Jul 25 11:20:25 Evertz-IPX user.notice IPX: FAN_1: Up
Jul 25 11:20:25 Evertz-IPX user.notice IPX: FAN_2: Up
Jul 25 11:20:25 Evertz-IPX user.notice IPX: FIN_1: Up
Jul 25 11:20:25 Evertz-IPX user.notice IPX: ROUTER: Source table (src, route) with 1 entries has been configured to HW.
Jul 25 11:20:25 Evertz-IPX user.crit IPX: ROUTER: Source Address Count/Limit = 2 / 2048
Jul 25 11:20:25 Evertz-IPX user.crit IPX: ROUTER: Source Ch-Mapped Count = 2
Jul 25 11:20:25 Evertz-IPX user.crit IPX: ROUTER: Source Routing Limit on Output Port = 1023
Jul 25 11:20:27 Evertz-IPX user.warn IPX: shared_param_thread is not ready yet.
Jul 25 11:20:27 Evertz-IPX user.notice IPX: ENS_BCM: Configured multicast entries to HW.
Jul 25 11:20:27 Evertz-IPX user.notice IPX: Initializing source discovery ...
Jul 25 11:20:29 Evertz-IPX user.notice IPX: IPX control system is READY.
Jul 25 11:20:29 Evertz-IPX user.warn IPX: MAIN: control application restarted abnormally.
Jul 25 11:20:29 Evertz-IPX user.notice IPX: MAIN: Syslog level changed to (6)
Jul 25 11:20:29 Evertz-IPX user.notice sys_app: MAIN: restarted syslog client with cfg (server_IP: 0, Port: 6514, TLS: Enabled, Reference Identifier: ipx21.evertz.com)
Jul 25 11:20:30 Evertz-IPX user.notice IPX: Initializing Synergy server...
Jul 25 17:06:02 Evertz-IPX user.info sys_app: Ctrl Name: controlPortIP, Type: Set, from user: admin
Jul 29 17:15:08 Evertz-IPX daemon.info init: process '/sbin/getty -L 115200 ttyS0' (pid 1330) exited. Scheduling for restart.
Jul 29 17:15:08 Evertz-IPX daemon.info init: starting pid 4418, tty '': '/sbin/getty -L 115200 ttyS0'
Jul 29 17:18:33 Evertz-IPX daemon.info init: process '/sbin/getty -L 115200 ttyS0' (pid 4418) exited. Scheduling for restart.
Jul 29 17:18:33 Evertz-IPX daemon.info init: starting pid 4565, tty '': '/sbin/getty -L 115200 ttyS0'
Jul 30 12:48:27 Evertz-IPX daemon.err lighttpd[1194]: (mod_openssl.c.1732) SSL: -1 5 104 Connection reset by peer
Jul 30 15:07:44 Evertz-IPX daemon.err lighttpd[1194]: (mod_openssl.c.1732) SSL: -1 5 104 Connection reset by peer
```

Figure 4-25 : WebEASY® – Syslog Panel

This section displays a log of System Control access System Client access and System access.

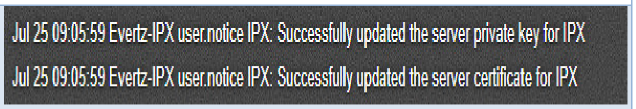
IPX generates audit logs that consist of various auditable events or actions. This includes logins, use of trusted channel/path and cryptographic operations. Each audit event contains an associated date/time stamp, a label for the type of event, a user ID (if applicable) and a description of the event. See Table 4 : Auditable Eventsbelow for the complete list of auditable events.

IPX stores audit logs internally. The internal logs are stored unencrypted, but in a location where only the CO/Administrator can access them. Logs information is also sent (encrypted) to an external Syslog server simultaneously, assuming one is connected and configured.

Table 4 : Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FAU_GEN.1	None	None	NA
FAU_GEN.2	None	None	NA
FAU_STG_EXT.1	None	None	NA
FCS_CKM.1	None	None	NA
FCS_CKM.2	None	None	NA
FCS_CKM.4	None	None	NA
FCS_COP.1/ DataEncryption	None	None	NA
FCS_COP.1/SigGen	None.	None	NA
FCS_COP.1/Hash	None	None	NA
FCS_COP.1/ KeyedHash	None	None	NA
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure	Evertz-IPX authpriv.warn WebEasy: User admin (192.168.100.10) authentication failure.
FCS_RBG_EXT.1	None	None	NA
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	Jul 24 15:14:32 Evertz-IPX user.warn syslog Certificate subject does not match configured hostname; hostname='acumensec.local', certificate='*.acumensec.local' Jul 24 15:14:37 Evertz-IPX user.warn syslog Syslog connection failed; fd='18', server='AF_INET(192.168.100.208:6514)', error='Connection refused (111)', time_reopen='5'
FCS_TLSS_EXT.2	Failure to establish a TLS Session	Reason for failure	Jul 23 13:07:24 Evertz-IPX user.err IPX: SYNERGY: TLS handshaking failed for client [192.168.100.208!
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address)	Jul 23 17:03:04 Evertz-IPX authpriv.warn WebEasy: User acumenadmin (192.168.100.201) authentication failure. Jul 23 17:03:04 Evertz-IPX authpriv.info WebEasy: User acumenadmin has been locked out because of reaching the authentication maximum attempts!
FIA_PMG_EXT.1	None	None	NA

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	***Local*** Jul 23 10:03:03 Evertz-IPX authpriv.notice login[1371]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=ttyS0 ruser= rhost= user=customer Jul 23 10:03:06 Evertz-IPX auth.warn login[1371]: pam_authenticate call failed: Authentication failure (7) Jul 23 10:03:25 Evertz-IPX authpriv.info login[1371]: pam_unix(login:session): session opened for user customer by LOGIN(uid=0) ***Remote*** Jul 23 14:10:59 Evertz-IPX authpriv.warn WebEasy: User admin (192.168.100.10) authentication failure. Jul 23 14:11:14 Evertz-IPX authpriv.info WebEasy: User admin (192.168.100.10) login.
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	***Local*** Jul 23 10:03:03 Evertz-IPX authpriv.notice login[1371]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=ttyS0 ruser= rhost= user=customer Jul 23 10:03:06 Evertz-IPX auth.warn login[1371]: pam_authenticate call failed: Authentication failure (7) Jul 23 10:03:25 Evertz-IPX authpriv.info login[1371]: pam_unix(login:session): session opened for user customer by LOGIN(uid=0) ***Remote*** Jul 23 14:10:59 Evertz-IPX authpriv.warn WebEasy: User admin (192.168.100.10) authentication failure. Jul 23 14:11:14 Evertz-IPX authpriv.info WebEasy: User admin (192.168.100.10) login.
FIA_UAU.7	None.	None.	NA

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FIA_X509_EXT.1/ Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation. Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	Jul 25 09:25:26 Evertz-IPX user.warn IPX: Invalid CA certificate
FIA_X509_EXT.2	None	None	NA
FIA_X509_EXT.3	None	None	NA
FMT_MOF.1/ Functions	None	None	NA
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None	Jul 24 16:08:34 Evertz-IPX authpriv.info root: Firmware was upgraded to ver: 3.2 build 83 from ver: 3.2 build 82
FMT_MTD.1/ CoreData	None	None	NA
FMT_MTD.1/ CryptoKeys	Management of cryptographic keys.	None	 Jul 25 09:05:59 Evertz-IPX user.notice IPX: Successfully updated the server private key for IPX Jul 25 09:05:59 Evertz-IPX user.notice IPX: Successfully updated the server certificate for IPX
FMT_SMF.1	All management activities of TSF data.	None	See audit events
FMT_SMR.2	None.	None	NA
FPT_SKP_EXT.1	None.	None	NA
FPT_APW_EXT.1	None.	None	NA
FPT_TST_EXT.1	None.	None	NA
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None	Jul 24 16:08:34 Evertz-IPX authpriv.info root: Firmware was upgraded to ver: 3.2 build 83 from ver: 3.2 build 82

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	***Remote*** Jul 22 15:55:17 Evertz-IPX user.info sys_app: Ctrl Name: TimezoneOffset, Type: Set, from user: admin Jul 22 16:55:17 Evertz-IPX user.notice sys_app: Time zone has changed! ***Local*** Jul 22 17:00:21 Evertz-IPX user.info sys_app: Ctrl Name: setDate, Type: Set, from user: customer Jul 22 16:22:00 Evertz-IPX user.notice IPX: Date changed to Mon Jul 22 16:22:00 GMT+4 2019 from Mon Jul 22 17:00:21 GMT+4 2019 manually from serial menu.
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.	Jul 22 15:36:15 Evertz-IPX authpriv.info login[4319]: pam_unix(login:session): session opened for user customer by LOGIN(uid=0) Jul 22 15:37:16 Evertz-IPX authpriv.info login[4319]: pam_unix(login:session): session closed for user customer
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	Jul 22 14:57:37 Evertz-IPX authpriv.info WebEasy: User admin (192.168.100.10) logout because of session timeout.
FTA_SSL.4	The termination of an interactive session.	None.	Jul 22 15:25:17 Evertz-IPX authpriv.info login[1346]: pam_unix(login:session): session opened for user customer by LOGIN(uid=0) Jul 22 15:25:46 Evertz-IPX authpriv.info login[1346]: pam_unix(login:session): session closed for user customer
FTA_TAB.1	None.	None.	NA

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	***Initiation*** Jul 23 16:34:56 Evertz-IPX user.warn syslog Syslog connection established; fd='16', server='AF_INET(192.168.100.201:6514)', local='AF_INET(0.0.0.0:0)' ***Termination*** Jul 23 16:35:43 Evertz-IPX user.warn syslog Syslog connection broken; fd='16', server='AF_INET(192.168.100.201:6514)', time_reopen='5' Jul 23 16:35:48 Evertz-IPX user.warn syslog Syslog connection failed; fd='16', server='AF_INET(192.168.100.201:6514)', error='Connection refused (111)', time_reopen='5' ***Failure*** Jul 23 16:35:43 Evertz-IPX user.warn syslog Syslog connection broken; fd='16', server='AF_INET(192.168.100.201:6514)', time_reopen='5' Jul 23 16:35:48 Evertz-IPX user.warn syslog Syslog connection failed; fd='16', server='AF_INET(192.168.100.201:6514)', error='Connection refused (111)', time_reopen='5'
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None	***Initiation*** Jul 24 09:19:59 Evertz-IPX authpriv.info WebEasy: User admin (192.168.100.10) login ***Termination*** Jul 24 09:19:31 Evertz-IPX authpriv.info WebEasy: User admin (192.168.100.10) logout. ***Failure*** Jul 24 09:19:41 Evertz-IPX authpriv.warn WebEasy: User admin (192.168.100.10) authentication failure.

5. FIRMWARE UPGRADE

The site administrators do not have access to install any applications on the TOE. The IPX embedded system can only be updated with the valid firmware release from Evertz. Operators may verify the current version with WebEasy interface.

The current firmware version is displayed on both webpage and in serial console menu.

Firmware updates are done from the IPX webpage interface under “upgrade”. During a firmware upgrade, IPX will first verify the HMAC of new firmware code with a local stored public key. No interface is provided to change the locally stored public key to administrators. When HMAC verification passes, IPX will verify the firmware binary header with an Evertz-defined proprietary format. If there is no mismatch, the new firmware code will overwrite the current one.

A verification of the firmware’s digital signature is performed next. A hashed-value of the images is generated and then signed with Evertz’s private key. The result file (signature) is included in the firmware package together with the actual firmware binary. During upgrade, the signature file is first decrypted using the public key stored on IPX, then the hashed value is re-calculated from the uploaded image binary file and then compared with the decrypted hash value. These hashes must match for this validation to succeed.

From time to time, firmware upgrades are needed to add or update features such as the graphical user interface.

NOTE: When upgrading process is done, IPX will reboot automatically. Having a backup system is highly recommended to minimize disruption time. Upgrading does not change the system settings or configurations.

On the top of the web page for the IPX modules, there is a tab labelled Upgrade. The Upgrade tab is used to check current firmware version and upload the latest firmware.

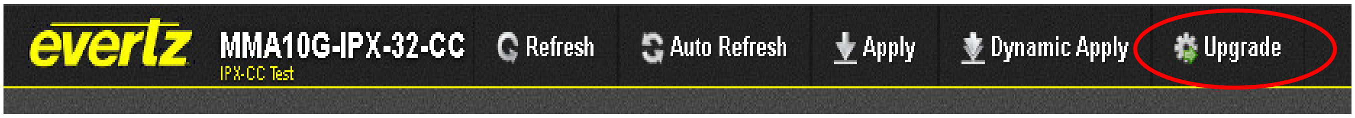
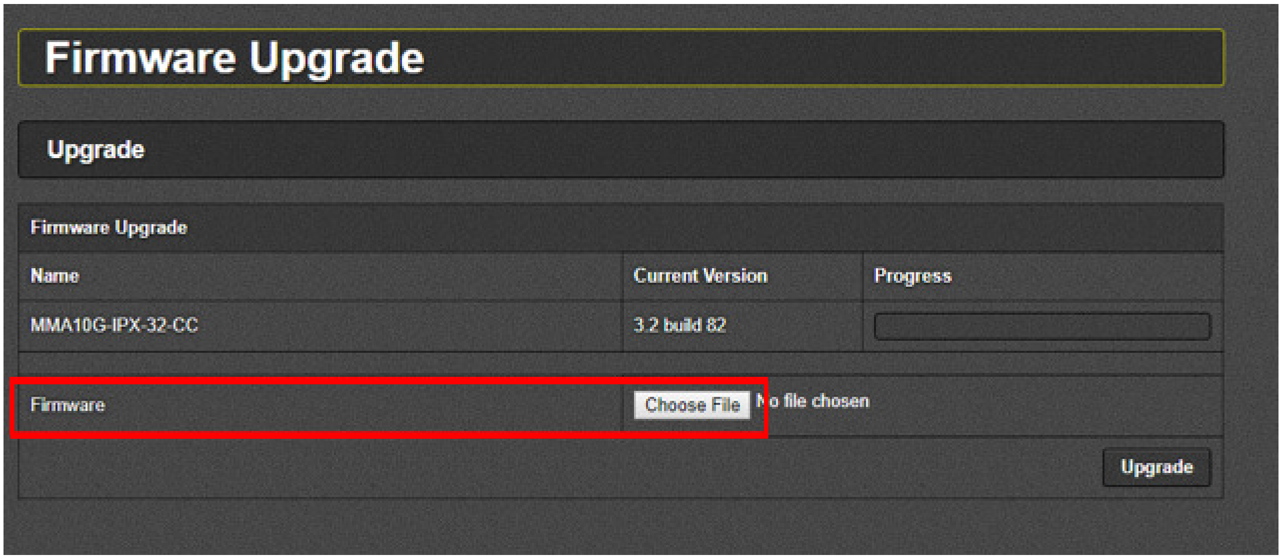


Figure 5-1 : WebEASY® – Upgrade Button on Top Menu Bar

Selecting the Upgrade tab, will take the user to Figure 5-2 where the current firmware version is shown. Should the firmware version be outdated, the user first needs to obtain a valid firmware image released from Evertz and then proceed with installing the firmware image on IPX. Contact Evertz service department for latest firmware image. Evertz service department will provide a fireware link for the customer to download the new image.



Firmware Upgrade

Upgrade

Firmware Upgrade

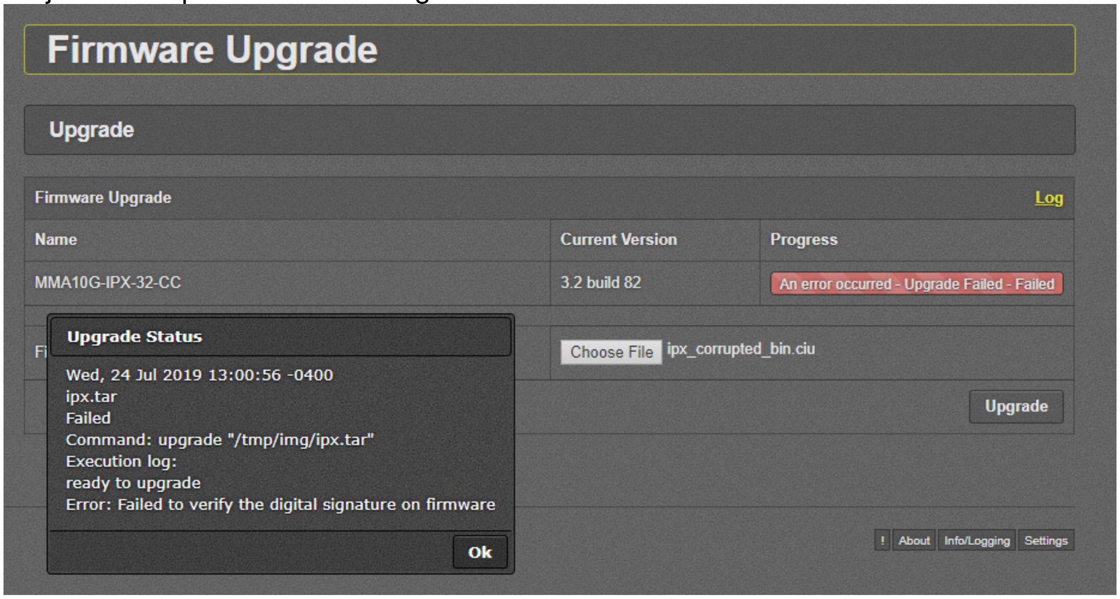
Name	Current Version	Progress
MMA10G-IPX-32-CC	3.2 build 82	

Firmware: Choose File No file chosen

Figure 5-2 : WebEASY® – Firmware Upgrade Menu

Click choose file and browse to locate image file. Once selected, click open to advance to next step. Click upgrade and watch progress bar for status. Once completed, the device will automatically restart. The IPX will reject all bad firmware images. Bad firmware images include firmware images that could be #1 corrupted, #2 missing digital signature and #3 invalid digital signature. After the failed image upgrade the IPX firmware version remains the same as previous firmware version. For instance, if the original IPX firmware version is 3.2 Build 82, then after a failed firmware upgrade attempt the IPX retains firmware version 3.2 Build 82.
If IPX rejects a corrupted firmware image, the following events will occur:

1) IPX rejects corrupted firmware image:



Firmware Upgrade

Upgrade

Firmware Upgrade

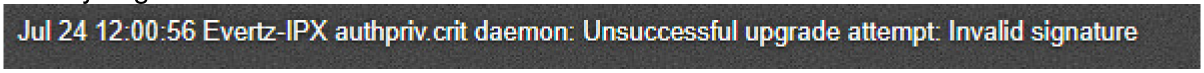
Name	Current Version	Progress
MMA10G-IPX-32-CC	3.2 build 82	An error occurred - Upgrade Failed - Failed

Choose File ipx_corrupted_bin.ciu

Upgrade Status

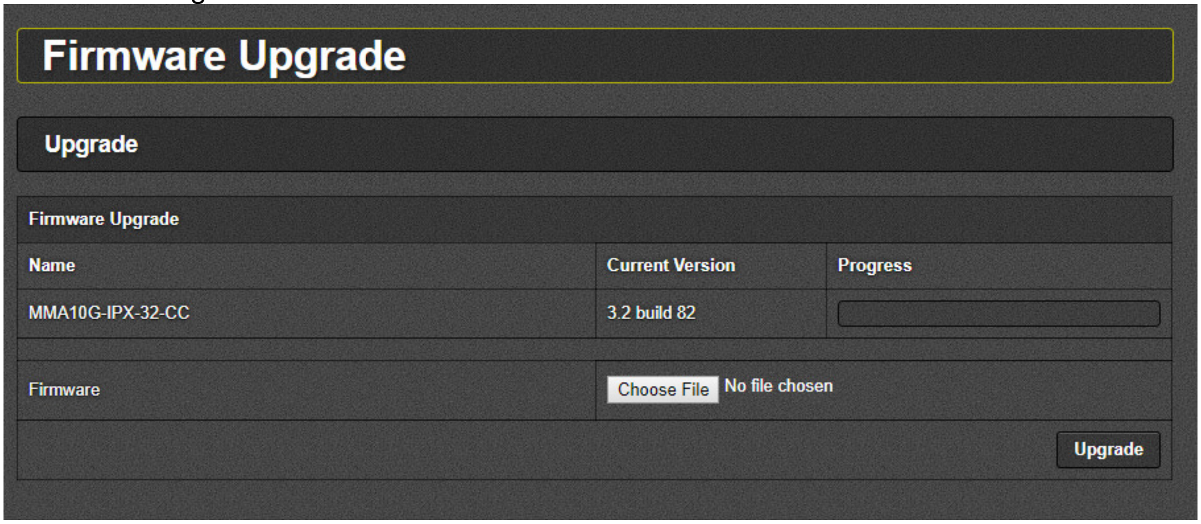
```
Wed, 24 Jul 2019 13:00:56 -0400
ipx.tar
Failed
Command: upgrade "/tmp/img/ipx.tar"
Execution log:
ready to upgrade
Error: Failed to verify the digital signature on firmware
```

2) IPX Syslog:



```
Jul 24 12:00:56 Evertz-IPX authpriv.crit daemon: Unsuccessful upgrade attempt: Invalid signature
```

3) IPX retains original firmware version:

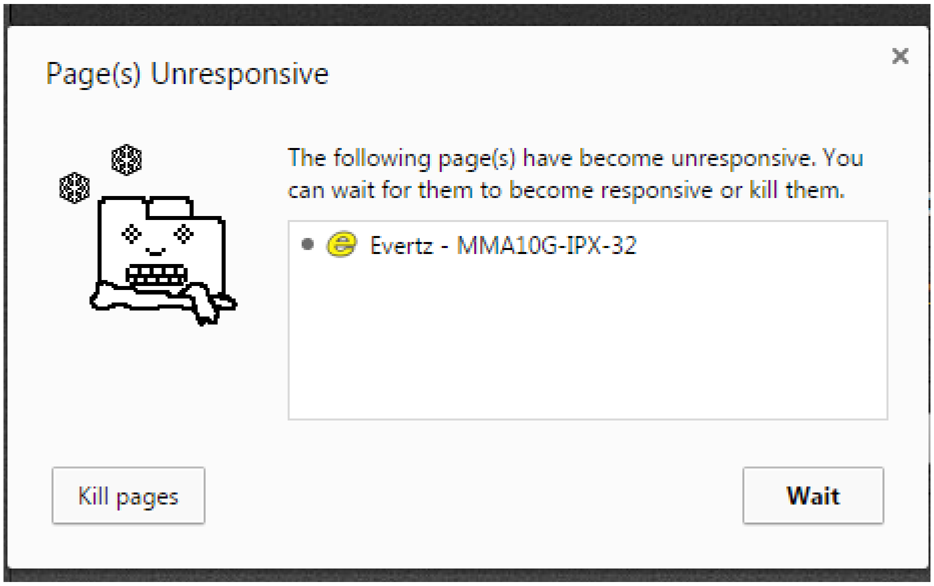


Firmware Upgrade

Upgrade

Firmware Upgrade		
Name	Current Version	Progress
MMA10G-IPX-32-CC	3.2 build 82	
Firmware	Choose File No file chosen	

The download time required will be dependent on the speed of the Internet connection or LAN connection. During that time, the web browser could time out. Should a message pop up that page is unresponsive, click Wait.



Page(s) Unresponsive

The following page(s) have become unresponsive. You can wait for them to become responsive or kill them.

- Evertz - MMA10G-IPX-32

Figure 5-3 : WebEASY® - Firmware Upgrade Menu – Web Browser Time Out Message Prompt

Once the firmware download has been completed, the unit will reboot automatically and user will be returned to the Login prompt.