Raritan EMX

User Guide
Release 2.1.0

Copyright © 2012 Raritan, Inc.

EMX-0C-v2.1-E

March 2012

255-80-6107-00

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2012 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

Contents

Chapter 1 Introduction 1

Overview 2
Product Models 3
EMX2-111 3
EMX2-888 3
Product Features 4
Package Contents 5

Chapter 2 Installing and Configuring the EMX Device 6

Before You Begin 6
Mounting the EMX Device 6
Mounting a Zero U EMX Device 7
Mounting a 1U EMX Device 8
Connecting the EMX to a Power Source 10
Configuring the EMX 10
Connecting the EMX to a Computer 11
Installing the USB-to-Serial Driver 11
Connecting the EMX to Your Network 13
Initial Network Configuration 14
Combining Asset Sensors 20
Connecting Asset Sensors to the EMX 22
Connecting AMS-M2-Z Asset Sensors (Optional) 24
Connecting Blade Extension Strips 25
Connecting Environmental Sensors (Optional) 29
About Contact Closure Sensors 31
Connecting Third-Party Detectors/Switches 31
Contact Closure Sensor LEDs 35
Connecting Differential Air Pressure Sensors 36
Connecting a Logitech Webcam (Optional) 37
Connecting a Schroff LHX Heat Exchanger (Optional) 37

Chapter 3 Getting Started 39

Supported Web Browsers 39
Connection Ports 39
LCD Display Panel 40
LCD Display 41
Control Buttons 43

Reset Button 46
Contact Closure Sensor Termination 46
Power Switch 46
Logging In 47
Logout 48
Changing Your Password 49
Introduction to the Web Interface 50
Menus 51
Setup Button 51
Status Bar 51
Add Page Icon 52
Data Pane 53
Warning Icon 53
Readings Highlighted in Yellow or Red 54
Browser-Defined Shortcut Menu 56
Viewing the Dashboard 57

Chapter 4 User and Role Management 58

Overview 58
Managing Users 58
Creating a User Profile 58
Modifying a User Profile 62
Deleting a User Profile 62
Changing the User List View 63
Viewing Connected Users 63
Managing Roles 64
Setting Up Roles 64
Creating a Role 64
Modifying a Role 65
Deleting a Role 66

Chapter 5 EMX Device Management 67

Overview 67
Naming the EMX Device 67
Displaying the Device Information 68
Setting the Date and Time 68
Specifying the Device Altitude 69
Changing the Measurement Units 70
Determining How to Display Tree Items 71
How to Display Asset Sensors 71
How to Display LHX Heat Exchangers 72
Modifying the Network Configuration 73
Modifying the Network Interface Settings 73
Modifying the Network Settings 75
Modifying the Network Service Settings 79
Changing the HTTP(S) Settings 79
Configuring the SNMP Settings 80
Changing the SSH Settings 80

Changing the Telnet Settings 81
Enabling Service Advertisement 81
Configuring the SMTP Settings 82
Setting Up an EMX Using Bulk Configuration 83
Saving an EMX Configuration 84
Copying a EMX Configuration 85
Firmware Upgrade 85
Updating the Firmware 86
Viewing Firmware Update History 87
Full Disaster Recovery 87
Updating the Asset Sensor Firmware 88
Network Diagnostics 88
Pinging a Host 88
Tracing the Network Route 89
Listing TCP Connections 89
Downloading Diagnostic Information 89
Rebooting the EMX 91
Resetting to Factory Defaults 91

Chapter 6 Security 93

Access Security Control 93
Forcing HTTPS Encryption 93
Configuring the Firewall 94
Setting Up User Login Controls 99
Setting Up Role-Based Access Control Rules 102
Setting Up an SSL Certificate 107
Certificate Signing Request 107
Creating a Self-Signed Certificate 109
Installing Existing Key and Certificate Files 110
Downloading Key and Certificate Files 111
Setting Up LDAP Authentication 112
Gathering the LDAP Information 112
Adding the LDAP Server Settings 113
Sorting the LDAP Access Order 115
Testing the LDAP Server Connection 116
Editing the LDAP Server Settings 116
Deleting the LDAP Server Settings 116
Disabling the LDAP Authentication 117
Enabling LDAP and Local Authentication Services 117

Chapter 7 Event Rules, Event Actions and Application Logs 118

Event Rules and Actions 118
Components of an Event Rule 118
Creating an Event Rule 119
Sample Event Rules 134
Modifying an Event Rule 136
Modifying an Action 137
Deleting an Event Rule or Action 138

A Note about Untriggered Rules 138
Event Logging 138
Viewing the Local Event Log 139
Clearing Event Entries 139
Viewing the Communication Log 140

Chapter 8 Managing External Devices 141

Overview 141
Server Accessibility 141
Adding IT Devices for Ping Monitoring 141
Editing Ping Monitoring Settings 142
Deleting Ping Monitoring Settings 143
Checking Server Monitoring States 143
Environmental Sensors 144
Identifying Environmental Sensors 144
Managing Environmental Sensors 145
Configuring Environmental Sensors 147
Setting Data Logging 150
Viewing Sensor Data 151
Unmanaging Environmental Sensors 155
Threshold Information 156
What is Deassertion Hysteresis? 156
What is Assertion Timeout? 157
Asset Sensors and Tags 157
Configuring the Asset Sensor 158
Changing a Specific LED's Color Settings 160
Connecting AMS-M2-Z Asset Sensors (Optional) 161
Expanding a Blade Extension Strip 163
Connecting Blade Extension Strips 164
Webcams 168
Configuring Webcams 168
Viewing Webcam Snapshots and Videos 170
Taking, Viewing and Managing Webcam Snapshots 171
Sending Videos in an Email or Instant Message 173
GSM Modems 174
Schroff LHX Heat Exchangers 175
Enabling and Disabling Schroff LHX Heat Exchanger Support 175
Naming a Heat Exchanger 176
Configuring Temperature and Fan Thresholds 177
Monitoring the Heat Exchanger 177
Controlling the Heat Exchanger 180

Chapter 9 Using SNMP 182

Enabling SNMP 182
Configuring Users for Encrypted SNMP v3 183
Configuring SNMP Traps 184
SNMP Gets and Sets 185
The EMX MIB 185

Chapter 10 Using the Command Line Interface 188

About the Interface 188
Logging in to CLI 188
- With HyperTerminal 189
- With SSH or Telnet 190
- Different CLI Modes and Prompts 191
- Closing a Serial Connection 191

Help Command 191
Showing Information 192
- Network Configuration 192
- Asset Sensor Settings 195
- Environmental Sensor Information 196
- Environmental Sensor Information 197
- Environmental Sensor Threshold Information 198
- Security Settings 199
- Existing User Profiles 199
- Existing Roles 200
- Rack Unit Settings of an Asset Sensor 201
- Blade Extension Strip Settings 202
- Command History 202
- History Buffer Length 203
- Examples 203

Configuring the EMX Device and Network 204
- Entering the Configuration Mode 204
- Device Configuration Commands 205
- Networking Configuration Commands 207
- Security Configuration Commands 231
- Environmental Sensor Configuration Commands 253
- Environmental Sensor Threshold Configuration Commands 257
- User Configuration Commands 263
- Role Configuration Commands 277
- Asset Management Commands 281
- Setting the History Buffer Length 289
- Multi-Command Syntax 289
- Quitting the Configuration Mode 290

Unblocking a User 290
Resetting the EMX 291
- Restarting the Device 291
- Resetting to Factory Defaults 291

Network Troubleshooting 292
- Entering the Diagnostic Mode 292
- Diagnostic Commands 292
- Quitting the Diagnostic Mode 295

Querying Available Parameters for a Command 295
Retrieving Previous Commands 295
Automatically Completing a Command 296
Logging out of CLI 296
Resetting to Factory Defaults (CLI) 296

Appendix A Dominion PX Asset Management 298

Overview 298

Appendix B Specifications 300

Altitude Correction Factors (EMX) 300
Maximum Ambient Operating Temperature (EMX) 300
Serial RS-232 Port Pinouts 301
Sensor RJ-12 Port Pinouts 301
RS-485 Port Pinouts 301

Appendix C LDAP Configuration Illustration 303

Step A. Determine User Accounts and Groups 303
Step B. Configure User Groups on the AD Server 304
Step C. Configure LDAP Authentication on the EMX Device 305
Step D. Configure User Groups on the EMX Device 307

Index 311

Chapter 1 Introduction

In This Chapter

Overview....2
Product Models....3
Product Features....4
Package Contents....5

Overview

The EMX device provides a rack management solution that combines both asset management and environmental monitoring capabilities.

With asset management capability, you can remotely track the location of IT equipment after tagging the IT devices electronically. This feature is especially useful when there are hundreds of IT devices to administer.

The following items are required for setting up an asset management system:

- Raritan asset tags: You tag an IT device by sticking an electronic asset tag on it
- Raritan asset management sensors (asset sensors): Each asset sensor transmits the tag and position information to the EMX device
- An EMX device: You can remotely locate each tagged IT device through the EMX device.

With Raritan environmental sensors connected to the EMX device, you can remotely monitor environmental conditions such as temperature or humidity in the data center or server room.

With a Logitech® QuickCam® Pro 9000 webcam connected, a simple camera and video surveillance system is built, displaying the real-time snapshots or videos inside the server room or data center to enhance monitoring and security.

Events and actions that are triggered when an event occurs are supported by the EMX. Specifically, email messages, log events, syslog messages, webcam snapshots, SNMP traps and SMS messages can be triggered when the events you define occur. Custom messages can be configured for email messages, and images captured by the webcam can be sent to users via email.

In addition, the EMX device integrates with a Schroff® LHX-20 or LHX-40 heat exchanger, which draws warm air into the air/water heat exchanger to cool the air. This integration provides a solution for remotely monitoring the heat exchanger. EMX can also be used in conjunction with Raritan's data center management application, dcTrack™.

This user guide describes the following models:

- EMX2-111
- EMX2-888

Product Models

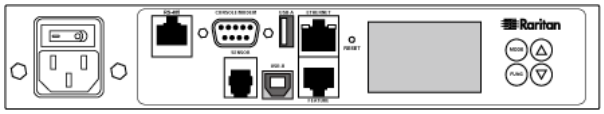
The EMX devices include two models: EMX2-111 and EMX2-888.

Different models are functionally identical, but vary in the size and total number of ports.

EMX2-111

EMX2-111 is a Zero U model with the following ports and components:

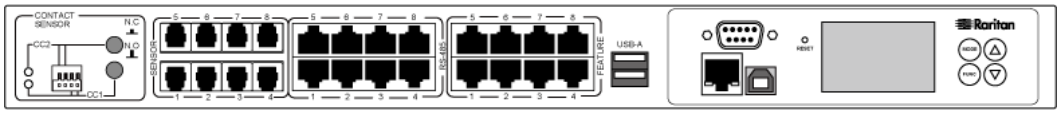
- 1 Sensor port
- 1 Feature port
- 1 RS-485 port
- 2 USB ports (1 USB-A and 1 USB-B)
- 1 RS-232 port
- 1 Ethernet port
- 1 LCD display
- Control buttons



EMX2-888

EMX2-888 is a 1U model with the following ports and components:

- 8 Sensor ports
- 8 Feature ports
- 8 RS-485 ports
- 3 USB ports (2 USB-A and 1 USB-B)
- 1 RS-232 port
- 1 Ethernet port
- 1 LCD display
- Control buttons
- Contact closure sensor termination



Product Features

In general, the EMX features include:

- The ability to remotely track the location of each IT equipment that is electronically tagged using Raritan asset tags
- LED color change on the asset sensor to distinguish between detected and undetected asset tags
- Support for a maximum of 10-meter cabling on the EMX-888 and 1-meter cabling for the EMX-111 for each connected asset sensor
- The ability to monitor environmental factors such as external temperature and humidity
- User-specified location attributes for environmental sensors
- The ability to display temperatures in Celsius or Fahrenheit, height in meters or feet, and pressure in Pascal or psi according to user credentials
- Support for a maximum of 130 environmental sensors for the EMX-888 and 16 for the EMX-111
- Support for cascading AMS devices and/or PX2 devices connected to the EMX
- Support for SNMP v1, v2, and v3
- The ability to send traps using the SNMP protocol
- The ability to configure and set values through SNMP
- Support for SSH and Telnet services
- For SSH, both of password and public key authentications are supported
- Service Advertisement support
- The ability to save one EMX device's configuration settings and then deploy those settings to other identical EMX devices
- Support for the tilt sensor implemented on the Raritan asset sensors
- Wireless connection via a Raritan-provided wireless USB LAN adapter
- The ability to visually monitor the data center environment through a connected Logitech® QuickCam® Pro 9000 webcam
- Support for webcam images sent via email to designated recipients
- Support of Cinterion® MC52i GSM modems, which allow you to send customized SMS messages to designated recipients for specific events
- The ability to send emails, log details, and/or set SNMP traps for specific events
- The ability to monitor a connected Schroff® LHX-20 or LHX-40 heat exchanger

- The ability to diagnose the network, such as pinging a host or listing TCP connections
- The ability to monitor sever accessibility
- Full disaster recovery option in case of a catastrophic failure during a firmware upgrade

Package Contents

The following describes the equipment shipped with an EMX device. If anything is missing or damaged, contact the local dealer or Raritan Technical Support for help.

- The EMX device
- Power cord
- Bracket pack and screws
- Asset sensors (optional)
- Asset tags (optional)

Chapter 2 Installing and Configuring the EMX Device

In This Chapter

Before You Begin 6
Mounting the EMX Device 6
Connecting the EMX to a Power Source 10
Configuring the EMX 10
Combining Asset Sensors 20
Connecting Asset Sensors to the EMX 22
Connecting AMS-M2-Z Asset Sensors (Optional) 24
Connecting Blade Extension Strips 25
Connecting Environmental Sensors (Optional) 29
Connecting Differential Air Pressure Sensors 36
Connecting a Logitech Webcam (Optional) 37
Connecting a Schroff LHX Heat Exchanger (Optional) 37

Before You Begin

Prepare the installation site. Make sure the installation area is clean and not exposed to extreme temperatures or humidity. Allow sufficient space around the EMX for cabling and asset sensor connections.

Mounting the EMX Device

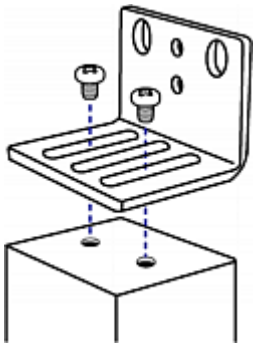
Depending on the model you purchased, the way to mount an EMX device varies.

Mounting a Zero U EMX Device

This section describes how to mount a Zero U EMX device using L-brackets and two buttons.

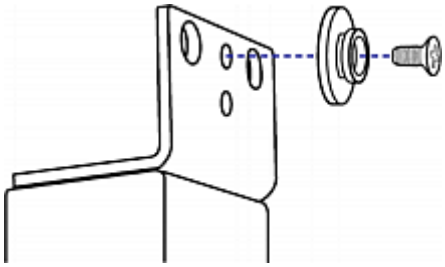
To mount Zero U models using L-brackets and two buttons:

1. Align the two edge slots of the L-bracket with the two screw holes on the top of the EMX device.
2. Screw the L-bracket to the device and ensure the bracket is fastened securely.



3. Repeat Steps 1 to 2 to screw another L-bracket to the bottom of the device.
4. After both L-brackets are installed on the device, you can choose either of the following ways to mount the device in the rack.
   - Using rack screws, fasten the device to the rack through two identical holes near the edge of each L-bracket.

- Mount the device by screwing a mounting button in the back center of each L-bracket and then having both buttons engage the mounting holes in the rack. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



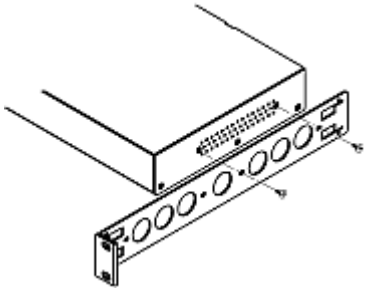
Mounting a 1U EMX Device

Using the appropriate brackets and tools, fasten the 1U EMX device to the rack or cabinet.

To mount the 1U EMX device:

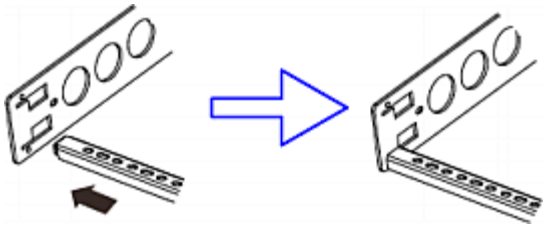
1. Attach one rackmount bracket to one side of the EMX device.
   a. Align two oval-shaped holes of the rackmount bracket with two threaded holes on one side of the EMX device.
   b. Secure the rackmount bracket with two of the Raritan-provided screws.

Note: The appropriate oval-shaped hole locations of the rackmount bracket may vary according to the threaded holes on you model.

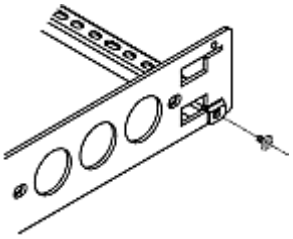


2. Repeat Step 1 for securing the other rackmount bracket to the other side of the EMX.

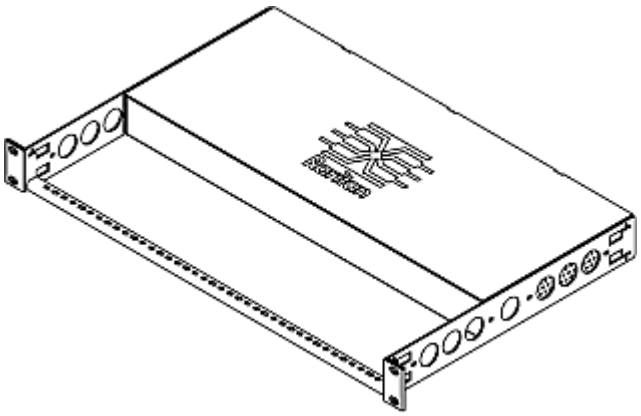
3. Insert one end of the cable-support bar into the L-shaped hole of the rackmount bracket, and align the hole on the end of the bar with the threaded hole adjacent to the L-shaped hole.



4. Secure the cable-support bar with one of the Raritan-provided cap screws.



5. Repeat Steps 3 to 4 to secure the other end of the cable-support bar to the other rackmount bracket.

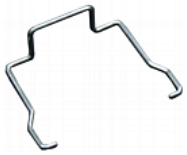


6. Mount the EMX device on the rack by securing the rackmount brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, or the like.

Connecting the EMX to a Power Source

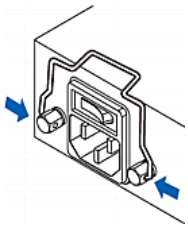
If your EMX device is designed to use a cable retention clip, install the clip before connecting a power cord. A cable retention clip prevents the connected power cord from coming loose or falling off.

The use of cable retention clips is highly recommended for regions with high seismic activities, and environments where shocks and vibrations are expected.

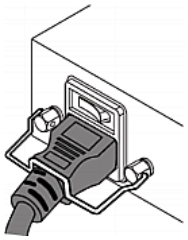


To connect the EMX device to a power source:

1. Install the cable retention clip by inserting both ends into the tiny holes on two hexagon screws adjacent to the power socket.



2. Plug one end of the Raritan-provided power cord into the power socket, and press the cable retention clip toward the power cord until it holds the cord firmly.



3. Connect the other end of the power cord to an appropriate power source.

Configuring the EMX

To configure the EMX device:

1. Connect the EMX device to a computer via a serial or USB connection.

2. Connect the EMX device to the network via a wired or wireless connection.
3. Configure the EMX device using the command line interface.

Connecting the EMX to a Computer

To configure the EMX using a computer, it must be connected to the computer with an RS-232 serial interface. The computer must have a communications program such as HyperTerminal or PuTTY.

If your computer does not have a serial port, use a regular USB cable to connect the EMX to the computer for initial configuration. The EMX device can emulate a USB-to-serial converter after the USB-to-serial driver is properly installed in the Windows® operating system.

Note: Not all serial-to-USB converters work properly with the EMX device so this section does not introduce the use of such converters.

Now connect the EMX to a computer for initial configuration by following either of the following procedures.

To make a serial connection:

1. Connect one end of the null-modem cable to the RS-232 port labeled CONSOLE / MODEM on the EMX.
2. Connect the other end of the null-modem cable to the serial port (COM) on the computer.

To make a USB connection:

1. Connect one end of a regular USB cable to the USB-B port on the EMX.
2. Connect the other end of the USB cable to the USB-A port on the computer.

Installing the USB-to-Serial Driver

The EMX can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion Serial Console" is required for Microsoft® Windows® operating systems. Download the *dominion-serial.zip* driver file, which contains *dominion-serial.inf* and *dominion-serial-setup.exe* files, from the ***Raritan website http://www.raritan.com*** under the ***Firmware and Documentation http://www.***, ***http://www.raritan.com/support/firmware-and-documentation/*** section for the EMX.

To install the driver in Windows® Vista and 7:

1. Disconnect the EMX's USB cable from the computer.

2. Run dominion-serial-setup.exe. A Dominion Serial Console Driver Setup Wizard appears.
3. Click Install to install the driver.
4. Click Finish when the installation is complete.
5. Connect the EMX's USB cable to the computer. The driver is automatically installed.

To install the driver in Windows® XP:

1. Disconnect the EMX's USB cable from the computer.
2. Check if the file "usbser.sys" is available in C:\Windows\ServicePackFiles\i386. If not, extract it from the Windows installation CD disc, and copy it to the same directory where the USB-to-serial driver is stored.
   - On a CD disc with SP3 included, it is extracted from I386\SP3.CAB.
   - On a CD disc with SP2 included, it is extracted from I386\SP2.CAB.
   - On a CD without an SP, it is extracted from I386\DRIVER.CAB.
3. Connect the EMX's USB cable to the computer.
4. The computer detects the new device and the "Found New Hardware Wizard" dialog appears. If this dialog does not appear, choose Control Panel > System > Hardware > Device Manager, right-click the Dominion Serial Console, and choose Update Driver.
5. Select "Install from a list or specific location," and specify the location where the driver is stored.
6. If you see the message requesting the file "usbser.sys," specify the location of the file.
7. The installation is complete.

In Linux:

No additional drivers are required, but you must provide the name of the tty device, which can be found in the output of the "dmesg" after connecting the EMX to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is "/dev/ttyACM0," perform the following commands:

> set line /dev/ttyACM0

> connect

Connecting the EMX to Your Network

To use the web interface to administer the EMX, you must connect the EMX to your local area network (LAN). The EMX can be connected to a wired or wireless network.

To make a wired connection:

1. Connect a standard Category 5e/6 UTP cable to the ETHERNET port on the EMX.
2. Connect the other end of the cable to your LAN.

To make a wireless connection:

Do one of the following:

- Plug a 802.11n wireless USB LAN adapter into the USB-A port on your EMX.
- Connect a USB docking station to the USB-A port on the EMX and plug the 802.11n wireless USB LAN adapter into the appropriate USB port on the docking station.

Supported Wireless LAN Configuration

If you select the wireless connection, ensure that both of your wireless USB LAN adapter and wireless network configuration meet the following requirements.

- Network type: 802.11n
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK
- Encryption: CCMP (AES)

Important: Currently only Raritan-provided wireless USB LAN adapters are supported. You may contact Raritan Technical Support for this information.

Initial Network Configuration

After the EMX device is connected to your network, you must provide it with an IP address and some additional networking information.

This section describes the initial configuration via a serial or USB connection. To configure the EMX via the LAN, see ***Modifying the Network Configuration (BCM, EMX, PX2, PXE)*** (see "***Modifying the Network Configuration***" on page 73).

To configure the EMX device:

1. Go to the computer that you connected to the EMX and open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and make sure the port settings are configured as follows:
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can find out which COM port is assigned to the EMX by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion Serial Console" under the Ports group.
3. Press Enter.
4. The EMX prompts you to log in. Note that both of user name and password are case sensitive.
   a. At the Username prompt, type `admin` and press Enter.
   b. At the Password prompt, type `raritan` and press Enter.
5. You are prompted to change the password if this is the first time you log in to the EMX. Follow the onscreen instructions to type your new password.
6. The # prompt appears when you log in successfully.
7. Type `config` and press Enter.
8. To configure network settings, type appropriate commands, and press Enter. All commands are case sensitive.
   a. To set the networking mode, type this command:

      ```
      network mode <mode>
      ```

      where <mode> is either *wired* for wired connection (default) or *wireless* for wireless connection.

b. For the wired network mode, you may configure the LAN interface settings. In most scenarios, the default setting (auto) works well and should not be changed unless required.

To set	Use this command
LAN interface speed	`network interface LANInterfaceSpeed <option>` where <option> is *auto*, *10Mbps*, or *100Mbps*.
LAN interface duplex mode	`network interface LANInterfaceDuplexMode <mode>` where <mode> is *half*, *full* or *auto*.

Tip: You can combine multiple commands to configure multiple parameters at a time. For example,
`network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>`

c. For the wireless network mode, you must configure the Service Set Identifier (SSID) parameter.

To set	Use this command
SSID	`network wireless SSID <ssid>` where <ssid> is the SSID string.

If necessary, configure more wireless parameters shown in the following table.

To set	Use this command
BSSID	`network wireless BSSID <bssid>` where <bssid> is the AP MAC address.
Authentication method	`network wireless authMethod <method>` where <method> is *psk* for Pre-Shared Key or *eap* for Extensible Authentication Protocol.

To set	Use this command
PSK	`network wireless PSK <psk>` where <psk> is the PSK string.
EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` where <outer_auth> is *PEAP*.
EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` where <inner_auth> is *MSCHAPv2*.
EAP identity	`network wireless eapIdentity <identity>` where <identity> is your user name for EAP authentication.
EAP password	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	`network wireless eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.

Note: The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE."

d. To determine which IP protocol is enabled and which IP address returned by the DNS server is used, configure the following parameters.

To set	Use this command
IP protocol	`network ip proto <protocol>` where <protocol> is *v4Only* for enabling IPv4, *v6Only* for enabling IPv6 or *both* for enabling both IPv4 and IPv6 protocols.

To set	Use this command
Which IP address returned by the DNS server is used	`network ip dnsResolverPreference <resolver>` where <resolver> is *preferV4* for IPv4 addresses or *preferV6* for IPv6 addresses.

e. If you enabled the IPv4 protocol in the previous step, configure the IPv4 network parameters.

To set	Use this command
IP configuration method	`network ipv4 ipConfigurationMode <mode>` where <mode> is either *dhcp* for auto configuration (default) or *static* for specifying a static IP address.

- For the IPv4 DHCP configuration, configure this parameter.

To set	Use this command
Preferred host name (optional)	`network ipv4 preferredHostName <name>` where <name> is the preferred host name.

Tip: To override the DHCP-assigned IPv4 DNS servers with those you specify manually, type this command:

`network ipv4 overrideDNS <option>`

where <option> is `enable` or `disable`. See the table below for the IPv4 commands for manually specifying DNS servers.

- For the static IPv4 configuration, configure these parameters.

To set	Use this command
Static IPv4 address	`network ipv4 ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Subnet mask	`network ipv4 subnetMask <netmask>` where <netmask> is the subnet mask.
Gateway	`network ipv4 gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network ipv4 primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network ipv4 secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

f. If you enabled IPv6 in the earlier step, configure the IPv6 network parameters.

To set	Use this command
IP configuration method	`network ipv6 ipConfigurationMode <mode>` where <mode> is either *automatic* for auto configuration (default) or *static* for specifying a static IP address.

Tip: To override the DHCP-assigned IPv6 DNS servers with those you specify manually, type this command:

`network ipv6 overrideDNS <option>`

where <option> is `enable` or `disable`. See the table below for the IPv6 commands for manually specifying DNS servers.

- For the static IPv6 configuration, you should configure the following parameters. Note that the IP address must follow the IPv6 format.

To set	Use this command
Static IPv6 address	`network ipv6 ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Gateway	`network ipv6 gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network ipv6 primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network ipv6 secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

9. To quit the configuration mode with or without saving the changes, type either command, and press Enter.

Command	Description
`apply`	Save all configuration changes and quit the configuration mode.
`cancel`	Abort all configuration changes and quit the configuration mode.

The # prompt appears, indicating that you have quit the configuration mode.

10. To verify whether all settings are correct, type the following commands one by one. Current network settings are displayed.

Command	Description
`show network`	Show network parameters.
`show network ip` all	Show all IP configuration parameters.
`show network wireless details`	Show all wireless parameters. (Perform this command only when you enable the wireless mode.)

Tip: You can also type "`show network wireless`" to display a shortened version of wireless settings.

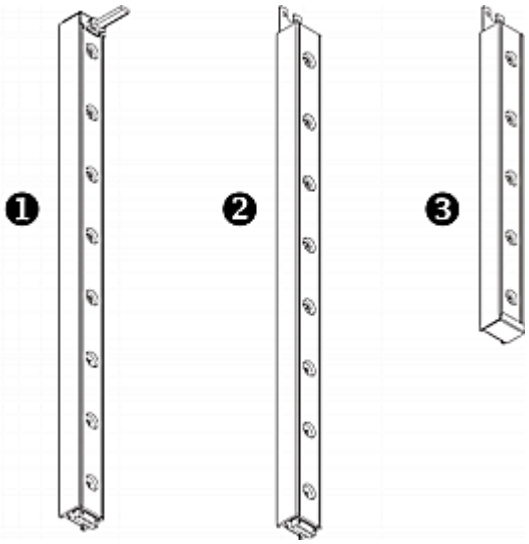
11. If all are correct, type `exit` to log out of the EMX. If any are incorrect, repeat Steps 7 to 10 to change any network settings.

The IP address configured may take seconds to take effect.

Combining Asset Sensors

Each tag port on the asset sensors corresponds to a rack unit and can be used to locate the IT devices on a specific rack (or cabinet). For each rack, you can attach asset sensors up to 64U long, consisting of one MASTER and multiple SLAVE asset sensors. The difference between the master and slave asset sensors is that the master asset sensor has an RJ-45 connector while the slave one does not.

The following diagram illustrates some asset sensors. Note that Raritan provides more types of asset sensors than the diagram.

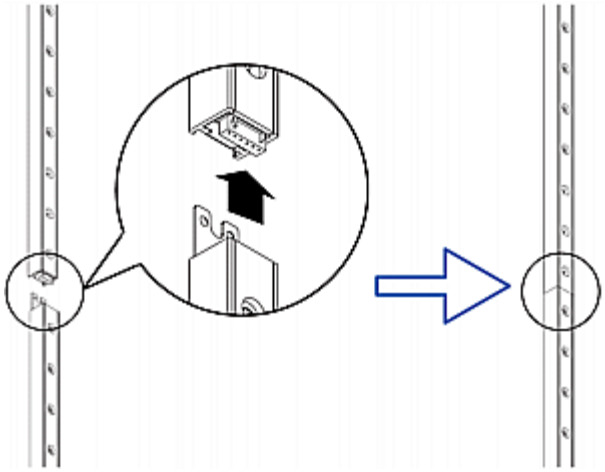


Number	Item
❶	8U MASTER asset sensor with 8 tag ports
❷	8U SLAVE asset sensor with 8 tag ports
❸	5U "ending" SLAVE asset sensor with 5 tag ports

Note: Unlike regular slave asset sensors, which have one DIN connector respectively on either end, the ending slave asset sensor has one DIN connector on only one end. An ending asset sensor is installed at the end of the asset sensor assembly.

To assemble asset sensors:

1. Connect a MASTER asset sensor to an 8U SLAVE asset sensor.
   - Plug the white male DIN connector of the slave asset sensor into the white female DIN connector of the master asset sensor.
   - Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master asset sensor. Screw up the U-shaped sheet metal to reinforce the connection.



2. Connect another 8U slave asset sensor to the one being attached to the master asset sensor in the same manner as Step 1.
3. Repeat the above step to connect more slave asset sensors. The length of the asset sensor assembly can be up to 64U.
   - The final asset sensor can be 8U or 5U, depending on the actual height of your rack.
   - It is strongly recommended using the "ending" asset sensor as the final asset sensor.

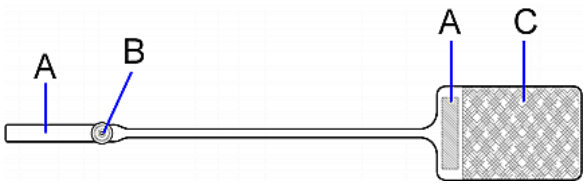
4. Vertically attach the asset sensor assembly to the rack, next to the IT equipment, making each tag port horizontally align with a rack unit. The asset sensors are automatically attracted to the rack because of magnetic stripes on the back.

Note: The asset sensor is implemented with a tilt sensor so it can be mounted upside down.

Connecting Asset Sensors to the EMX

You need both of asset sensors and asset tags for tracking IT devices. Asset tags, which are affixed to IT devices, provide an ID number for each IT device, while the asset sensors transmit ID numbers and positioning information to the connected EMX device.

The following diagram illustrates an asset tag.



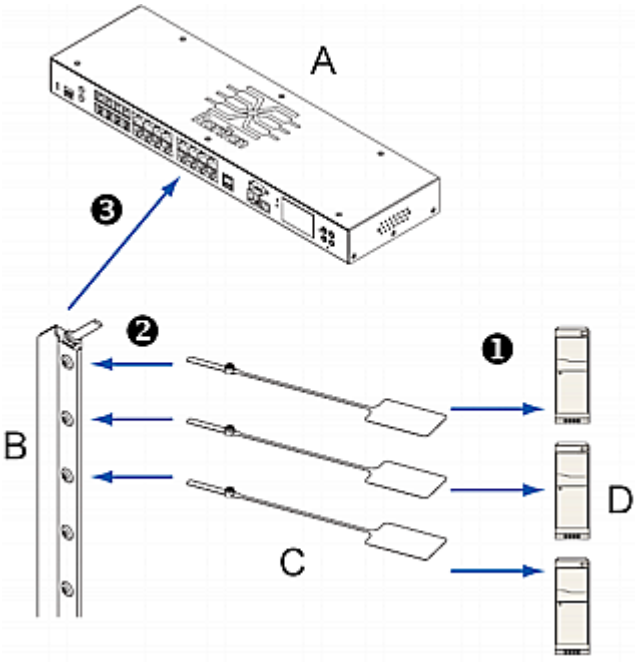
Letter	Item
A	Barcode (ID number), which is available on either end of the asset tag
B	Tag connector
C	Adhesive area with the tape

Note: Each asset tag has a unique barcode, which is displayed in the EMX's web interface for identifying each asset tag.

To connect asset sensors to the EMX device:

1. Affix the adhesive end of an asset tag to each IT device through the tag's tape.
2. Plug the connector on the other end of each asset tag into the corresponding tag port on the asset sensor.
3. Connect the asset sensor assembly on the rack to the EMX device by following this procedure:
   a. Connect one end of the Category 5e/6 cable to the RJ-45 connector on the MASTER asset sensor.
   b. Connect the other end of the cable to the FEATURE port on the EMX device.

The EMX device supplies power to the asset sensor assembly through the Category 5e/6 cable. All LEDs on the asset sensor assembly may cycle through different colors during the power-on process if the asset sensor's firmware is being upgraded by the EMX device. After the power-on process completes, the LEDs show solid colors. Note that the LED color of the tag ports with asset tags connected will be different from the LED color of the tag ports without asset tags connected.



Letter	Item
A	The EMX device
B	Asset sensors
C	Asset tags
D	IT devices, such as servers

EMX2-111 supports a maximum of 1-meter cable length for connecting the asset sensor assembly while EMX2-888 supports a maximum of 10-meter cable length for connecting each asset sensor assembly.

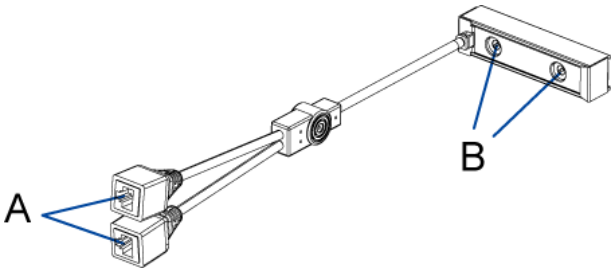
4. If your device has more than one FEATURE port, repeat the above steps to connect additional asset sensors to the rest of FEATURE ports.
5. Configure the asset sensor. See ***Configuring the Asset Sensor*** (on page 158).

Connecting AMS-M2-Z Asset Sensors (Optional)

The AMS-M2-Z is a special type of asset sensor that functions the same as regular MASTER asset sensors with the following differences.

- It provides two RJ-45 connectors.
- Multiple AMS-M2-Z asset sensors can be daisy chained.
- Only two tag ports are available on each AMS-M2-Z so only two asset tags can be connected.

This product is especially useful for tracking large devices such as SAN boxes in the cabinet.



Item	Description
A	RJ-45 connectors
B	Tag ports

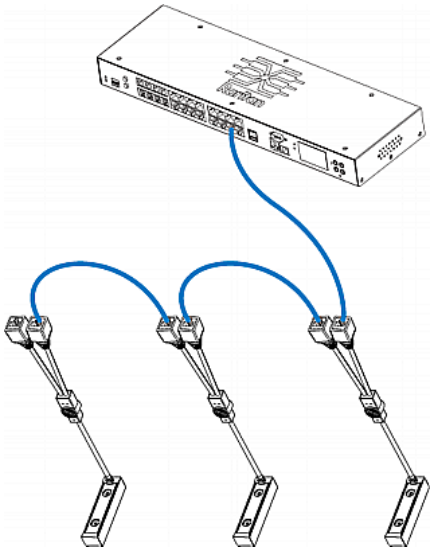
To connect the AMS-M2-Z asset sensors to the EMX:

1. Connect the AMS-M2-Z to the EMX via a Category 5e/6 cable.
   a. Connect one end of the cable to the RJ-45 port labeled "Input" on the AMS-M2-Z.
   b. Connect the other end of the cable to the FEATURE port on the EMX.
2. Affix an asset tag to the IT device and connect this asset tag to the AMS-M2-Z by plugging the tag connector into the tag port on the AMS-M2-Z. See ***Connecting Asset Sensors to the EMX*** (see "***Combining Asset Sensors***" on page 20) for details.
3. If necessary, daisy chain multiple AMS-M2-Z to track more than two IT devices via this EMX.
   a. Verify that the Category 5e/6 cable length is within the limitation. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 162) for the cable length limitations.
   b. Connect one end of the Category 5e/6 cable to the RJ-45 connector labeled "Output" on the AMS-M2-Z being connected to the EMX.

c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on another AMS-M2-Z.

d. Repeat the above steps to daisy chain additional AMS-M2-Z. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 162) for the maximum number of AMS-M2-Z asset sensors supported in the chain.

e. It is highly recommended using the cable ties to help hold the weight of all connecting cables.



4. Repeat Step 2 to connect IT devices to the other AMS-M2-Z's in the chain via the asset tags.

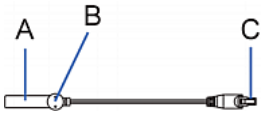
Connecting Blade Extension Strips

For blade servers, which are contained in a single chassis, you can use a blade extension strip to track individual blade servers.

Raritan's blade extension strip functions similar to a Raritan asset sensor but requires a tag connector cable for connecting to a tag port on the regular asset sensor or AMS-M2-Z. The blade extension strip contains 4 to 16 tag ports, depending on which model you purchased.

The diagram illustrates a tag connector cable and a blade extension strip with 16 tag ports.

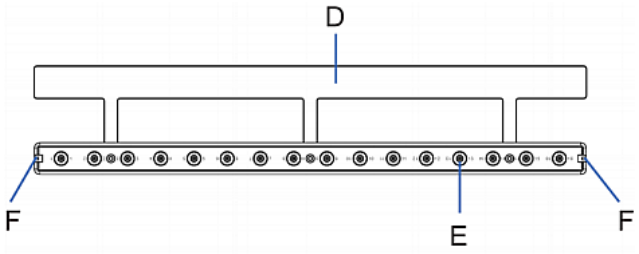
Tag connector cable



Item	Description
A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

Note: A tag connector cable has a unique barcode, which is displayed in the EMX's web interface for identifying each blade extension strip where it is connected.

Blade extension strip

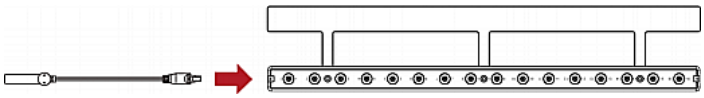


Item	Description
D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

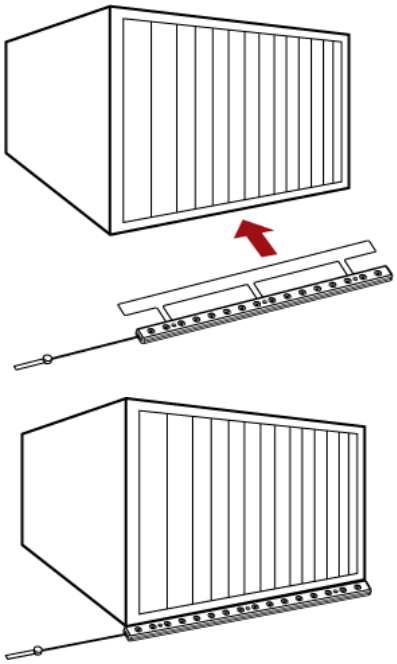
Note: Each tag pot on the blade extension strip is labeled a number, which is displayed as the slot number in the EMX's web interface.

To install a blade extension strip:

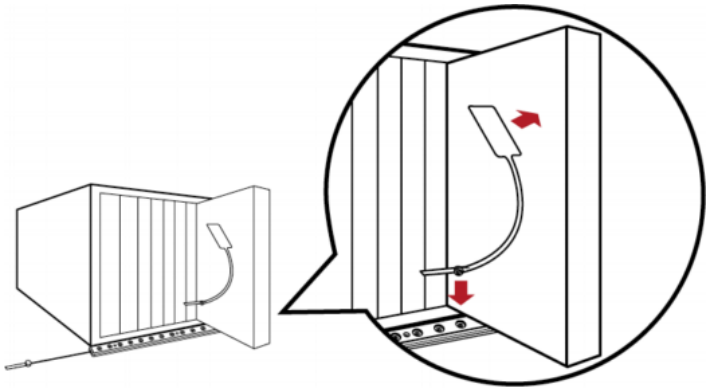
1. Connect the tag connector cable to the blade extension strip.
   - Plug the cable's connector into the socket at either end of the blade extension strip.



2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.

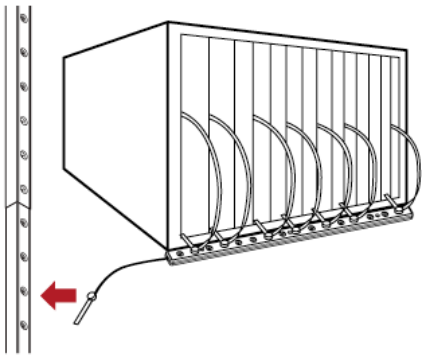


3. Connect one end of an asset tag to a blade server and connect the other end to the blade extension strip.
   a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.
   b. Plug the tag connector of the asset tag into the tag port on the blade extension strip.



4. Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.

5. Plug the tag connector of the blade extension strip into the closest tag port of the asset sensor assembly or the AMS-M2-Z asset sensor on the rack.



Note: If you need to temporarily disconnect the tag connector of the blade extension strip, wait at least 1 second before connecting it back, or the EMX may not detect it.

Connecting Environmental Sensors (Optional)

To enable the detection of environmental factors around the EMX, connect one or more Raritan environmental sensors to the EMX device.

The maximum distance for all sensor cabling plugged into the product's sensor port should not exceed 30 meters/100 feet. Contact Raritan Technical Support if you have questions.

If a Raritan sensor hub is used, you can connect up to 16 environmental sensors per SENSOR port. That is,

- For EMX2-111, which has only 1 SENSOR port, a maximum of 16 environmental sensors can be connected.
- For EMX2-888, which has 8 SENSOR ports, a maximum of 128 environmental sensors can be connected. Since the EMX2-888 device is implemented with two channels of onboard contact closure termination, it supports a maximum of 130 environmental sensors.

Each SENSOR port can only support a maximum of two Raritan contact closure sensors, which has the shortest update interval among all Raritan sensors. See ***Information about Update Interval*** (on page 151).

Note that a Raritan environmental sensor usually contains more than one sensor. For example, a DPX-T2H2 counts as 4 sensors, and a DPX-T3H1 counts as 4 sensors.

Warning: For proper operation, wait for 15~30 seconds between each connection operation or each disconnection operation of environmental sensors.

To directly connect one or multiple environmental sensors:

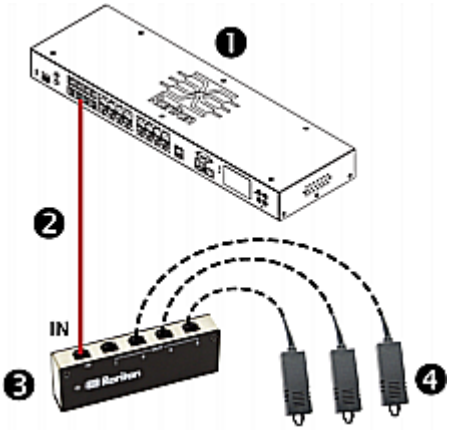
- Plug the connector of the environmental sensor into the SENSOR port on your EMX device.

Note: Depending on the model you purchased, the total number of SENSOR ports varies.

To connect environmental sensors via an optional PX sensor hub:

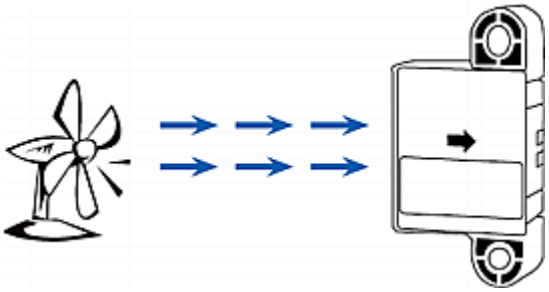
1. Connect a Raritan sensor hub to the EMX device.
   a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.
   b. Plug the other end into one of the SENSOR ports on the EMX device.
2. Connect Raritan environmental sensors to any of the four OUT ports on the hub.

Raritan sensor hubs CANNOT be cascaded so at most a sensor hub can be connected to each SENSOR port on the EMX device. This diagram illustrates a configuration with a sensor hub connected.



❶	The EMX device
❷	Raritan-provided phone cable
❸	Raritan PX sensor hub
❹	Raritan environmental sensors

3. If there are any Raritan air flow sensors attached, make sure that sensor faces the source of the wind (such as a fan) in the appropriate orientation as indicated by the arrow on that sensor.



4. Configure the environmental sensor. See ***Configuring Environmental Sensors*** (on page 147).

About Contact Closure Sensors

Raritan's contact closure sensor (DPX-CC2-TR) can detect the open-and-closed status of the connected detectors/switches.

This feature requires the integration of at least a discrete (on/off) detector/switch to work properly. The types of discrete detectors/switches that can be plugged into DPX-CC2-TR include those for:

- Door open/closed detection
- Door lock detection
- Floor water detection
- Smoke detection
- Vibration detection

Raritan does NOT provide discrete detectors/switches. They are third-party probes, so you must test them with Raritan's DPX-CC2-TR to ensure they work properly.

Important: Integration and testing for third-party detectors/switches is the sole responsibility of the customer. Raritan cannot assume any liability as a result of improper termination or failure (incidental or consequential) of third-party detectors/switches that customers provide and install. Failure to follow installation and configuration instructions can result in false alarms or no alarms. Raritan makes no statement or claim that all third-party detectors/switches will work with DPX-CC2-TR.

Connecting Third-Party Detectors/Switches

There are two ways to connect third-party detectors/switches to the EMX device:

- Connect the detectors/switches to DPX-CC2-TR, which will be connected to a SENSOR port on the EMX device
- Connect the detectors/switches to the contact closure sensor termination on the EMX device if your EMX device is EMX2-888

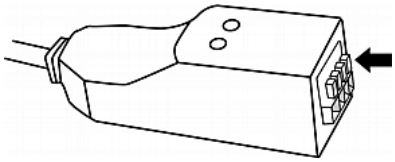
Connecting Third-Party Detectors/Switches to DPX-CC2-TR

A DPX-CC2-TR unit provides two channels for connecting two third-party detectors/switches. There are four spring-loaded termination points on the body of DPX-CC2-TR: the two to the right are associated with one channel (as indicated by the LED number), and the two to the left are associated with another channel. You must plug the third-party detectors/switches into these termination points.

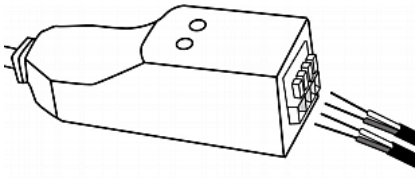
To connect third-party detectors/switches:

1. Strip the insulation around 12mm from the end of each wire of two third-party detectors/switches.
2. Press and hold down the tiny rectangular buttons above the termination points on the body of DPX-CC2-TR.

Note: Each button controls the spring of each corresponding termination point.



3. Fully insert each wire of both third-party detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.
   - Plug both wires of another detector/switch into the two termination points to the right.



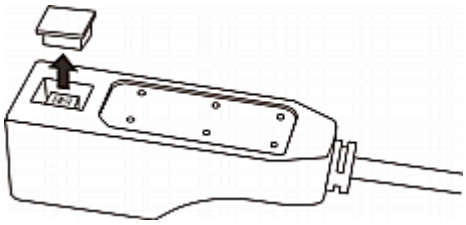
4. Release the tiny rectangular buttons after inserting the wires properly.
5. Verify that these wires are firmly fastened.

Configuring a Contact Closure Sensor

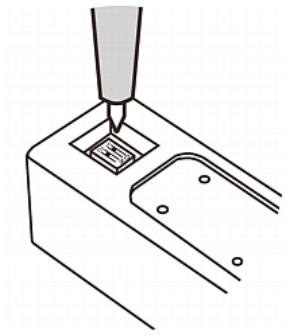
Before using DPX-CC2-TR to detect the contact closure status, water, smoke or vibration, you must determine the normal state by adjusting its dip switch, which controls the LED state on the body of DPX-CC2-TR. A dip switch is associated with a channel.

To adjust the dip switch setting:

1. Place the detectors/switches connected to DPX-CC2-TR to the position where you want to detect a specific environmental situation.
2. Uncover the dip switch on the body of DPX-CC2-TR.



3. To set the Normal state for channel 1, locate the dip switch labeled 1.
4. Use a pointed tip such as a pen to move the slide switch to the end labeled NO (Normally Open) or NC (Normally Closed).
   - Normally Open: The open status of the connected detector/switch is considered normal.
   - Normally Closed: The closed status of the connected detector/switch is considered normal. This is the default.



5. To set the Normal state for channel 2, repeat Step 4 for adjusting the other dip switch's setting.
6. Install back the dip switch cover.

Note: The dip switch setting must be properly configured, or the sensor LED may be incorrectly lit in the Normal state.

Connecting Third-Party Detectors/Switches to the EMX

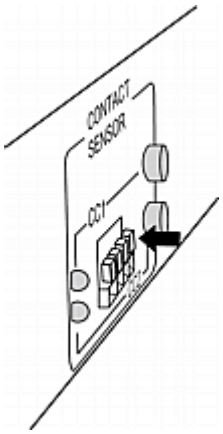
A specific EMX model (EMX2-888) provides two channels of contact closure sensor termination points, allowing for direct connection of third-party contact closure detectors/switches.

It is not guaranteed that all third-party detectors/switches are compatible with the EMX device. You need to test the compatibility after properly installing them.

To connect third-party detectors/switches:

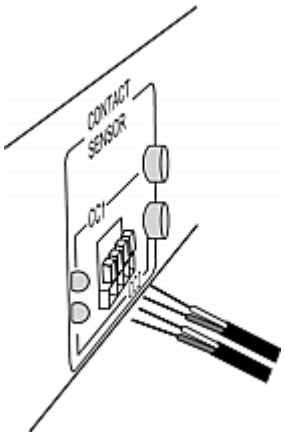
1. Strip the insulation around 12mm from the end of each wire of two third-party detectors/switches.
2. Press and hold down the tiny rectangular buttons above the termination points.

Note: Each button controls the spring of each corresponding termination point.



3. Fully insert each wire of both third-party detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.

- Plug both wires of another detector/switch into the two termination points to the right.



4. Release the tiny rectangular buttons after inserting the wires properly.
5. Verify that these wires are firmly fastened.
6. By default the open status of the detector/switch is considered normal. To set the "normal" setting to "closed" , press down the corresponding button adjacent to the termination points.

Contact Closure Sensor LEDs

Two LEDs are located near the contact closure termination points on the EMX device or Raritan contact closure sensor module (DPX-CC2-TR). Each LED shows the state of the corresponding channel.

The LED is lit when the associated detector/switch is in the "abnormal" state, which is the opposite of the Normal state.

The meaning of a lit LED varies depending on the Normal state settings.

- **When the Normal state is set to Closed:**

LED	Sensor state
Not lit	Closed
Lit	Open

- **When the Normal state is set to Open:**

LED	Sensor state
Not lit	Open
Lit	Closed

Connecting Differential Air Pressure Sensors

You can have a Raritan differential air pressure sensor connected to the EMX device if the differential air pressure data is desired.

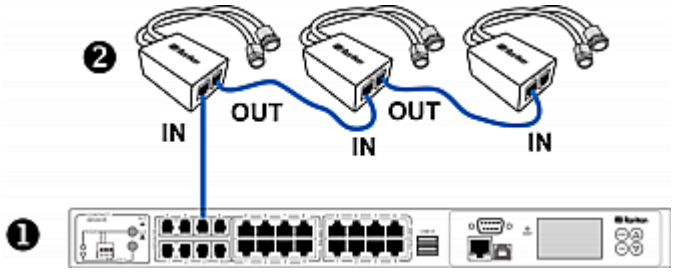
With this sensor, the temperature around the sensor can be also detected through a temperature sensor implemented inside it.

Multiple differential air pressure sensors can be cascaded.

To connect differential air pressure sensors:

1. Plug one end of a Raritan-provided phone cable to the SENSOR port of the EMX device.
2. Plug the other end of this phone cable to the IN port of the differential air pressure sensor.
3. To connect additional Raritan differential air pressure sensors, do the following:
   a. Plug one end of a Raritan-provided phone cable to the OUT port of the previous differential air pressure sensor.
   b. Plug the other end of this phone cable to the IN port of the newly-added differential air pressure sensor.
   c. Repeat Steps a to b to cascade more differential air pressure sensors. Note that each SENSOR port supports a maximum of 16 environmental sensors.

❶	The EMX device
❷	The Raritan differential air pressure sensor



Connecting a Logitech Webcam (Optional)

The EMX supports Logitech® QuickCam® Pro 9000 webcams connected to it, allowing you to view video or snapshots of the area surrounding the webcam. The EMX 888 device supports up to two (2) webcams, and the EMX 111 supports one (1) webcam. After connecting a webcam, you can visually monitor environmental conditions near the EMX through the web interface from anywhere.

For more information on the QuickCam webcam, see the user documentation accompanying it.

To connect a webcam:

1. Connect the webcam to the USB-A port on the EMX device. The EMX automatically detects the webcam.
2. Position the webcam properly.

Static images or videos captured by the webcam are immediately displayed in the EMX web interface. See ***Webcams*** (on page 168) for additional information on the feature, and ***Configuring Webcams*** (on page 168) for information on configuring the webcam once it has been connected.

Note: You must have Change Webcam Configuration permission applied to your role in order to configure webcams, and the View Webcam Images and Configuration permission to view images in EMX.

Connecting a Schroff LHX Heat Exchanger (Optional)

To remotely monitor and administer the Schroff® LHX-20 or LHX-40 heat exchangers through the EMX device, you must establish a connection between the heat exchanger and the EMX device.

For more information on the LHX heat exchanger, see the user documentation accompanying that product.

To connect an LHX heat exchanger:

1. Plug one end of a standard Category 5e/6 UTP cable into the RS-485 port on the Schroff LHX heat exchanger.
2. Plug the other end of the cable into one of available RS-485 ports on your EMX device.

To connect an LHX heat exchanger to the serial FEATURE port using a serial cable (provided by Schroff):

1. Plug DB9 end of cable into the RS232 port on the Schroff LHX heat exchanger.

2. Plug the other end of the cable into one of available serial FEATURE ports on your EMX device.

See ***Schroff LHX Heat Exchangers*** (on page 175) for how to monitor and administer the heat exchanger using the EMX.

Chapter 3 Getting Started

In This Chapter

Supported Web Browsers....39
Connection Ports....39
LCD Display Panel....40
Reset Button....46
Contact Closure Sensor Termination....46
Power Switch....46
Logging In....47
Logout....48
Changing Your Password....49
Introduction to the Web Interface....50
Viewing the Dashboard....57

Supported Web Browsers

The following web browsers can be used to access the EMX web interface:

- Internet Explorer® 7 and 8
- Firefox® 3.x
- Safari® 5.1 (MacOS Lion)
- Konqueror
- Google® Chrome® 16.0

The following smart phone browsers are supported:

- Safari on iOS 5.01
- Dolphin® 3.2.1

Connection Ports

Depending on the model you purchased, the total number of ports available varies.

The table below explains the function of each port.

Port	Used for...
USB-B	Establishing a USB connection between a computer and the EMX device. This port can be used for disaster recovery of the EMX device. Contact Raritan Technical Support for instructions.
USB-A	Connecting a USB device. This is a "host" port, which is powered, per USB 2.0 specifications.

Port	Used for...
FEATURE	Connection to asset sensors via a Category 5e/6 cable. *Note: The EMX device supplies power to the connected asset sensors after the connection is established.*
CONSOLE/ MODEM	Establishing a serial connection between a computer and the EMX device: This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect the EMX device to the computer.
SENSOR	Connection to Raritan's environmental sensors. A Raritan sensor hub may be required if you want to connect more environmental sensors.
ETHERNET	Connecting the EMX device to your company's network: Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the EMX device remotely using the web interface. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. *Note: Connection to this port is not required unless the EMX device is connected to a wireless network.*
RS-485	Connection to an electrical device with the RS-485 interface. Currently the EMX only supports the Schroff® LHX-20 and LHX-40 heat exchangers.

LCD Display Panel

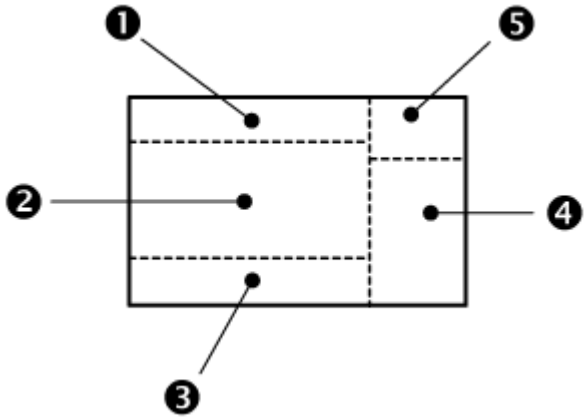
The LCD display panel shows the sensor reading or status, asset management states and the device's MAC address.

It consists of:

- An LCD display
- Control buttons

LCD Display

Different types of information are shown in different sections of the LCD display. The diagram indicates the sections.



Section	Information shown
1	Depending on your selection, the information displayed includes: • The selected environmental sensor, including the sensor's ID number. The EMX shows the selected environmental sensor in two ways: ▪ For a sensor whose ID number is below 100, it is displayed as "SENSOR X" or "SENSOR XX," where X and XX are numeric digits. ▪ For a sensor whose ID number is equal to or over 100, it is displayed as "1 SENSOR XX" where XX are the last two numeric digits of the ID number. • The number of the FEATURE port where the selected asset sensor is connected.

Section	Information shown
❷	Depending on your selection, the information displayed includes: • Sensor reading comprising numeric digits or sensor state comprising alphabetical characters. • Number of the SENSOR port where the selected sensor is physically connected. • X, Y or Z coordinates of the selected environmental sensor. • Serial number of the selected environmental sensor. • The selected rack unit number of the selected asset sensor. *Note: For the Raritan asset sensor, a rack unit refers to a tag port.* • MAC address of the EMX
❸	The text "ALARM" may appear to indicate either of the following scenarios: • For a numeric environmental sensor, such as a temperature sensor, it means the sensor reading reaches or crosses the upper or lower thresholds if these thresholds have been enabled. • For a discrete (on/off) environmental sensor, such as a contact closure sensor, it means the sensor enters the abnormal state. • For an asset sensor, it means NO asset tag is detected on the selected rack unit.
❹	The measurement unit for the selected environmental sensor appears. The measurement unit varies according to the sensor type: • % is displayed for a humidity sensor. • °C is displayed for a temperature sensor.
❺	When the term "ASSET" appears, the displayed information is associated with asset sensors and asset tags.

Control Buttons

There are four control buttons.

- Up and Down buttons for selecting a specific ID or port number
- MODE button for switching between different types of target information, including environmental sensor information, asset management information, and MAC address
- FUNC button for switching between different types of data for a selected environmental sensor

By default the display panel shows the first environmental sensor listed on the External Sensors page of the web interface until you select a different environmental sensor or a different target.

Environmental Sensor Information

The environmental sensor information is displayed as "SENSOR" in the LCD display. Operate the LCD display to view information about the selected environmental sensor, including the sensor reading or state, the sensor's physical port number, X, Y, Z coordinates and its serial number.

To display the environmental sensor information:

1. Press the Up or Down button until the desired environmental sensor's ID number is displayed in the top of the LCD display. See ***LCD Display*** (on page 41). For example, "SENSOR 1" refers to the #1 sensor listed on the External Sensors page of the web interface.
   - Pressing the △ (UP) button moves up one selection.
   - Pressing the ▽ (DOWN) button moves down one selection.
   - "1 SENSOR 24" refers to the #124 sensor.

   Note: Press and hold the Up or Down buttons for at least two (2) seconds to quickly move through several items at once.

2. The LCD display shows the reading or state of the selected sensor in the middle of the LCD display.

   For a numeric sensor's reading, the appropriate measurement unit is displayed to the right of the reading.
   - % is displayed for a humidity sensor.
   - °C is displayed for a temperature sensor.

   For a discrete sensor, either of the following sensor states is displayed.
   - on: The sensor is in the abnormal state.
   - oFF: The sensor is in the normal state.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state.

3. If your EMX device has more than one SENSOR ports, press the FUNC button to display the physical port number of the environmental sensor. The port number is shown as "P:X," where X is the port number. For the onboard contact closure sensor, it is displayed as CC1 or CC2.
4. Press the FUNC button to display the X, Y and Z coordinates of the sensor respectively.
   - X coordinate is shown as "x:XX," where XX are the first two numeric digits entered for the X coordinate in the web interface.
   - Y coordinate is shown as "y:XX," where XX are the first two numeric digits entered for the Y coordinate in the web interface.
   - Z coordinate is shown as "z:XX," where XX are the first two numeric digits entered for the Z coordinate in the web interface.

   If one or both of the first two digits for a specific coordinate are alphabetical characters, one or two underscores are displayed in place of the alphabetical characters.
5. Press the FUNC button again to display the serial number of the sensor, which is shown as "s:XX," where XX are two digits of the serial number. The LCD will cycle through the serial number from the first two digits to the final two.

   For example, if the serial number is AE17A00022, the LCD display shows the following information one after another:

   s:AE --> s:17 --> s:A0 --> s:00 --> s:22

If no button is pressed after tens of seconds, the LCD display returns to the sensor reading or state.

Asset Management Information

The LCD display can display the asset sensor state on each FEATURE port as well as the asset tag state of each rack unit. For the Raritan asset sensor, a rack unit refers to a tag port.

To display the asset management information:

1. Press the MODE button until the term "ASSET" is displayed in the top-right corner of the LCD display.
2. Press the Up or Down button until the desired FEATURE port number is displayed in the top of the LCD display. See ***LCD Display*** (on page 41).
   - Pressing the △ (UP) button moves up one selection.

- Pressing the ▽ (DOWN) button moves down one selection.

If no asset sensor is detected or physically connected to the selected FEATURE port, the term "nA" appears.

Note: Press and hold the Up or Down buttons for at least two (2) seconds to quickly move through several items at once.

3. Press the FUNC button. When an blinking double-arrow symbol ◇ appears on the left side of the LCD display, press the Up or Down button to select the desired rack unit on the currently selected asset sensor. The rack unit number appears in the middle of the LCD display.
   - If the term "ALARM" appears below the rack unit number, it means no asset tag is detected or physically connected to that rack unit.
   - If the term "ALARM" does NOT appear, it means a connected asset tag is detected on the rack unit.

MAC Address

The EMX's MAC address is available by operating the LCD display. Using commonly-used network tools, you can find this device's IP address via the MAC address. Contact your LAN administrator for assistance.

To display the MAC address:

1. Press the MODE button until the character "M" appears in the left side of the LCD display.
2. The MAC address is displayed as "M:XX", where XX are two digits of the MAC address. The LCD will cycle through the MAC address from the first two digits to the final two.

   For example, if the MAC address is 00:0d:5d:03:5E:1A, the LCD display shows the following information one after another:

   M:00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

Note: Press and hold the Up or Down buttons for at least two (2) seconds to quickly move through several items at once.

IP Address

The IP Address is also available in the EMX LCD display. Use the Mode button to switch between sensor, asset and device mode. When in device mode, a small "d" is displayed in the upper left corner. The address starts with the IPv4 address, indicated by "i4" in the upper right corner of the display. Use the Function button to switch to the MAC address, in which case an "M" is displayed in the upper right corner.

Reset Button

The reset button is located inside a small hole which is labeled RESET.

The EMX device can be reset to its factory default values using this button when a serial connection is available. See ***Resetting to Factory Defaults*** (on page 91).

Without the serial connection, pressing this reset button restarts the EMX device's software.

Contact Closure Sensor Termination

Two channels for connecting two third-party contact closure sensors are provided on the EMX2-888 model.

For more information, see:

- ***Connecting Third-Party Detectors/Switches to the EMX*** (on page 34)
- ***Contact Closure Sensor LEDs*** (on page 35)

Power Switch

The power switch turns on or off the EMX device.

To power cycle the EMX, press the power switch to turn off the device, **wait at least 10 seconds** and then press the power switch again to turn it on. Note that a minimum of 10-second power-off period is required, or the device may not boot up properly.

Logging In

To log in to the web interface, you must enter a user name and password. The first time you log in to the EMX, use the default user name (admin) and password (raritan). You are then prompted to change the password for security purposes.

Exception: If you already changed the password for the admin account during the Initial Network Configuration, use the new password instead to log in to the web interface, and the EMX will NOT prompt you to change the password.

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See ***Creating a User Profile*** (on page 58).

The web interface allows a maximum of 16 users to log in simultaneously.

You must enable JavaScript in the web browser for proper operation.

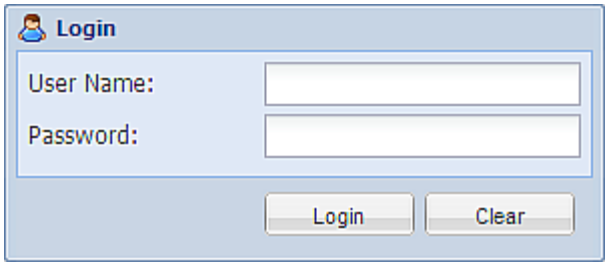
To log in to the web interface:

1. Open a browser, such as Microsoft Internet Explorer or Mozilla Firefox, and type this URL:

   http(s)://<ip address>

   where *<ip address>* is the IP address of the EMX device.

2. If any security alert message appears, click OK or Yes to accept. The Login page then opens.



3. Type your user name in the User Name field, and password in the Password field.

   Note: Both the user name and password are case sensitive, so make sure you capitalize them correctly. If you typed them incorrectly, click Clear to clear either the inputs or any error message that appears.

4. Click Login or press Enter. The EMX page opens.

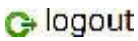
Note: Depending on your hardware configuration, elements shown on the EMX page may appear slightly different from this image.

Logout

After finishing your tasks with the EMX, you should log out to prevent others from accessing the web interface.

To log out of the web interface:

1. Do one of these:
   - Click "logout" on the top-right corner of the web interface.

   - Close the web browser by clicking the Close button ( ) on the top-right corner of the browser.
   - Close the web browser by choosing File > Close, or File > Exit. The command varies according to the version of the browser you use.
   - Choose the Refresh command or click the Refresh button on the web browser.
2. Either the login page opens or the browser is closed, depending on your choice in the previous step.

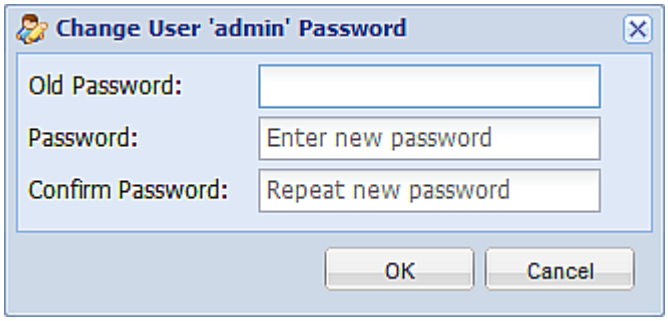
Changing Your Password

Normal users can change their own passwords if they have the Change Own Password permission. See ***Setting Up Roles*** (on page 64).

If you are the administrator (admin), the EMX web interface automatically prompts you to change the password if this is your first time to log in to the EMX. If you have the Administrator Privileges, you can change other users' passwords, as well. See ***Modifying a User Profile*** (on page 62).

To change your password:

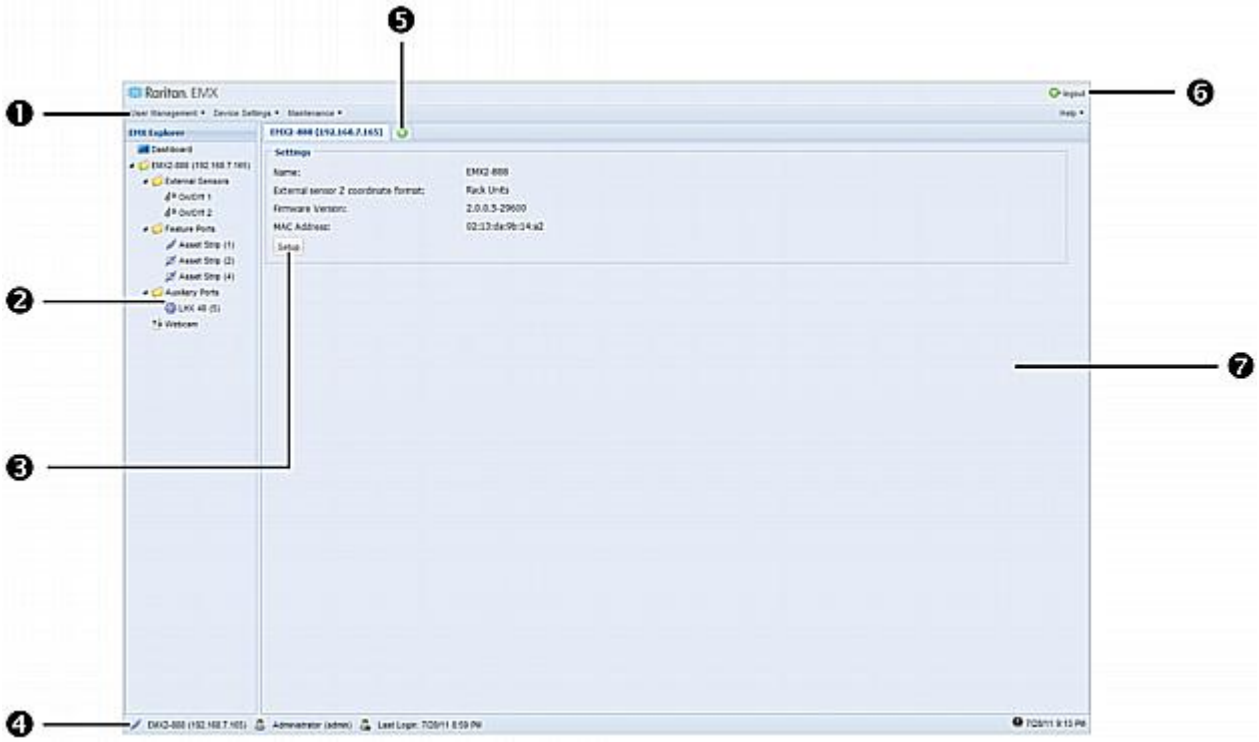
1. Choose User Management > Change Password. The Change User Password dialog appears.



2. Type the current password in the Old Password field.
3. Type your new password in the Password and Confirm Password fields. The password can be 4 to 64 characters long. It is case sensitive.
4. Click OK to save the changes.

Introduction to the Web Interface

The web interface provides two panes, a menu bar, a status bar, an Add Page icon, and a logout button throughout every page.



Number	Web interface element
❶	Menus
❷	EMX Explorer pane
❸	Setup button*
❹	Status bar
❺	Add Page icon
❻	Logout button
❼	Data pane

* The Setup button is not available on some pages, such as the *Dashboard* page.

For detailed information about these web interface elements, see the sections that follow.

Menus

Four menus are available for managing different tasks or showing information.

- **User Management** contains menu items for managing user profiles, permissions (roles), and password.
- **Device Settings** deals with device-related settings, such as the device name, network settings, security settings, and system time.
- **Maintenance** provides tools that are helpful for maintaining the EMX, such as the event log, hardware information, firmware upgrade and so on.
- **Help** displays information regarding the firmware and all open source packages embedded on the EMX. In addition, you can access the user guide from this menu.

Setup Button

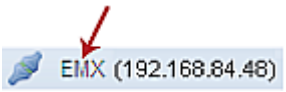
The Setup button is available for most tree items. It triggers a setup dialog where you can change settings for the selected tree item.

Status Bar

The status bar shows five pieces of information from left to right.

- **Device name:**

  This is the name assigned to the EMX device. The default is "EMX." See ***Naming the EMX Device*** (on page 67).



- **IP address:**

  The numbers enclosed in parentheses is the IP address assigned to the EMX device. See Initial Network Configuration or ***Modifying the Network Settings*** (on page 75).

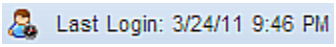
Tip: The presence of the device name and IP address in the status bar indicates the connection to the EMX device. If the connection is lost, it shows " *disconnected " instead.*

- **Login name:**

  This is the user name you used to log in to the web interface.

- **Last login time:**

  This shows the date and time this login name was used to log in to this EMX device last time.

  When the mouse pointer hovers over the last login time, detailed information about the last login is displayed, including the access client and IP address.

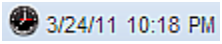
  For the login via a serial connection, <local> is displayed instead of an IP address.

  There are different types of access clients:

  - Web GUI: Refers to the EMX web interface.
  - CLI: Refers to the command line interface (CLI).
    The information in parentheses following "CLI" indicates how this user was connected to the CLI.
    - *Serial*: Represents the local connection (serial or USB).
    - *SSH*: Represents the SSH connection.
    - *Telnet*: Represents the Telnet connection.

- **System date and time:**

  Current date, year, and time are displayed to the right of the bar. If positioning the mouse pointer over the system date and time, the time zone information is also displayed.

Sometimes a flag icon ( ) may appear to the far right of the bar when a communication error between the EMX device and the graphical user interface (GUI) occurs. When the icon appears, you can click the icon to view the communications log. See ***Viewing the Communication Log*** (on page 140).

Add Page Icon

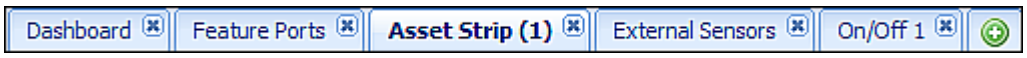
The Add Page icon , located on the top of the data pane, lets you open data pages of multiple tree items without overriding any opened page.

To open new data pages:

1. Click the Add Page icon . A new tab along with a blank data page appears.
2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank page.

3. To open more data pages, repeat Steps 1 to 2. All tabs representing opened pages are shown across the top of the page.

   The following diagram shows a multi-tab example.



4. With multiple pages opened, you can take these actions:
   - To switch to one of the opened data pages, click the corresponding tab.

     If there are too many tabs to be all shown, two arrows (and) appear at the left and right borders of the pane. Click either arrow to navigate through all tabs.
   - To close any data page, click the Close button ( ) on the corresponding tab.

Data Pane

The right pane shows the data page of the selected tree item. The data page includes the item's current status, settings and a Setup button (if available).

All tabs above the pane represent the opened data pages. The highlighted tab indicates the current selection.

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the left border of the right pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

Warning Icon

If the value you entered in a specific field is invalid, a red warning icon appears to the right and the field in question is surrounded by a red frame as shown in this illustration.

When this occurs, position your mouse pointer over the warning icon to view the reason and modify the entered value accordingly.

Readings Highlighted in Yellow or Red

When a numeric sensor's reading crosses any upper or lower threshold, the background color of the whole row turns to yellow or red for alerting users.

For a discrete (on/off) sensor, the row changes the background color when the sensor enters the abnormal state.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state.

See the table for the meaning of each color:

Color	State
White	The background is white in one of the following scenarios: • For a numeric sensor, no thresholds have been enabled. • If any thresholds have been enabled for a numeric sensor, the sensor reading is between the lower and upper warning thresholds. • For a discrete (on/off) sensor, the sensor state is normal. • The sensor reading or state is unavailable.
Yellow	The reading drops below the lower warning threshold or rises above the upper warning threshold.
Red	The meaning of the red color varies depending on the sensor type: • For a numeric sensor, this color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold. • For a discrete (on/off) sensor, this color indicates the sensor is in the "alarmed" state. • For a Schroff® LHX heat exchanger (if available), this color indicates that at least one sensor implemented on that heat exchanger fails. See ***Schroff LHX Heat Exchangers*** (on page 175).

To find the exact meaning of the alert, read the information shown in the State (or Status) column:

- below lower critical: The numeric sensor's reading drops below the lower critical threshold.
- below lower warning: The numeric sensor's reading drops below the lower warning threshold.
- above upper critical: The numeric sensor's reading reaches or exceeds the upper critical threshold.
- above upper warning: The numeric sensor's reading reaches or exceeds the upper warning threshold.
- alarmed: The discrete sensor is NOT in the normal state.

For information on the thresholds, see ***Configuring Environmental Sensors*** (on page 147).

Browser-Defined Shortcut Menu

A shortcut menu, which is built in the web browser, may appear when right-clicking anywhere in the EMX web interface.

The shortcut menu functions are defined by the browser. For example, the Back command on the Internet Explorer® (IE) shortcut menu works the same as the Back button in the IE browser. Both of these functions take you to the previous page.

For information on each shortcut menu command or item, see the online help or documentation accompanying your web browser.

Below is the illustration of the IE browser's shortcut menu. Available menu commands or items may slightly differ based on your web browser version.

Viewing the Dashboard

When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the EMX device's status.

The page is divided into several sections according to connected equipment, such as asset sensors and environmental sensors. Double-clicking any item on the Dashboard page opens the data page specific to the selected item.

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or at least one LHX built-in sensor fails on the heat exchanger. See **Readings Highlighted in Yellow or Red (EMX)** *(see "***Readings Highlighted in Yellow or Red***" on page 54).*

After clicking any other icon in the hierarchical tree, the Dashboard page is overridden. To return to the Dashboard page, click the Dashboard icon.

When the Dashboard page is opened, you can do the following to uncover or hide specific data.

To collapse any section:

1. Locate the section you want to collapse.
2. Click the upward arrow prior to the section title. The data specific to the section is hidden.

To expand a collapsed section:

1. Locate the section you want to expand.
2. Click the downward arrow prior to the section title. The data specific to the section appears.

Chapter 4 User and Role Management

In This Chapter

Overview....58
Managing Users....58
Managing Roles....64

Overview

The EMX is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full system permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. Every user profile must have at least a role to determine the user's system permissions. See ***Setting Up Roles*** (on page 64). To manage any settings, you must log in to the user account with appropriate permissions.

By default, multiple users can log in simultaneously using the same login name.

Managing Users

Creating a User Profile

Creating new users adds a new login to the EMX.

To create a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Click New. The Create New User dialog appears.
3. Type the information about the user in the corresponding fields. Note that User Name, Password and Confirm Password fields are required.

Field	Type this...
User Name	The name the user enters to log in to the EMX. ▪ The name can be 4 to 32 characters long. ▪ It is case sensitive.

Field	Type this...
	▪ Spaces are NOT permitted
Full Name	The user's first and last names.
Password, Confirm Password	The password the user enters to log in. Type it first in the Password field and then again in the Confirm Password field. ▪ The password can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are permitted.
Telephone Number	A phone number where the user can be reached.
eMail Address	An email address where the user can be reached. ▪ The email can be up to 32 characters long. ▪ It is case sensitive.

4. Select the Enabled checkbox. If not, the user CANNOT log in to the EMX device.
5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.
6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.
   a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring the SNMP Settings** *(on page 80).*

   b. Set up SNMPv3 parameters if enabling the SNMPv3 access permission.

Field	Description
Security Level	Click the drop-down arrow to select a preferred security level from the list: ▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This

Field	Description
	is the default.
Use Password as Authentication Pass Phrase	*This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.* When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase, disable the checkbox.
Authentication Pass Phrase	Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Authentication Pass Phrase	Re-type the same authentication pass phrase for confirmation.
Use Authentication Pass Phrase as Privacy Pass Phrase	*This checkbox is configurable only if AuthPriv is selected.* When the checkbox is selected, the privacy pass phrase is identical to the authentication pass phrase. To specify a different privacy pass phrase, disable the checkbox.
Privacy Pass Phrase	Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Privacy Pass Phrase	Re-type the same privacy pass phrase for confirmation.
Authentication Protocol	Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: ▪ DES (default) ▪ AES-128

7. Click the SSH tab to enter the public key if the public key authentication for the SSH service is enabled. See ***Changing the SSH Settings*** (on page 80).
   a. Open the SSH public key with a text editor.
   b. Copy and paste all contents in the text editor into the Public Key field on the SSH tab.
8. Click the Roles tab to determine the permissions of the user.
9. Select one or multiple roles by selecting corresponding checkboxes.
   - The Admin role provides full permissions.
   - The Operator role provides limited permissions for frequently-used functions. See ***Setting Up Roles*** (on page 64) for the scope of permissions. This role is selected by default.
   - If no roles meet your needs, you can:
     - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 65).
     - *Create a new role by clicking the Manage Roles button:* See ***Creating a Role*** (on page 64).

   Note: With multiple roles selected, a user has the union of all roles' permissions.
10. To change any measurement units displayed in the web interface for this new user, click the Preferences tab, and do any of the following:
    - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
    - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
    - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

    A Pascal is equal to one newton per square meter. Psi stands for pounds per square inch.

    Note: The measurement unit change only applies to the web interface and command line interface.
11. Click OK to save the changes.

Modifying a User Profile

You can change any user profile's information except for the user name.

To modify a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Make all necessary changes to the information shown.

   To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.
5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 58).
6. To change the permissions, click the Roles tab and do one of these:
   - Select or deselect any role's checkbox.
   - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 65).
7. To change the measurement unit for temperature, length or pressure, click the Preferences tab, and select a different option from the drop-down list.

   Note: The measurement unit change only applies to the web interface and command line interface.
8. Click OK to save the changes.

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

To delete user profiles:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the User List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See Changing the View of a List.

Viewing Connected Users

You can see which users are connected to the EMX device and their status. If you have administrator privileges, you can terminate any user's connection to the EMX device.

To view connected users:

1. Choose Maintenance > Connected Users. The Connected Users dialog appears, showing a list of connected users with the following information:

Column	Description
User Name	The login name used by each connected user.
IP Address	The IP address of each user's host. For the login via a serial connection, <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the EMX. ▪ Web GUI: Refers to the EMX web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user was connected to the CLI. - *Serial*: Represents the local connection (serial or USB). - *SSH*: Represents the SSH connection. - *Telnet*: Represents the Telnet connection.
Idle Time	The length of time for which a user remains idle. The unit "min" represents minutes.

2. To disconnect any user, click the corresponding Disconnect button.
   a. A dialog appears, prompting you to confirm the operation.
   b. Click Yes to disconnect the user or No to abort the operation. If clicking Yes, the connected user is forced to log out.
3. You may change the sorting order of the list if necessary. See Changing the Sorting.
4. Click Close to quit the dialog.

Managing Roles

Setting Up Roles

To manage any settings, you must log in to the user account with appropriate permissions. A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

The EMX is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:
  - View Event Settings
  - View Local Event Log
  - Change Event Settings
  - Change Own Password
  - Change EMD Configuration
- The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 58).

Creating a Role

Create a new role when you need a new combination of permissions.

To create a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.
5. Click the Privileges tab to assign one or multiple permissions.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission you want from the Privileges list.

c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.

d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

6. Click OK to save the changes.

Now you can assign the new role to any users. See ***Creating a User Profile*** (on page 58) or ***Modifying a User Profile*** (on page 62).

Modifying a Role

You can change an existing role's settings except for the name.

To modify a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to modify by clicking it.
3. Click Edit or double-click the role. The Edit Role 'XXX' dialog appears, where XXX is the role name.

   Tip: You can also access the Edit Role 'XXX' dialog by clicking the Edit Role button in the Edit User 'XXX' dialog.

4. Modify the text shown in the Description field if necessary.
5. To change the permissions, click the Privileges tab.

   Note: You cannot change the Admin role's permissions.

6. To delete any permissions, do this:

   a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   b. Click Delete.

7. To add any permissions, do this:

   a. Click Add. The Add Privileges to Role 'XXX' dialog appears, where XXX is the role name.

   b. Select the permission you want from the Privileges list.

   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.

   d. Click Add to add the selected permission (and arguments if any).

e. Repeat Steps *a* to *d* until you add all necessary permissions.

8. To change a specific permission's arguments, do this:
   a. Select the permission by clicking it.
   b. Click Edit. The "Edit arguments of privilege 'XXX'" dialog appears, where XXX is the privilege name.

   Note: If the permission you selected does not contain any arguments, the Edit button is disabled.

   c. Select the argument you want. You can make multiple selections.
   d. Click OK.
9. Click OK to save the changes.

Deleting a Role

You can delete any role other than the Admin role.

To delete a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Chapter 5 EMX Device Management

In This Chapter

Overview 67
Naming the EMX Device 67
Displaying the Device Information 68
Setting the Date and Time 68
Specifying the Device Altitude 69
Changing the Measurement Units 70
Determining How to Display Tree Items 71
Modifying the Network Configuration 73
Modifying the Network Service Settings 79
Configuring the SMTP Settings 82
Setting Up an EMX Using Bulk Configuration 83
Firmware Upgrade 85
Network Diagnostics 88
Downloading Diagnostic Information 89
Rebooting the EMX 91
Resetting to Factory Defaults 91

Overview

Following is information on setting up and managing the EMX after the EMX device is installed.

Optionally, if you have already installed and configured an EMX and are now configuring a different EMX, you can use the Bulk Configuration feature to make the configuration process easier. See ***Setting Up an EMX Using Bulk Configuration*** (on page 83).

Naming the EMX Device

The default name for an EMX device is *EMX*, which can be changed as needed.

To change the device name:

1. In left navigation panel, click the EMX folder. The Settings page opens.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click Setup on the Settings page. The EMX Setup dialog appears.
3. Type a new name in the Device Name field.

4. Click OK to save the changes.

Displaying the Device Information

The Device Information dialog displays information specific to the EMX device that you are accessing, such as IDs and protocol versions of asset sensors.

To display the device information:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Click the tab containing the information you want to view.

Tab	Information shown
Device Information	General device information, such as model name, serial number, firmware version, hardware revision, and so on.
Asset Strips	Each asset sensor's ID, boot version, application version and protocol version.

3. Enlarge the dialog if necessary.
4. You can re-sort the list or change the columns displayed.
5. Click Close to quit the dialog.

Tip: The firmware version is also available by clicking the EMX folder in the EMX Explorer pane.

Setting the Date and Time

Set the internal clock on the EMX device manually, or link to a Network Time Protocol (NTP) server and let it set the date and time for the EMX.

To set the date and time:

1. Choose Device Settings > Date/Time. The Configure Date/Time Settings dialog appears.
2. In the Time Zone field, click the drop-down arrow, and select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.

   If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.
4. Choose one of the methods to set the date and time:

- To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
  - To set the date, delete existing numbers in the Date field and type new ones, or click the calendar icon to select a date.
  - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on. You can enter the time by deleting existing numbers and typing new ones in the hour, minute and second fields, or clicking the arrows to adjust each number.
- To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two ways to assign the NTP servers.
  - To use the DHCP-assigned NTP servers, make sure the "Always use the servers below and ignore DHCP-provided servers" checkbox is deselected. This method is usable only when either IPv4 or IPv6 DHCP is enabled.
  - To use the NTP servers that are manually specified, select the "Always use the servers below and ignore DHCP-provided servers" checkbox, and specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

Note: If the EMX device's IP address is assigned through IPv4 or IPv6 DHCP, the NTP servers can be automatically discovered. When this occurs, the data you entered in the fields of First and Second Time Server will be overridden.

5. Click OK to save the changes.

Specifying the Device Altitude

You must specify the EMX device's altitude above sea level if a Raritan differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (see "***Altitude Correction Factors (EMX)***" on page 300).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See ***Changing the Measurement Units*** (on page 70).

To specify the altitude of the EMX device:

1. In left navigation panel, click the EMX folder. The Settings page opens.

Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click Setup on the Settings page. The EMX Setup dialog appears.
3. Type an integer number in the Altitude field. Depending on the measurement unit displayed, the range of valid numbers differs.
   - For meters (m), the value ranges between 0 and 3000.
   - For feet (ft), the value ranges between 0 and 9842.
4. Click OK to save the changes.

Changing the Measurement Units

By default, the following measurement units are applied to all data shown in the EMX web interface:

- Temperature: degrees in Celsius (°C)
- Length or height: meters (m)
- Air pressure: pascal (pa)

The EMX web interface allows shows different measurement units based on user login name. That is, different users may see different measurement units displayed according to their preferences. The other alternatives for each measurement unit include:

- Temperature: degrees in Fahrenheit (°F)
- Length or height: feet (ft)
- Air pressure: psi

Determine the desired measurement unit when creating user profiles. See ***Creating a User Profile*** (on page 58). To change the measurement unit setting, you must have the administrator privileges.

To set the preferred measurement units:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Click the Preferences tab.
5. To change the temperature unit, select the desired option in the Temperature Unit field.
   - °C: This option displays the temperature in Celsius.

- °F: This option displays the temperature in Fahrenheit.

6. To change the length or height unit, select the desired option in the Length Unit field.
   - Meter: This option displays the length or height in meters.
   - Feet: This option displays the length or height in feet.
7. To change the pressure unit, select the desired option in the Pressure Unit field.
   - Pascal: This option displays the pressure value in Pascals (Pa). A Pascal is equal to one newton per square meter.
   - psi: This option displays the pressure value in psi. Psi stands for pounds per square inch.
8. Click OK to save the changes.

Determining How to Display Tree Items

By default the EMX web interface displays connected devices in the tree only if there are devices physically connected to FEATURE and RS-485 (auxiliary) ports and displays nothing if no devices are connected.

The EMX web interface allows you to determine when and how to display icons for connected and disconnected devices in the tree.

How to Display Asset Sensors

There are two ways to display connected asset sensors in the tree of the web interface:

- Asset sensors are displayed only when they are physically connected.
- Asset sensors are always displayed no matter they are physically connected or not, but their icons change to indicate the connection status.

To determine how to display connected asset sensors:

1. Click the Feature Ports folder. The Feature Ports page opens in the right pane, listing all FEATURE ports.
2. Select the number of the port that you want to configure, and click Setup. Or you can simply double-click that port number. The Feature Port Setup dialog for the selected port appears.
3. In the Detection Mode field, select the way to display connected asset sensors.
   - Disabled: When applied, disables to port and nothing connected to the port is detected.

- Auto: An icon is displayed for this port only when the EMX device detects the physical connection of the asset sensor on this port. Otherwise, nothing is displayed. This is the default approach.
- Pinned: An icon is displayed for this port all the time, but the icon image varies according to the connection status. If the connection of an asset sensor is detected on a specific Feature port, this icon is displayed on that port. If not detected, this icon appears instead. See ***Determining How to Display Tree Items*** (on page 71).

  When the Pinned checkbox is selected, click the drop-down arrow to select the device type to be displayed. Select Asset Strip for asset sensors.

4. Click OK to save the changes.

In the tree, the icon, if present, is followed by the device name if available, device type and the port number.

How to Display LHX Heat Exchangers

There are two ways to display connected Schroff® LHX heat exchangers in the tree of the web interface:

- LHX heat exchangers are displayed only when they are physically connected.
- LHX heat exchangers are always displayed no matter they are physically connected or not, but their icons change to indicate the connection status.

The EMX supports the LHX-20 and LHX-40 models.

Note: Schroff LHX Support must be enabled in order for the LHX to be displayed. See **Enabling and Disabling Schroff LHX Heat Exchanger Support** *(on page 175).*

To determine how to display connected LHX heat exchangers:

1. Click the Auxiliary Ports folder or the Feature Ports folder depending on which port you want to connect the sensor to.
2. Select the number of the port that you want to configure, and click Setup. Or you can simply double-click that port number. The Auxiliary Port Setup dialog for the selected port appears.
3. In the Detection Mode field, select the way to display connected LHX heat exchangers.
   - Disabled: When applied, disables to port and nothing connected to the port is detected.

- Auto: An icon is displayed for this port only when the EMX device detects the physical connection of the LHX heat exchanger on this port. Otherwise, nothing is displayed. This is the default approach.
- Pinned: An icon is displayed for this port all the time, but the icon image varies according to the connection status. See ***Device States and Icon Variations*** (on page 179).

  When the Pinned checkbox is selected, click the drop-down arrow to select the appropriate device type for this port: LHX 20 or LHX 40.

4. Click OK to save the changes.

In the tree, the icon, if present, is followed by the device name if available, device type and the port number or FEATURE port (if applicable).

Modifying the Network Configuration

The network settings you can change via the web interface include wired, wireless, IPv4 and/or IPv6 settings.

Modifying the Network Interface Settings

The EMX supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See ***Connecting the EMX to Your Network*** (on page 13).

Wired Network Settings

The LAN interface speed and duplex mode were set during the installation and configuration process. See Initial Network Configuration.

By default, the LAN speed and duplex mode are set to "Auto" (automatic), which works in nearly all scenarios. You can change them if there are special local requirements.

To modify the network interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wired from the list.
4. To change the LAN speed, click the drop-down arrow in the Speed field and select an option from the list.

- Auto: System determines the optimum LAN speed through auto-negotiation.
- 10 Mbit/s: The LAN speed is always 10 Mbps.
- 100 Mbit/s: The LAN speed is always 100 Mbps.

5. To change the duplex mode, click the drop-down arrow in the Duplex field and select an option from the list.
   - Auto: The EMX selects the optimum transmission mode through auto-negotiation.
   - Full: Data is transmitted in both directions simultaneously.
   - Half: Data is transmitted in one direction (to or from the EMX device) at a time.
6. Click OK to save the changes.

Tip: You can check the LAN status in the Current State field, including the speed and duplex mode.

Wireless Network Settings

Wireless SSID, PSK and BSSID parameters were set during the installation and configuration process. See Initial Network Configuration. You can change them via the web interface.

To modify the wireless interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the EMX device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See ***Connecting the EMX to Your Network*** (on page 13).
5. Type the name of the wireless access point (AP) in the SSID field.
6. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

   Note: BSSID refers to the MAC address of an access point in the wireless network.

7. In the Authentication field, click the drop-down arrow, and select an appropriate option from the list.

Option	Description
No Authentication	Select this option when no authentication data is required.
PSK	A Pre-Shared Key is required for this option. ▪ In the Pre-Shared Key field, type the PSK string.
EAP - PEAP	PEAP stands for Protected Extensible Authentication Protocol. The following authentication data is required: ▪ Inner Authentication: Only Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) is supported, allowing authentication to databases that support MSCHAPv2. ▪ Identity: Type your user name for EAP authentication. ▪ Password: Type your password for EAP authentication. ▪ CA Certificate: A third-party CA certificate must be provided for EAP authentication. Click Browse to select a valid certificate file. - To view the contents of the selected certificate file, click Show. - If the selected certificate file is invalid, click Remove. Then select a new file.

8. Click OK to save the changes.

Modifying the Network Settings

The EMX was configured for network connectivity during the installation and configuration process. See ***Configuring the EMX*** (on page 10). If necessary, you can modify any network settings using the web interface.

Selecting the Internet Protocol

The EMX device supports two types of Internet protocols -- IPv4 and IPv6. You can enable either or both Internet protocols. After enabling the desired Internet protocol(s), all but not limited to the following protocols will be compliant with the enabled Internet protocol(s):

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

To select the appropriate Internet Protocol:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IP Protocol tab.
3. Select one checkbox according to the Internet protocol(s) you want to enable:
   - IPv4 only: Enables IPv4 only on all interfaces. This is the default.
   - IPv6 only: Enables IPv6 only on all interfaces.
   - IPv4 and IPv6: Enables both IPv4 and IPv6 on all interfaces.
4. If you selected the "IPv4 and IPv6" checkbox in the previous step, you must determine which IP address is used when the DNS resolver returns both of IPv4 and IPv6 addresses.
   - IPv4 Address: Use the IPv4 addresses returned by the DNS server.
   - IPv6 Address: Use the IPv6 addresses returned by the DNS server.
5. Click OK to save the changes.

Modifying the IPv4 Settings

You must enable the IPv4 protocol before you can modify the IPv4 network settings. See ***Selecting the Internet Protocol*** (on page 76).

To modify the IPv4 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IPv4 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
DHCP	To auto-configure the EMX, select DHCP. With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Netmask ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Note: The EMX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the EMX only uses the primary IPv4 and IPv6 DNS servers.

Modifying the IPv6 Settings

You must enable the IPv6 protocol before you can modify the IPv6 network settings. See ***Selecting the Internet Protocol*** (on page 76).

To modify the IPv6 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IPv6 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
Automatic	To auto-configure EMX, select Automatic. With this option selected, you can enter a preferred host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Note: The EMX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the EMX only uses the primary IPv4 and IPv6 DNS servers.

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or the EMX may fail to connect to the given host.

Therefore, DNS server settings are important for LDAP authentication. With appropriate DNS settings, the EMX can resolve the LDAP server's name to an IP address for establishing a connection. If the *SSL encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on LDAP authentication, see ***Setting Up LDAP Authentication*** (on page 112).

Modifying the Network Service Settings

The EMX supports these network communication services: HTTPS, HTTP, Telnet and SSH.

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the command line interface.

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

In addition, the EMX also supports the SNMP protocol.

Changing the HTTP(S) Settings

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the EMX device so it is a more secure protocol than HTTP.

By default, any access to the EMX device via HTTP is automatically redirected to HTTPS. See ***Forcing HTTPS Encryption*** (on page 93).

To change the HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP. The HTTP Settings dialog appears.

2. To use a different port for HTTP or HTTPS, type a new port number in the corresponding field. Valid range is 1 to 65535.

   Warning: Different network services cannot share the same TCP port.

3. Click OK to save the changes.

Configuring the SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the EMX device. Enabling SNMP communication allows the manager to retrieve the status of the EMX device.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Trap Rule" is enabled and the trap destination has not been set yet. See ***Event Rules and Actions*** (on page 118).

To configure the SNMP communication:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Enter the trap destination information that applies to either or both trap types.
3. Select the MIB to be downloaded and browse to locate it. The SNMP MIB for your EMX is used by the SNMP manager.
4. Click OK.

Changing the SSH Settings

You can enable or disable the SSH access to the command line interface, or change the default TCP port for the SSH service. In addition, you can decide to log in using either the password or the public key over the SSH connection.

To change the SSH service settings:

1. Choose Device Settings > Network Services > SSH. The SSH Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the SSH application, select the Enable SSH checkbox. To disable it, deselect the checkbox.
4. To select a different authentication method, select one of the checkboxes.
   - Allow password authentication only: Enables the password-based login only.

- Allow public key authentication only: Enables the public key-based login only.
- Allow password and public key authentication: Enables both the password- and public key-based login. This is the default.

5. Click OK to save the changes.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating a User Profile*** (on page 58).

Changing the Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the default TCP port for the Telnet service.

To change the Telnet service settings:

1. Choose Device Settings > Network Services > Telnet. The Telnet Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the Telnet application, select the Enable Telnet Access checkbox. To disable it, deselect the checkbox.
4. Click OK to save the changes.

Enabling Service Advertisement

The EMX advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and mDNS (multicast DNS). The advertised services are discovered by clients that have implemented DNS-SD and mDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

This feature is enabled by default.

To enable Service Advertisement:

1. Click Device Settings > Network Services > Service Advertisement

2. Click "Yes" in the "Changing Service Advertisement" confirmation dialog box. The feature is enabled and the Service Advertisement checkbox is selected in the menu.

To disable Service Advertisement:

1. Click Device Settings > Network Services > Service Advertisement.
2. Click "No" in the "Changing Service Advertisement " confirmation dialog box. The feature is disabled and the Service Advertisement checkbox is deselected in the menu.

Configuring the SMTP Settings

The EMX can be configured to send alerts or event messages to a specific administrator by email. To do this, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

Note: See **Configuring Event Rules** *(see "***Event Rules and Actions***" on page 118) for information on creating event rules to send email notifications.*

To set the SMTP server settings:

1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the Number of Sending Retries field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.
7. If your SMTP server requires password authentication, do this:
   a. Select the Server Requires Authentication checkbox.
   b. Type a user name in the User Name field.
   c. Type a password in the Password field.
8. Now that you have set the SMTP settings, you can test it to ensure it works properly. Do the following:

a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.

b. Click Send Test Email.

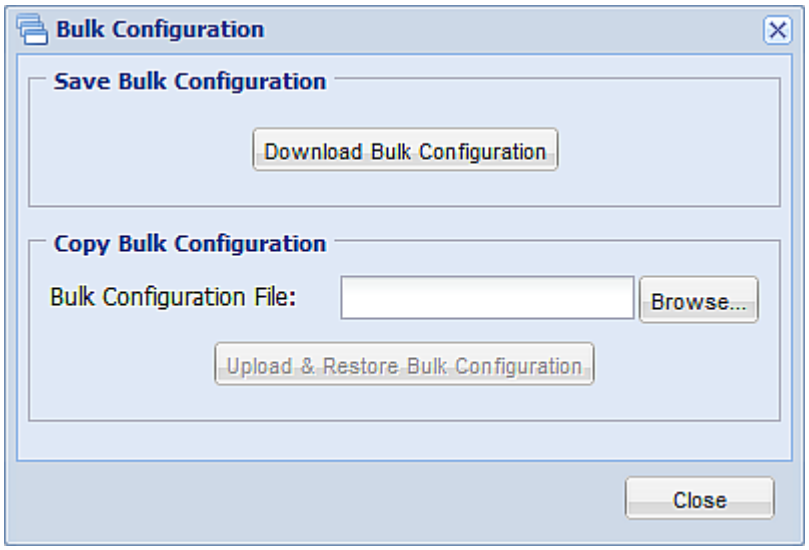
9. Click OK to save the changes.
10. Check if the recipient(s) receives the email successfully.

Setting Up an EMX Using Bulk Configuration

Use this feature if you have already set up an EMX and are now setting up another. The Bulk Configuration feature lets you save the settings of a configured EMX device to your PC. You can use this configuration file to:

- Copy that configuration to other EMX devices of the same model and firmware version.
- Restore the settings of the same EMX device to previous configuration.

You must have the administrator privileges to save and copy the EMX configurations.



Saving an EMX Configuration

A source device is an already configured EMX device that is used to create a configuration file containing the settings that can be shared between EMX devices. These settings include user and role configurations, event rules, security settings, and so on.

This file does NOT contain device-specific information, including:

- Device name
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Environmental sensor names
- Environmental sensor states and values
- SSL Certificate
- Asset management sensor names and rack unit names
- SNMP name, location, and contact
- Server monitor entries

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the EMX devices in a different time zone than the source device.

To save a configuration file:

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
2. Click Download Bulk Configuration.
3. When the web browser prompts you to open or save the configuration file, click Save. Choose a suitable location and save the configuration file to your PC.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

Copying a EMX Configuration

A target device is an EMX device that loads another EMX device's configuration file.

Copying an EMX configuration to a target device adjusts that EMX device's settings to match those of the source EMX device. In order to successfully copy an EMX configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target EMX device must be of the same model type as the source EMX device.
- The target EMX device must be running the same firmware version as the source EMX device.

To copy a EMX Configuration:

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See ***Firmware Upgrade*** (on page 85).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse and select the configuration file stored on your PC.
5. Click Upload & Restore Bulk Configuration to copy the file.
6. A message appears, prompting you to confirm the operation. Click Yes to confirm the operation.
7. Wait until the EMX device resets and the Login page re-appears, indicating that the configuration copy is complete.

Firmware Upgrade

You may upgrade your EMX device to benefit from the latest enhancements, improvements and features.

The EMX firmware files are available on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).

Updating the Firmware

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the EMX device's firmware.

If applicable to your model, download the latest firmware file from the Raritan website, read the release notes, then start the upgrade. If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Warning: Do NOT perform the firmware upgrade over a wireless connection.

To update the firmware:

1. Choose Maintenance > Update Firmware. The Firmware Update dialog appears.
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

   Warning: Do NOT power off the EMX device during the update.

   During the firmware update:

   - A progress bar appears in the web interface, indicating the update status.
   - No users can successfully log in to the EMX.
   - In the web interface, all logged-in users see the EMX time out message, and the "disconnected" state is shown in the status bar.
   - The user management operation, if any, is forced to suspend.
7. When the update is complete, a message appears, indicating the update is successful.
8. The EMX device resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

Note 2: If you are using the EMX with an SNMP manager, you should re-download the EMX MIB after the firmware update. This ensures your SNMP manager has the correct MIB for the latest release you are using. See **Using SNMP** *(on page 182).*

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the EMX device.

This history indicates when a firmware upgrade event occurred, the prior and new versions associated with the firmware upgrade event, and the upgrade result.

To view the firmware update history:

1. Choose Maintenance > View Firmware Update History. The Firmware Update History dialog appears, with the following information displayed.
   - Date and time of the firmware upgrade event
   - Previous firmware version
   - Update firmware version
   - Firmware upgrade result
2. You may change the number of displayed columns or re-sort the list for better viewing the data. See Changing the View of a List.
3. To view the details of any firmware upgrade event, select it and click Details, or simply double-click the event. The Firmware Update Details dialog appears, showing detailed information of the selected event.
4. Click Close to quit the dialog.

Full Disaster Recovery

If the firmware upgrade fails, causing the EMX device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7 and Linux. In addition, an appropriate EMX firmware file is required in the recovery procedure.

Updating the Asset Sensor Firmware

After connecting the asset sensor to the EMX device, it automatically checks its own firmware version against the version of the asset sensor firmware stored in the EMX firmware. If two versions are different, the asset sensor automatically starts downloading the new firmware from the EMX device to upgrade its own firmware.

During the firmware upgrade, the following events take place:

- The asset sensor is completely lit up, with the blinking LEDs changing the color from red to green.
- A firmware upgrade process is indicated in the EMX web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

Network Diagnostics

The EMX provides the following tools in the web interface for diagnosing potential networking issues.

- Ping
- Trace Route
- List TCP Connections

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 292).*

Pinging a Host

The Ping tool is useful for checking whether a host is accessible through the network or Internet.

To ping a host:

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 10 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

Trace Route lets you find out the route over the network between two hosts or systems.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > Trace Route. The Trace Route to Host dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. Click Run. A dialog appears, displaying the Trace Route results.
4. Click Close to quit the dialog.

Listing TCP Connections

You can use the "List TCP Connections" to display a list of TCP connections.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > List TCP Connections. The TCP connections dialog appears.
2. Click Close to quit the dialog.

Downloading Diagnostic Information

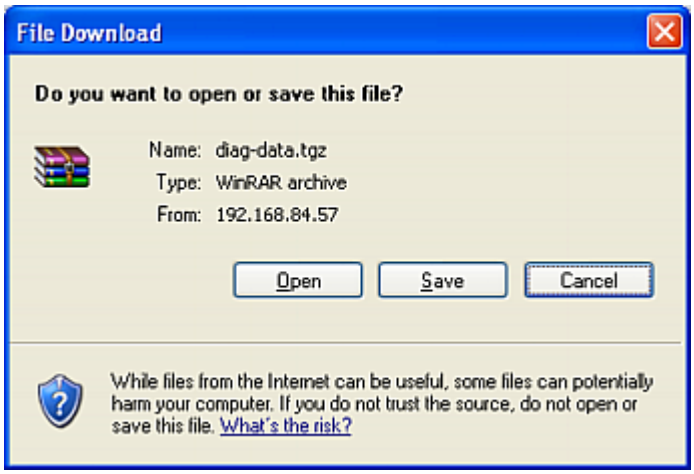
Important: This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the EMX device to a client machine. The file is compressed into a .tgz file and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges.

To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic Information. The File Download dialog appears.



2. Click Save. The Save As dialog appears.
3. Navigate to the desired directory and click Save.
4. E-mail this file as instructed by Raritan Technical Support.

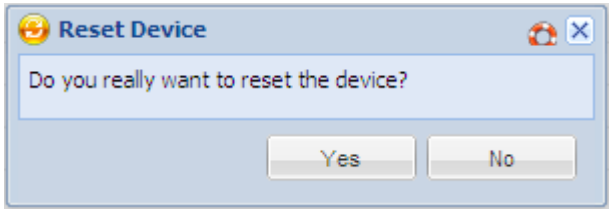
Rebooting the EMX

You can remotely reboot the EMX device via the web interface. Rebooting the EMX does not reset the configuration of the device as is done during a factory reset.

Note: Rebooting the EMX snapshots taken via webcam.

To reboot the device:

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reset the EMX.
3. A message appears with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the reset is complete, the Login page opens. Now you can log back in to the EMX device.

Note: If you are not redirected to the Login page after the reset is complete, click the underlined text "this link" in the message.

Resetting to Factory Defaults

For security reasons, the EMX device can be reset to factory defaults only at the local console.

Important: Exercise caution before resetting the EMX to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on.

You can use either the reset button or the command line interface (CLI) to reset the EMX.

To reset to factory defaults using the reset button:

1. Connect a computer to the EMX device. See ***Connecting the EMX to a Computer*** (on page 11).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the EMX.

3. Press (and release) the Reset button of the EMX device while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.
4. Type *defaults* to reset the EMX to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Chapter 6 Security

In This Chapter

Access Security Control 93
Setting Up an SSL Certificate.....107
Setting Up LDAP Authentication 112

Access Security Control

The EMX provides tools to control access. You can require HTTPS encryption, enable the internal firewall and create firewall rules, and create login limitations.

Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up an SSL Certificate** *(on page 107) and* **Setting Up LDAP Authentication** *(on page 112).*

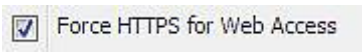
Forcing HTTPS Encryption

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the EMX device so it is a more secure protocol than HTTP.

You can force users to access the EMX web interface through the HTTPS protocol only. By default, this protocol is enabled.

To force HTTPS access to the web interface:

1. Choose Device Settings > Security > Force HTTPS for Web Access.
2. A message appears, prompting you to confirm the operation. Click Yes to enforce the HTTPS service.
3. Choose Device Settings > Security to verify the "Force HTTPS for Web Access" checkbox is selected as shown in this diagram.



If the checkbox is not selected, repeat these steps.

After enabling the HTTPS protocol, all access attempts using HTTP are redirected to HTTPS automatically.

Configuring the Firewall

The EMX has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the EMX device. By default the firewall is disabled.

To configure the firewall:

1. Enable the firewall. See ***Enabling the Firewall*** (on page 94).
2. Set the default policy. See ***Changing the Default Policy*** (on page 94).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See ***Creating Firewall Rules*** (on page 95).

Changes made to firewall rules take effect immediately. Any unauthorized IP activities cease instantly.

Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the device.

Enabling the Firewall

The firewall rules, if any, take effect only after the firewall is enabled.

To enable the EMX firewall:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To enable the IPv4 firewall, click the IPv4 tab, and select the Enable IPv4 Access Control checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the Enable IPv6 Access Control checkbox.
4. Click OK to save the changes.

Changing the Default Policy

After enabling the firewall, the default policy is to accept traffic from all IP addresses. This means only IP addresses discarded by a specific rule will NOT be permitted to access the EMX.

You can change the default policy to Drop or Reject, in which case traffic from all IP addresses is discarded except the IP addresses accepted by a specific rule.

To change the default policy:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.

2. To determine the default policy for IPv4 addresses:
   a. Click the IPv4 tab if necessary.
   b. Ensure the Enable IPv4 Access Control checkbox is selected.
   c. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
      - Accept: Accepts traffic from all IPv4 addresses.
      - Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
      - Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.
3. To determine the default policy for IPv6 addresses:
   a. Click the IPv6 tab.
   b. Ensure the Enable IPv6 Access Control checkbox is selected.
   c. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
      - Accept: Accepts traffic from all IPv6 addresses.
      - Drop: Discards traffic from all IPv6 addresses, without sending any failure notification to the source host.
      - Reject: Discards traffic from all IPv6 addresses, and an ICMP message is sent to the source host for failure notification.
4. Click OK to save the changes. The new default policy is applied.

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic intended for the EMX, based on the IP address of the host sending the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches the EMX device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by the EMX.

- **Subnet mask may be required.**

  When typing the IP address, you may or may not need to specify BOTH the address and a subnet mask. The default subnet mask is /32 (that is, 255.255.255.255). You must specify a subnet mask only when it is not the same as the default. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IP addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IP addresses entered are within the scope.

To create firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Click the IPv4 tab for creating firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Create specific rules. See the table for different operations.

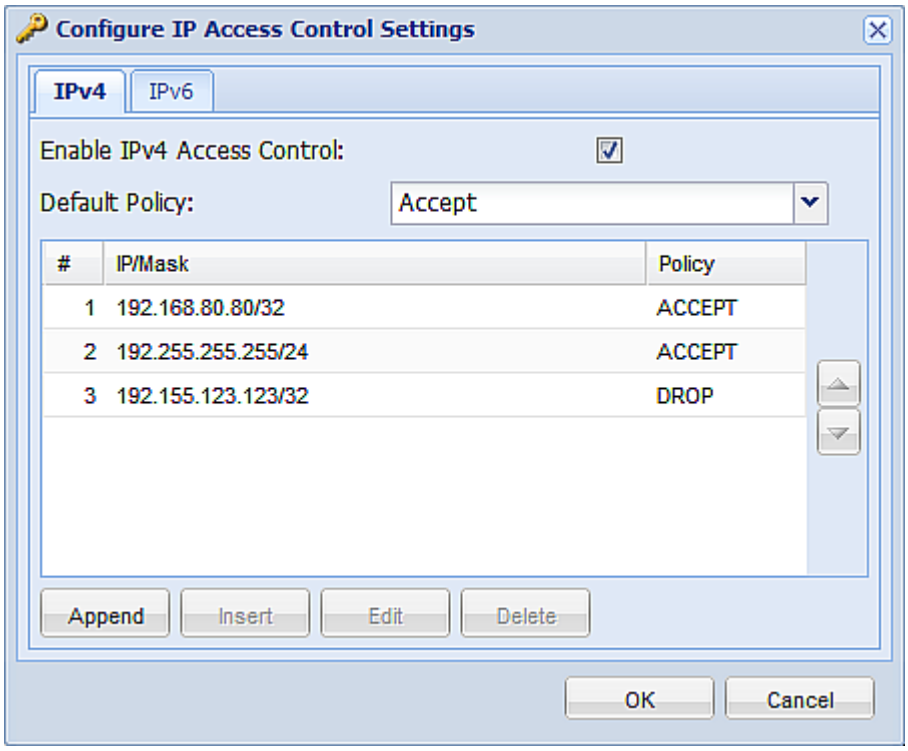
Action	Procedure

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from the specified IP address(es).
	  ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
	  ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.
	▪ Click OK to save the changes.
	The system automatically numbers the rule.

Action	Procedure

Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
	▪ Click Insert. The "Insert new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from the specified IP address(es).
	  ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
	  ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.
	▪ Click OK to save the changes.
	The system inserts the rule and automatically renumbers the following rules.

5. When finished, the rules appear in the Configure IP Access Control Settings dialog.



6. Click OK to save the changes. The rules are applied.

Editing Firewall Rules

When an existing firewall rule requires updates of IP address range and/or policy, modify them accordingly.

To modify a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule to be modified in the rules list.
5. Click Edit or double-click the rule. The Edit Rule dialog appears.
6. Make changes to the information shown.
7. Click OK to save the changes.
8. Click OK to quit the Configure IP Access Control Settings dialog, or the changes are lost.

Sorting Firewall Rules

The rule order determines which one of the rules matching the same IP address is performed.

To sort the firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select a specific rule by clicking it.
5. Click or to move the selected rule up or down until it reaches the desired location.
6. Click OK to save the changes.

Deleting Firewall Rules

When any firewall rules become obsolete or unnecessary, remove them from the rules list.

To delete a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule that you want to delete. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to remove the selected rule(s) from the rules list.
7. Click OK to save the changes.

Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access the EMX and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who log in using the same user name at the same time, and force users to create strong passwords.

Enabling User Blocking

User blocking determines how many times a user can attempt to log in to the EMX and fail authentication before the user's login is blocked.

Note that this function applies only to local authentication instead of authentication through external AA servers.

Note: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command via a serial connection. See **Unblocking a User** *(on page 290).*

To enable user blocking:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the User Blocking section.

3. To enable the user blocking feature, select the "Block user on login failure" checkbox.
4. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user's login is blocked from accessing the EMX device.
5. To determine how long the login is blocked, select the desired length of time from the drop-down list in the "Block timeout" field. The following describes available options.
   - Infinite: This option sets no time limit on blocking the login.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.

   Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.
6. Click OK to save the changes.

Enabling Login Limitations

Login limitations determine whether more than one person can use the same login name at the same time, and how long users are permitted to stay idle before being forced to log out.

To enable login limitations:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the Login Limitations section.
3. To prevent more than one person from using the same login at the same time, select the "Prevent concurrent login with same username" checkbox.
4. To adjust how long users can remain idle before they are forcibly logged out by the EMX, select a time option in the Idle Timeout Period field. The default is 10 minutes.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.

5. Click OK to save the changes.

Tip: Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the EMX.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the EMX device. By default, strong passwords should be at least eight characters long and contain upper- and lower-case letters, numbers, and special characters, such as @ or &.

To force users to create strong passwords:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Strong Passwords checkbox to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of restricted passwords in history	= 5

Note: The maximum password length accepted by the EMX is 32 characters.

3. Make necessary changes to the default settings.
4. Click OK to save the changes.

Enabling Password Aging

Password Aging determines whether users are required to change passwords at regular intervals. The default interval is 60 days.

To force users to change passwords regularly:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Password Aging checkbox to enable the password aging feature.
3. To determine how often users are requested to change their passwords, select a number of days in the Password Aging Interval field. Users are required to change their password every time that number of days has passed.

   Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "9 d" to set the password aging time to 9 days.

4. Click OK to save the changes.

Setting Up Role-Based Access Control Rules

Role-based access control rules are similar to firewall rules, except they are applied to members sharing a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

To set up role-based access control rules:

1. Enable the feature. See ***Enabling the Feature*** (on page 102).
2. Set the default policy. See ***Changing the Default Policy*** (on page 103).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See ***Creating Role-Based Access Control Rules*** (on page 104).

Changes made do not affect users currently logged in until the next login.

Enabling the Feature

You must enable this access control feature before any relevant rule can take effect.

To enable role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.

2. To enable the IPv4 firewall, click the IPv4 tab, and select the Enable Role Based Access Control for IPv4 checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the Enable Role Based Access Control for IPv6 checkbox.
4. Click OK to save the changes.

Changing the Default Policy

The default policy is to accept all traffic from all IP addresses regardless of the role applied to the user.

To change the default policy:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To determine the default policy for IPv4 addresses:
   a. Click the IPv4 tab if necessary.
   b. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected.
   c. Select the action you want from the Default Policy drop-down list.
      - Allow: Accepts traffic from all IPv4 addresses regardless of the user's role.
      - Deny: Drops traffic from all IPv4 addresses regardless of the user's role.
3. To determine the default policy for IPv6 addresses:
   a. Click the IPv6 tab.
   b. Ensure the Enable Role Based Access Control for IPv6 checkbox is selected.
   c. Select the action you want from the Default Policy drop-down list.
      - Allow: Accepts traffic from all IPv6 addresses regardless of the user's role.
      - Deny: Drops traffic from all IPv6 addresses regardless of the user's role.
4. Click OK to save the changes.

Creating Role-Based Access Control Rules

Role-based access control rules accept or drop traffic, based on the user's role and IP address. Like firewall rules, the order of rules is important, since the rules are executed in numerical order.

To create role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Click the IPv4 tab for creating firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Create specific rules:

Action	Do this...

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type a starting IP address in the Starting IP Address field.
	▪ Type an ending IP address in the Ending IP Address field.
	▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.
	▪ Select Allow or Deny from the drop-down list in the Policy field.
	  ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
	  ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role
	▪ Click OK to save the changes.
	The system automatically numbers the rule.

Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field.

Action	Do this...

	▪ Type an ending IP address in the Ending IP Address field.
	▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only.
	▪ Select Allow or Deny from the drop-down list in the Policy field.
	  ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role
	  ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role
	▪ Click OK to save the changes.
	The system inserts the rule and automatically renumbers the following rules.

5. Click OK to save the changes.

Editing Role-Based Access Control Rules

You can modify existing rules when these rules do not meet your needs.

To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Select the rule to be modified in the rules list.
5. Click Edit or double-click the rule. The Edit Rule dialog appears.
6. Make changes to the information shown.
7. Click OK to save the changes.

Sorting Role-Based Access Control Rules

Similar to firewall rules, the order of role-based access control rules determines which one of the rules matching the same IP address is performed.

To sort role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Select a specific rule by clicking it.
5. Click or to move the selected rule up or down until it reaches the desired location.
6. Click OK to save the changes.

Deleting Role-Based Access Control Rules

When any access control rule becomes unnecessary or obsolete, remove it.

To delete a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Select the rule to be deleted in the rules list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
7. Click OK to save the changes.

Setting Up an SSL Certificate

Having an X.509 digital certificate ensures that both parties in an SSL connection are who they say they are.

To obtain a certificate for the EMX, create a Certificate Signing Request (CSR) and submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with an SSL certificate, which you must install on the EMX device.

Note: See **Forcing HTTPS Encryption** *(on page 93) for instructions on forcing users to employ SSL when connecting to the EMX.*

A CSR is not required in either of the following scenarios:

- You decide to generate a *self-signed* certificate on the EMX device.
- Appropriate, valid certificate and key files have been available.

Certificate Signing Request

When appropriate certificate and key files for the EMX are NOT available, one of the alternatives is to create a CSR and private key on the EMX device, and send the CSR to a CA for signing the certificate.

Creating a Certificate Signing Request

Follow this procedure to create the CSR for your EMX device.

To create a CSR:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.
   - In the Subject section:

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your EMX device.

Field	Type this information
Email Address	An email address where you or another administrative user can be reached.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields. If you generate a CSR without values entered in the required fields, you cannot obtain third party certificates.

- In the Key Creation Parameters section:

Field	Do this
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the EMX device's response.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**
Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional, and the value should be 4 to 64 characters long. The password is case sensitive, so ensure you capitalize the letters correctly.
Confirm Challenge	Type the same password again for confirmation.

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.
5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.
   a. You are prompted to open or save the file. Click Save to save it on your computer.
   b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.
   c. If desired, click Delete Certificate Signing Request to remove the CSR file permanently from the EMX device.
6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

After the CA provides a signed certificate according to the CSR you submitted, you must install it on the EMX device.

To install the certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. In the Certificate File field, click Browse to select the certificate file provided by the CA.
4. Click Upload. The certificate is installed on the EMX device.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the EMX device are unavailable, the alternative other than submitting a CSR to the CA is to generate a self-signed certificate.

To create and install a self-signed certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your EMX device.
Email Address	An email address where you or another administrative user can be reached.

Field	Type this information
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the EMX device's response.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate is valid in this field.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear after the Self Sign checkbox is selected.

4. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.
5. You can also do any of the following:
   - Click "Install Key and Certificate" to immediately install the self-signed certificate and private key. When any confirmation and security messages appear, click Yes to continue.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

   - To download the self-signed certificate or private key, click Download Certificate or Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
   - To remove the self-signed certificate and private key permanently from the EMX device, click "Delete Key and Certificate".
6. If you installed the self-signed certificate in Step 5, after the installation completes, the EMX device resets and the login page re-opens.

Installing Existing Key and Certificate Files

If the SSL certificate and private key files are already available, you can install them directly without going through the process of creating a CSR or a self-signed certificate.

To install the existing key and certificate files:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.

3. Select the "Upload Key and Certificate" checkbox. The Key File and Certificate File fields appear.
4. In the Key File field, click Browse to select the private key file.
5. In the Certificate File field, click Browse to select the certificate file.
6. Click Upload. The selected files are installed on the EMX device.

   Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

7. Click Close to quit the dialog.

Downloading Key and Certificate Files

You can download the key and certificate files currently installed on the EMX device for backup or other operations. For example, you can install the files on a replacement EMX device, add the certificate to your browser and so on.

To download the certificate and key files from an EMX device:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. The Active SSL Certificate tab should open. If not, click it.
3. Click Download Key to download the private key file installed on the EMX device. You are prompted to open or save the file. Click Save to save it on your computer.
4. Click Download Certificate to download the certificate file installed on the EMX device. You are prompted to open or save the file. Click Save to save it on your computer.
5. Click Close to quit the dialog.

Setting Up LDAP Authentication

For security purposes, users attempting to log in to the EMX must be authenticated. The EMX supports the access using one of the following authentication mechanisms:

- Local database of user profiles on the EMX device
- Lightweight Directory Access Protocol (LDAP)

By default, the EMX is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user. If you prefer to use an external LDAP server, you must:

- Provide the EMX with information about the LDAP server.
- Create user profiles for users who are authenticated externally because a user profile on the EMX device determines the role(s) applied to the user, and determines the permissions for the user accordingly.

When configured for LDAP authentication, all EMX users must have an account on the LDAP server. Local-authentication-only users will have no access to the EMX except for the admin, who always can access the EMX.

Gathering the LDAP Information

It requires knowledge of your LDAP server and directory settings to configure the EMX for LDAP authentication. If you are not familiar with the settings, consult your LDAP administrator for help.

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over SSL) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*

  - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Adding the LDAP Server Settings

To activate and use external LDAP/LDAPS server authentication, enable LDAP authentication and enter the information you have gathered for any LDAP/LDAPS server.

Note: An LDAPS server refers to an SSL-secured LDAP server.

To add the LDAP/LDAPS server settings:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. IP Address / Hostname - Type the IP address or hostname of your LDAP/LDAPS authentication server.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.
5. Type of external LDAP/LDAPS server. Choose from among the options available:
   - OpenLDAP
   - Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
6. LDAP over SSL - Select this checkbox if you would like to use SSL. Secure Sockets Layer (SSL) is a cryptographic protocol that allows the EMX to communicate securely with the LDAP/LDAPS server.
7. Port - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
8. SSL Port - The default is 636. Either use the default port or specify another port. This field is enabled when the "LDAP over SSL" checkbox is selected.

9. Use only trusted LDAP Server Certificates - Select this checkbox if you would like to use a trusted LDAP server certificate file, that is, a certificate file signed by the CA. When NOT selected, you can use all LDAP/LDAPS server certificates, including a self-signed certificate file. A certificate file is required after enabling this option.
10. Server Certificate - Consult your authentication server administrator to get the CA certificate file for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This file is required when the "Use only trusted LDAP Server Certificates" checkbox is selected.

    Tip: You can first upload the CA certificate file for a future use before selecting the "Use only trusted LDAP Server Certificates" checkbox, and then select the checkbox when you need to utilize the certificate file.

11. Anonymous Bind - For "OpenLDAP," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, select this checkbox.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
12. Use Bind Credentials - For "Microsoft Active Directory," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, deselect this checkbox. By default it is deselected.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, select this checkbox.
13. Bind DN - Specify the DN of the user who is permitted to search the LDAP directory in the defined search base. This information is required only when the Use Bind Credentials checkbox is selected.
14. Bind Password and Confirm Bind Password - Enter the Bind password in the Bind Password field first and then the Confirm Bind Password field. This information is required only when the Use Bind Credentials checkbox is selected.
15. Base DN for Search - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
16. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
    - Login name attribute (also called AuthorizationString)
    - User entry object class

- User search subfilter (also called BaseSearch)

Note: The EMX will preoccupy the login name attribute and user entry object class with default values, which should not be changed unless required.

17. Active Directory Domain - Type the name of the Active Directory Domain. For example, testradius.com. Consult with your Active Directory Administrator for a specific domain name.
18. To verify if the LDAP/LDAPS configuration is done correctly, you may click Test Connection to check whether the EMX can connect to the LDAP/LDAPS server successfully.

Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.

19. Click OK to save the changes. The new LDAP server is listed in the Authentication Settings dialog.
20. To add additional LDAP/LDAPS servers, repeat Steps 3 to 19.
21. Click OK to save the changes. The LDAP authentication is now in place.

Note: If the EMX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the EMX and the LDAP server to use the same NTP server.

More Information about AD Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see ***LDAP Configuration Illustration*** (on page 303).

Sorting the LDAP Access Order

The order of the LDAP list determines the access priority of remote LDAP/LDAPS servers. The EMX first tries to access the top LDAP/LDAPS server in the list for authentication, then the next one if the access to the first one fails, and so on until the EMX device successfully connects to one of the listed LDAP/LDAPS servers.

Note: After successfully connecting to one LDAP/LDAPS server, the EMX STOPS trying to access the remaining LDAP/LDAPS servers in the list regardless of the user authentication result.

To re-sort the LDAP server access list:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server whose priority you want to change.

3. Click "Move up" or "Move down" until the selected server reaches the desired position in the list.
4. Click OK to save the changes.

Testing the LDAP Server Connection

You can test the connection to any LDAP/LDAPS server to verify the server accessibility or the validity of the authentication settings.

To test the connection to an LDAP/LDAPS server:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to test.
3. Click Test Connection to start the connection test.

Editing the LDAP Server Settings

If the configuration on any LDAP/LDAPS server has been changed, such as the port number, bind DN and password, you must modify the LDAP/LDAPS settings on the EMX device accordingly, or the authentication fails.

To modify the LDAP authentication configuration:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to edit.
3. Click Edit. The Edit LDAP Server Configuration dialog appears.
4. Make necessary changes to the information shown.
5. Click OK to save the changes.

Deleting the LDAP Server Settings

You can delete the authentication settings of a specific LDAP/LDAPS server when the server is not available or used for remote authentication.

To remove one or multiple LDAP/LDAPS servers:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP/LDAPS server that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.

4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click OK to save the changes.

Disabling the LDAP Authentication

When the remote authentication service is disabled, the EMX authenticates users against the local database stored on the EMX device.

To disable the LDAP authentication service:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Local Authentication radio button.
3. Click OK to save the changes.

Enabling LDAP and Local Authentication Services

To make authentication function properly all the time -- even when external authentication is not available, you can enable both the local and remote authentication services.

When both authentication services are enabled, the EMX follows these rules for authentication:

- When any of the LDAP/LDAPS servers in the access list is accessible, the EMX authenticates against the connected LDAP/LDAPS server only.
- When the connection to every LDAP/LDAPS server fails, the EMX allows authentication against the local database.

To enable both authentication services:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Ensure the LDAP radio button has been selected.
3. Select the "Use Local Authentication if Remote Authentication service is not available" checkbox.
4. Click OK to save the changes.

Chapter 7 Event Rules, Event Actions and Application Logs

In This Chapter

Event Rules and Actions 118
Event Logging.....138
Viewing the Communication Log.....140

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of and react to a change in conditions. This event notification or reaction is an "event rule."

The EMX is shipped with two built-in event rules, which cannot be deleted.

- System Event Log Rule: This rule causes ANY event occurred to the EMX to be recorded in the internal log. The rule is enabled by default.
- System SNMP Trap Rule: This rule causes SNMP traps to be sent to specified IP addresses or hosts when ANY event occurs to the EMX. The rule is disabled by default.

If these two do not satisfy your needs, you can create additional rules to respond to different events.

Note: Internet Explorer® 8 (IE8) does not use compiled JAVA script. When using IE8 to create or change event rules, the CPU performance may be degraded, resulting in the appearance of the connection time out message. When this occurs, click Ignore to continue.

Components of an Event Rule

An event rule defines what the EMX does in certain situations and is composed of two parts:

- Event: This is the situation where the EMX or part of it meets a certain condition. For example, the temperature sensor exceeds the warning threshold.
- Action: This is the response to the event. For example, the EMX notifies the system administrator of the event and records the event in the log.

Note: Asset management sensor event rules must be recreated after an EMX firmware upgrade.

Creating an Event Rule

The best way to create a new set of event rule, in sequence, is:

- Create actions for responding to one or multiple events.
- Create rules to determine what actions are taken when these events occur.

Creating Rules

After required actions are available, you can create event rules to determine what actions are taken to respond to specific events.

By default, the EMX provides two built-in event rules -- System Event Log Rule and System SNMP Trap Rule. If the built-in rules do not satisfy you needs, create new ones.

To create event rules:

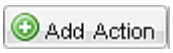
1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, click New Rule.
3. In the "Rule name" field, type a new name for identifying the rule. The default name is New Rule <number>, where <number> is a sequential number.
4. Select the Enabled checkbox to enable this event rule.
5. Click Event to select an event for which you want to trigger an action. A pull-down menu showing all types of events appears.
   - Select the desired event type from the pull-down menu, and if a submenu appears, continue the navigation until the desired event is selected.

   Note: The option <Any sub-event> refers to all events/items listed on the same submenu, <Any slot> refers to all slots, <Any server> refers to all servers, and <Any user> refers to all users.
6. According to the event you selected in the previous step, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or asset tag connections or disconnections	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The EMX takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The EMX takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The EMX takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts).
Discrete (on/off) sensor state change	Available radio buttons include "Alarmed," "No longer alarmed" and "Both." ▪ Alarmed: The EMX takes the action only when the chosen sensor enters the alarmed state, that is, the abnormal state. ▪ No longer alarmed: The EMX takes the action only when the chosen sensor returns to normal. ▪ Both: The EMX takes the action both when the chosen sensor enters or quits the alarmed state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The EMX takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The EMX takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The EMX takes the action both when the chosen sensor becomes unavailable or available.

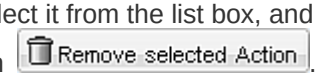
Event types	Radio buttons
Network interface link state	Available radio buttons include "Link state is up," "Link state is down" and "Both." ▪ Link state is up: The EMX takes the action only when the network link state changes from down to up. ▪ Link state is down: The EMX takes the action only when the network link state changes from up to down. ▪ Both: The EMX takes the action whenever the network link state changes.
Function enabled or disabled	Available radio buttons include "Enabled," "Disabled" and "Both." ▪ Enabled: The EMX takes the action only when the chosen function is enabled. ▪ Disabled: The EMX takes the action only when the chosen function is disabled. ▪ Both: The EMX takes the action when the chosen function is either enabled or disabled.
User login or logout	Available radio buttons include "Logged in," "Logged out," and "Both." ▪ Logged in: The EMX takes the action only when the selected user logs in. ▪ Logged out: The EMX takes the action only when the selected user logs out. ▪ Both: The EMX takes the action both when the selected user logs in and logs out.
Server monitoring event	Available radio buttons include "Monitoring started," "Monitoring stopped," and "Both." ▪ Monitoring started: The EMX takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The EMX takes the action only when the monitoring of any specified server stops. ▪ Both: The EMX takes the action when the monitoring of any specified server starts or stops.

Event types	Radio buttons
Server reachability	Available radio buttons include "Unreachable," "Reachable," and "Both." ▪ Unreachable: The EMX takes the action only when any specified server becomes inaccessible. ▪ Reachable: The EMX takes the action only when any specified server becomes accessible. ▪ Both: The EMX takes the action when any specified server becomes either inaccessible or accessible.

7. In the Actions field, click the drop-down arrow, select the desired action from the list, and click the Add Action button 

to add the action.

   The added action will be listed in the list box to the right of the Actions filed.

8. To add additional actions, repeat Step 7.
9. To remove any added action, select it from the list box, and click the "Remove selected Action" button 

.
10. Click Save to save the new event rule.

    Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

11. Repeat Steps 2 to 10 to create additional event rules.
12. Click Close to quit the dialog.

Note: Asset management sensor event rules must be recreated after an EMX firmware upgrade.

Creating Actions

The EMX comes with two built-in actions:

- System Event Log Action: This action records the selected event in the internal log when the event occurs.
- System SNMP Trap Action: This action sends SNMP traps to one or multiple IP addresses after the selected event occurs.

Note: No IP addresses are specified for the "System SNMP Trap Action" by default so you must specify IP addresses before applying this action to any event rule.

The built-in actions cannot be deleted. If these actions do not satisfy your needs, then create new ones.

To create new actions:

1. Click the Actions tab.
2. Click New Action.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number.
4. In the Action field, click the drop-down arrow, and select the desired action from the list. See below for descriptions.
5. Click Save.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

6. Click Close to quit the dialog.

Option	Description
Execute an action group	This option allows you to select what action will be performed when an event is triggered. • SMS • System Event Action Log • System SNMP Trap Action *Note: A Cinterion® GSM MC52i modem must be plugged in to the EMX in order to send SMS messges.*
Log event message	This option records the selected events in the internal log.

Option	Description
Send Snapshots via Email	This option notifies one or multiple persons of the selected events by emailing snapshots or videos captured by a connected Logitech® QuickCam® Pro 9000 Webcam (if any). ▪ In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses. ▪ To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox. To use a different SMTP server, select the Use Custom SMTP Settings checkbox. If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 82) for the information of each field. ▪ Select the webcam that is capturing the images you want sent in the email. ▪ In the Number of Snapshots field, enter the number of snapshots to be included in the sequence of images that are taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action. ▪ In the Snapshots/Mail field, enter the maximum number of snapshots from the sequence to be sent at one time in the email. ▪ In the "Time before first Snapshot (s):" field, enter the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots. ▪ In the "Time between Snapshots (s):" field, enter the amount of time between when each snapshot is taken.

Option	Description
Send EMail	This action sends an email to specified recipients notifying them that the event has occurred. • In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses. • To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox. To use a different SMTP server, select the Use Custom SMTP Settings checkbox. If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 82) for the information of each field. Default messages are sent based on the event. See ***Default Log Messages*** (on page 129) for a list of default log messages and events that trigger them. • If needed, select the Use Custom Log Message checkbox, and then create a custom message in the provided field. See ***Creating Custom Email Messages*** (on page 127).
Send SNMP trap	This option sends SNMP traps to one or multiple SNMP managers. • You can specify up to 3 SNMP trap destinations in the Host *x* fields, where *x* is a number between 1 and 3. • Specify a port number for each destination in the Port *x* fields, where *x* is a number between 1 and 3. • Specify a community string for each destination in the Community *x* fields, where *x* is a number between 1 and 3.
Syslog message	This option makes the EMX automatically forward event messages to the specified syslog server. ▪ In the "Syslog server" field, specify the IP address to which syslog is forwarded. ▪ In the Port field, specify an appropriate port number.

Option	Description
Send SMS message	Sends a text message to the designated mobile phone. A Cinterion® GSM MC52i modem must be plugged in to the EMX in order to send SMS messges. *Note: The EMX cannot receive SMS messages.* *Note: Only English is supported for SMS messages.* • Enter the phone number in the Recipient's Phone Number field.
Record Snapshots to Webcam Storage	This option allows you to define an action that starts or stops a specific webcam from taking snapshots. ▪ Enter the total number of snapshots to be taken when the event occurs. The maximum amount of snapshots that can be stored on the EMX is ten (10). If you set it for a number greater than ten, after the tenth snapshot is taken and stored, the snapshots are overwritten. ▪ In the "Time before first Snapshot (s):" field, enter the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots. ▪ In the "Time between Snapshots (s):" field, enter the amount of time between when each snapshot is taken.

Creating Custom Email Messages

If you have configured emails to be sent when an event occurs, you can customize the message that is included in the email.

Messages consist of a combination of free text and EMX placeholders. The placeholders represent information is pulled from the EMX and inserted into the message.

For example:

```
[USESRNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See ***Email Message Placeholders*** (on page 127) for a list and definition of available variables.

To create a custom message:

1. Click Device Settings > Event Rules.
2. Click the Actions tab.
3. From the left pane, select the event the action is associated with, or create a new action. See ***Creating Actions*** (on page 123).
4. Select Send EMail from the Actions drop-down in the Action Settings section of the dialog.
5. Check the Use Custom Log Message checkbox.
6. Build the message in the open text field that is provided by entering custom information. If needed, use placeholders as part of the message.

   Note: Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions.

7. Click Save.

Email Message Placeholders

Following are placeholders that can be used in custom event email messages.

Note: Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions.

Placeholder	Description
[ASSERTION]	Boolean flag whether an event condition was entered (1) or left (0)

Placeholder	Description
[EXTSENSORNAME]	The name of an external sensor
[EXTSENSORSLOT]	The ID of an external sensor slot
[IFNAME]	The human readable name of an network interface
[VALUE]	The new value of a parameter
[VERSION]	The firmware version the device is upgrading to
[OLDVERSION]	The firmware version the device is being upgraded from
[PARAMETER]	The name of a configuration parameter
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (e.g. 'feature' or 'auxiliary', the event triggering device is connected to
[RECIPIENTS]	The list of recipients, an SMTP message was sent to
[TARGETROLE]	The name of a user management role, an action was applied on
[SERVER]	The name or IP address of a server
[TARGETUSER]	The user, an action was triggered for
[TIMESTAMP]	The timestamp of the event occurance
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[LEDCOLOR]	The RGB LED color
[LEDMODE]	The LED indication mode
[LEDOPMODE]	The LED operating mode
[STATE]	The human readable state of an asset strip
[RACKUNIT]	The (vertical) rack unit position, an action applies to
[RACKSLOT]	The (horizontal) slot position, an action applies to
[STRIPNAME]	The name of an asset strip
[STRIPID]	The numeric ID of an asset strip
[TAGID]	The asset tag ID

Placeholder	Description
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX
[LHXPOWERSUPPLYID]	The ID of an LHX power supply
[LHXSENSORID]	The ID of an LHX sensor probe
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name
[INLET]	The power inlet label
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[POLESENSOR]	The sensor name for a certain power line

Default Log Messages

Following are default log messages triggered and emailed to specified recipients when EMX events occur (are TRUE) or, in some cases, do not occur (are FALSE). See ***Event Rules and Actions*** (on page 118) for information configuring email messages to be sent when specified events occur.

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update	Firmware upgrade failed from version	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
failed	'[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device identification changed	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied from host '[USERIP]'.	
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	
Device > An LDAP error occured	An LDAP error occured: [LDAPERRORDESC].	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > Features > Schroff LHX Support	Schroff LHX support enabled.	Schroff LHX support disabled.
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role added	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
	'[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User logged in	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available.
External Sensor Slot > * > Numeric Sensor > Unavailable	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
External Sensor Slot > * > Numeric Sensor > Above upper critical threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'.
External Sensor Slot > * > Numeric Sensor > Above upper warning threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning'.
External Sensor Slot > * > Numeric Sensor > Below lower warning threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning'.
External Sensor Slot > * > Numeric Sensor > Below lower critical threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'.
External Sensor Slot > * > State Sensor > Unavailable	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
External Sensor Slot > * > State Sensor > Closed	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is closed.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is open.
External Sensor Slot > * > State	External sensor '[EXTSENSORNAME]'	External sensor '[EXTSENSORNAME]' in slot

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Sensor > On	in slot '[EXTSENSORSLOT]' is on.	'[EXTSENSORSLOT]' is off.
External Sensor Slot > * > State Sensor > Alarmed	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is alarmed.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is no longer alarmed.
Server Monitoring > * > Monitored	Server '[SERVER]' is now being monitored.	Server '[SERVER]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[SERVER]' is unreachable.	Server '[SERVER]' is reachable.
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'.	
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Firmware Update	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'.	
Asset Management > Device Config Changed	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]'	
Asset Management > Blade Extension Overflow	Blade extension overflow occured on strip [STRIPID] ('[STRIPNAME]').	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]').
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]').	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
**LHX > Connected	LHX has been connected to [PORTTYPE] port [PORTID].	LHX has been disconnected from [PORTTYPE] port [PORTID].
**LHX > Operational State	LHX connected to [PORTTYPE] port [PORTID] has been switched on.	LHX connected to [PORTTYPE] port [PORTID] has been switched off.
**LHX > Sensor > Unavailable	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available.
**LHX > Sensor > Above upper critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'.
**LHX > Sensor > Above upper warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'.
**LHX > Sensor > Below lower warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'.
**LHX > Sensor > Below lower critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'.
**LHX > Emergency Cooling	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated.	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated.
**LHX > Maximum cooling request	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'.	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'.
**LHX > Parameter Data Loss	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'.	
**LHX > ST-Bus Communication Error	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'.	
**LHX > Collective fault	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'.	
**LHX > Door Contact	The door of LHX at [PORTTYPE] port '[PORTID]' was opened.	The door of LHX at [PORTTYPE] port '[PORTID]' was closed.
**LHX > Sensor Failure	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
**LHX > Fan Failure	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'.	
**LHX > Power Supply Failure	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'.	
**LHX > Threshold Humidity	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
**LHX > External Water Cooling Failure	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'.	
**LHX > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'.	

**Note: Not set for 'trigger' events (see [ASSERTION] ctx)*

***Note: LHX events are only available if Schroff LHX Support is enabled.*

Sample Event Rules

Sample Asset-Management-Level Event Rule

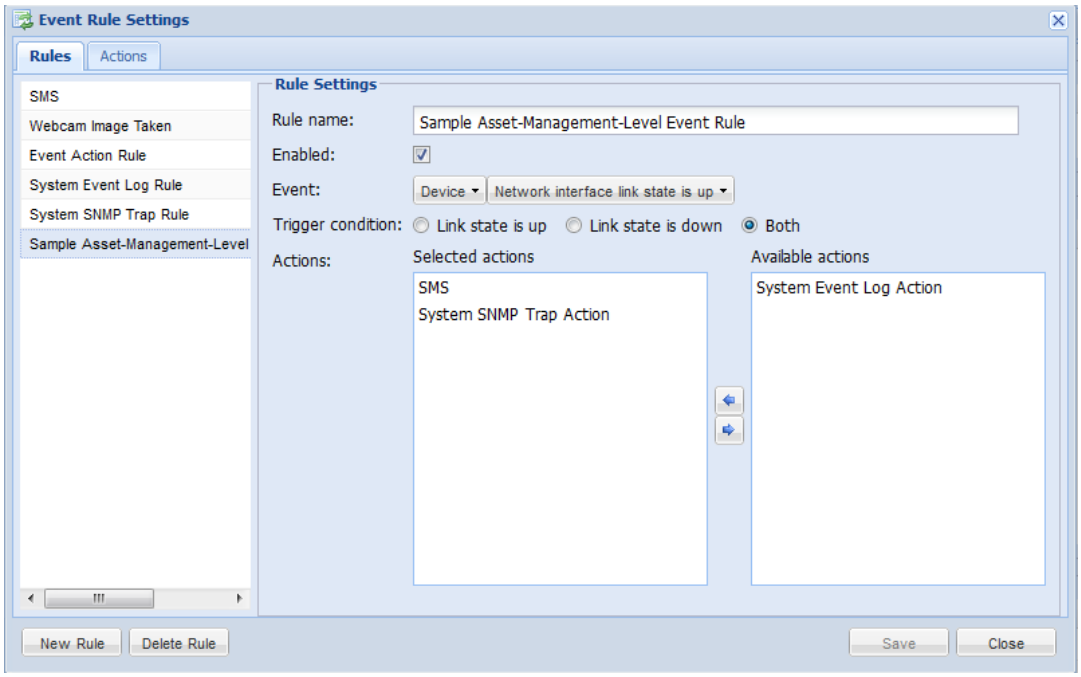
In this example, we want the EMX to record in the internal log when an asset sensor network link goes up or down. The sample event rule looks like this:

- Event: Device > Network interface link state is up
- Trigger condition: Both
- Actions: System Event Log Action

To create the above event rule:

1. Enter a name for the rule.
2. Select the Enabled checkbox to enable the rule.
3. From the Event drop-down, select Device > "Network interface link state is up". These selections indicate we are specifying an event regarding asset sensor management, and we want the EMX to respond to the event related to physical connections and/or disconnections.
4. Select the Both radio button since we want both connection and disconnection actions to be recorded when either action is taken.

5. Select "System Event Log Action" as we intend to record this event in the internal log when the specified events occur.



Sample Sensor-Level Event Rule

In this example, we want the EMX device to send SNMP traps to the SNMP manager when the reading of the temperature sensor connected to the sensor port #1 crosses any threshold or when the sensor is unavailable. To do that we would set up an event rule like this:

- Event: External sensor slot > Slot 1 > Numeric Sensor > Any sub-event
- Actions: System SNMP Trap Action

To create the above event rule:

1. Select "External sensor slot" in the Event field to indicate we are specifying an event at the environmental sensor level.
2. Select "Slot 1" from the submenu because we want the report about the sensor connected to sensor port #1.
3. Select "Numeric Sensor" to indicate the sensor is a numeric sensor.

Note: A numeric sensor uses numeric values to indicate the environmental condition while a discrete (on/off) sensor uses alphabetical characters to indicate the sensor state.

4. Select "<Any sub-event>" because we want to specify all events related to the sensor connected to sensor port #1, including the sensor's unavailable state and threshold-crossing events -- "Above upper critical, "Above upper warning," "Below lower warning," and "Below lower critical."
5. Select "System SNMP Trap Action" as we want to send SNMP traps to respond to the specified events when these events occur.

Sample User-Activity-Level Event Rule

In this example, we want the EMX to record the user activity event in the internal log when any user logs in or logs out. The event rule is set like this:

- Event: User activity > Any user > User logged in
- Trigger condition: Both
- Actions: System Event Log Action

To create the above event rule:

1. Select "User activity" in the Event field to indicate we are specifying an event regarding the user activity.
2. Select "<Any user>" from the submenu because we want to record the activity of all users.
3. Select "User logged in" to select the user login-related events.
4. Select the Both radio button since we want both login and logout actions to be recorded when either event occurs.
5. Select "System Event Log Action" as we intend to record this event in the internal log when the specified events occur.

Modifying an Event Rule

You can change an event rule's event, action, trigger condition and other settings, if any.

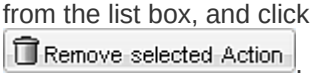
Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule and System SNMP Trap Rule.

To modify an event rule:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify in the left pane.
3. To disable the event rule, deselect the Enabled checkbox.

4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

   For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all user names (referred to as <*Any user*>).

5. If radio buttons are available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
   - To add a new action, click the drop-down arrow, select the action from the list, and click the Add Action button .
   - To remove any added action, select it from the list box, and click the "Remove selected Action" button  .
7. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

8. Click Close to quit the dialog.

Modifying an Action

An existing action can be changed so that all event rules where this action is involved change their behavior accordingly.

Exception: The built-in action "System Event Log Action" is not user-configurable.

To modify an action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify from the left list.
4. Make necessary changes to the information shown.
5. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort the changes or Cancel to return to the current settings page.

6. Click Close to quit the dialog.

Deleting an Event Rule or Action

If any event rule or action is obsolete, simply remove it.

Note: You cannot delete the built-in event rules and actions.

To delete an event rule or action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
   a. Ensure the Rules tab is selected. If not, click the Rules tab.
   b. Select the desired rule from the left list, and click Delete Rule.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
3. To delete an action:
   a. Click the Actions tab.
   b. Select the desired action from the left list, and click Delete Action.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the EMX to generate an alert. The measurement then returns to a value within the threshold, but the EMX does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the EMX uses. See ***What is Deassertion Hysteresis?*** (on page 156).

Event Logging

By default, the EMX captures certain system events and saves them in a local (internal) event log.

Viewing the Local Event Log

You can view up to 2,000 historical events that occurred to the EMX device in the local event log.

When the log already contains 2,000 entries, each new entry overwrites the oldest entry.

To display the local log:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

   Each event entry in the local log consists of:

   - Date and time of the event
   - Type of the event
   - A description of the event
   - ID number of the event

2. The dialog shows the final page by default. You can:

   - Switch between different pages by doing one of the following:

     - Click or to go to the first or final page.

     - Click or to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.

   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon takes the place of the Show Details button. In that case, click and select Show Details to view details.

   - Click to view the latest events.

3. Enlarge the dialog if necessary.
4. You can re-sort the list or change the columns displayed.
5. Click Close to quit the dialog.

Clearing Event Entries

If it is not necessary to keep existing event history, you can remove all of it from the local log.

To delete all event entries:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

2. Click Clear Event Log.
3. Click Close to quit the dialog.

Viewing the Communication Log

The EMX allows you to inspect all communications occurred between the EMX device and its graphical user interface (GUI). The information is usually useful for a technical support engineer only and you may not need to view it.

This feature is accessible only by users with Administrative Privileges.

To view the communication log:

1. Choose Maintenance > View Communication Log. The Communication Log dialog appears.
2. The dialog shows the final page by default. You can:
   - Switch between different pages by doing one of the following:

     - Click ⏮ or ⏭ to go to the first or final page.

     - Click ◀ or ▶ to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.
   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon » takes the place of the Show Details button. In that case, click » and select Show Details to view details.

3. To immediately update the communication log, click .
4. To save the communication log on your computer, click .
5. Enlarge the dialog if necessary.
6. You can re-sort the list or change the columns displayed.
7. Click Close to quit the dialog.

Chapter 8 Managing External Devices

In This Chapter

Overview....141
Server Accessibility....141
Environmental Sensors....144
Asset Sensors and Tags....157
Webcams....168
GSM Modems....174
Schroff LHX Heat Exchangers....175

Overview

The EMX provides you with ability to monitor devices and conditions in your data center such as the status of servers, environmental conditions, and so on using third party sensors and devices.

You are also able to use a webcam to view data center activity, and a GSM modem to send SMS messages when a specific event occurs.

Server Accessibility

You can monitor whether specific IT devices are alive by having the EMX device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

This function is especially useful when you are not located in an area with Internet connectivity.

Adding IT Devices for Ping Monitoring

You can have the EMX monitor the accessibility of any IT equipment, such as DB servers and remote authentication servers.

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable Ping Monitoring for this Server" checkbox is selected. If not, select it to enable the ping monitoring feature.
4. Provide the information required.

Field	Description
IP Address/Hostname	IP address or host name of the IT equipment whose accessibility you want to monitor.
Number of Successful Pings to Enable Feature	The number of successful pings required to enable this feature. Valid range is 0 to 200.
Wait Time (in seconds) after Successful Ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait Time (in seconds) after Unsuccessful Ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of Consecutive Unsuccessful Pings for Failure	The number of consecutive pings without any response before the IT equipment is declared unresponsive. Valid range is 1 to 100.
Wait Time (in seconds) before Resuming Pinging	The wait time before resuming pinging after the IT equipment is declared unresponsive. Valid range is 1 to 1200 (seconds).

5. Click OK to save the changes.
6. To add more IT devices, repeat Steps 2 to 5.
7. Click Close to quit the dialog.

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever it requires changes.

To modify the ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose settings you want to modify by clicking it.
3. Click Edit or double-click the IT device. The Edit Server 'XXX' dialog appears, where XXX is the IP address or host name of the IT device.
4. Make changes to the information shown.
5. Click OK to save the changes.

Deleting Ping Monitoring Settings

When it is not necessary to monitor the accessibility of any IT device, just remove it.

To delete ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose ping monitoring settings you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click Close to quit the dialog.

Checking Server Monitoring States

Server monitoring results are available in the Server Reachability dialog after specifying servers for the EMX device to monitor.

To check the server monitoring states and results:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding server is activated or not.
   - : This icon denotes that the monitoring for the corresponding server is enabled.
   - : This icon denotes that the monitoring for the corresponding server is disabled.
3. The column labeled "Status" indicates the accessibility of each monitored server.

Status	Description
Reachable	The server is accessible.
Unreachable	The server is inaccessible.
Waiting for reliable connection	The connection between the EMX device and the server is not established yet.

4. You may change the sorting order of the list if necessary. See Changing the Sorting.
5. Click Close to quit the dialog.

Environmental Sensors

The EMX can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed.

To add environmental sensors:

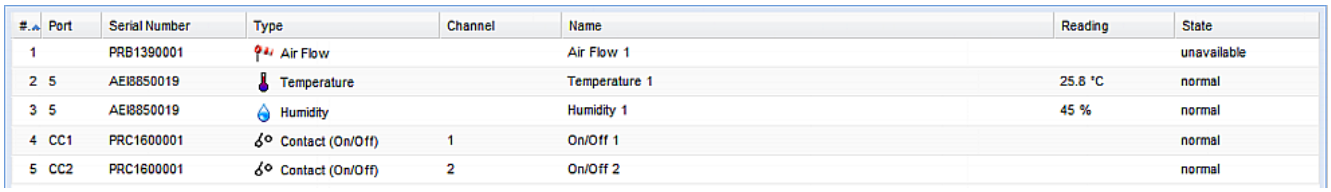
1. Physically connect environmental sensors to the EMX device. See ***Connecting Environmental Sensors (Optional)*** (on page 29).
2. Log in to the EMX web interface. The EMX should have detected the connected sensors, and display them in the web interface.
3. Identify each sensor through the sensor's serial number. See ***Identifying Environmental Sensors*** (on page 144).
4. The EMX should automatically manage the detected sensors. Verify whether detected sensors are managed. If not, have them managed. See ***Managing Environmental Sensors*** (on page 145).
5. Configure the sensors. See ***Configuring Environmental Sensors*** (on page 147). The steps include:
   a. Name the sensor.
   b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
   c. Mark the sensor's physical location on the rack or in the room.
   d. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state. Only numeric sensors have the threshold settings.

Identifying Environmental Sensors

An environmental sensor includes a serial number tag on the sensor cable.

The serial number for each sensor appears listed in the web interface after each sensor is detected by the EMX.



#	Port	Serial Number	Type	Channel	Name	Reading	State
1		PRB1390001	Air Flow		Air Flow 1		unavailable
2	5	AEI8850019	Temperature		Temperature 1	25.8 °C	normal
3	5	AEI8850019	Humidity		Humidity 1	45 %	normal
4	CC1	PRC1600001	Contact (On/Off)	1	On/Off 1		normal
5	CC2	PRC1600001	Contact (On/Off)	2	On/Off 2		normal

Match the serial number from the tag to those listed in the sensor table.

Note that the information in the "#" and "Port" columns is different.

Column	Information
#	The ID number assigned to each environmental sensor.
Port	The number of the SENSOR port where each environmental sensor is physically connected. "CC1" and "CC2" refer to the onboard contact closure sensor termination.

Managing Environmental Sensors

The EMX starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed.

If a Raritan sensor hub is used, you can connect up to 16 environmental sensors per SENSOR port. That is,

- For EMX2-111, which has only 1 SENSOR port, a maximum of 16 environmental sensors can be connected.
- For EMX2-888, which has 8 SENSOR ports, a maximum of 128 environmental sensors can be connected. Since the EMX2-888 device is implemented with two channels of onboard contact closure termination, it supports a maximum of 130 environmental sensors.
- Each SENSOR port can only support a maximum of two Raritan contact closure sensors, which has the shortest update interval among all Raritan sensors. See ***Information about Update Interval*** (on page 151).

When the total number of managed sensors has not reached the maximum, the EMX automatically brings detected environmental sensors under management. You should only have to manually manage a sensor when it is not under management.

To manually manage an environmental sensor:

1. If the EMX folder is not expanded, expand it to show all components.

Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click the External Sensors folder in the EMX Explorer pane, and the External Sensors page opens in the right pane.
3. Click the sensor you want to manage on the External Sensors page.

Note: To identify all detected sensors, see **Identifying Environmental Sensors** *(on page 144).*

4. Click Manage. The "Manage sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor's serial number and <sensor type> is the sensor's type.

Note: For a contact closure sensor, a channel number is added to the end of the <sensor type>.

5. There are two ways to manage the sensor:
   - To manage this sensor by letting the EMX assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors.
   - To manage this sensor by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

     If the number you selected was already assigned to a sensor, that sensor becomes released after losing this ID number.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to any sensor. If it has been assigned to a sensor, it shows that sensor's serial number. Otherwise, it shows the term "unused."

6. Click OK. The EMX starts to track and display the managed sensor's reading and/or state.
7. To manage additional sensors, repeat Steps 3 to 6.

Note: When the number of managed sensors reaches the maximum, you CANNOT manage additional sensors until you remove or replace any managed sensors. To remove a sensor, see **Unmanaging Environmental Sensors** *(on page 155).*

Configuring Environmental Sensors

You may change the default name for easily identifying the managed sensor, and describe its location with X, Y and Z coordinates.

To configure environmental sensors:

1. If the EMX folder is not expanded, expand it to show all components.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click the External Sensors folder in the EMX Explorer pane, and the External Sensors page opens in the right pane.
3. Select the sensor that you want to configure.
4. Click Setup. The "Setup of external sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the serial number of this sensor and <sensor type> is the sensor's type.

   Tip: You can also trigger the same setup dialog by selecting the desired environmental sensor icon in the tree and then clicking Setup on that sensor's page opened in the right pane.

5. If the selected environmental sensor is the Raritan contact closure sensor connected with a third-party detector/switch, select the appropriate sensor type in the Binary Sensor Subtype field.
   - Contact: The detector/switch is designed to detect the door lock or door open/closed status.
   - Smoke Detection: The detector/switch is designed to detect the appearance of smoke.
   - Water Detection: The detector/switch is designed to detect the appearance of water on the floor.
   - Vibration: The detector/switch is designed to detect the vibration in the floor.
6. Type a new name in the Name field.
7. Describe the sensor's location by assigning alphanumeric values to the X, Y and Z coordinates. See ***Describing the Sensor Location*** (on page 149).
8. If the selected environmental sensor is a numeric sensor, its threshold settings are displayed in the dialog. Click Edit or double-click the Threshold Configuration table to adjust the threshold, deassertion hysteresis and assertion timeout settings.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.

- After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
- To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 156).
- To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 157).

The Upper Critical and Lower Critical values are points at which the EMX considers the operating environment critical and outside the range of the acceptable threshold.

9. Click OK to save the changes.

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors.

To determine the Z coordinate format:

1. In left navigation panel, click the EMX folder. The Settings page opens.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click Setup on the Settings page. The EMX Setup dialog appears.
3. In the "External sensors Z coordinate format" field, click the drop-down arrow and select an option from the list.
   - Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.
   - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.
4. Click OK to save the changes.

Describing the Sensor Location

Use the X, Y and Z coordinates to describe each sensor's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = *Brown Cabinet Row*

Y = *Third Rack*

Z = *Top of Cabinet*

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 24 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 24 characters.

Tip: To configure and retrieve these coordinate values over SNMP, see the EMX MIB. To configure and retrieve these values over the CLI, see Using the Command Line Interface.

Setting Data Logging

The EMX can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the environmental sensors are measured per second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in log gets overwritten.

Though the environmental sensors are measured per second, their readings may not be updated per second. See ***Information about Update Interval*** (on page 151). The update interval varies depending on how many environmental sensors are connected to the EMX device and the sensor type. The more the environmental sensors are connected, the larger the update interval is. Therefore, type a large number in the Measurements Per Log Entry field when there are a large number of environmental sensors connected.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: The EMX's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** *(on page 182) for more details. In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is disabled. Only users having the "Administrator" or "Change Data Logging Settings" permissions can enable or disable this feature. See ***Setting Up Roles*** (on page 64).

To configure the data logging feature:

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Select the environmental sensors whose data logging you want to enable.

- To select partial sensors, select the corresponding checkboxes of the desired sensors in the Logging Enabled column.
- To select all sensors, click Enable All or Enable All in Page.
- To deselect all sensors, click Disable All or Disable All in Page.

5. Click OK to save the changes.

Information about Update Interval

Raritan environmental sensors can be divided into two categories according to the update interval of the sensor's reading or state.

- Normal type: Sensor readings or states are updated in a longer interval, which varies between 3 to 40 seconds according to the total number of connected environmental sensors. Most Raritan environmental sensors belong to this type, such as the temperature or humidity sensor.
- High priority type: Sensor readings or states are updated in a shorter interval, which is less than or equal to 3 seconds. Raritan contact closure sensors belong to this type.

Viewing Sensor Data

Readings of the environmental sensors will display in the web interface after these sensors are properly connected and managed.

The Dashboard page shows the information for managed environmental sensors only, while the External Sensors page shows the information for both of managed and unmanaged ones.

If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or at least one LHX built-in sensor fails on the heat exchanger. See ***Readings Highlighted in Yellow or Red (EMX)*** (see "***Readings Highlighted in Yellow or Red***" on page 54).

To view managed environmental sensors only:

1. Click the Dashboard icon in the EMX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the External Sensors section on the Dashboard page. The section shows:
   - Total number of managed sensors
   - Total number of unmanaged sensors
   - Information of each managed sensor, including:
     - Name
     - Reading
     - State

To view both of managed and unmanaged environmental sensors:

1. If the EMX folder is not expanded, expand it to show all components.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click the External Sensors folder in the EMX Explorer pane, and the External Sensors page opens in the right pane.

   Detailed information for each connected sensor is displayed, including:

   - Label (number)
   - Serial number
   - Sensor type
   - Name
   - Reading
   - State
   - Channel (for a contact closure sensor only)

Sensor Measurement Accuracy

Raritan environmental sensors are with the following factory specifications. Calibration is not required for environmental sensors.

- Temperature: +/-2%
- Humidity: +/-5%
- Differential air pressure: +/-1.5%
- Air flow: +/-6.5%

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete. For example, a contact closure sensor is a discrete sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters to indicate the state.

Sensor state	Applicable to
unavailable	All sensors

Sensor state	Applicable to
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity to the sensor is lost.

The EMX pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor module show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The EMX continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

Note: See **Configuring a Contact Closure Sensor** *(on page 33) for setting the normal state. For the onboard contact closure sensor termination, see* **Connecting Third-Party Detectors/Switches to the EMX** *(on page 34) for how to set the normal state.*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

Lower Warning threshold <= Reading < Upper Warning threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

For a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

Note: See **Configuring a Contact Closure Sensor** *(on page 33) for setting the normal state. For the onboard contact closure sensor termination, see* **Connecting Third-Party Detectors/Switches to the EMX** *(on page 34) for how to set the normal state.*

Tip: A contact closure sensor's LED is lit after entering the alarmed *state. If the sensor module has two channels for connecting two switches, two LEDs are available. Check which contact closure switch is in the "abnormal" status according to the channel number of the LED.*

"below lower critical" State

This state means a numeric sensor's reading is below the lower critical threshold as indicated below:

Reading < Lower Critical Threshold

"below lower warning" State

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

Lower Critical Threshold <= Reading < Lower Warning Threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper warning" State

This state means a numeric sensor's reading is above the upper warning threshold as indicated below:

Upper Warning Threshold <= Reading < Upper Critical Threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

Upper Critical Threshold <= Reading

Note: The symbol <= means smaller than (<) or equal to (=).

Unmanaging Environmental Sensors

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the EMX device stops retrieving the sensor's reading and/or state.

To release a managed sensor:

1. If the EMX folder is not expanded, expand it to show all components.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click the External Sensors folder in the EMX Explorer pane, and the External Sensors page opens in the right pane.
3. Click the sensor you want to unmanage on the External Sensors page.
4. Click Release.

After a sensor is removed from management, the ID number assigned to that sensor is released and can be automatically assigned to any newly-detected sensor.

Threshold Information

Setting and enabling the thresholds causes the EMX to generate alert notifications when it detects that any sensor's state crosses the thresholds.

There are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning range before the critical threshold.
- Upper and Lower Critical thresholds indicate the sensor reading is at the critical level.

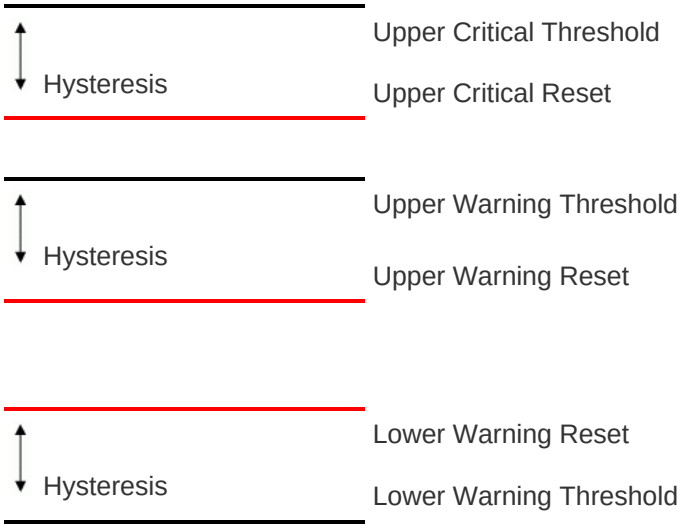
To avoid generating a large amount of alert events, the deassertion hysteresis for each threshold is enabled. You can change the default hysteresis value if necessary. For more information on the deassertion hysteresis, see ***What is Deassertion Hysteresis?*** (on page 156).

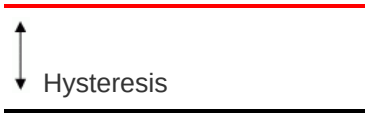
Note: After setting the thresholds, remember to configure the event rules. See **Configuring Event Rules** *(see "***Event Rules and Actions***" on page 118).*

For information on configuring an environmental sensor's threshold, see ***Configuring Environmental Sensors*** (on page 147). For information on configuring thresholds for a Schroff LHX heat exchanger, see ***Configuring Temperature and Fan Thresholds*** (on page 177).

What is Deassertion Hysteresis?

The hysteresis setting determines when a threshold condition is reset. This diagram illustrates how hysteresis values relate to thresholds:





The hysteresis values define a reset threshold. For upper thresholds, the measurement must fall past this reset threshold before a deassertion event is generated. For lower thresholds, the measurement must rise above this reset threshold before a deassertion event is generated.

What is Assertion Timeout?

When the assertion timeout is enabled, the EMX device asserts any warning or critical condition only after a specified number of consecutive samples that cross a particular threshold are generated. This prevents a number of threshold alerts from being generated if the measurements return to normal immediately after rising above any upper threshold or dropping below any lower threshold.

Asset Sensors and Tags

A Feature port is identified with a combination of the name "Asset Strip" and the port number.

After connecting an asset sensor, you must provide the total number of rack units (tag ports) the connected asset sensor has to the EMX device.

If necessary, you can also manually change the LED color settings for a specific rack unit on the asset sensor to make that LED behave differently from other LEDs.

A daisy chain AMS-M2-Z asset sensors is supported by the EMX. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 162) for information on AMS-M2-Z daisy chain limitations. Once connected, EMX recognizes each AMS-M2-Z asset sensor that is part of the chain. Blade extensions can be connected to each AMS-M2-Z asset sensor in the chains, as needed. As AMS-M2-Z asset sensors are added or removed from the chain, events are generated in EMX.

Configuring the Asset Sensor

The EMX CANNOT detect how many rack units (tag ports) a connected asset sensor supports so you must provide this information manually.

In addition, you can name the asset sensor or determine the numbering way for all rack units in the web interface. Additionally, you can provide a description to identify each asset sensor.

The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the port number where the asset sensor is connected.

To configure an asset sensor:

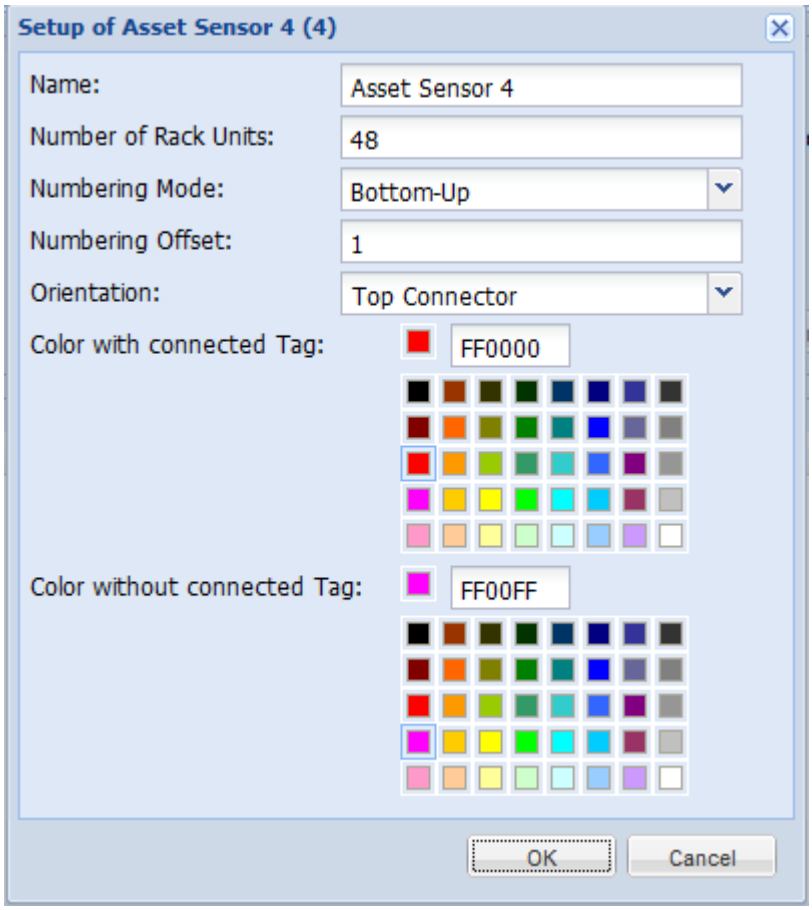
1. Connect the asset sensor to the EMX if it is not already. See ***Connecting Asset Sensors to the EMX*** (on page 22).
2. Click on the Feature Ports folder in the navigation tree to expand it.
3. Click the desired asset sensor. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.
4. Click Setup in the Settings section. The Setup of Asset Strip dialog appears.
5. Enter a name of the asset sensor.
6. Type the total number of rack units the selected asset sensor has in the "Number of Rack Units" field. This field shows 48 by default.
7. Determine how to number all rack units on the asset sensor by selecting an option in the Numbering Mode.
   - Top-Down: The rack units are numbered in the ascending order from the highest to the lowest rack unit.
   - Bottom-Up: The rack units are numbered in the descending order from the highest to the lowest rack unit.
8. In the Numbering Offset field, select the starting number. For example, if you select 3, the first rack unit is numbered 3, the second is numbered 4, the third is numbered 5, and so on until the final number.
9. Indicate how the asset sensor is mounted in the rack in the Orientation field. The rack unit that is most close to the RJ-45 connector of the asset sensor will be marked with the index number 1 in the web interface.

For the latest version of asset sensors with a built-in tilt sensor, it is NOT necessary to configure the orientation setting manually. The EMX device can detect the orientation of the asset sensors and automatically configure it.

- Top Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
- Bottom Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

10. To change the LED color denoting the presence of a connected tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color with connected Tag" field.
11. To change the LED color denoting the absence of a connected tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color without connected Tag" field.
12. Click OK to save the changes.



Changing a Specific LED's Color Settings

In the EMX web interface, a rack unit refers to a tag port on the asset sensor. You can name a specific rack unit, or change its LED color settings so that this LED behaves differently from others on the same asset sensor.

To change an LED's settings:

1. Connect the asset sensor to the EMX if it is not already. See ***Connecting Asset Sensors to the EMX*** (on page 22).
2. Click on the Feature Ports folder in the navigation tree to expand it.
3. Click the desired asset sensor. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

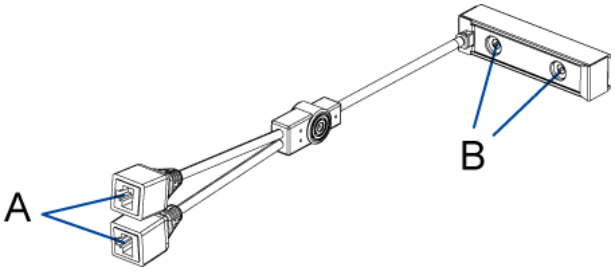
4. Select the rack unit whose LED settings you want to change.
5. Click Configure Rack Unit or double-click the selected rack unit. The setup dialog for the selected rack unit appears.
6. In the Name field, type a name for identifying this rack unit.
7. Select either Auto or Manual Override as this rack unit's LED mode.
   - Auto (based on Tag): This is the default setting. With this option selected, the LED follows the global LED color settings.
   - Manual Override: This option differentiates this LED's behavior. After selecting this option, you must select an LED mode and/or an LED color for the selected rack unit.
     - LED Mode: Select On to have the LED stay lit, Off to have it stay off, "Slow blinking" to have it blink slowly, or "Fast blinking" to have it blink quickly.
     - LED Color: If you select On, "Slow blinking" or "Fast blinking" in the LED Mode field, select an LED color by either clicking a color in the color palette or typing the hexadecimal RGB value of a color in the accompanying text box.
8. Click OK to save the changes.

Connecting AMS-M2-Z Asset Sensors (Optional)

The AMS-M2-Z is a special type of asset sensor that functions the same as regular MASTER asset sensors with the following differences.

- It provides two RJ-45 connectors.
- Multiple AMS-M2-Z asset sensors can be daisy chained.
- Only two tag ports are available on each AMS-M2-Z so only two asset tags can be connected.

This product is especially useful for tracking large devices such as SAN boxes in the cabinet.



Item	Description
A	RJ-45 connectors
B	Tag ports

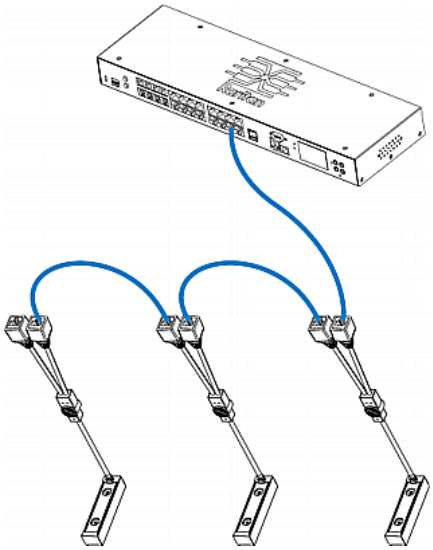
To connect the AMS-M2-Z asset sensors to the EMX:

1. Connect the AMS-M2-Z to the EMX via a Category 5e/6 cable.
   a. Connect one end of the cable to the RJ-45 port labeled "Input" on the AMS-M2-Z.
   b. Connect the other end of the cable to the FEATURE port on the EMX.
2. Affix an asset tag to the IT device and connect this asset tag to the AMS-M2-Z by plugging the tag connector into the tag port on the AMS-M2-Z. See ***Connecting Asset Sensors to the EMX*** (see "***Combining Asset Sensors***" on page 20) for details.
3. If necessary, daisy chain multiple AMS-M2-Z to track more than two IT devices via this EMX.
   a. Verify that the Category 5e/6 cable length is within the limitation. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 162) for the cable length limitations.
   b. Connect one end of the Category 5e/6 cable to the RJ-45 connector labeled "Output" on the AMS-M2-Z being connected to the EMX.

c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on another AMS-M2-Z.

d. Repeat the above steps to daisy chain additional AMS-M2-Z. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 162) for the maximum number of AMS-M2-Z asset sensors supported in the chain.

e. It is highly recommended using the cable ties to help hold the weight of all connecting cables.



4. Repeat Step 2 to connect IT devices to the other AMS-M2-Z's in the chain via the asset tags.

AMS-M2-Z Daisy-Chain Limitations

There are some limitations when daisy chaining the AMS-M2-Z asset sensors. The limitations vary according to the Raritan product model connected to the first AMS-M2-Z.

Models	Daisy-chain limitations
All PDUs whose model names begin with PX2	• Up to 4 AMS-M2-Z can be daisy chained. • The maximum cable length between each AMS-M2-Z in the chain is 2 meters.
EMX2-111	• Up to 2 AMS-M2-Z can be daisy chained. • The maximum cable length between each AMS-M2-Z in the chain is 2 meters.

Models	Daisy-chain limitations
EMX2-888	• Up to 6 AMS-M2-Z can be daisy chained. • The maximum cable length between each AMS-M2-Z in the chain is 3 meters.

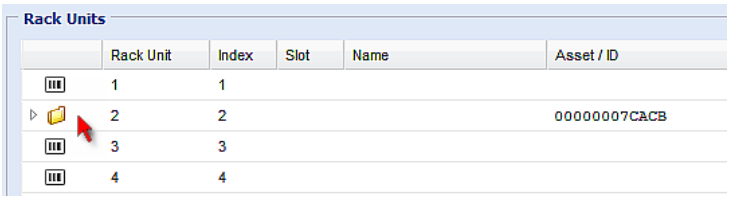
Expanding a Blade Extension Strip

A blade extension strip, like an asset sensor, has multiple tag ports. After connecting it to a specific asset sensor, it is displayed as a folder on that asset sensor's page.

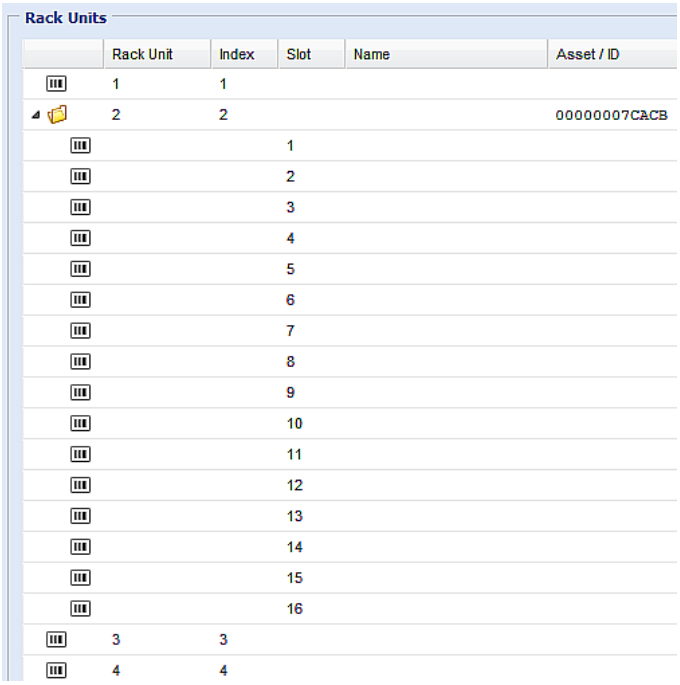
Note: If you need to temporarily disconnect the tag connector of the blade extension strip, wait at least 1 second before connecting it back, or the EMX may not detect it.

To expand a blade extension strip folder:

1. Click the desired asset sensor in the left pane. The selected asset sensor's page opens in the right pane.
2. Locate the rack unit (tag port) where the blade extension strip is connected.



3. Double-click that rack unit or click the white arrow ▷ prior to the folder icon. The arrow then turns into a black, gradient arrow ◢, and all tag ports appear below the folder.



To collapse a blade extension strip:

- Double-click the blade extension strip folder, or click the black, gradient arrow ◢ prior to the folder icon. All tag ports under the folder are hidden.

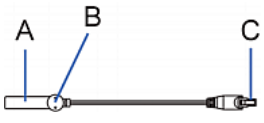
Connecting Blade Extension Strips

For blade servers, which are contained in a single chassis, you can use a blade extension strip to track individual blade servers.

Raritan's blade extension strip functions similar to a Raritan asset sensor but requires a tag connector cable for connecting to a tag port on the regular asset sensor or AMS-M2-Z. The blade extension strip contains 4 to 16 tag ports, depending on which model you purchased.

The diagram illustrates a tag connector cable and a blade extension strip with 16 tag ports.

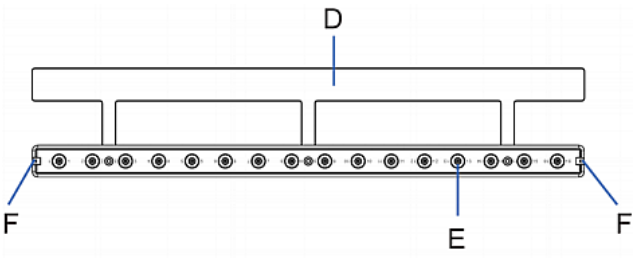
Tag connector cable



Item	Description
A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

Note: A tag connector cable has a unique barcode, which is displayed in the EMX's web interface for identifying each blade extension strip where it is connected.

Blade extension strip

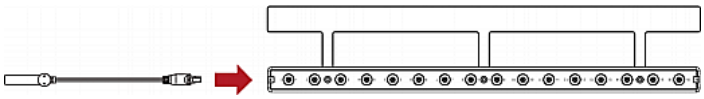


Item	Description
D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

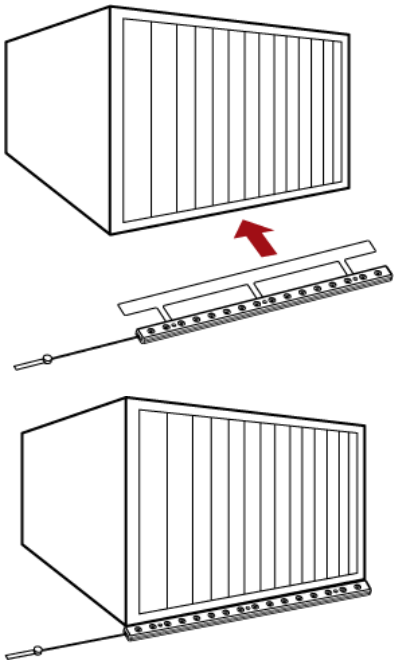
Note: Each tag pot on the blade extension strip is labeled a number, which is displayed as the slot number in the EMX's web interface.

To install a blade extension strip:

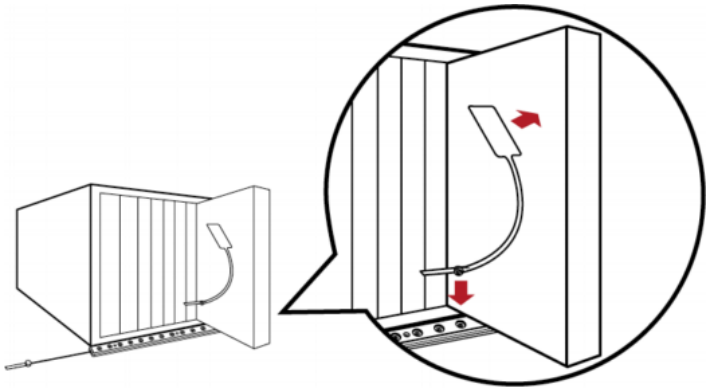
1. Connect the tag connector cable to the blade extension strip.
   - Plug the cable's connector into the socket at either end of the blade extension strip.



2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.

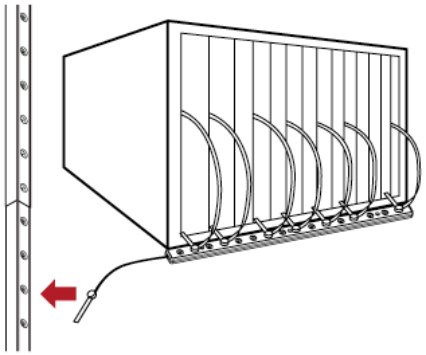


3. Connect one end of an asset tag to a blade server and connect the other end to the blade extension strip.
   a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.
   b. Plug the tag connector of the asset tag into the tag port on the blade extension strip.



4. Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.

5. Plug the tag connector of the blade extension strip into the closest tag port of the asset sensor assembly or the AMS-M2-Z asset sensor on the rack.



Note: If you need to temporarily disconnect the tag connector of the blade extension strip, wait at least 1 second before connecting it back, or the EMX may not detect it.

Webcams

The EMX supports Logitech® QuickCam® Pro 9000 webcams connected to it, allowing you to view video or snapshots of the area surrounding the webcam. The EMX 888 device supports up to two (2) webcams, and the EMX 111 supports one (1) webcam. After connecting a webcam, you can visually monitor environmental conditions near the EMX through the web interface from anywhere.

For more information on the QuickCam webcam, see the user documentation accompanying it. For information connecting a webcam to the EMX, see ***Connecting a Logitech Webcam (Optional)*** (on page 37).

Snapshots or videos captured by the webcam are displayed in the right pane of EMX web interface once a webcam is selected in the navigation tree. Snapshots and videos can also be displayed in Live Preview mode in the Primary Standalone Live Preview window by clicking on the Live Preview icon .

EMX allows you to take and store snapshots from each webcam. See ***Taking, Viewing and Managing Webcam Snapshots*** (on page 171) for additional information.

Links to video being captured by a webcam can be sent via email or instant message. See ***Sending Videos in an Email or Instant Message*** (on page 173).

Events that trigger emails containing snapshots from a webcam can be created. Events can be defined for each individual webcam. See ***Event Rules and Actions*** (on page 118).You must have Change Webcam Configuration permission applied to your role in order to configure webcams, and the View Webcam Images and Configuration permission to view images in EMX.

Configuring Webcams

Before you can configure a webcam, it must be connected to the EMX. See ***Connecting a Logitech Webcam (Optional)*** (on page 37).

To configure a webcam:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Click on the webcam you want to configure and then click Setup at the bottom right of page. The Webcam Setup dialog opens.
3. Enter a name for the webcam. Up to 64 characters are supported.
4. Select a resolution for the webcam.

5. Select the webcam mode. This can be changed as needed once the webcam is configured.
   a. Video - the webcam is in video mode. Set the Framerate (frames per second) rate.
   b. Snapshot - the webcam displays images from the webcam. Set the Time Between Image(s) rate as measured in seconds.
6. Click OK. The image or video from the webcam is now available in the EMX once you click on the webcam in the navigation tree.

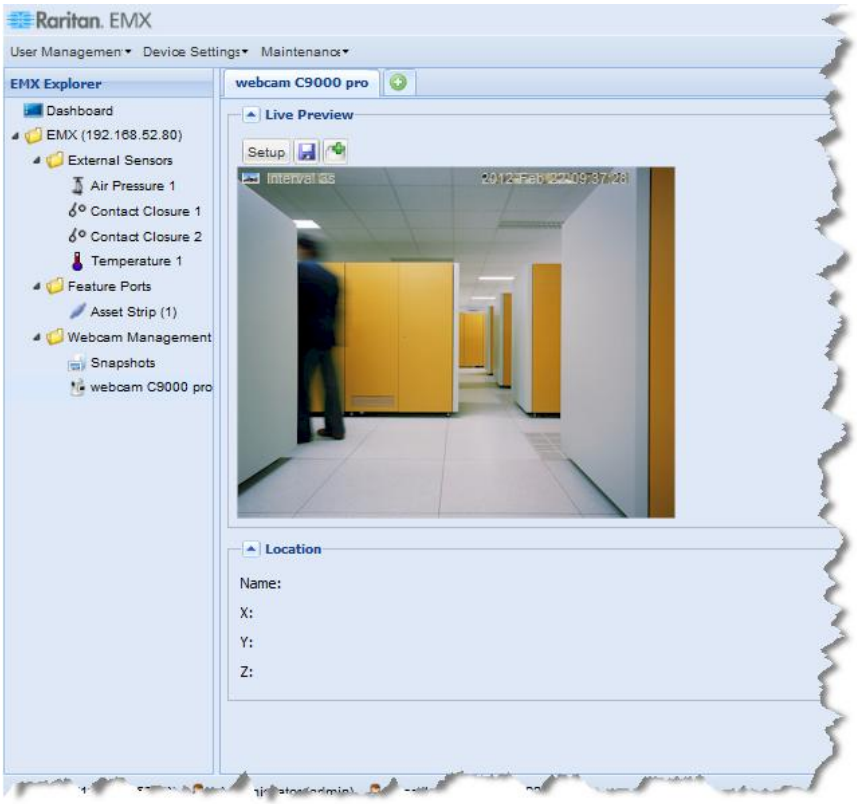
To edit a webcam configuration:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Double-click on the webcam you want to edit. The webcam image or video opens in a new tab.
3. Click Setup.
4. Edit the information as needed. Changes to the resolution do not apply to existing, stored images - it applies only to images and videos taken after the resolution is changed.
5. Click OK.

Viewing Webcam Snapshots and Videos

By default, once a webcam is attached, it is set to take snapshots every five (5) seconds. Change the webcam settings and/or switch between snapshots and live video from the Webcam Setup dialog by clicking on a webcam in the navigation tree and then clicking the Setup button in the Live Preview pane. See ***Configuring Webcams*** (on page 168).

Snapshots or videos captured by a webcam are displayed in the right pane of EMX web interface once a webcam is selected in the navigation tree.



In the snapshot mode, a snapshot mode icon appears on the top-left corner of the image along with the number of images the webcam is set to take per second. In the video mode, a video mode icon appears on the top-left corner of the image. Switch between snapshot mode and video mode, click Setup and select either the Image or Video radio buttons.

A date and time stamp is displayed on each snapshot, as well. The location of the webcam is displayed in the Location pane below the image, along with any labels applied to the webcam. See ***Configuring Webcams*** (on page 168).

Up to five (5) Live Preview sessions can be displayed at once in different tabs in the EMX interface, or in separate Live Preview windows that are accessed by clicking on the Live Preview icon located above the snapshot/video.

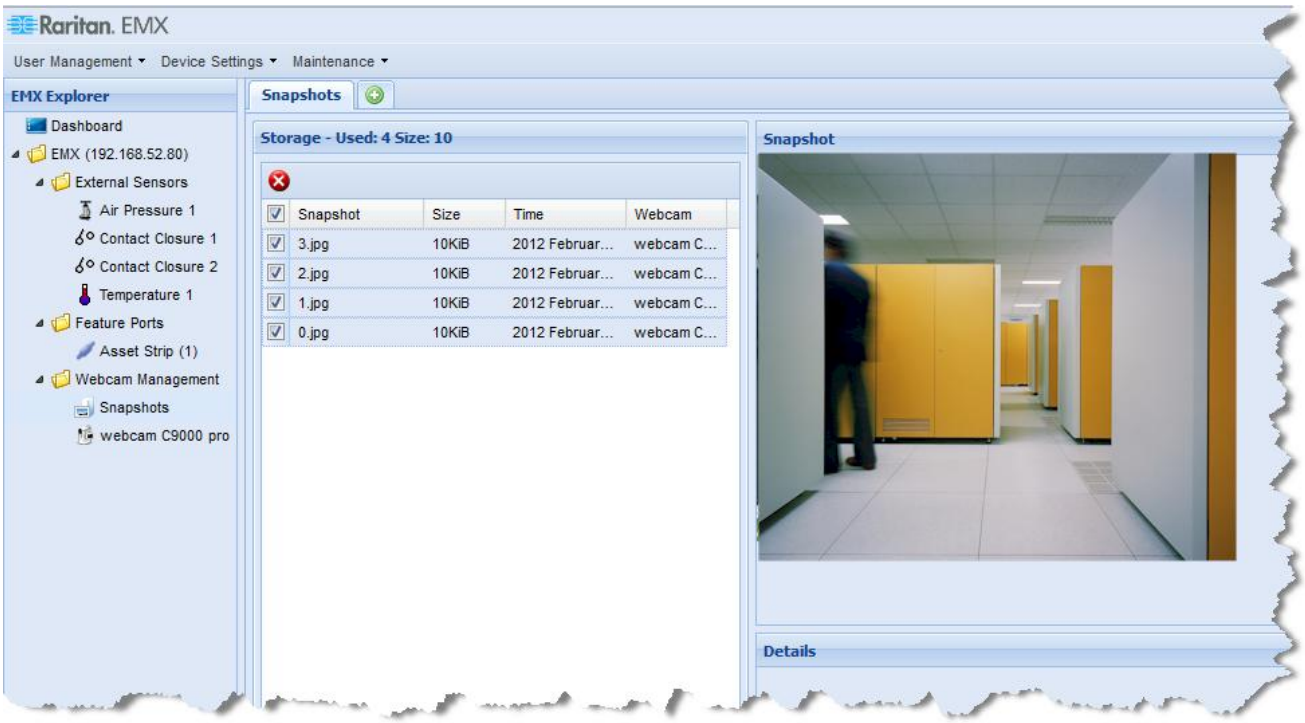
Note: For remote Live Preview sessions, such as those accessed via link in an email or instant message, a total of up to three (3) simultaneous Live Preview sessions are supported at a time. One (1) from the originator in the EMX interface, and up to two (2) remote sessions.

Individual snapshots taken by a webcam are viewed by clicking on Snapshots under Webcam Management in the navigation tree. Once selected, the Snapshots tab opens in the right pane. See ***Taking, Viewing and Managing Webcam Snapshots*** (on page 171) and Viewing and Managing Stored Snapshots for details.

Taking, Viewing and Managing Webcam Snapshots

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored on the EMX. Up to ten (10) images can be stored on the EMX at once. Unless snapshots are deleted manually, the oldest snapshot is automatically deleted from the device when the number of snapshots exceeds ten.

Snapshot files are saved as JPG files. The snapshot file is named based on the number of the snapshot starting from 1. So the first snapshot that is taken is named 1.jpg, the second is 2.jpg and so on.



To take a snapshot from webcam:

1. In the navigation tree, click on the webcam you want to take a snapshot with. The webcam image is displayed in the right pane.

   The webcam must be in snapshot mode in order to take snapshots. If the webcam is in video mode, click Setup in the right pane above the video image to open the Webcam Setup dialog, then select the Snapshot radio button.

2. Once the snapshot image being taken by the selected webcam is displayed in the right pane, click the Store Snapshot to Webcam Storage icon above the image to take a snapshot. Up to ten (10) snapshots can be stored at once on the device.

To view existing snapshots:

1. In the navigation tree, click Snapshot under the Webcam Management folder. The snapshots are displayed in the right pane in the Storage section of the page.

2. View an individual snapshot by clicking on a snapshot file in the Storage section of the page.

   The size of each snapshot file, the date and time each snapshot was taken, and the webcam that took each snapshot, is displayed when viewing snapshots.

Details, such as the webcam location and/or labels, if any, are displayed in the Details section below the snapshot in the right pane. This information is defined when the webcam is initially configured. See ***Configuring Webcams*** (on page 168).

To delete snapshots manually:

- Delete snapshots by selecting the checkbox next to the snapshot you want to delete, then clicking the Delete icon at the top of the section. To select and delete all snapshots at once, click the checkbox in the checkbox column header, then click the Delete icon.

Sending Videos in an Email or Instant Message

You are able to email or instant message up to two (2) recipients a link to webcams attached to the EMX. Users can then click on the links and view snapshots or videos.

Note: For remote Live Preview sessions, such as those accessed via link in an email or instant message, a total of up to three (3) simultaneous Live Preview sessions are supported at a time. One (1) from the originator in the EMX interface, and up to two (2) remote sessions.

Note: For the purposes of this topic, the message sender is User A and the recipient is User B.

The recipient is able to access the video image via the link so long as either:

- The video remains open in Live Preview mode in the User A's EMX interface, and User A does not log out of the interface and the session does not time out.

  Or

- The video remains open in a secondary Live Preview window in the User A's EMX interface. So long as the secondary Live Preview window is open in User A's interface, even after User A logs out of the EMX interface or the session times out, the link is available.

Best Practice

As a best practice, in the EMX interface, User A should open the video in a secondary Live Preview window and leave the Live Preview window open at least until User B opens the video via the link.

Once User B opens the video via the link, the secondary Live Preview mode window can be closed in the User A's EMX interface.

User B must manually let User A know they have opened the link, or User A can check to see if User B is currently connected to the application by clicking Maintenance > Connected Users.

To send a video link via email or instant message:

1. In the navigation tree, click on the webcam that is capturing the video you want to provide a link to in the email. The video is displayed in Live Preview mode in the right pane.
2. Click on the Live Preview icon located above the video. The video opens in a secondary Live Preview window.
3. Copy the URL from the Live Preview window, paste it into the email or instant message application. Leave the Live Preview window open at least until the recipient opens the video via the link.

GSM Modems

A Cinteron® MC52i/MC55iGSM modem must be connected to the EMX in order to send SMS event messages. See ***Creating Actions*** (on page 123) for more information on SMS event messages.

Note: The EMX cannot receive SMS messages.

To connect the GSM modem:

1. Connect the GSM modem to the DB9 serial port on the EMX.
2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.

Schroff LHX Heat Exchangers

After connecting the Schroff® LHX heat exchanger to the EMX device via the Feature port or the RS-485 port, the EMX detects LHX. The LHX is viewed under the Feature folder or the Auxiliary Port folder in the navigation tree, depending on the port it is connected to.

Note: If connecting the LHX to the Feature port, use the serial cable provided with the LHX.

From the EMX, you can remotely do the following:

- Name a connected LHX heat exchanger
- Configure the air outlet temperature setpoint
- Configure air outlet temperature thresholds
- Configure air inlet temperature thresholds
- Configure water inlet temperature thresholds
- Configure fan speed thresholds
- Monitor the air inlet temperature
- Monitor the air outlet temperature
- Monitor the fan speed
- Configure basic settings for the connected heat exchanger, such as the sensor thresholds

Note: These settings are stored on the EMX port where the heat exchanger is connected, and are lost if that heat exchanger is moved to a different port.

See ***Connecting a Schroff LHX Heat Exchanger (Optional)*** (on page 37) for how to connect the heat exchanger.

Enabling and Disabling Schroff LHX Heat Exchanger Support

By default, Schroff LHX Heat Exchanger support is disabled. As such, support needs to be enabled before the device appears in the navigation tree or on the dashboard. Additionally, Schroff LHX Heat Exchanger support must be enabled in order for the LHX-MIB to be accessible through SNMP.

To enable the Schroff LHX Heat Exchanger:

1. Select Device Settings > Features, and then select the Schroff Heat Exchanger checkbox on the menu.
2. Click Yes to confirm.
3. Reboot the EMX.

Naming a Heat Exchanger

To help identify an LHX heat exchanger in the EMX web interface, assign a name to it. The customized LHX heat exchanger's name is followed by the device type and RS-485 port number in parentheses.

The web interface provides two types of setup dialogs for naming a specific LHX heat exchanger.

To name a heat exchanger using the Auxiliary Port Setup dialog:

1. Connect the LHX heat exchanger to EMX if it is not already connected.
2. If the EMX folder is not expanded, expand it to show all components.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

3. Click the Auxiliary Ports folder. The Auxiliary Ports page opens in the right pane, listing all RS-485 ports.
4. Select the port where the desired heat exchanger is connected on the Auxiliary Ports page, and click Setup. Or simply double-click that port. The Auxiliary Ports Setup dialog for the selected port appears.
5. Type a name for the heat exchanger in the Name field.
6. Click OK to save the changes.

To name a heat exchanger using the setup dialog for a heat exchanger:

1. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.
2. Click the desired heat exchanger in the EMX Explorer pane. The page specific to that heat exchanger opens in the right pane.
3. Click Setup in the Settings section.
4. Type a name for the heat exchanger in the Name field.
5. Click OK to save the changes.

Configuring Temperature and Fan Thresholds

An LHX heat exchanger is implemented with various sensors for detecting the air temperature, water temperature, and fan speed. You can set thresholds for these sensors so that the EMX alerts you when any sensor readings are getting close to a critical condition. These settings are stored on the EMX port where the heat exchanger is connected, and are lost if that heat exchanger is moved to a different port.

To configure the thresholds for a sensor:

1. Connect the LHX heat exchanger to EMX if it is not already connected.
2. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.
3. Click the desired heat exchanger in the EMX Explorer pane. The page specific to that heat exchanger opens in the right pane.
4. Select the desired sensor in the Sensors table and click Setup Thresholds, or simply double-click that sensor. The setup dialog for the selected sensor appears.
5. Adjust the threshold and deassertion hysteresis settings. The Upper Critical and Lower Critical values are points at which the EMX considers the operating environment critical and outside the range of the acceptable threshold.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 156).
6. Click OK to save the changes.

Monitoring the Heat Exchanger

The EMX web interface lets you monitor the status of each connected LHX heat exchanger as well as the status of each LHX built-in sensor.

Viewing the Summary

Both the Dashboard and Auxiliary Port pages display the summary of all connected LHX heat exchangers, including the RS-485 port number where each heat exchanger is connected, and each heat exchanger's status.

If any LHX heat exchanger is highlighted in red in the summary, it indicates that there is LHX sensor failure on that heat exchanger. View the State or Status column to identify failed sensors.

To view the LHX summary on the Dashboard page:

1. Click the Dashboard icon in the EMX Explorer pane. The Dashboard page opens in the right pane.
2. Locate the LHX Heat Exchanger section where a list of connected LHX heat exchangers is displayed.

To view the LHX summary on the Auxiliary Ports page:

1. If the EMX folder is not expanded, expand it to show all components.

   Note: The EMX folder is named "EMX" by default. The name changes after customizing the device name. See **Naming the EMX Device** *(on page 67).*

2. Click the Auxiliary Ports folder. The Auxiliary Ports page opens in the right pane, listing all RS-485 ports.

Viewing Details

An LHX heat exchanger page shows detailed information, including:

- Device information and settings, such as the RS-485 port number and device name
- The air outlet temperature
- Readings and states of all LHX built-in sensors
- Accumulative operating hours
- Errors, such as failed LHX sensors or emergency cooling activation

To view details of a specific LHX heat exchanger:

1. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.

   Click the desired heat exchanger in the EMX Explorer pane. The page specific to that heat exchanger opens in the right pane.

If any LHX sensor reading reaches or crosses the critical or warning threshold, that sensor reading row is highlighted in red or yellow. See ***Readings Highlighted in Yellow or Red*** (on page 54).

Device States and Icon Variations

The EMX web interface changes icons to represent different statuses of each connected LHX heat exchanger.

Icons	Device status
	The heat exchanger is turned ON and operating normally.
	The heat exchanger is turned OFF.
	The heat exchanger is turned ON but enters the critical state because of any LHX sensor failure.
	At least one of the LHX sensor readings has crossed the upper or lower warning threshold.
	NO device is detected on this RS-485 port.

To identify the cause of the critical state, view one of the following:

- The LHX Heat Exchanger section of the Dashboard page. See ***Monitoring the Heat Exchanger*** (on page 177).
- The Auxiliary Ports page. See ***Monitoring the Heat Exchanger*** (on page 177).
- The Alert States section of the LHX heat exchanger page. See ***Alert States and LHX Event Log*** (on page 179).

Alert States and LHX Event Log

When an LHX heat exchanger is physically connected to the EMX device, a section labeled Alert States appears on its device page. The Alert States section shows information identifying the LHX sensors that currently fail.

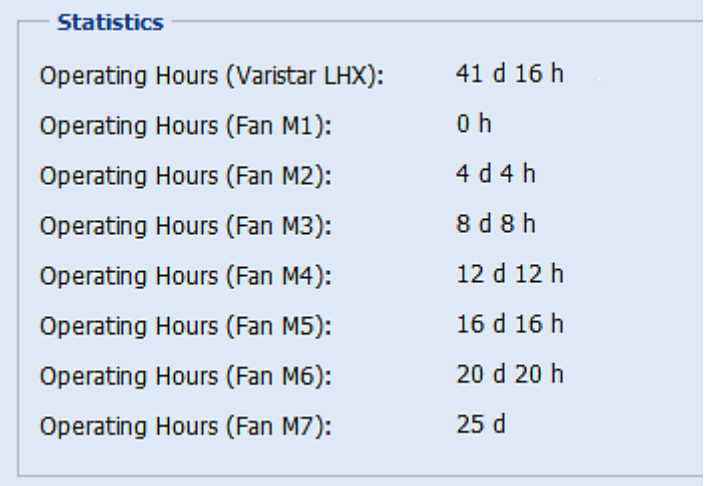
Tip: The Dashboard and Auxiliary Ports pages also point out failed sensors. See **Monitoring the Heat Exchanger** *(on page 177).*

A button labeled Show Event Log is located in the Alert States section. To view the events associated with the EMX, click this button.

Operating Hours

Operating hours are the accumulative time since the LHX heat exchanger is first connected to the EMX device and turned ON.

The EMX web interface displays the operating hours both for the heat exchanger and its fans. Operating hour information is located in the Statistics section of each heat exchanger page.



Below are the time units used for operating hours:

- h: hour(s)
- d: day(s)

For example, "3d 5h" means the total operating time is 3 days and 5 hours.

Controlling the Heat Exchanger

The EMX allows you to remotely turn on or off a connected heat exchanger.

To control the LHX heat exchanger:

1. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.

   Click the desired heat exchanger in the EMX Explorer pane. The page specific to that heat exchanger opens in the right pane.

2. Locate the Information section.
   - To turn off the LHX heat exchanger, click Switch Off.
   - To turn on the LHX heat exchanger, click Switch On.

3. If you clicked Switch Off in the previous step, a dialog appears, prompting you to confirm the operation. Click Yes to turn it off or No to abort the operation.

The heat exchanger's icon shown in the web interface changes after being turned on or off. See ***Device States and Icon Variations*** (on page 179).

Chapter 9 Using SNMP

This SNMP section helps you set up the EMX for use with an SNMP manager. The EMX can be configured to send traps to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

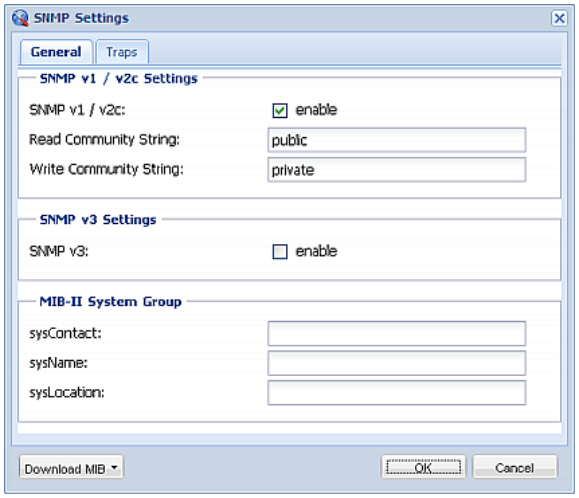
Enabling SNMP 182
Configuring Users for Encrypted SNMP v3 183
Configuring SNMP Traps.....184
SNMP Gets and Sets 185

Enabling SNMP

To communicate with an SNMP manager, you must first enable the SNMP agent on the EMX device.

To enable SNMP:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."

- Type the read/write community string in the Write Community String field. Usually the string is "private."

3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

Tip: You can permit or disallow a user to access the EMX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 183).*

4. Type the SNMP MIB-II sysContact value in the sysContact field.
5. Type the SNMP MIB-II sysName value in the sysName field.
6. Type the SNMP MIB-II sysLocation value in the sysLocation field.
7. Click OK to save the changes.

Important: You must download the SNMP MIB for your EMX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see *Downloading SNMP MIB* (on page 185).

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and the EMX.

To configure users for SNMP v3 encrypted communication:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 58).
5. Click OK to save the changes. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Traps

The EMX automatically keeps an internal log of events that occur. See ***Configuring Event Rules*** (see "***Event Rules and Actions***" on page 118). These events can also be used to send SNMP traps to a third party manager.

To configure the EMX to send SNMP traps:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the System SNMP Trap Rule.
3. Select the Enabled checkbox to enable this event rule.
4. Click Save to save the changes.
5. Click the Actions tab if you have not configured the SNMP trap actions.
6. Select System SNMP Trap Action to set up the trap destinations.
7. Type an IP address in the Host 1 field. This is the address to which traps are sent by the SNMP system agent.
8. Type the communication port number in the Port 1 field.
9. Type the name of the SNMP community in the Community field. The community is the group representing the EMX and all SNMP management stations.
10. To specify more than one SNMP trap destination, repeat Steps 8 to 10 for additional destinations. A maximum of 3 destinations can be specified.
11. Click Save to save the changes.
12. Click Close to quit the dialog.

Note: You should update the MIB used by your SNMP manager when updating to a new EMX release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** *(on page 185).*

SNMP Gets and Sets

In addition to sending traps, the EMX is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the EMX, such as the system location.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the EMX device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The EMX does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom EMX MIB.

The EMX MIB

The SNMP MIB file is required for using your EMX device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for the EMX can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

To download the file from the SNMP Settings dialog:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB. A submenu of MIB files appear.
3. Select the desired MIB file to download.
   - EMD-MIB: The SNMP MIB file for managing the EMX device.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
   - LHX-MIB: The SNMP MIB file for managing the LHX heat exchanger(s).

   Note: Schroff LHX Support must be enabled in order for the LHX-MIB to be available. See **Enabling and Disabling Schroff LHX Heat Exchanger Support** *(on page 175).*
4. Click Save to save the file onto your computer.

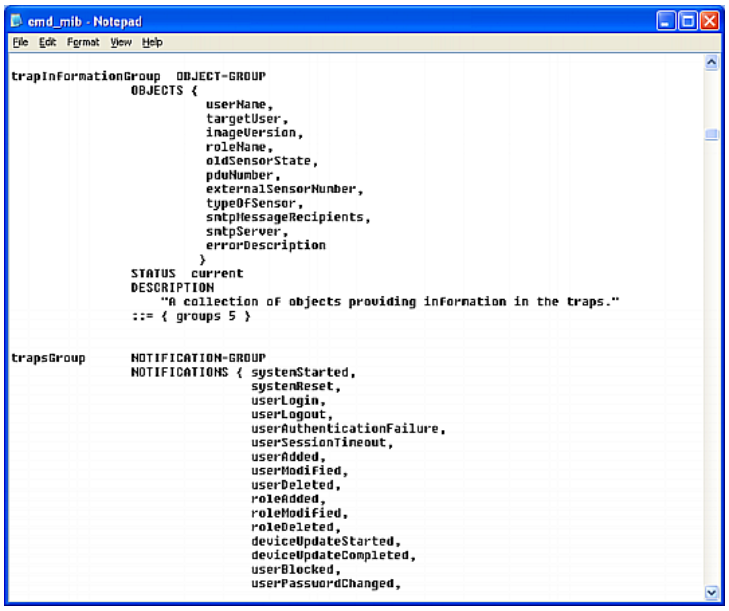
To download the file from the Device Information dialog:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Click the "download" link in the EMD-MIB, ASSETMANAGEMENT-MIB or LHX-MIB field to download the desired SNMP MIB.
3. Click Save to save the file onto your computer.

Layout

Opening the MIB reveals the custom objects that describe the EMX system.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



For example, the measurementsGroup group contains objects for environmental sensors connected to the EMX device. One object listed under this group, measurementsExternalSensorState, is described later in the MIB as "The sensor state." boardFirmwareVersion, part of the configGroup group, describes the firmware version.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the EMX to generate a warning and send an SNMP trap when certain parameters are exceeded. See ***Threshold Information*** (on page 156) for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

Chapter 10 Using the Command Line Interface

In This Chapter

About the Interface 188
Logging in to CLI 188
Help Command 191
Showing Information 192
Configuring the EMX Device and Network 204
Unblocking a User 290
Resetting the EMX 291
Network Troubleshooting 292
Querying Available Parameters for a Command 295
Retrieving Previous Commands 295
Automatically Completing a Command 296
Logging out of CLI 296
Resetting to Factory Defaults (CLI) 296

About the Interface

The EMX provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the EMX device
- Display the EMX and network information, such as the device name, firmware version, IP address, and so on
- Configure the EMX and network settings
- Troubleshoot network problems

You can access the interface over a serial connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying the Network Service Settings** *(on page 79).*

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

With HyperTerminal

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

To log in using HyperTerminal:

1. Connect your computer to the EMX device via a local connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

   Make sure the COM port settings use this configuration:

   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can find out which COM port is assigned to the EMX by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion Serial Console" under the Ports group.

3. Press Enter. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters. Then you are prompted to enter a password.

   ```
   Username: admin
   Password: _
   ```

5. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.

   After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 191) for details.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the EMX web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the EMX device.

With SSH or Telnet

You can remotely log in to the command line interface using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

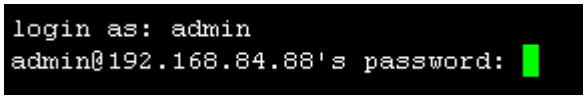
To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled. See ***Modifying the Network Service Settings*** (on page 79).
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

3. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters.

   Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

   Then you are prompted to enter a password.



4. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.
5. After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 191) for details.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the EMX web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the EMX device.

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who does not have full permissions to configure the EMX device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the EMX device, the # prompt appears.
- Configuration Mode: You can enter the configuration mode from the administrator mode. In this mode, the prompt changes to **config:#** and you can change EMX device and network configurations. See ***Entering the Configuration Mode*** (on page 204).
- Diagnostic Mode: You can enter the diagnostic mode from the administrator mode. In this mode, the prompt changes to **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See ***Entering the Diagnostic Mode*** (on page 292).

Closing a Serial Connection

Close the window or terminal emulation program when you finish accessing a EMX device over the serial connection.

When accessing or upgrading multiple EMX devices, do not transfer the serial cable from one device to another without closing the serial connection window first.

Help Command

The help command shows a list of main CLI commands. This is helpful when you are not familiar with the commands.

The help command syntax is:

```
#     help
```

Press Enter after typing the command, and a list of main commands is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding a question mark to the end of the command. See **Querying Available Parameters for a Command** *(on page 295).*

Showing Information

You can use the show commands to view current settings or status of the EMX device or part of it, such as the IP address, networking mode, firmware version, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt.

Network Configuration

This command shows all network configuration, such as the IP address, networking mode, and MAC address.

```
#        show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

```
#        show network ip <option>
```

Variables:

- <option> is one of the options: *all*, *v4* or *v6*.

Option	Description
all	This options shows both of IPv4 and IPv6 settings. *Tip: You can also type the command without adding this option "all" to get the same data.*
v4	This option shows the IPv4 settings only.
v6	This option shows the IPv6 settings only.

LAN Interface Settings

This command shows the LAN interface information only, such as LAN interface speed, duplex mode, and current LAN interface status.

```
#        show network interface
```

Networking Mode

This command shows whether the current networking mode is wired or wireless.

```
#        show network mode
```

Note: If the EMX is a slave device connected to the LAN via the master Dominion PX or EMX device, the `show network mode` *command displays* wired(USB) *instead of* wired.

Wireless Configuration

This command only shows the wireless configuration of the EMX device, such as the SSID parameter.

```
#        show network wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show network wireless details
```

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS and SSH services, and SNMP settings.

```
#       show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
zeroconfig	Only displays the settings of the zero-config(uration) advertising.

Asset Sensor Settings

This command shows the asset sensor settings, such as the total number of rack units (tag ports), asset sensor state, numbering mode, orientation, available tags and LED color settings.

```
#        show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset sensor information. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific asset sensor number	Displays the settings of the asset sensor connected to the specified FEATURE port number. For the EMX device with only one FEATURE port, the valid number is always 1.

This command syntax sets the LED color for all rack units on the connected asset sensor(s) to indicate the absence of a connected asset tag.

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Environmental Sensor Information

This command syntax shows specified environmental sensor's information.

```
#        show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor externalsensor <n> details
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the EMX web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.

Note: For a discrete (on/off) sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#        show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show externalsensors <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all environmental sensors. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the EMX web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A discrete (on/off) sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number and X, Y, and Z coordinates.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#        show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show sensor externalsensor <n> details
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the EMX web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.

Note: For a discrete (on/off) sensor, the threshold-related and accuracy-related data is NOT available.

Security Settings

This command shows the security settings of the EMX.

```
#        show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time and user idle timeout.

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
#        show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, "enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred temperature unit and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#        show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

Rack Unit Settings of an Asset Sensor

For the Raritan asset sensor, a rack unit refers to a tag port. This command shows the settings of a specific rack unit or all rack units on an asset sensor, such as a rack unit's LED color and LED mode.

```
#        show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset sensor. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the settings of the specified rack unit on the specified asset sensor. Use the index number to specify the rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.

Blade Extension Strip Settings

This command shows the information of a blade extension strip, including the total number of tag ports, and if available, the ID (barcode) number of any connected tag.

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit (tag port) on the selected asset sensor. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <blade_slot> is one of the options: *all* or a specific number of a tag port on the blade extension strip.

Option	Description
all	Displays the information of all tag ports on the specified blade extension strip connected to a particular rack unit. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the information of the specified tag port on the blade extension strip connected to a particular rack unit. The number of each tag port on the blade extension strip is available on the Asset Strip page.

Command History

This command syntax shows the command history for current connection session.

```
#       show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing the history commands.

```
#        show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Configuring the EMX Device and Network

To configure the EMX device or network settings through the CLI, you must log in as the administrator.

Entering the Configuration Mode

You must enter the configuration mode since configuration commands function in the configuration mode only.

To enter the configuration mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.

   Note: If you enter the configuration mode from the user mode, you may have limited permissions to make configuration changes. See **Different CLI Modes and Prompts** *(on page 191).*

2. Type `config` and press Enter. The config:# prompt appears, indicating that you have entered the configuration mode.

   ```
   config:# _
   ```

3. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the "apply" command before closing the terminal emulation program.

Closing the program does not save any configuration changes. See *Quitting the Configuration Mode* (on page 290).

Device Configuration Commands

A device configuration command begins with *emd*. You can use the device configuration commands to change the settings that apply to the whole EMX device.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the Device Name

This command syntax changes the EMX device's name.

```
config:#    emd name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "my emx888" to the EMX device.

```
config:#    emd name "my emx888"
```

Setting the Z Coordinate Format for Environmental Sensors

This command syntax enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#    emd externalSensorsZCoordinateFormat <option>
```

Variables:

- <option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** *(on page 256).*

Example

The following command determines that the unit of rack is used for specifying the Z coordinate of environmental sensors.

```
config:#    emd externalSensorsZCoordinateFormat rackUnits
```

Enabling or Disabling Data Logging

This command syntax enables or disables the data logging feature.

```
config:#    emd dataRetrieval <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see ***Setting Data Logging*** (on page 150).

Example

The following command enables the data logging feature.

```
config:#    emd dataRetrieval enable
```

Setting the Data Logging Measurements Per Entry

This command syntax defines the number of measurements accumulated per log entry.

```
config:#    emd measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

For more information, see ***Setting Data Logging*** (on page 150).

Example

The following command determines that 66 measurements are accumulated per log entry for sensors, that is, 66 seconds.

```
config:#    emd measurementsPerLogEntry 66
```

Networking Configuration Commands

A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Setting the Networking Mode

If your EMX device is implemented with both of the wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command syntax enables the wired or wireless networking mode.

```
config:#   network mode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and the EMX does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Example

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Configuring IP Protocol Settings

By default, only the IPv4 protocol is enabled. You can enable both the IPv4 and IPv6 protocols, or only the IPv6 protocol for your EMX device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command syntax determines which IP protocol is enabled on the EMX.

```
config:#   network ip proto <protocol>
```

Variables:

- <protocol> is one of the options: *v4Only*, *v6Only* or *both*.

Mode	Description
v4Only	Enables IPv4 only on all interfaces. This is the default.
v6Only	Enables IPv6 only on all interfaces.
both	Enables both IPv4 and IPv6 on all interfaces.

Example

The following command determines that both of IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Selecting IPv4 or IPv6 Addresses

This command syntax determines which IP address is used when the DNS server returns both of IPv4 and IPv6 addresses. You need to configure this setting only after both of IPv4 and IPv6 protocols are enabled on the EMX.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variables:

- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Example

The following command determines that only IPv4 addresses returned by the DNS server are used.

```
config:#   network ip dnsResolverPreference preferV4
```

Setting the Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the SSID

This command syntax specifies the SSID string.

```
config:#   network wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

The following command assigns "myssid" as the SSID.

```
config:#   network wireless SSID myssid
```

Setting the Authentication Method

This command syntax sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#   network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Example

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command syntax.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

This command assigns "encryp-key" as the PSK.

```
config:#   network wireless PSK encryp-key
```

Setting the EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

Setting the Outer Authentication

This command syntax determines the outer authentication protocol for the EAP.

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

Variables:

- The value of <outer_auth> is *PEAP* because EMX only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.

Example

The following command determines the outer authentication protocol for the EAP authentication is Protected Extensible Authentication Protocol (PEAP).

```
config:#   network wireless eapOuterAuthentication PEAP
```

Setting the Inner Authentication

This command syntax determines the inner authentication protocol for the EAP.

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

Variables:

- The value of <inner_auth> is *MSCHAPv2* because EMX only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.

Example

The following command determines the inner authentication protocol for the EAP authentication is MSCHAPv2.

```
config:#   network wireless eapInnerAuthentication MSCHAPv2
```

Setting the EAP Identity

This command syntax determines the EAP identity.

```
config:#   network wireless eapIdentity <identity>
```

Variables:

- <identity> is your user name for the EAP authentication.

Example

The following command sets the EAP identity to "eap_user01."

```
config:#   network wireless eapIdentity eap_user01
```

Setting the EAP Password

This command syntax determines the EAP password.

```
config:#   network wireless eapPassword
```

Variables:

- <password> is your password for EAP authentication.

Example

The following command sets the EAP password to "user01_password."

```
config:#   network wireless eapPassword user01_password
```

Providing the EAP CA Certificate

You may need to provide a third-party CA certificate for the EAP authentication.

To provide a CA certificate:

1. Type the CA certificate command as shown below and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

2. The system prompts you to enter the contents of the CA certificate. Do the following to input the contents:
   a. Open your CA certificate with a text editor.
   b. Copy the contents between the "--- BEGIN CERTIFICATE ---" and "--- END CERTIFICATE ---" lines in a certificate.
   c. Paste the certificate contents into the terminal.

d. Press Enter.

Tip: To remove an existing CA certificate, simply press Enter without typing or pasting anything when the system prompts you to input the certificate contents.

3. If the certificate is valid, the system shows the command prompt "`config:#`" again. If not, it shows a message indicating that the certificate is not valid.

Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

To provide a CA certificate:

1. Make sure you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 204).
2. Type the following command and press Enter.

   ```
   config:#  network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE" as illustrated below.

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

   ```
   config:#
   ```

Setting the BSSID

This command syntax specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is the MAC address of the wireless access point.

Example

The following command specifies that the BSSID is 00:14:6C:7E:43:81.

```
config:#   network wireless BSSID 00:14:6C:7E:43:81
```

Configuring the IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv4 Configuration Mode

This command syntax determines the IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Example

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Setting the Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command syntax:

```
config:#   network ipv4 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Example

The following command sets the preferred host name to "my-host."

```
config:#   network ipv4 preferredHostName my-host
```

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the EMX device.

```
config:#   network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your EMX device. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command assigns the static IPv4 address "192.168.84.222" to the EMX device.

```
config:#   network ipv4 ipAddress 192.168.84.222
```

Setting the IPv4 Subnet Mask

After selecting the static IP configuration mode, you can use this command syntax to define the subnet mask.

```
config:#   network ipv4 subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the subnet mask to 192.168.84.0.

```
config:#   network ipv4 subnetMask 192.168.84.0
```

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the IPv4 gateway to 255.255.255.0.

```
config:#   network ipv4 gateway 255.255.255.0
```

Setting the IPv4 Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server.

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command determines that the primary DNS server is 192.168.84.30.

```
config:#   network ipv4 primaryDNSServer 192.168.84.30
```

Setting the IPv4 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server.

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Note: The EMX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the EMX only uses the primary IPv4 and IPv6 DNS servers.

Example

The following command determines that the secondary DNS server is 192.168.84.33.

```
config:#   network ipv4 secondaryDNSServer 192.168.84.33
```

Overriding the IPv4 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS enable
```

Configuring the IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv6 Configuration Mode

This command syntax determines the IP configuration mode.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Example

The following command sets the IP configuration mode to the static IP address mode.

```
config:#   network ipv6 ipConfigurationMode static
```

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the EMX device.

```
config:#   network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your EMX device. This value uses the IPv6 address format.

Example

The following command assigns the static IPv6 address "3210:4179:0:8:0:800:200C:417A" to the EMX device.

```
config:#   network ipv6 ipAddress 3210:4179:0:8:0:800:200C:417A
```

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Example

The following command sets the gateway to 500:0:330:0:4:9:3:2.

```
config:#   network ipv6 gateway 500:0:330:0:4:9:3:2
```

Setting the IPv6 Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server. It is required to enable overriding the auto-assigned DNS server before you can specify the DNS servers manually. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 223).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. This value uses the IPv6 address format.

Example

The following command determines that the primary DNS server is 2103:288:8201:1::14.

```
config:#   network ipv6 primaryDNSServer 2103:288:8201:1::14
```

Setting the IPv6 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server. It is required to enable overriding the auto-assigned DNS server before you can specify the DNS servers manually. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 223).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. This value uses the IPv6 address format.

Note: The EMX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the EMX only uses the primary IPv4 and IPv6 DNS servers.

Example

The following command determines that the secondary DNS server is 2103:288:8201:1::700.

```
config:#   network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

Overriding the IPv6 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS enable
```

Setting the LAN Interface Parameters

A LAN interface configuration command begins with *network interface*.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the LAN Interface Speed

This command syntax determines the LAN interface speed.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Example

The following command lets the EMX determine the optimal LAN interface speed through auto-negotiation.

```
config:#   network interface LANInterfaceSpeed auto
```

Changing the LAN Duplex Mode

This command syntax determines the LAN interface duplex mode.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The EMX selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the EMX device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Example

The following command lets the EMX determine the optimal transmission mode through auto-negotiation.

```
config:#   network interface LANInterfaceDuplexMode auto
```

Setting the Network Service Parameters

A network service command begins with *network services*.

Changing the HTTP Port

This command syntax changes the HTTP port.

```
config:#   network services http <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.

Example

The following command sets the HTTP port to 81.

```
config:#   network services http 81
```

Changing the HTTPS Port

This command syntax changes the HTTPS port.

```
config:#   network services https <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.

Example

The following command sets the HTTPS port to 333.

```
config:#   network services https 333
```

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command syntax enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

Example

The following command enables the Telnet service.

```
config:#   network services telnet enabled true
```

Changing the Telnet Port

This command syntax changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Example

The following command syntax sets the TCP port for Telnet to 44.

```
config:#   network services telnet port 44
```

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command syntax enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Example

The following command enables the SSH service.

```
config:#   network services ssh enabled true
```

Changing the SSH Port

This command syntax changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Example

The following command syntax sets the TCP port for SSH to 555.

```
config:#   network services ssh port 555
```

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:#   network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Specifying the SSH Public Key*** (on page 274).

Example

The following command causes users to have to type a password for the SSH login. Use of the SSH public key is not permitted.

```
config:#   network services ssh authentication passwordOnly
```

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command syntax enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.

Option	Description
disable	The SNMP v1/v2c protocol is disabled.

Example

The following command enables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c enable
```

Enabling or Disabling SNMP v3

This command syntax enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Example

The following command enables the SNMP v3 protocol.

```
config:#   network services snmp v3 enable
```

Setting the SNMP Read Community

This command syntax sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Example

This command syntax sets the SNMP read-only community string to "public."

```
config:#   network services snmp readCommunity public
```

Setting the SNMP Write Community

This command syntax sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Example

The following command sets the SNMP read/write community string to "private."

```
config:#   network services snmp writeCommunity private
```

Setting the sysContact Value

This command syntax sets the SNMP sysContact MIB-II value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysContact to "John_Krause."

```
config:#   network services snmp sysContact John_Krause
```

Setting the sysName Value

This command syntax sets the SNMP sysName MIB-II value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysName to "Win7_system"

```
config:#   network services snmp sysName Win7_system
```

Setting the sysLocation Value

This command syntax sets the SNMP sysLocation MIB-II value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysLocation to "New_TAIPEI"

```
config:#   network services snmp sysLocation New_TAIPEI
```

Security Configuration Commands

A security configuration command begins with *security*.

Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the EMX device from specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying the Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- **IPv4 commands**

To enable or disable the IPv4 firewall control feature, use this command syntax:

```
config:#   security ipAccessControl ipv4 enabled <option>
```

To determine the default IPv4 firewall control policy, use this command syntax:

```
config:#   security ipAccessControl ipv4 defaultPolicy <policy>
```

- **IPv6 commands**

To enable or disable the IPv6 firewall control feature, use this command syntax:

```
config:#   security ipAccessControl ipv6 enabled <option>
```

To determine the default IPv6 firewall control policy, use this command syntax:

```
config:#   security ipAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.

Option	Description
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command sets up two parameters of the IPv4 access control feature.

```
config:#    security ipAccessControl ipv4 enabled true defaultPolicy accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy is set to "accept."

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command syntax for adding a rule varies.

- **IPv4 commands**

To add a new rule to the bottom of the IPv4 rules list, use this command syntax:

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy>
```

To add a new IPv4 rule by inserting it above or below a specific rule, use this command syntax:

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy>
            <insert> <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv4 rule add <insert>
            <rule_number> <ip_mask> <policy>
```

- **IPv6 commands**

To add a new rule to the bottom of the IPv6 rules list, use this command syntax:

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy>
```

To add a new IPv6 rule by inserting it above or below a specific rule, use this command syntax:

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy> <insert> <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv6 rule add <insert> <rule_number> <ip_mask> <policy>
```

Variables:

- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from the specified IP address(es).
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:#    security ipAccessControl ipv4 rule add
            192.168.84.123/24 accept insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added, allowing all packets from the IPv4 address 192.168.84.123 to be accepted.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command syntax varies.

- **IPv4 commands**

▶ **The command syntax to modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#    security ipAccessControl ipv4 rule modify
            <rule_number> ipMask <ip_mask>
```

▶ **The command syntax to modify an IPv4 rule's policy:**

```
config:#    security ipAccessControl ipv4 rule modify
            <rule_number> policy <policy>
```

The command syntax to modify all contents of an existing IPv4 rule:

```
config:#    security ipAccessControl ipv4 rule modify
            <rule_number> ipMask <ip_mask> policy
            <policy>
```

- **IPv6 commands**

The command syntax to modify an IPv6 rule's IP address and/or subnet mask:

```
config:#    security ipAccessControl ipv6 rule modify
            <rule_number> ipMask <ip_mask>
```

The command syntax to modify an IPv6 rule's policy:

```
config:#    security ipAccessControl ipv6 rule modify
            <rule_number> policy <policy>
```

The command syntax to modify all contents of an IPv6 existing rule:

```
config:#    security ipAccessControl ipv6 rule modify
            <rule_number> ipMask <ip_mask> policy
            <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from the specified IP address(es).

Option	Description
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

Example

The following command modifies all contents of the 5th IPv4 rule.

```
config:#    security ipAccessControl ipv4 rule modify 5
            ipMask 192.168.84.123/24 policy accept
```

Results:

- The IPv4 address is changed to 192.168.84.123, and the subnet mask to 255.255.255.0.
- The policy now becomes "accept."

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

- **IPv4 commands**

```
config:#    security ipAccessControl ipv4 rule delete <rule_number>
```

- **IPv6 commands**

```
config:#    security ipAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 5th rule from the IPv6 access control list.

```
config:#   security ipAccessControl ipv6 rule delete 5
```

HTTPS Access

This command determines whether the HTTPS access to the EMX web interface is forced. If yes, all HTTP access attempts are automatically directed to HTTPS.

```
config:#   security enforceHttpsForWebAccess <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the HTTPS access to the web interface.
disable	Disables the HTTPS access to the web interface.

Example

The following command disables the HTTPS access feature.

```
config:#   security enforceHttpsForWebAccess disable
```

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before being forced to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify the login limitation parameters at a time. See ***Multi-Command Syntax*** (on page 289).

Single Login Limitation

This command syntax enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:#   security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Example

The following command disables the single login feature so that more than one user can log in using the same user name at the same time.

```
config:#   security loginLimits singleLogin disable
```

Password Aging

This command syntax enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:#   security loginLimits passwordAging <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Example

The following command enables the password aging feature.

```
config:#   security loginLimits passwordAging enable
```

Password Aging Interval

This command syntax determines how often the password should be changed.

```
config:#   security loginLimits passwordAgingInterval <value>
```

Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Example

The following command sets the password again interval to 90 days.

```
config:#   security loginLimits passwordAgingInterval 90
```

Idle Timeout

This command syntax determines how long a user can remain idle before that user is forced to log out of the EMX web interface.

```
config:#   security loginLimits idleTimeout <value>
```

Variables:

- <value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

Example

The following command sets the idle timeout to 10 munites.

```
config:#   security loginLimits idleTimeout 10
```

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

- **To determine the maximum number of failed logins before blocking a user, use this command syntax:**

```
config:#    security userBlocking maximumNumberOfFailedLogins <value1>
```

- **To determine how long a user's login is blocked, use this command syntax:**

```
config:#    security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value in minutes.

Tip: You can combine multiple commands to modify the user blocking parameters at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command sets up two user blocking parameters.

```
config:#    security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time. See ***Multi-Command Syntax*** (on page 289).

Enabling or Disabling Strong Passwords

This command syntax enables or disables the strong password feature.

```
config:#   security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Example

This command syntax enables the strong password feature.

```
config:#   security strongPasswords enabled true
```

Minimum Password Length

This command syntax determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Example

This command syntax determines a password must comprise at least 8 characters.

```
config:#    security strongPasswords minimumLength 8
```

Maximum Password Length

This command syntax determines the maximum length of the password.

```
config:#    security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Example

This command syntax determines that a password must NOT comprise more than 20 characters.

```
config:#    security strongPasswords maximumLength 20
```

Lowercase Character Requirement

This command syntax determines whether a strong password includes at least a lowercase character.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Example

This command syntax determines that a password must include at least a lowercase character.

```
config:#    security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

Uppercase Character Requirement

This command syntax determines whether a strong password includes at least a uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Example

This command determines a password must comprise at least one uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

Numeric Character Requirement

This command syntax determines whether a strong password includes at least a numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Example

The following command determines that a password must comprise at least one numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter enable
```

Special Character Requirement

This command syntax determines whether a strong password includes at least a special character.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Example

The following command determines that a password must comprise at least one special character.

```
config:#    security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

Maximum Password History

This command syntax determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#    security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Example

The following command determines that the previous 7 passwords CANNOT be re-used when changing the password.

```
config:#    security strongPasswords passwordHistoryDepth 7
```

Role-Bassed Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying the Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- **IPv4 commands**

▶ **To enable or disable the IPv4 role-based access control feature, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 enabled <option>
```

▶ **To determine the IPv4 role-based access control policy, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- **IPv6 commands**

▶ **To enable or disable the IPv6 role-based access control feature, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 enabled <option>
```

▶ **To determine the IPv6 role-based access control policy, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command sets two parameters of the role-based IPv4 access control feature.

```
config:#    security roleBasedAccessControl ipv4 enabled true defaultPolicy allow
```

Results:

- The role-based IPv4 access control feature is enabled.
- The default policy is set to "allow."

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

- An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.
- An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

- **IPv4 commands**

▶ **To add a new rule to the bottom of the IPv4 rules list, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **To add a new IPv4 rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role> <policy>
          <insert> <rule_number>
```

- **IPv6 commands**

▶ **To add a new rule to the bottom of the IPv6 rules list, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
```

▶ **To add a new IPv6 rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role> <policy>
          <insert> <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command creates a newIPv4 role-based access control rule and specifies its location in the list.

```
config:# security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100 admin
deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- **IPv4 commands**

To modify a rule's IPv4 address range, use this command syntax:

```
config:# security roleBasedAccessControl ipv4 rule modify <rule_number>
startIpAddress <start_ip> endIpAddress <end_ip>
```

To modify an IPv4 rule's role, use this command syntax:

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

- **To modify an IPv4 rule's policy, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> policy <policy
```

- **To modify all contents of an existing IPv4 rule, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- **IPv6 commands**

- **To modify a rule's IPv6 address range, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

- **To modify an IPv6 rule's role, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

- **To modify an IPv6 rule's policy, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> policy <polic
```

- **To modify all contents of an existing IPv6 rule, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Example

The following command modifies all contents of the 8th IPv4 rule.

```
config:#    security roleBasedAccessControl ipv4 rule modify 8
            startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
            policy allow
```

Results:

- The starting IPv4 address is changed to 192.168.8.8, and the ending IPv4 address to 192.168.90.90.
- The role is changed to "operator."
- The policy now becomes "allow."

Deleting a Role-Based Access Control Rule

This command removes a specific rule from the list.

- **IPv4 commands**

```
config:#    security roleBasedAccessControl ipv4 rule delete <rule_number>
```

- **IPv6 commands**

```
config:#    security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 7th IPv6 rule.

```
config:#    security roleBasedAccessControl ipv6 rule delete 7
```

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

Changing the Sensor Name

This command syntax names an environmental sensor.

```
config:#    externalsensor <n> name "<name>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#    externalsensor 4 name "Cabinet humidity"
```

Specifying the Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party detectors/switches, and you must specify the type of connected detector/switch for proper operation. Use this command syntax when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Example

The following indicates that a smoke detector is being connected to Raritan's contact closure sensor (DPX-CC2-TR) whose ID number shown in the EMX web interface is 2.

```
config:#   externalsensor 2 sensorSubType smokeDetection
```

Setting the X Coordinate

This command syntax specifies the X coordinate of an environmental sensor.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 2nd cabinet" to the X coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

Setting the Y Coordinate

This command syntax specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 4th row" to the Y coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 ylabel "The 4th row"
```

Setting the Z Coordinate

This command syntax specifies the Z coordinate of an environmental sensor.

config:# externalsensor <n> zlabel "<coordinate>"

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units. See **Setting the Z Coordinate Format for Environmental Sensors** *(on page 206).*

Example

The following command sets the value "The 5th rack" to the Z coordinate of the environmental sensor with the ID number 4 after the Z coordinate's format is set to *freeForm*.

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

Changing the Sensor Description

This command syntax provides a description for a specific environmental sensor.

```
config:#   externalsensor <n> description "<description>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command gives the description "humidity detection" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 description "humidity detection"
```

Environmental Sensor Threshold Configuration Commands

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

Setting the Sensor's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified environmental sensor.
disable	Disables the upper critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper critical threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#   sensor externalsensor 2 temperature upperCritical 40
```

Setting the Sensor's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified environmental sensor.
disable	Disables the upper warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper warning threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command enables the Upper Warning threshold of the environmental "temperature" sensor with the ID number 4.

```
config:#   sensor externalsensor 4 temperature upperWarning enable
```

Setting the Sensor's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified environmental sensor.
disable	Disables the lower critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower critical threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command sets the Lower Critical threshold of the environmental "humidity" sensor with the ID number 1 to 15%. It also enables the lower critical threshold if this threshold has not been enabled yet.

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

Setting the Sensor's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified environmental sensor.
disable	Disables the lower warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower warning threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command disables the Lower Warning threshold of the environmental "humidity" sensor with the ID number 3.

```
config:#   sensor externalsensor 3 humidity lowerWarning disable
```

Setting the Sensor's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***What is Deassertion Hysteresis?*** (on page 156) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the environmental "temperature" sensor with the ID number 4 to 2 degrees Celsius. That is, the temperature must drop by at least 2 degrees Celsius below the upper threshold or rise by at least 2 degrees Celsius above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor externalsensor 4 temperature hysteresis 2
```

Setting the Sensor's Assertion Timeout

This command syntax configures the assertion timeout value of a numeric environmental sensor.

```
config:#    sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the EMX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. See ***What is Assertion Timeout?*** (on page 157).

Example

The following command sets the assertion timeout of the environmental "temperature" sensor with the ID number 3 to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#    sensor externalsensor 3 temperature assertionTimeout 4
```

User Configuration Commands

Most of user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command syntax creates a new user profile.

```
config:#    user create <name> <option> <roles>
```

After performing the user creation command, the EMX prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.
- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 289).*

Changing a User's Password

This command syntax allows you to change an existing user's password if you have the Administrator Privileges.

```
config:#   user modify <name> password
```

After performing the above command, EMX prompts you to enter a new password. Then:

1. Type a new password and press Enter.
2. Re-type the new password for confirmation and press Enter.

Variables:

- <name> is the name of the user whose settings you want to change.

Example

The following procedure illustrates how to change the password of the user "May."

1. Verify that you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 204).
2. Type the following command to change the password for the user profile "May."

   ```
   config:#   user modify May password
   ```
3. Type a new password when prompted, and press Enter.
4. Type the same new password and press Enter.
5. If the password change is completed successfully, the config:# prompt appears.

Modifying a User's Personal Data

You can change a user's personal data, including the user's full name, telephone number, and email address.

To change a user's full name, use this command syntax:

```
config:#   user modify <name> fullName "<full_name>"
```

To change a user's telephone number, use this command syntax:

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

To change a user's email address, use this command syntax:

```
config:#   user modify <name> eMailAddress <email_address>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.
- <email_address> is the email address of the specified user.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 289).*

Example

The following command modifies two parameters for the user profile -- May:

```
config:#   user modify May fullName "May Turner" telephoneNumber 123-4567
```

Results:

- May's full name is specified as May Turner.
- May's telephone number is set to 123-4567.

Enabling or Disabling a User Profile

This command syntax enables or disables a user profile. A user can log in to the EMX device only after that user's user profile is enabled.

```
config:#   user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Example

The following command enables the user profile -- May.

```
config:#   user modify May enabled true
```

Forcing a Password Change

This command syntax determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:#    user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Example

The following command enforces a password change on May's next login.

```
config:#    user modify May forcePasswordChangeOnNextLogin true
```

Modifying the SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See ***Multi-Command Syntax*** (on page 289).

To enable or disable the SNMP v3 access to EMX for the specified user:

```
config:#    user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

To determine the security level:

```
config:#    user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

To determine whether the authentication passphrase is identical to the password:

```
config:#    user modify <name> userPasswordAsAuthenticationPassPhrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

To determine the authentication passphrase:

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising up to 32 ASCII printable characters.

To determine whether the privacy passphrase is identical to the authentication passphrase:

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.
false	Privacy passphrase is different from the authentication passphrase.

To determine the privacy passphrase:

```
config:#    user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <privacy_passphrase> is a string used as a privacy passphrase, comprising up to 32 ASCII printable characters.

To determine the authentication protocol:

```
config:#    user modify <name> authenticationProtocol <option5>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

To determine the privacy protocol:

```
config:#    user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.
AES-128	AES-128 privacy protocol is applied.

Example

The following command sets three SNMPv3 prameters of the user "May."

```
config:#    user modify May snmpV3Access enable securityLevel authNoPriv
            userPasswordAsAuthenticationPassPhrase true
```

Results:

- The user's SNMPv3 access permission is enabled.
- The SNMPv3 security level is authentication only, no privacy.
- The authentication passphrase is identical to the user's password.

Changing the Role(s)

This command syntax changes the role(s) of a specific user.

```
config:#    user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command assigns two roles to the user "May."

```
config:#    user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Changing the Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a specific user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time. To combine all commands, see ***Multi-Command Syntax*** (on page 289).

Note: The measurement unit change only applies to the web interface and command line interface.

To set the preferred temperature unit:

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

To set the preferred length unit:

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

To set the preferred pressure unit:

```
config:#    user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Example

The following command sets all measurement unit preferences for the user "May."

```
config:#    user modify May preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

Results:

- The preferred temperature unit is set to Fahrenheit.
- The preferred length unit is set to feet.
- The preferred pressure unit is set to psi.

Specifying the SSH Public Key

If the SSH key-based authentication is enabled, specify the SSH public key for each user profile using the following procedure.

To specify the SSH public key for a specific user:

1. Type the SSH public key command as shown below and press Enter.

   ```
   config:#    user modify <name> sshPublicKey
   ```

2. The system prompts you to enter the contents of the SSH public key. Do the following to input the contents:

   a. Open your SSH public key with a text editor.

b. Copy all contents in the text editor.

c. Paste the contents into the terminal.

d. Press Enter.

Tip: To remove an existing SSH public key, simply press Enter without typing or pasting anything when the system prompts you to input the contents.

Example

This section illustrates how to specify an SSH public key for an existing user "May" if the SSH public key-based authentication is enabled. See ***Determining the SSH Authentication Method*** (on page 228). Your SSH public key contents should be different from the contents displayed in this example.

To specify the SSH public key for the user "May":

1. Make sure you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 204).
2. Type the following command and press Enter.

   ```
   config:#   user modify May sshPublicKey
   ```

1. The system prompts you to enter the contents of the SSH public key.
2. Open the SSH public key using a text editor. You should see the SSH public key contents similar to the following.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDLZMx/ETBqjczWo0uU6JHZ54H7PwIoHyAa
OdeKdCq8i0h59p1VVa6vS4agObxMU8FjHIZ0uQSLknTjWw3wy358BpJVYmyz8HlTOm
QBR59VvIrSjn77cI7U8DbYQOVgqm8NvFami1Fbd7yX/pMXikeSXZCxP4QtonDvqgZ36l
vjQ== May@raritan.com
```

3. Select and copy all contents of the SSH public key.
4. Paste the contents in the terminal.
5. Press Enter.

Deleting a User Profile

This command syntax deletes an existing user profile.

```
config:#   user delete <name>
```

Example

The following command deletes the user profile "May."

```
config:#   user delete May
```

Changing Your Own Password

Every user can change their own password via this command syntax if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:#   password
```

After performing this command, the EMX prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately no matter you type the command "apply" or not to save the changes.

Example

This procedure changes your own password:

1. Verify that you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 204).
2. Type the following command and press Enter.

   ```
   config:#   password
   ```

3. Type the existing password and press Enter when the following prompt appears.

   ```
   Current password:
   ```

4. Type the new password and press Enter when the following prompt appears.

   ```
   Enter new password:
   ```

5. Re-type the new password for confirmation and press Enter when the following prompt appears.

   ```
   Re-type new password:
   ```

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command syntax creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create "<name>" <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:#    role create "<name>" <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 277).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument with a colon.

All Privileges

This table lists all privileges.

Privilege	Description
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changeEmdConfiguration	Change EMD Configuration
changeEventSetup	Change Event Settings

Privilege	Description
changeExternalSensorsConfiguration	Change External Sensors Configuration
changeLhxConfiguration	Change LHX Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
viewEventSetup	View Event Settings
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Images and Configuration

Example

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

To modify a role's description:

```
config:#    role modify <name> description <description>
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

To add more privileges to a specific role:

```
config:#    role modify <name> addPrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#    role modify <name> addPrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 277).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument with a colon.

To remove specific privileges from a role:

```
config:#    role modify <name> removePrivileges
            <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#    role modify <name> removePrivileges
            <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 277).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument with a colon.

Example

The following command modifies the privileges of the role "tester."

```
config:#    role modify tester addPrivileges changeAuthSettings removePrivileges
            firmwareUpgrade
```

Results:

- The "changeAuthSettings" (Change Authentication Settings) privilege is added to the role.
- The "firmwareUpgrade" (Firmware Upgrade) privilege is removed from the role.

Deleting a Role

This command syntax deletes an existing role.

```
config:#    role delete <name>
```

Example

The following command deletes an existing role.

```
config:#    role delete tester
```

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset sensor (if any) or the settings of LEDs on the asset sensor.

Asset Sensor Management

An asset sensor management configuration command begins with `assetStrip`.

Naming an Asset Sensor

This command syntax names or changes the name of an asset sensor connected to the EMX device.

```
config:#    assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

This command syntax names or changes the name of an asset sensor connected to the EMX device.

```
config:#    assetStrip 1 name "Red Rack"
```

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset sensor connected to the EMX device.

```
config:#    assetStrip <n> numberOfRackUnits <number>
```

Note: For the Raritan asset sensor, a rack unit refers to a tag port.

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <number> is the total number of rack units available on the connected asset sensor. This value ranges from 8 to 64.

Example

The following command specifies the total number of rack units on the asset sensor #1 to 48 rack units.

```
config:#    assetStrip 1 numberOfRackUnits 48
```

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset sensors connected to the EMX device. The numbering mode changes the rack unit numbers.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Example

The following command causes the rack units of the asset sensor #1 to be numbered in an ascending order from the one closest to the asset sensor's RJ-45 connector to the farthest one. That is, the rack unit that is most close to the RJ-45 connector is numbered 1.

```
config:#   assetStrip 1 rackUnitNumberingMode topDown
```

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset sensors connected to the EMX device.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <number> is a starting number for numbering rack units on the connected asset sensor. This value is an integer number.

Example

The following command specifies the starting number of rack units of the asset sensor #1 to be 5. That is, the rack units are numbered 5, 6, 7 and so on from the first to the final rack unit on the asset sensor #1.

```
config:#   assetStrip 1 rackUnitNumberingOffset 5
```

Specifying the Asset Sensor Orientation

This command syntax specifies the orientation of the asset sensors connected to the EMX device. Usually you do not need to perform this command unless your asset sensors do NOT come with the tilt sensor, causing the EMX unable to detect the asset sensors' orientation.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

Example

The following command specifies the orientation of the RJ-45 connector on the asset sensor #1 to be on the top.

```
config:#   assetStrip 1 assetStripOrientation topConnector
```

Rack Unit Configuration

For the Raritan asset sensor, a rack unit refers to a tag port. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset sensor.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#   rackUnit 1 25 name "Linux server"
```

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset sensor follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See Global LED Color Settings. This is the default.
manual	This option enables selection of a different LED color and LED mode for the specified rack unit. When this option is selected, see ***Setting an LED Color for a Rack Unit*** (on page 287) and ***Setting an LED Mode for a Rack Unit*** (on page 288) to set different LED settings.

Example

The following command allows the rack unit whose index number is 25 on the asset sensor#1 to have a different LED color and mode.

```
config:#   rackUnit 1 25 LEDOperationMode manual
```

Setting the LED Disconnect Color

This command syntax sets the LED color for all rack units on the connected asset sensor(s) to indicate the absence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it. See Global LED Color Settings.

Example

The following command sets the LED color of the rack unit whose index number is 25 on the asset sensor#1 to PINK (that is, FF00FF).

```
config:#   rackUnit 1 25 LEDColor #FF00FF
```

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Example

The following command causes the LED of the rack unit whose index number is 25 on the asset sensor#1 to blink quickly.

```
config:#   rackUnit 1 25 LEDMode blinkFast
```

Setting the History Buffer Length

This command syntax changes the history buffer length. The default length is 25.

```
config:#   history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.
- If you leave the <n> variable blank when using the command, the history buffer is set to 25 by default.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command and perform all of them at a time.

A multi-command syntax looks like this:

```
<setting 1> <value 1> <setting 2> <value 2> <setting 3>
<value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask 255.255.255.0
           gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of SSID and PSK Parameters

This multi-command syntax configures both of SSID and PSK parameters simultaneously for the wireless feature.

```
config:#    network wireless SSID myssid PSK encryp_key
```

Results:

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

Quitting the Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

To quit the configuration mode, use either command:

```
config:#    apply
```

-- OR --

```
config:#    cancel
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Unblocking a User

If any user is blocked from accessing the EMX, you can unblock them at the local console.

To unblock a user:

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 189).
2. When the Username prompt appears, type `unblock` and press Enter.

```
Username: unblock
```

3. When the "Username to unblock" prompt appears, type the login name of the user to be unblocked and press Enter.

```
Username to unblock:
```

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the EMX

You can reset the EMX device to factory defaults or simply restart it using the CLI commands.

Restarting the Device

This command restarts the EMX device. It is not a factory default reset.

To restart the EMX device:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the EMX device.

```
#      reset unit
```

-- OR --

```
#      reset unit /y
```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Resetting to Factory Defaults

This command restores all settings of the EMX device to factory defaults.

To reset EMX settings, use either command:

```
#      reset factorydefaults
```

-- OR --

```
#      reset factorydefaults /y
```

See Using the CLI Command for more information.

Network Troubleshooting

The EMX provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering the Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

To enter the diagnostic mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `diag` and press Enter. The diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying the DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>       nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Example

The following command checks the DNS information regarding the host 192.168.84.222.

```
diag>       nslookup 192.168.84.222
```

Showing the Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>       netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Example

The following command displays the server connections to your EMX device.

```
diag>       netstat connections
```

Testing the Network Connectivity

This command syntax sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good, or the host is shut down or not being connected to the network.

```
diag>       ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number.

Options	Description
size <number2>	Determines the packet size. <number2> is an integer number in bytes.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds.

The command looks like this syntax when it includes all options:

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Example

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>       ping 192.168.84.222 count 5
```

Tracing the Route

This command syntax traces the network route between your EMX device and a network host.

```
diag>       traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example

The following command displays the existing network routing for the host 192.168.84.222.

```
diag>       traceroute 192.168.84.222
```

Quitting the Diagnostic Mode

- **To quit the diagnostic mode, use this command:**

```
diag>       exit
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command, you can have the CLI show them by adding a space and then a question mark to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

- **To query available parameters for the "show" command, the syntax is:**

```
#           show ?
```

- **To query available network configuration parameters, the syntax is:**

```
config:#    network ?
```

- **To query available role configuration parameters, the syntax is:**

```
config:#    role ?
```

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. For some *unique* CLI commands, such as the "reset" command, you can easily complete them by pressing the Tab or Ctrl+i instead of typing the whole command word by word.

To have a unique command completed automatically:

1. Type initial letters or words of the command. For example, type the first word of the "`reset factorydefaults`" command, that is, `reset`.
2. Press Tab or Ctrl+i until the complete command appears. For example, although you typed only one word for the reset command, the rest of the command appears after pressing Tab or Ctrl+i.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

To log out of the CLI:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Resetting to Factory Defaults (CLI)

The Command Line Interface (CLI) provides a reset command for restoring the EMX to factory defaults. For information on CLI, see Using the Command Line Interface.

To reset to factory defaults using the CLI command:

1. Connect a computer to the EMX device. See ***Connecting the EMX to a Computer*** (on page 11).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the EMX.
3. Log in to the CLI by typing the user name "admin" and its password. See Step 4 of Initial Network Configuration.
4. After the # system prompt appears, type either of the following commands and press Enter.
5. Type:

```
#    reset factorydefaults
OR
#   reset factorydefaults /y
```

6. Wait until the Username prompt appears, indicating the reset is complete.
7. If you entered the command without "/y", a message appears prompting you to confirm the operation. Type y to confirm the reset.

Appendix A Dominion PX Asset Management

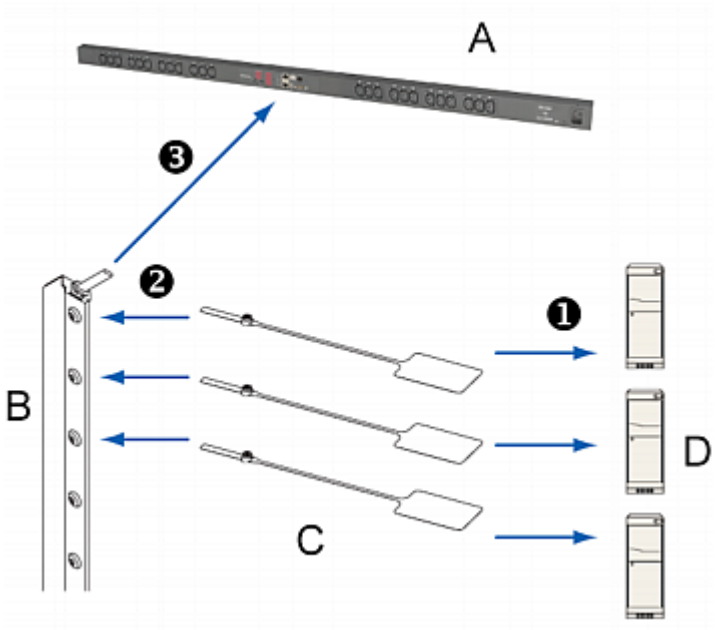
In This Chapter

Overview.....298

Overview

Raritan's PX2 power distribution unit (PDU) also supports asset sensors so that you can remotely track IT devices through the PDU's web interface while monitoring the PDU's power status. Only PDUs with model names that begin with 'PX2' support the asset management function.

Important: When handling asset sensors that are connected to each, put as little stress as possible on the joints between the asset sensors in order to avoid them breaking at the connection point.



Letter	Item
A	The Dominion PX device
B	Asset sensors
C	Asset tags

Letter	Item
D	IT devices, such as servers

To set up an asset management system:

1. Affix the adhesive end of an asset tag to each IT device through the tag's tape.
2. Plug the connector on the other end of each asset tag into the corresponding tag port on the asset sensor.
3. Connect the asset sensor assembly on the rack to the Dominion PX device by following this procedure:
   a. Connect one end of the Category 5e/6 UTP cable to the RJ-45 connector on the asset sensor.
   b. Connect the other end of the cable to the FEATURE port on the Dominion PX device.

For more information on the Dominion PX product, see the Dominion PX documentation that accompanies the Dominion PX device, which can be downloaded from the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***). Or you can access the product's online help in the Product Online Help section (http://www.raritan.com/support/online-help/).

Appendix B Specifications

In This Chapter

Altitude Correction Factors (EMX).....300
Maximum Ambient Operating Temperature (EMX).....300
Serial RS-232 Port Pinouts.....301
Sensor RJ-12 Port Pinouts.....301
RS-485 Port Pinouts.....301

Altitude Correction Factors (EMX)

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Maximum Ambient Operating Temperature (EMX)

The maximum ambient operating temperature (TMA) for the EMX is the same for all models regardless of the certification standard (CE or UL).

Specification	Measure
Max Ambient Temperature	60 degrees Celsius

Serial RS-232 Port Pinouts

RS-232 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

Sensor RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	—	—	—
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		Used for Feature Port

RS-485 Port Pinouts

RS-485 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	—	—	—
2	—	—	—

RS-485 Pin/signal definition			
3	D+	bi-directional	Data +
4	—	—	—
5	—	—	—
6	D-	bi-directional	Data -
7	—	—	—
8	—	—	—

Appendix C LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

a. Determine user accounts and groups intended for the EMX

b. Create user groups for the EMX on the AD server

c. Configure LDAP authentication on the EMX device

d. Configure roles on the EMX device

In This Chapter

Step A. Determine User Accounts and Groups 303
Step B. Configure User Groups on the AD Server 304
Step C. Configure LDAP Authentication on the EMX Device 305
Step D. Configure User Groups on the EMX Device 307

Step A. Determine User Accounts and Groups

Determine the user accounts and groups that are authenticated for accessing the EMX. In this example, we will create two user groups with different permissions. Each group will consist of two user accounts available on the AD server.

User groups	User accounts (members)
EMX_User	usera
	emxuser2
EMX_Admin	userb
	emxuser

Group permissions:

- The EMX_User group will only have read-only permissions.
- The EMX_Admin group will have full system permissions.

Step B. Configure User Groups on the AD Server

You must create the groups for the EMX on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for the EMX are named *EMX_Admin* and *EMX_User*.
- User accounts *emxuser*, *emxuser2*, *usera* and *userb* already exist on the AD server.

To configure the user groups on the AD server:

1. On the AD server, create new groups -- *EMX_Admin* and *EMX_User*.

   Note: See the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *emxuser2* and *usera* accounts to the EMX_User group.
3. Add the *emxuser* and *userb* accounts to the EMX_Admin group.
4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the EMX Device

You must enable and set up LDAP authentication properly on the EMX device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Modifying the Network Settings*** (on page 75) and ***Role of a DNS Server*** (on page 79).
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over SSL.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

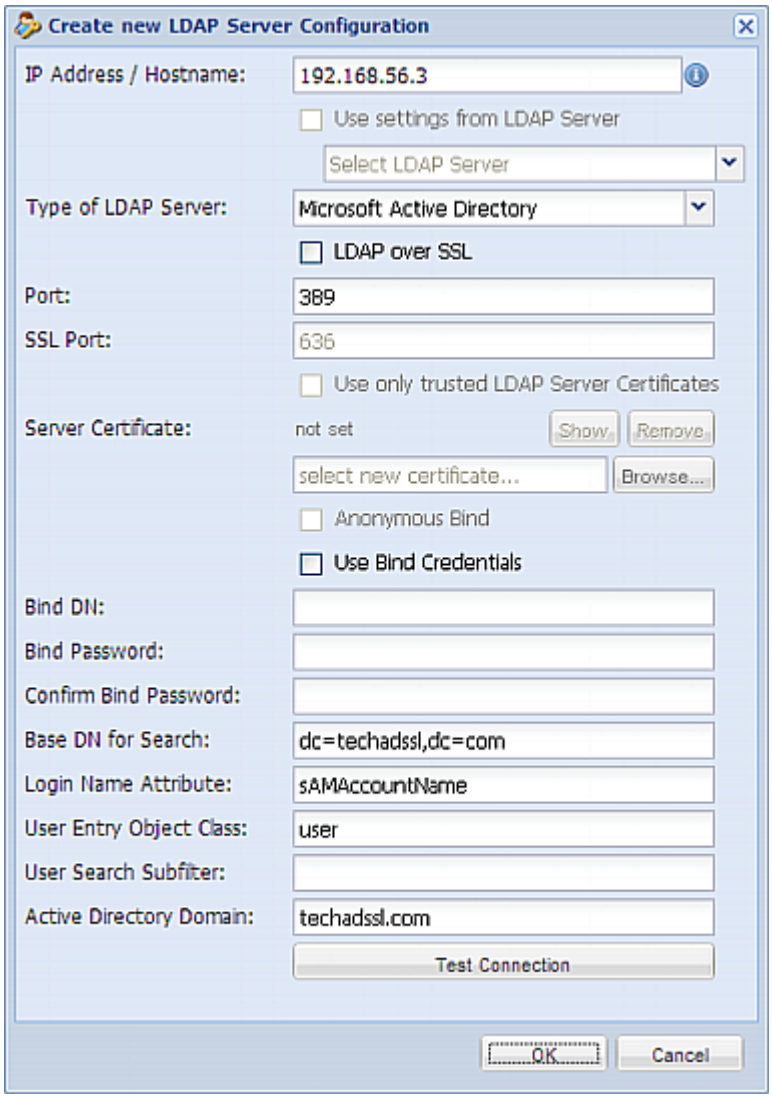
To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. Provide the EMX with the information about the AD server.
   - IP Address / Hostname - Type the domain name `techadssl.com` or IP address `192.168.56.3`.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.

   - Use settings from LDAP server - Leave the checkbox deselected.
   - Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
   - LDAP over SSL - Have the checkbox deselected since the SSL encryption is not applied in this example.
   - Port - Ensure the field is set to `389`.
   - SSL Port and Server Certificate - Skip the two fields since the SSL encryption is not enabled.
   - Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.
   - Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.

- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.



Note: For more information on LDAP configuration, see **Setting Up LDAP Authentication** *(on page 112).*

5. Click OK to save the changes. The LDAP server is saved.
6. Click OK to save the changes. The LDAP authentication is activated.

Note: If the EMX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the EMX and the LDAP server to use the same NTP server.

Step D. Configure User Groups on the EMX Device

A role on the EMX device determines the system permissions. You must create the roles whose names are identical to the user groups created for the EMX on the AD server or authorization will fail. Therefore, we will create the roles named *EMX_User* and *EMX_Admin* on the EMX device.

In this illustration, we assume:

- Users assigned to the *EMX_User* role can only access the EMX device and view settings.
- Users assigned to the *EMX_Admin* role can both access and configure the EMX device because they have the Administrator permissions.

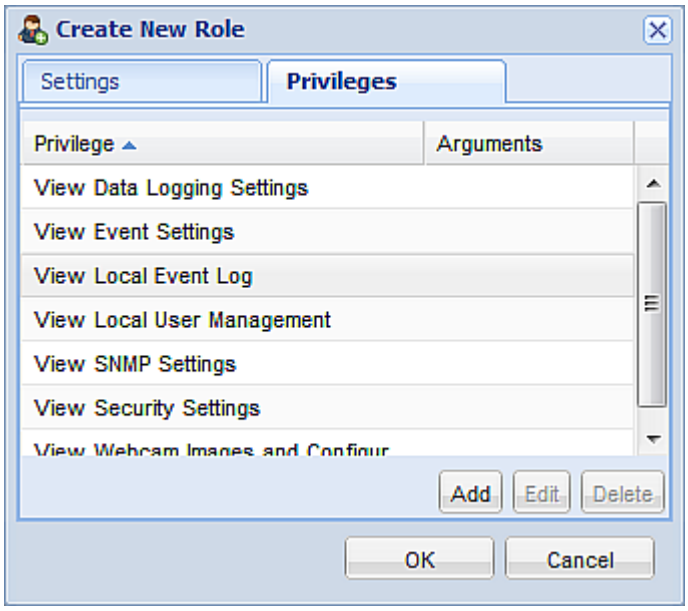
To create the EMX_User role with appropriate permissions assigned:

1. Choose User Management > Roles. The Manage Roles dialog appears.

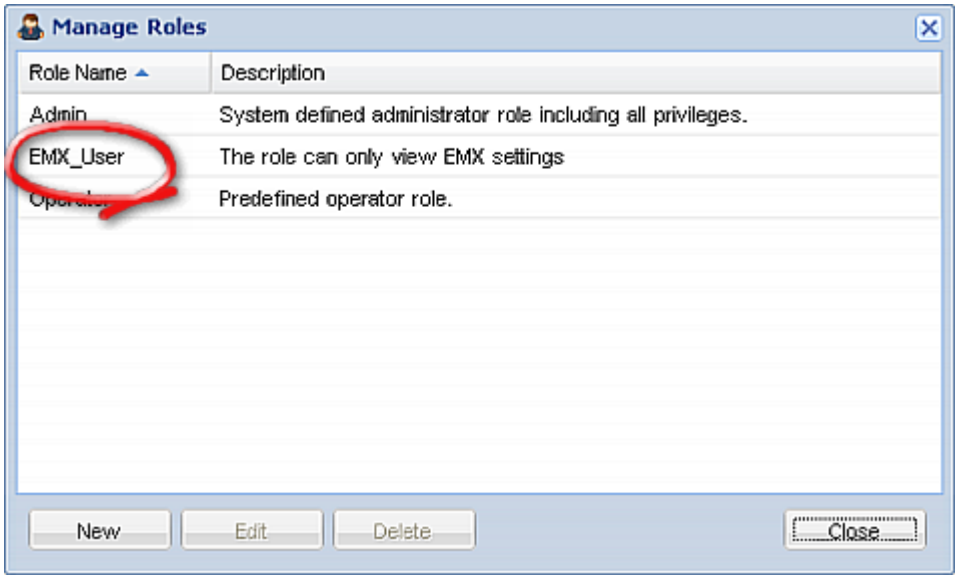
Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `EMX_User` in the Role Name field.
4. Type a description for the EMX_User role in the Description field. In this example, we type "The role can only view EMX settings" to describe the role.
5. Click the Privileges tab to select all View XXX permissions (where XXX is the name of the setting). A View XXX permission lets users view the XXX settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select a permission beginning with the word "View" from the Privileges list, such as View Event Settings.
   c. Click Add.

d. Repeat Steps a to c to add all permissions beginning with "View."



6. Click OK to save the changes. The EMX_User role is created.

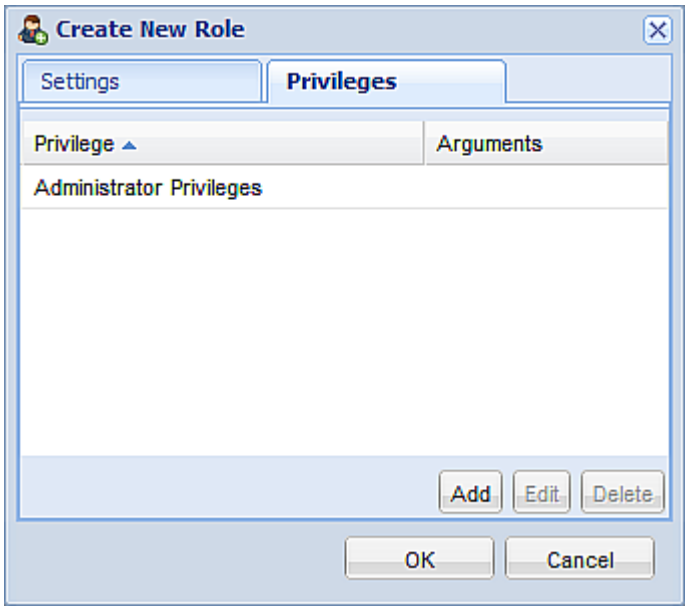


7. Keep the Manage Roles dialog opened to create the EMX_Admin role.

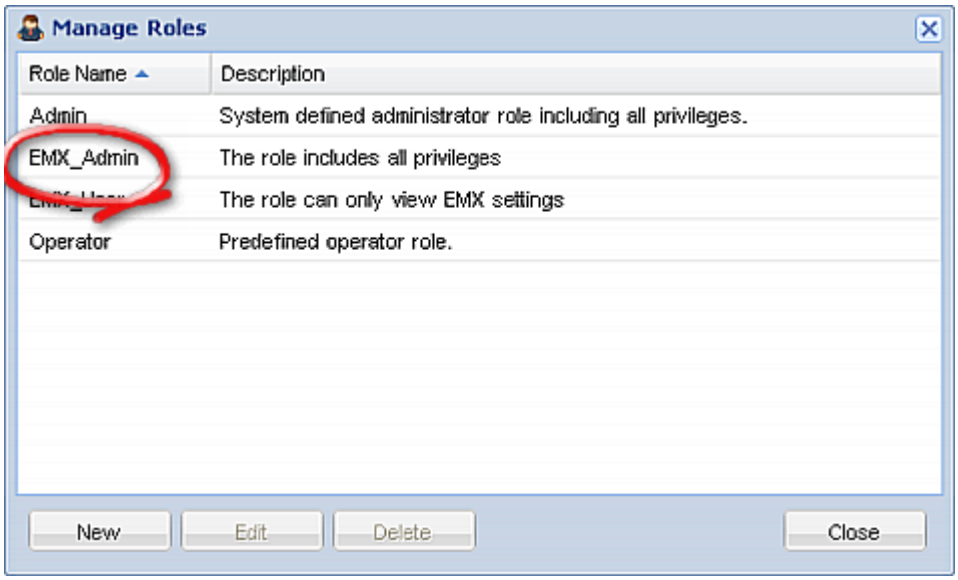
To create the EMX_Admin role with full permissions assigned:

1. Click New. The Create New Role dialog appears.

2. Type `EMX_Admin` in the Role Name field.
3. Type a description for the EMX_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.
4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all EMX settings.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission named Administrator Privileges from the Privileges list.
   c. Click Add.



5. Click OK to save the changes. The EMX_Admin role is created.



6. Click Close to quit the dialog.

Index

A

A Note about Untriggered Rules • 138
About Contact Closure Sensors • 31
About the Interface • 188
Access Security Control • 93
Add Page Icon • 52
Adding a Firewall Rule • 234
Adding a Role-Based Access Control Rule • 249
Adding IT Devices for Ping Monitoring • 141
Adding the LDAP Server Settings • 113
Alert States and LHX Event Log • 179
All Privileges • 277, 280
Altitude Correction Factors (EMX) • 69, 300
AMS-M2-Z Daisy-Chain Limitations • 24, 25, 157, 161, 162
Asset Management Commands • 281
Asset Management Information • 44
Asset Sensor Management • 281
Asset Sensor Settings • 195
Asset Sensors and Tags • 157
Automatically Completing a Command • 296

B

Before You Begin • 6
Blade Extension Strip Settings • 202
Browser-Defined Shortcut Menu • 56

C

Certificate Signing Request • 107
Changing a Specific LED's Color Settings • 160
Changing a User's Password • 265
Changing the Default Policy • 94, 102, 103
Changing the Device Name • 205
Changing the HTTP Port • 225
Changing the HTTP(S) Settings • 79
Changing the HTTPS Port • 225
Changing the LAN Duplex Mode • 224
Changing the LAN Interface Speed • 224
Changing the Measurement Units • 69, 70, 273
Changing the Role(s) • 272
Changing the Sensor Description • 257
Changing the Sensor Name • 253
Changing the SSH Configuration • 227
Changing the SSH Port • 227
Changing the SSH Settings • 61, 80
Changing the Telnet Configuration • 226
Changing the Telnet Port • 226
Changing the Telnet Settings • 81
Changing the User List View • 63
Changing Your Own Password • 276
Changing Your Password • 49
Checking Server Monitoring States • 143
Clearing Event Entries • 139
Closing a Serial Connection • 191
Combining Asset Sensors • 20, 24, 161
Command History • 202
Components of an Event Rule • 118
Configuring a Contact Closure Sensor • 33, 153, 154
Configuring Environmental Sensors • 30, 55, 144, 147, 156
Configuring IP Protocol Settings • 208
Configuring SNMP Traps • 184
Configuring Temperature and Fan Thresholds • 156, 177
Configuring the Asset Sensor • 23, 158
Configuring the EMX • 10, 75
Configuring the EMX Device and Network • 204
Configuring the Firewall • 94
Configuring the IPv4 Parameters • 216
Configuring the IPv6 Parameters • 220
Configuring the SMTP Settings • 82, 124, 125
Configuring the SNMP Settings • 59, 80
Configuring Users for Encrypted SNMP v3 • 183
Configuring Webcams • 37, 168, 170, 171, 173
Connecting a Logitech Webcam (Optional) • 37, 168
Connecting a Schroff LHX Heat Exchanger (Optional) • 37, 175
Connecting AMS-M2-Z Asset Sensors (Optional) • 24, 161
Connecting Asset Sensors to the EMX • 22, 158, 160
Connecting Blade Extension Strips • 25, 164
Connecting Differential Air Pressure Sensors • 36
Connecting Environmental Sensors (Optional) • 29, 144
Connecting the EMX to a Computer • 11, 91, 296

Connecting the EMX to a Power Source • 10
Connecting the EMX to Your Network • 13, 73, 74
Connecting Third-Party Detectors/Switches • 31
Connecting Third-Party Detectors/Switches to DPX-CC2-TR • 32
Connecting Third-Party Detectors/Switches to the EMX • 34, 46, 153, 154
Connection Ports • 39
Contact Closure Sensor LEDs • 35, 46
Contact Closure Sensor Termination • 46
Control Buttons • 43
Controlling the Heat Exchanger • 180
Copying a EMX Configuration • 85
Creating a Certificate Signing Request • 107
Creating a Role • 61, 64, 277
Creating a Self-Signed Certificate • 109
Creating a User Profile • 47, 58, 62, 64, 65, 70, 81, 183, 263
Creating Actions • 123, 127, 174
Creating an Event Rule • 119
Creating Custom Email Messages • 125, 127
Creating Firewall Rules • 94, 95
Creating Role-Based Access Control Rules • 102, 104
Creating Rules • 119

D

Data Pane • 53
Default Log Messages • 125, 129
Deleting a Firewall Rule • 238
Deleting a Role • 66, 281
Deleting a Role-Based Access Control Rule • 252
Deleting a User Profile • 62, 275
Deleting an Event Rule or Action • 138
Deleting Firewall Rules • 99
Deleting Ping Monitoring Settings • 143
Deleting Role-Based Access Control Rules • 106
Deleting the LDAP Server Settings • 116
Describing the Sensor Location • 147, 149
Determining How to Display Tree Items • 71, 72
Determining the SSH Authentication Method • 228, 275
Device Configuration Commands • 205
Device States and Icon Variations • 73, 179, 181
Diagnostic Commands • 292
Different CLI Modes and Prompts • 189, 190, 191, 204
Disabling the LDAP Authentication • 117
Displaying the Device Information • 68
Dominion PX Asset Management • 298
Downloading Diagnostic Information • 89
Downloading Key and Certificate Files • 111
Downloading SNMP MIB • 183, 184, 185

E

Editing Firewall Rules • 98
Editing Ping Monitoring Settings • 142
Editing Role-Based Access Control Rules • 105
Editing the LDAP Server Settings • 116
Email Message Placeholders • 127
EMX Device Management • 67
EMX2-111 • 3
EMX2-888 • 3
Enabling and Disabling Schroff LHX Heat Exchanger Support • 72, 175, 185
Enabling Data Logging • 150
Enabling IPv4 or IPv6 • 209
Enabling LDAP and Local Authentication Services • 117
Enabling Login Limitations • 100
Enabling or Disabling a User Profile • 267
Enabling or Disabling Data Logging • 206
Enabling or Disabling SNMP v1/v2c • 228
Enabling or Disabling SNMP v3 • 229
Enabling or Disabling SSH • 227
Enabling or Disabling Strong Passwords • 243
Enabling or Disabling Telnet • 226
Enabling Password Aging • 102
Enabling Service Advertisement • 81
Enabling SNMP • 150, 182
Enabling Strong Passwords • 101
Enabling the Feature • 102
Enabling the Firewall • 94
Enabling User Blocking • 99
Entering the Configuration Mode • 191, 204, 214, 265, 275, 276
Entering the Diagnostic Mode • 191, 292
Environmental Sensor Configuration Commands • 253
Environmental Sensor Information • 43, 196, 197
Environmental Sensor Threshold Configuration Commands • 257
Environmental Sensor Threshold Information • 198

Environmental Sensors • 144
Event Logging • 138
Event Rules and Actions • 80, 82, 118, 129, 156, 168, 184
Event Rules, Event Actions and Application Logs • 118
Example • 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 234, 236, 238, 239, 240, 241, 242, 243, 244, 245, 246, 248, 250, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 271, 272, 274, 275, 276, 278, 281, 282, 283, 284, 285, 286, 287, 288, 292, 293, 294
Example 1 - Basic Security Information • 203
Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 289
Example 2 - Combination of SSID and PSK Parameters • 290
Example 2 - In-Depth Security Information • 204
Examples • 203
Existing Roles • 200
Existing User Profiles • 199
Expanding a Blade Extension Strip • 163

F

Firewall Control • 232
Firmware Upgrade • 85
Forcing a Password Change • 267
Forcing HTTPS Encryption • 79, 93, 107
Full Disaster Recovery • 87

G

Gathering the LDAP Information • 112
Getting Started • 39
GSM Modems • 174

H

Help Command • 191
History Buffer Length • 203
How to Display Asset Sensors • 71
How to Display LHX Heat Exchangers • 72
HTTPS Access • 239

I

Identifying Environmental Sensors • 144, 146
Idle Timeout • 241
Information about Update Interval • 29, 145, 150, 151
Initial Network Configuration • 14
Installing a CA-Signed Certificate • 109
Installing and Configuring the EMX Device • 6
Installing Existing Key and Certificate Files • 110
Installing the USB-to-Serial Driver • 11
Introduction • 1
Introduction to the Web Interface • 50
IP Address • 45
IP Configuration • 192

L

LAN Interface Settings • 193
Layout • 186
LCD Display • 41, 43, 44
LCD Display Panel • 40
LDAP Configuration Illustration • 115, 303
Listing TCP Connections • 89
Logging In • 47
Logging in to CLI • 188
Logging out of CLI • 296
Login Limitation • 239
Logout • 48
Lowercase Character Requirement • 244

M

MAC Address • 45
Managing Environmental Sensors • 144, 145
Managing External Devices • 141
Managing Firewall Rules • 234
Managing Role-Based Access Control Rules • 248
Managing Roles • 64
Managing Users • 58
Maximum Ambient Operating Temperature (EMX) • 300
Maximum Password History • 246
Maximum Password Length • 244
Menus • 51
Minimum Password Length • 243
Modifying a Firewall Rule • 236
Modifying a Role • 61, 62, 65, 279
Modifying a Role-Based Access Control Rule • 250
Modifying a User Profile • 49, 62, 65, 264
Modifying a User's Personal Data • 266
Modifying an Action • 137
Modifying an Event Rule • 136
Modifying the Firewall Control Parameters • 233
Modifying the IPv4 Settings • 77

Modifying the IPv6 Settings • 78
Modifying the Network Configuration • 14, 73
Modifying the Network Interface Settings • 73
Modifying the Network Service Settings • 79, 188, 190
Modifying the Network Settings • 51, 75, 305
Modifying the Role-Based Access Control Parameters • 247
Modifying the SNMPv3 Settings • 268
Monitoring the Heat Exchanger • 177, 179
More Information about AD Configuration • 115
Mounting a 1U EMX Device • 8
Mounting a Zero U EMX Device • 7
Mounting the EMX Device • 6
Multi-Command Syntax • 234, 239, 242, 243, 248, 264, 266, 268, 273, 289

N

Naming a Heat Exchanger • 176
Naming a Rack Unit • 285
Naming an Asset Sensor • 282
Naming the EMX Device • 51, 67, 70, 146, 147, 148, 152, 155, 176, 178
Network Configuration • 192
Network Diagnostics • 88
Network Service Settings • 194
Network Troubleshooting • 88, 292
Networking Configuration Commands • 207
Networking Mode • 193
Numeric Character Requirement • 245

O

Operating Hours • 180
Overriding the IPv4 DHCP-Assigned DNS Server • 219
Overriding the IPv6 DHCP-Assigned DNS Server • 222, 223
Overview • 2, 58, 67, 141, 298

P

Package Contents • 5
Password Aging • 240
Password Aging Interval • 241
Pinging a Host • 88
Power Switch • 46
Product Features • 4
Product Models • 3
Providing the EAP CA Certificate • 213

Q

Querying Available Parameters for a Command • 191, 295
Querying the DNS Servers • 292
Quitting the Configuration Mode • 205, 290
Quitting the Diagnostic Mode • 295

R

Rack Unit Configuration • 284
Rack Unit Settings of an Asset Sensor • 201
Readings Highlighted in Yellow or Red • 54, 57, 151, 179
Rebooting the EMX • 91
Reset Button • 46
Resetting the EMX • 291
Resetting to Factory Defaults • 46, 91, 291
Resetting to Factory Defaults (CLI) • 296
Restarting the Device • 291
Retrieving Previous Commands • 295
Role Configuration Commands • 277
Role of a DNS Server • 79, 305
Role-Bassed Access Control • 247
RS-485 Port Pinouts • 301

S

Sample Asset-Management-Level Event Rule • 134
Sample Event Rules • 134
Sample Sensor-Level Event Rule • 135
Sample User-Activity-Level Event Rule • 136
Saving an EMX Configuration • 84
Schroff LHX Heat Exchangers • 38, 54, 175
Security • 93
Security Configuration Commands • 231
Security Settings • 199
Selecting IPv4 or IPv6 Addresses • 209
Selecting the Internet Protocol • 76, 77, 78
Sending Videos in an Email or Instant Message • 168, 173
Sensor Measurement Accuracy • 152
Sensor RJ-12 Port Pinouts • 301
Serial RS-232 Port Pinouts • 301
Server Accessibility • 141
Setting an LED Color for a Rack Unit • 286, 287
Setting an LED Mode for a Rack Unit • 286, 288
Setting Data Logging • 150, 207
Setting the Authentication Method • 211

Setting the BSSID • 215
Setting the Data Logging Measurements Per Entry • 207
Setting the Date and Time • 68
Setting the EAP Identity • 213
Setting the EAP Parameters • 212
Setting the EAP Password • 213
Setting the History Buffer Length • 289
Setting the Inner Authentication • 212
Setting the IPv4 Address • 217
Setting the IPv4 Configuration Mode • 216
Setting the IPv4 Gateway • 218
Setting the IPv4 Primary DNS Server • 218
Setting the IPv4 Secondary DNS Server • 219
Setting the IPv4 Subnet Mask • 217
Setting the IPv6 Address • 221
Setting the IPv6 Configuration Mode • 220
Setting the IPv6 Gateway • 221
Setting the IPv6 Primary DNS Server • 222
Setting the IPv6 Secondary DNS Server • 222
Setting the LAN Interface Parameters • 223
Setting the LED Disconnect Color • 286
Setting the LED Operation Mode • 286
Setting the Network Service Parameters • 225
Setting the Networking Mode • 208
Setting the Outer Authentication • 212
Setting the Preferred Host Name • 216
Setting the PSK • 211
Setting the Sensor's Assertion Timeout • 262
Setting the Sensor's Deassertion Hysteresis • 261
Setting the Sensor's Lower Critical Threshold • 259
Setting the Sensor's Lower Warning Threshold • 260
Setting the Sensor's Upper Critical Threshold • 257
Setting the Sensor's Upper Warning Threshold • 258
Setting the SNMP Configuration • 228
Setting the SNMP Read Community • 229
Setting the SNMP Write Community • 230
Setting the SSID • 210
Setting the sysContact Value • 230
Setting the sysLocation Value • 231
Setting the sysName Value • 231
Setting the Wireless Parameters • 210
Setting the X Coordinate • 255
Setting the Y Coordinate • 255
Setting the Z Coordinate • 206, 256
Setting the Z Coordinate Format • 148
Setting the Z Coordinate Format for Environmental Sensors • 206, 256
Setting Up an EMX Using Bulk Configuration • 67, 83
Setting Up an SSL Certificate • 93, 107
Setting Up LDAP Authentication • 79, 93, 112, 307
Setting Up Role-Based Access Control Rules • 102
Setting Up Roles • 49, 58, 61, 64, 150
Setting Up User Login Controls • 99
Setup Button • 51
Showing Information • 192
Showing the Network Connections • 293
Single Login Limitation • 240
SNMP Gets and Sets • 185
SNMP Sets and Thresholds • 187
Sorting Firewall Rules • 98
Sorting Role-Based Access Control Rules • 106
Sorting the LDAP Access Order • 115
Special Character Requirement • 246
Specifications • 300
Specifying the Asset Sensor Orientation • 284
Specifying the Device Altitude • 69
Specifying the Number of Rack Units • 282
Specifying the Rack Unit Numbering Mode • 283
Specifying the Rack Unit Numbering Offset • 283
Specifying the Sensor Type • 254
Specifying the SSH Public Key • 228, 274
States of Managed Sensors • 152
Status Bar • 51
Step A. Determine User Accounts and Groups • 303
Step B. Configure User Groups on the AD Server • 304
Step C. Configure LDAP Authentication on the EMX Device • 305
Step D. Configure User Groups on the EMX Device • 307
Strong Passwords • 243
Supported Web Browsers • 39
Supported Wireless LAN Configuration • 13

T

Taking, Viewing and Managing Webcam Snapshots • 168, 171
Testing the LDAP Server Connection • 116
Testing the Network Connectivity • 293
The EMX MIB • 185

Threshold Information • 156, 187
Tracing the Network Route • 89
Tracing the Route • 294

U

Unblocking a User • 99, 290
Unmanaging Environmental Sensors • 146, 155
Updating the Asset Sensor Firmware • 88
Updating the Firmware • 86
Uppercase Character Requirement • 245
User and Role Management • 58
User Blocking • 242
User Configuration Commands • 263
Using SNMP • 87, 182
Using the Command Line Interface • 188

V

Viewing Connected Users • 63
Viewing Details • 178
Viewing Firmware Update History • 87
Viewing Sensor Data • 151
Viewing the Communication Log • 52, 140
Viewing the Dashboard • 57
Viewing the Local Event Log • 139
Viewing the Summary • 178
Viewing Webcam Snapshots and Videos • 170

W

Warning Icon • 53
Webcams • 37, 168
What is Assertion Timeout? • 148, 157, 263
What is Deassertion Hysteresis? • 138, 148, 156, 177, 262
Wired Network Settings • 73
Wireless Configuration • 193
Wireless Network Settings • 74
With HyperTerminal • 189, 290
With SSH or Telnet • 190

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com