Raritan EMX

User Guide

Xerus™ Firmware v3.3.10

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, 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。　　　VCCI－A

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.

If a power cable is included with this product, it must be used exclusively for this product.

Contents

Chapter 5   Using the EMX   65

Chapter 6   Using the Web Interface   86

Chapter 7   Using SNMP   284

Chapter 8   Using the Command Line Interface   291

Chapter 9   Using SCP Commands   421

Appendix A   Specifications   426

Appendix B   Configuration or Firmware Upgrade with a USB Drive   430

What's New in the EMX User Guide

The following sections have changed or information has been added to the EMX User Guide based on enhancements and changes to the equipment and/or user documentation.

Please see the Release Notes for a more detailed explanation of the changes applied to this version of EMX.

Chapter 1   Introduction

In This Chapter

Overview

The EMX provides a rack management solution that combines the capabilities of asset management, environmental monitoring, image surveillance, event notifications and support for Schroff® heat exchangers.

▶ **Asset management:**

You can remotely track the location of IT equipment after tagging 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 the 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.
- *An EMX device*: You can remotely locate each tagged IT device through the EMX.

▶ **Environmental monitoring and/or system control:**

After connecting Raritan environmental sensor packages to the EMX, you can remotely monitor environmental conditions, such as temperature or humidity in the data center, or control a system if actuators are connected.

▶ **Image surveillance:**

With a Logitech® webcam connected, a simple camera and video surveillance system is established so that you can remotely view real-time snapshots or videos of the data center.

▶ **Event notifications:**

Event rules and actions that are triggered when an event occurs are supported by the EMX.

Email messages, log events, syslog messages, webcam snapshots, SNMP traps and SMS messages can be triggered when the events you define occur.

In addition, images captured by the webcam can be emailed to users in response to a specific event.

▶ **Integration with Schroff® LHX/SHX heat exchangers:**

The EMX can integrate with a Schroff® LHX-20, LHX-40 and SHX-30 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.

Product Models

There are two EMX models:

- EMX2-111
- EMX2-888

All models are functionally identical, but vary in the dimension and total number of ports.

Note: For a list of available asset sensor kits and tags, visit the Raritan website's **Product Selector page (http://www.findmypdu.com/)**.
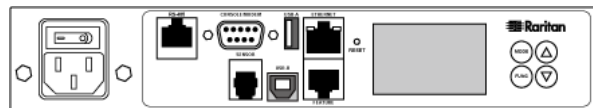
EMX2-111

EMX2-111 has 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

For details on each port, see *Connection Ports* (on page 65).

EMX2-888
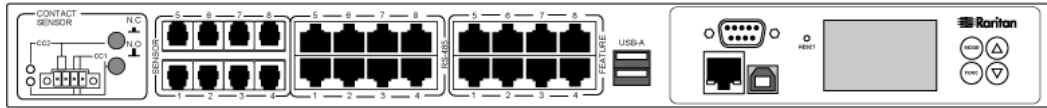
EMX2-888 has the following ports and components:

- 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

For details on each port, see *Connection Ports* (on page 65).

Note: If your EMX is EMX2-888, which contains built-in contact closure sensor terminals, see **Connecting Contact Closure Sensors to OLD EMX2-888** *(on page 534) and* **Connecting Contact Closure Sensors to EMX2-888** *(on page 80), respectively, based on your device type.*

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 strips (optional)
- Asset tags (optional)

APIPA and Link-Local Addressing

The EMX supports Automatic Private Internet Protocol Addressing (APIPA).

With APIPA, your EMX automatically configures a link-local IP address and a link-local host name when it cannot obtain a valid IP address from any DHCP server in the TCP/IP network.

Only IT devices connected to *the same subnet* can access the EMX using the link-local address/host name. Those in a different subnet cannot access it.

Exception: The EMX in the Port Forwarding mode does not support APIPA. See **Setting the Cascading Mode** *(on page 162).*

Once the EMX can get a DHCP-assigned IP address, it stops using APIPA and the link-local address is replaced by the DHCP-assigned address.

▶ **Scenarios where APIPA applies:**

- DHCP is enabled on the EMX, but no IP address is assigned to the EMX.

  This may be caused by the absence or malfunction of DHCP servers in the network.

  Note: Configuration by connecting the EMX to a computer using a network cable is an application of this scenario. See **Connecting the EMX to a Computer** *(on page 12).*

- The EMX previously obtained an IP address from the DHCP server, but the lease of this IP address has expired, and the lease cannot be renewed, or no new IP address is available.

▶ **Link-local addressing:**

- IPv4 address:

  Factory default is to enable IPv4 only. The link-local IPv4 address is *169.254.x.x/16*, which ranges between 169.254.1.0 and 169.254.254.255.

- IPv6 address:

  A link-local IPv6 address is available only after IPv6 is enabled on the EMX. See *Configuring Network Settings* (on page 149).

- Host name - **pdu.local**:

  You can type *https://pdu.local* to access the EMX instead of typing the link-local IP address.

Raritan.
A brand of Legrand

▶ **Retrieval of the link-local IPv4 address:**

- See *IPv4 Address* (on page 75).

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 strip connections.

Chapter 2 Rack Mounting an EMX

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

In This Chapter

Mounting a Zero U EMX

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.
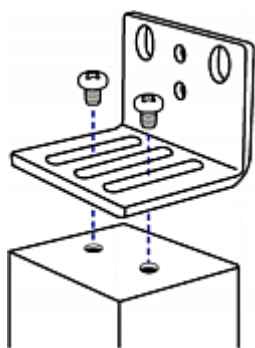
3. Repeat Steps 1 to 2 to screw another L-bracket to the bottom of the device.

4. After both L-brackets are installed, 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).
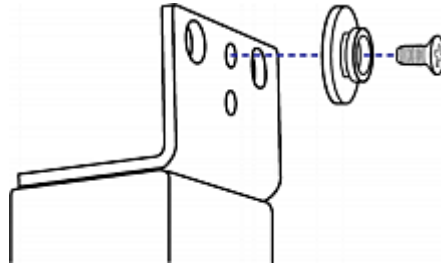
Mounting a 1U EMX

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

▶ **To mount the 1U EMX device:**

1. Attach a rackmount bracket to both sides of the EMX with the provided screws.
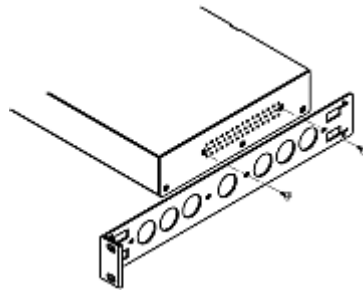
2. Insert the cable-support bar into rackmount brackets.
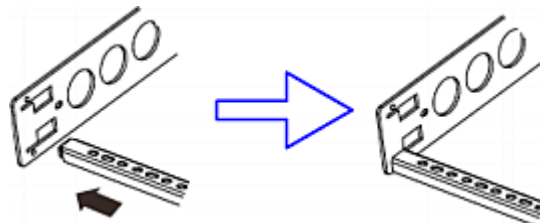
3. Secure with the provided end cap screws.
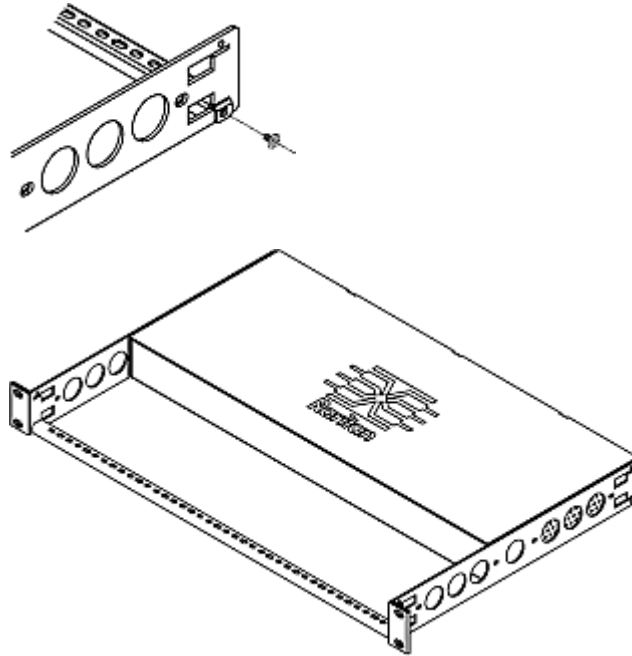
4. Fasten the rackmount brackets' ears to the rack using your own fasteners.

Chapter 3   Initial Installation and Configuration

This chapter explains how to install a EMX device and configure it for network connectivity.

In This Chapter

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 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.
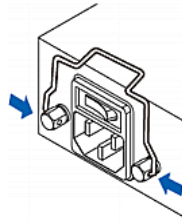
2. Plug one end of the Raritan-provided power cord into the power socket, and press the cable retention clip toward the power cord until it holds the cord firmly.
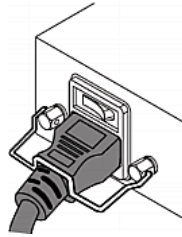
3. Connect the other end of the power cord to an appropriate power source.

Connecting the EMX to Your Network

To remotely administer the EMX, you must connect the EMX to your local area network (LAN).

EMX can be connected to a wired or wireless network.

Note: If your EMX will work as a master device in the bridging mode, make a wired connection. See **Cascading the EMX via USB** *(on page 22).*

▶ **To make a wired connection:**

1. Connect a standard network patch cable to the ETHERNET port on the EMX.
2. Connect the other end of the cable to your LAN.
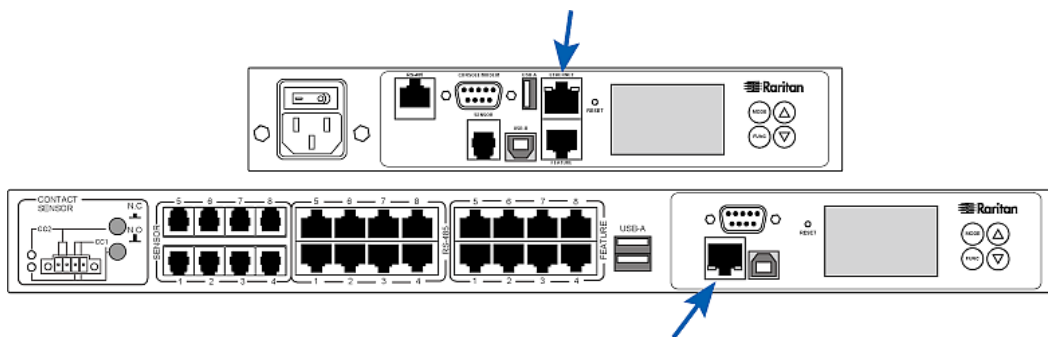
▶ **To make a wireless connection:**

Do one of the following:

- Plug a supported USB wireless LAN adapter into the USB-A port on your EMX.
- Connect a USB hub to the USB-A port on the EMX. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the hub.

See *USB Wireless LAN Adapters* (on page 11) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The EMX supports the following USB Wi-Fi LAN adapters.

Wi-Fi LAN adapters	Supported 802.11 protocols
SparkLAN WUBR-508N	A/B/G/N
Proxim Orinoco 8494	A/B/G
Zyxel NWD271N	B/G
Edimax EW-7722UnD	A/B/G/N
TP-Link TL-WDN3200 v1	A/B/G/N
Raritan USB WIFI	A/B/G/N

Note: To use the Edimax EW-7722UnD or Raritan USB WIFI wireless LAN adapter to connect to an 802.11n wireless network, the handshake timeout setting must be changed to 500 or greater, or the wireless connection will fail.

Supported Wireless LAN Configuration

If wireless networking is preferred, ensure that the wireless LAN configuration of your EMX matches the access point. The following is the wireless LAN configuration that the EMX supports.

- Network type: 802.11 A/B/G/N
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- Encryption: CCMP (AES)

Important: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the EMX. See *USB Wireless LAN Adapters* **(on page 11).**

Configuring the EMX

You can initially configure the EMX by connecting it to a computer, or to a TCP/IP network that supports DHCP.

▶ **Configuration over a DHCP-enabled network:**

1. Connect the EMX to a DHCP IPv4 network. See *Connecting the EMX to Your Network* (on page 10).

2. Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it. See *IPv4 Address* (on page 75).

3. Launch a web browser to configure the EMX. See *Login* (on page 87).

▶ **Configuration using a connected computer:**

1. Connect the EMX to a computer. See *Connecting the EMX to a Computer* (on page 12).

2. Use the connected computer to configure the EMX via the command line or web interface.

   ▪ Command line interface: See *Initial Network Configuration via CLI* (on page 15).

   ▪ Web interface: Launch the web browser on the computer, and type the link-local IP address or *pdu.local* to access the EMX. See *Login* (on page 87). For IP address retrieval, see *IPv4 Address* (on page 75).

Tip: To configure a number of EMX devices quickly, see **Bulk Configuration Methods** *(on page 20).*

Connecting the EMX to a Computer

The EMX can be connected to a computer for configuration via one of the following ports.

- USB-B port (male)
- ETHERNET port (female)
- RS-232 serial port (model dependent -- male DB9 or female RJ-45 connector)

EMX2-111:
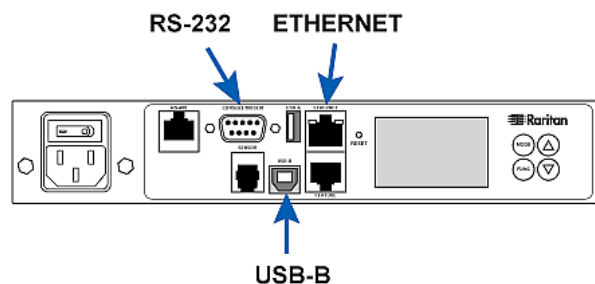
EMX2-888:
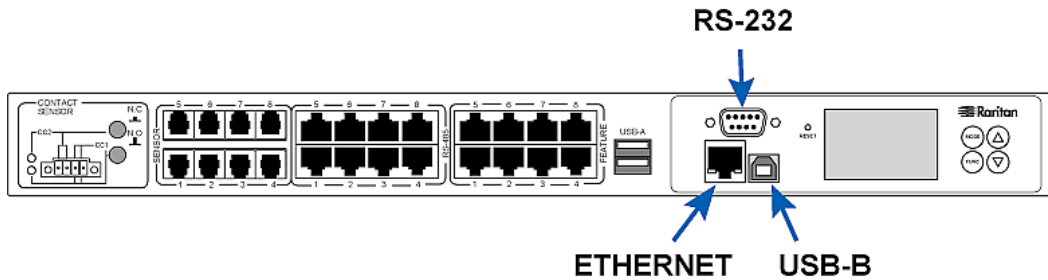
To use the command line interface (CLI) for configuration, establish an RS-232 or USB connection.

To use a web browser for configuration, make a network connection to the computer. The EMX is automatically configured with the following link-local addressing in any network without DHCP available:

- *https://169.254.x.x* (where x is a number)
- *https://pdu.local*

Establish one of the following connections to a computer.

▶ **Serial connection for "DB9" RS-232 connector on EMX:**

1. Connect one end of the null-modem DB9 cable to the male "DB9" RS-232 port labeled CONSOLE / MODEM on the EMX.
2. Connect the other end to your computer's RS-232 port (COM).
3. Perform *Initial Network Configuration via CLI* (on page 15).

▶ **USB connection:**

1. A USB-to-serial driver is required in Windows®. Install this driver before connecting the USB cable. See *Installing the USB-to-Serial Driver (Optional)* (on page 14).
2. Connect a USB cable between the EMX device's USB-B port and a computer's USB-A port.
3. Perform *Initial Network Configuration via CLI* (on page 15).

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

▶ **Direct network connection:**

1. Connect one end of a standard network patch cable to the ETHERNET port of the EMX.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access the EMX, using either link-local addressing: *pdu.local* or *169.254.x.x*. See *Login* (on page 87).

Installing the USB-to-Serial Driver (Optional)

The EMX can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion EMX Serial Console" is required for Microsoft® Windows® operating systems.

Download the Windows driver for USB serial console from the Raritan website's *Support page* (*http://www.raritan.com/support/*). The downloaded driver's name is *dominion-serial-setup-<n>.exe*, where <n> represents the file's version number.

There are two ways to install this driver: automatic and manual installation. Automatic driver installation is highly recommended.

▶ **Automatic driver installation in Windows®:**

1. Make sure the EMX is NOT connected to the computer via a USB cable.

2. Run dominion-serial-setup-<n>.exe on the computer and follow online instructions to install the driver.

   Note: If any Windows security warning appears, accept it to continue the installation.

3. Connect the EMX to the computer via a USB cable. The driver is automatically installed.

▶ **Manual driver installation in Windows®:**

1. Make sure the EMX has been connected to the computer via a USB cable.

2. 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 EMX Serial Console*, and choose Update Driver.

3. Select the option of driver installation from a specific location, and then specify the location where both *dominion-serial.inf* and *dominion-serial.cat* are stored.

   Note: If any Windows security warning appears, accept it to continue the installation.

4. Wait until the installation is complete.

Note: If the EMX enters the disaster recovery mode when the USB serial driver is not installed yet, it may be shown as a 'GPS camera' in the Device Manager on the computer connected to it.

▶ **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

Initial Network Configuration via CLI

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

This section describes the initial network configuration via a serial RS-232 or USB connection. To configure the network settings using the web interface, see *Configuring Network Settings* (on page 149).

▶ **To configure the EMX device:**

1. On the computer connected to the EMX, open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and set the following port settings:
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion EMX Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the EMX.
4. The EMX prompts you to log in. Both user name and password are case sensitive.
   a. Username: `admin`
   b. Password: `raritan` (or a new password if you have changed it).

5. If prompted to change the default password, change or ignore it.
   - To change it, follow onscreen instructions to type your new password.
   - To ignore it, simply press Enter.

6. The # prompt appears.

7. Type `config` and press Enter.

8. To configure network settings, type appropriate commands and press Enter. Refer to the following commands list. CLI commands are case sensitive.

9. After finishing the network settings, type `apply` to save changes. To abort, type `cancel`.

▶ **Commands for wired networking:**

The <ipvX> variable in the following commands is either *ipv4* or *ipv6*, depending on the type of IP protocol you are configuring. Replace the <ETH> variable with the word 'ethernet' when you are configuring the wired networking.

- **General IP settings:**

To set or enable	Use this command
IPv4 or IPv6 protocol	`network <ipvX> interface <ETH> enabled <option>` <option> = *true*, or *false*
IPv4 configuration method	`network ipv4 interface <ETH> configMethod <mode>` <mode> = *dhcp* (default) or *static*
IPv6 configuration method	`network ipv6 interface <ETH> configMethod <mode>` <mode> = *automatic* (default) or *static*
Preferred host name (optional)	`network <ipvX> interface <ETH> preferredHostName <name>` <name> = preferred host name
IP address returned by the DNS server	`network dns resolverPreference <resolver>` <resolver> = *preferV4* or *preferV6*

- Static IP configuration:

To set	Use this command
Static IPv4 or IPv6 address	`network <ipvX> interface <ETH> address <ip address>` <ip address> = static IP address, with a syntax similar to the example below. ▪ Example: *192.168.7.9/24*
Static IPv4 or IPv6 gateway	`network <ipvX> gateway <ip address>` <ip address> = gateway's IP address
IPv4 or IPv6 primary DNS server	`network dns firstServer <ip address>` <ip address> = DNS server's IP address
IPv4 or IPv6 secondary DNS server	`network dns secondServer <ip address>` <ip address> = DNS server's IP address
IPv4 or IPv6 third DNS server	`network dns thirdServer <ip address>` <ip address> = DNS server's IP address

▶ **Commands for wireless networking:**

- **General wireless settings**:

To set or enable	Use this command
Wireless interface	`network wireless enabled <option>` <option> = *true*, or *false*
SSID	`network wireless SSID <ssid>` <ssid> = SSID string
BSSID	`network wireless BSSID <bssid>` <bssid> = AP MAC address or *none*

To set or enable	Use this command
802.11n protocol	`network wireless enableHT <option>` <option> = *true*, or *false*
Authentication method	`network wireless authMethod <method>` <method> = *psk* or *eap*
PSK	`network wireless PSK <psk>` <psk> = PSK string
EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP*
EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2*
EAP identity	`network wireless eapIdentity <identity>` <identity> = 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.

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." If a certificate is installed, configure the following:

Whether to	Use this command
Verify the certificate	`network wireless enableCertVerification <option1>` <option1> = *true* or *false*
Accept an expired or not valid certificate	`network wireless allowOffTimeRangeCerts <option2>` <option2> = *true* or *false*
Make the connection successful by ignoring the "incorrect" system time	`network wireless allowConnectionWithIncorrectClock <option3>` <option3> = *true* or *false*

- **Wireless IPv4 / IPv6 settings:**

Commands for wireless IP settings are identical to those for wired networking. Just replace the variable <ETH> with the word 'wireless'. The following illustrates a few examples.

To set or enable	Use this command
IPv4 configuration method	`network ipv4 interface WIRELESS configMethod <mode>` <mode> = *dhcp* (default) or *static*
IPv6 configuration method	`network ipv6 interface WIRELESS configMethod <mode>` <mode> = *automatic* (default) or *static*

▶ **To verify network settings:**

After exiting the above configuration mode and the # prompt re-appears, type this command to verify all network settings.

- `show network`

The IP address configured may take seconds to take effect.

Bulk Configuration Methods

If you have to set up multiple EMX devices, you can use one of the following configuration methods to save your time.

▶ **Use a bulk configuration file:**

- Requirement: All EMX devices to configure are of the same model and firmware.
- Procedure: First finish configuring one EMX. Then save the bulk configuration file from it and copy this file to all of the other EMX devices.

  See *Bulk Configuration* (on page 272).

▶ **Use a TFTP server:**

- Requirement: DHCP is enabled in your network and a TFTP server is available.
- Procedure: Prepare special configuration files, which must include *fwupdate.cfg*, and copy them to the root directory of the TFTP server. Re-boot all EMX after connecting them to the network.

  See *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 442).

▶ **Use a USB flash drive:**

- Requirement: A FAT32- or supperfloppy-formatted USB flash drive containing special configuration files is required.
- Procedure: Plug this USB drive into the EMX. When a happy smiley is shown on the front panel display, press and hold one of the control buttons on the front panel until the display turns blank.

  See *Configuration or Firmware Upgrade with a USB Drive* (on page 430).

Raritan.
A brand of O'legrand'

Cascading Multiple EMX Devices for Sharing Ethernet Connectivity

You can have multiple EMX devices share one Ethernet connection by cascading them via USB.

Warning: To upgrade an existing USB-cascading chain from a version older than 3.3.10, you must start from the last slave device and so on until the master device. Otherwise, a networking issue occurs. See *Upgrade Guidelines for Existing USB-Cascading Chains* **(on page 270).**

The first one in the cascading chain is the master device and all the other are slave devices. Only the master device is physically connected to the LAN -- wired or wireless.

Each device in the chain is accessible over the network, with the bridging or port-forwarding cascading mode activated on the master device. See *Setting the Cascading Mode* (on page 162).

- Bridging: Each device in the cascading chain is accessed with a different IP address.
- Port Forwarding: Each device in the cascading chain is accessed with the same IP address but with a different port number assigned.

▶ **Cascading restrictions:**

- In the bridging mode, the master device can have "only one" connection to the network.

Note: The port forwarding mode does NOT have such a restriction. In the port forwarding mode, you can enable both wired and wireless networking.

- Do NOT connect slave devices to the LAN via a standard network patch cable or a USB wireless LAN adapter.
- An Ethernet-cascaded device must have its Ethernet interface enabled for the networking to work properly. By default the Ethernet interface is enabled.

▶ **USB-cascading tip:**

The "USB-cascading" configuration can be a combination of diverse Raritan products that support the USB-cascading feature, including PX2, PX3, PX3-iX7, transfer switch, BCM and EMX.

▶ *Troubleshooting:*

When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain. See *Cascading Troubleshooting* (on page 535).

Cascading Guidelines for Port Forwarding

The following guidelines must be obeyed for establishing a cascading chain in the **port forwarding** mode.

- Each cascaded device, except for the master device, must have only one upstream device.
- Each cascaded device, except for the last slave device, must have only one downstream device.
- Use only one cable to cascade two devices.

Cascading the EMX via USB

Any certified USB 2.0 cable up to 16 feet (5 meters) long can be used.

Decide the cascading mode first before establishing the chain. All cascading modes support a maximum of 16 devices in a chain.

For more information on the USB-cascading configuration, see the *Cascading Guide*, which is available from Raritan website's *Support page* (*http://www.raritan.com/support/*).

▶ **To cascade EMX devices via USB:**

1. Make sure all Raritan devices to be cascaded are running firmware version 3.3.10 or later.
2. Select one as the master device.
   - When the port forwarding mode over wireless LAN is intended, the master device must be a Raritan product with two USB-A ports, such as PX3, EMX2-888, PX3TS or BCM2.

3. Log in to all devices one by one and select the same cascading mode. See *Setting the Cascading Mode* (on page 162).

    - **Bridging mode**:

      Set the cascading mode of all devices to Bridging.

    - **Port Forwarding mode**:

      Set the cascading mode of all devices to Port Forwarding. Make sure the cascading role and downstream interface are also set correctly.

4. Connect the master device to the LAN, using a method below.

    - Bridging mode: Use a standard network patch cable (CAT5e or higher).

      Port Forwarding mode: Use a standard network patch cable or a Raritan USB WIFI wireless LAN adapter. For information on the Raritan USB WIFI adapter, see *USB Wireless LAN Adapters* (on page 11).

5. Connect the USB-A port of the master device to the USB-B port of an additional EMX via a USB cable. This additional device is Slave 1.

6. Connect Slave 1's USB-A port to the USB-B port of an additional EMX via another USB cable. The second additional device is Slave 2.

7. Repeat the same step to connect more slave devices.
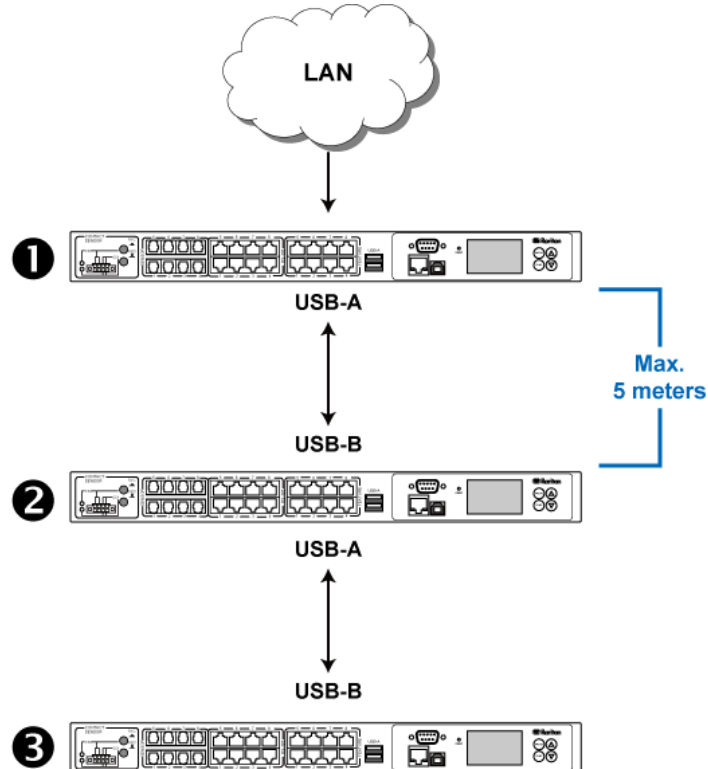
Number	Device role
1	Master device
2	Slave 1
3	Slave 2

8. Configure or change the network settings of the master and/or slave devices as needed.

- Bridging: Each cascaded device has its own network settings. For example, some devices can have DHCP-assigned IP and the others can have static IP addresses.

- Port forwarding: Only the master device's network settings should be configured.

Chapter 4   Connecting External Equipment (Optional)

More features are available if you connect Raritan's or third-party external equipment to your EMX.

In This Chapter

Connecting Asset Management Strips

You can remotely track the locations of up to 64 IT devices in the rack by connecting asset management strips (asset strips) to the EMX after IT devices are tagged electronically.

To use the asset management feature, you need the following items:

- *Raritan asset strips*: An asset strip transmits the asset management tag's ID and positioning information to the EMX.
- *Raritan asset tags*: An asset management tag (asset tag) is adhered to an IT device. The asset tag uses an electronic ID to identify and locate the IT device.

Combining Regular Asset Strips

Each tag port on the regular asset strips corresponds to a rack unit and can be used to locate IT devices in a specific rack (or cabinet).

For each rack, you can attach asset strips up to 64U long, consisting of one MASTER and multiple SLAVE asset strips.

The difference between the master and slave asset strips is that the master asset strip has an RJ-45 connector while the slave does not.

The following diagram illustrates some asset strips. Note that Raritan provides more types of asset strips than the diagram.
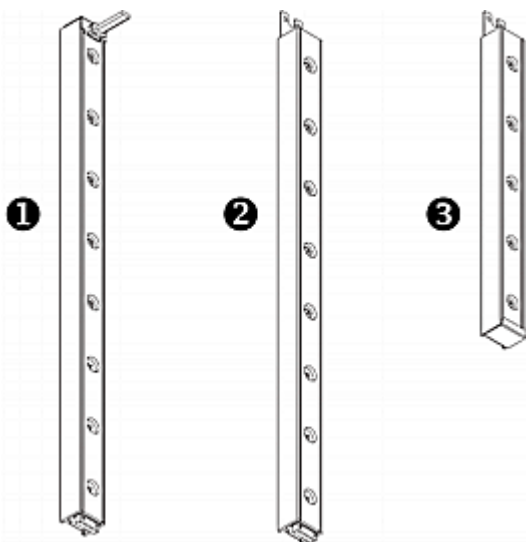
❶	8U MASTER asset strip with 8 tag ports
❷	8U SLAVE asset strip with 8 tag ports
❸	5U "ending" SLAVE asset strip with 5 tag ports

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

▶ **To assemble asset strips:**

1. Connect a MASTER asset strip to an 8U SLAVE asset strip.
   - Plug the white male DIN connector of the slave strip into the white female DIN connector of the master strip.

- Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master strip. Screw up the U-shaped sheet metal to reinforce the connection.
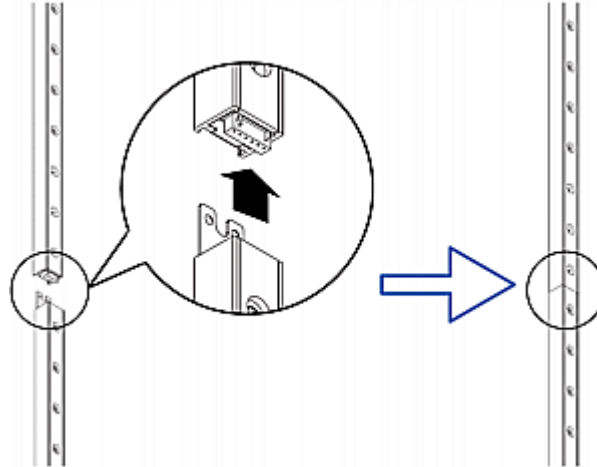
2. Connect another 8U slave strip to the one being attached to the master strip in the same manner as Step 1.

3. Repeat the above step to connect more slave strip. The length of the asset strip assembly can be up to 64U.

   - The final slave strip can be 8U or 5U, depending on the actual height of your rack.
   - Connect the "ending" asset strip as the final one in the assembly.

4. Vertically attach the asset strip assembly to the rack, next to the IT equipment, making each tag port horizontally align with a rack unit.

5. The asset strips are automatically attracted to the rack because of magnetic stripes on the back.

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

Introduction to Asset Tags

You need both asset strips and asset tags for tracking IT devices.

Asset tags provide an ID number for each IT device. The asset tags are adhered to an IT device at one end and plugged in to an asset strip at the other.

The asset strip is connected to the EMX, and the asset tag transmits the ID and positioning information to the asset strip.

The following diagram illustrates an asset tag. Note that there are two types of asset tags: non-programmable and programmable tags. The only difference is that programmable asset tags allow you to customize each tag's ID or barcode number while non-programmable ones have factory default ID or barcode numbers, which you cannot change.

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

Note: The barcode of each "non-programmable" asset tag is unique and is displayed in the EMX device's web interface for identification.

Connecting Regular Asset Strips to the EMX

The cabling distance between an asset strip assembly and the EMX can be up to 10 meters.

The EMX supplies power to the connected asset strips.

After powered by the EMX, all LEDs on the asset strip may cycle through different colors if the asset strip's firmware is being upgraded by the EMX. When the power-on or firmware upgrade process completes, all LEDs show solid colors.

Note: To configure asset strips after finishing the asset strip connection, see **Asset Strip** *(on page 121).*

EMX2-111 Connection

The FEATURE port of EMX2-111 supports 5 volts of power only, which is insufficient for connecting the latest generation (G3) of asset strips. Therefore, the use of a Raritan X cable is required for EMX2-111 to connect current asset strips, or EMX2-111 cannot detect them.

▶ **To connect a regular asset strip assembly to EMX2-111:**

1. Assemble regular asset strips according to your needs. See *Combining Regular Asset Strips* (on page 26).

2. Affix the adhesive end of an asset tag to each IT device through the tag's tape. See *Introduction to Asset Tags* (on page 28).

3. Plug the connector of each asset tag into the corresponding tag port on the asset strip.

   Note: If an IT device occupies more than one rack unit in the rack, it is suggested to plug the asset tag into the lowest tag port. For example, if a device occupies the 5th and 6th rack units, plug the asset tag into the tag port matches the 5th rack unit.

4. Connect the MASTER asset strip's RJ-45 connector to the male RJ-45 connector at the longer end of the Raritan X cable.

5. Plug the male RJ-12 phone connector at the shorter end of the X cable into the RJ-12 SENSOR port on the EMX2-111 device.

6. Plug the male RJ-45 connector at the shorter end of the X cable into the FEATURE port on the EMX2-111 device.

EMX2-111

RJ-12   RJ-45

(D)

RJ-12   RJ-45

(A)

(B)

(C)
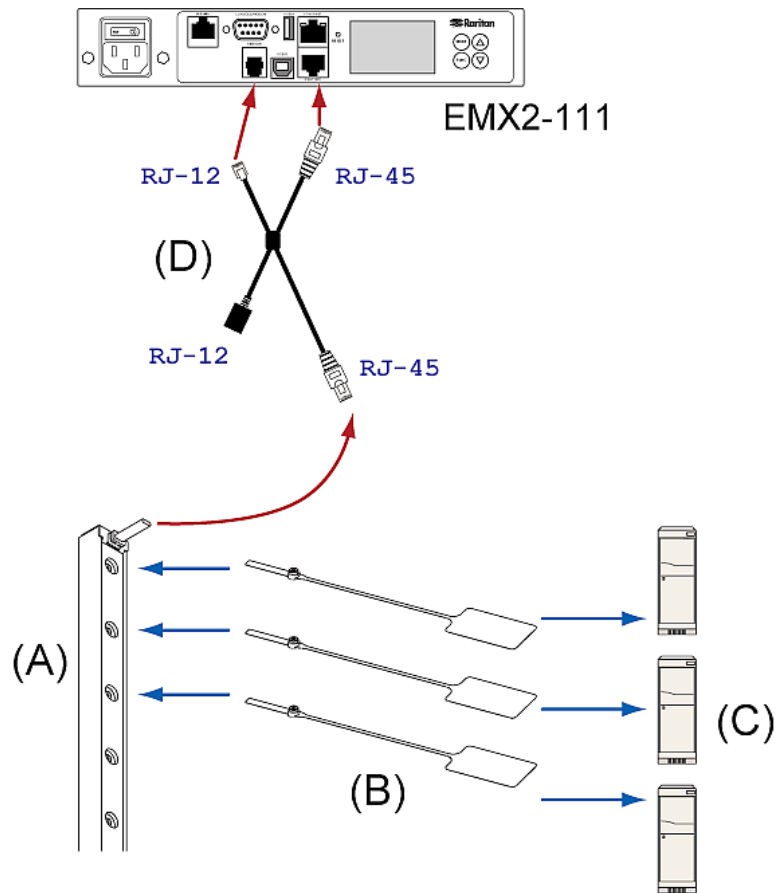
(A)	MASTER asset strip
(B)	Asset tags
(C)	IT devices
(D)	Raritan X cable

Tip: To connect Raritan's environmental sensor packages to EMX2-111, connect them to the female RJ-12 connector of the X cable. For details, see **Using an X Cable** *(on page 37).*

EMX2-888 Connection

Unlike EMX2-111, EMX2-888 does NOT need to use a Raritan X cable because its FEATURE port supports 12 volts of power.

▶ **To connect a regular asset strip assembly to EMX2-888:**

1. Assemble regular asset strips according to your needs. See *Combining Regular Asset Strips* (on page 26).

2. Affix the adhesive end of an asset tag to each IT device through the tag's tape. See *Introduction to Asset Tags* (on page 28).

3. Plug the connector of each asset tag into the corresponding tag port on the asset strip.

   Note: If an IT device occupies more than one rack unit in the rack, it is suggested to plug the asset tag into the lowest tag port. For example, if a device occupies the 5th and 6th rack units, plug the asset tag into the tag port matches the 5th rack unit.

4. Use a standard network patch cable to connect the MASTER asset strip's RJ-45 connector to a FEATURE port on the EMX2-888.
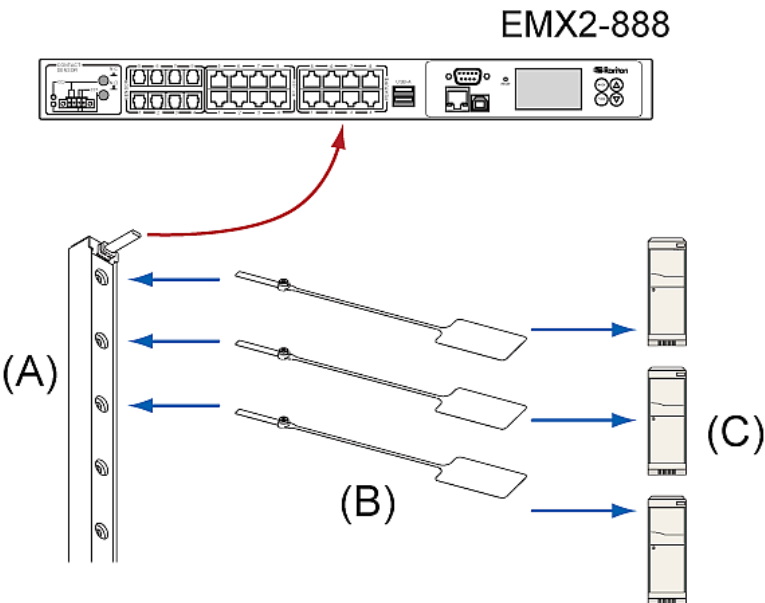
(A)	MASTER asset strip
(B)	Asset tags
(C)	IT devices

5. Repeat the above steps if you want to connect more asset sensors to the other FEATURE ports.

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 strip but requires a tag connector cable for connecting it to a tag port on the regular or composite asset strip. A blade extension strip contains 4 to 16 tag ports.

The following diagrams illustrate a tag connector cable and a blade extension strip with 16 tag ports.

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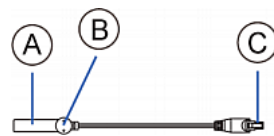
A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

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

Blade extension strip with 16 tag ports
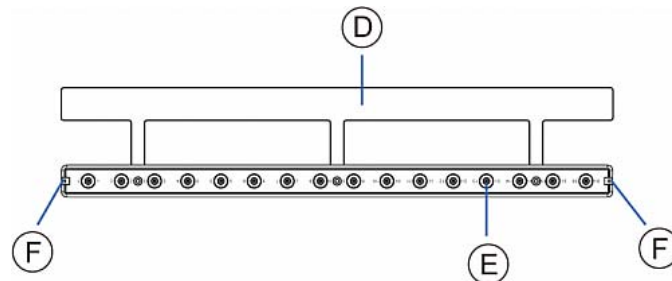
D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the EMX device'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.
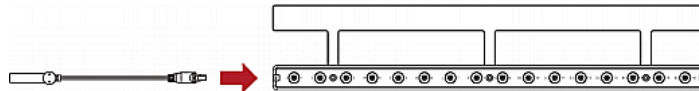
2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.
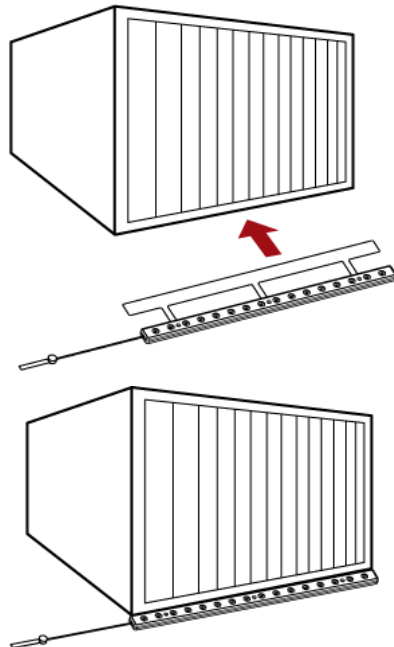
3. Connect one end of an asset tag to a blade server and the other end to the blade extension strip.

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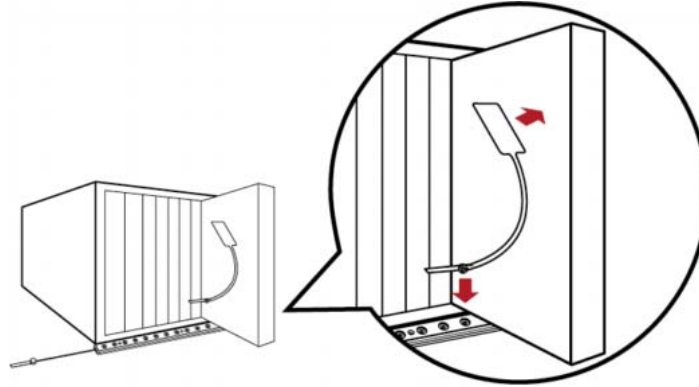
4.   Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.

5.   Plug the tag connector of the blade extension strip into the closest tag port of the regular or composite asset strip on the rack.
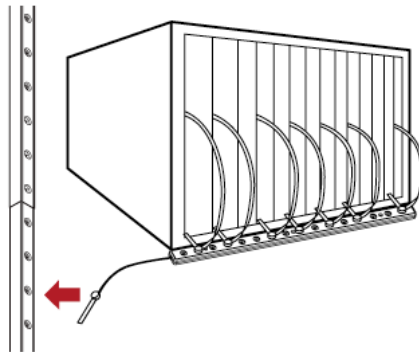
6.   Repeat the above steps to connect additional blade extension strips. Up to 128 asset tags on blade extension strips are supported per FEATURE port.

Note: If you need to temporarily disconnect the blade extension strip from the asset strip, wait at least 1 second before re-connecting it back, or the EMX device may not detect it.

Raritan.

Connecting Composite Asset Strips (AMS-Mx-Z)

A composite asset strip is named AMS-Mx-Z, where x is a number, such as AMS-M2-Z or AMS-M3-Z. It is a type of asset strip that functions the same as regular MASTER asset strips except for the following differences:

- It has two RJ-45 connectors.
- Multiple composite asset strips can be daisy chained.
- It contains less tag ports than regular asset strips.

  For example, AMS-M2-Z contains two tag ports, and AMS-M3-Z contains three tag ports only.

The composite asset strip is especially useful for tracking large devices such as SAN boxes in the cabinet.

The following diagram illustrates AMS-M3-Z.
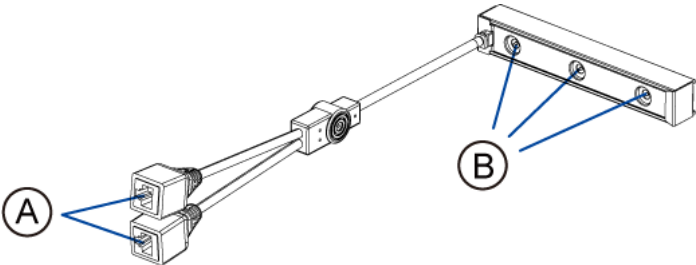
A	Two RJ-45 connectors
B	Tag ports

▶ **To connect composite asset strips to the EMX device:**

1. Connect a composite asset strip to the EMX device via a standard network patch cable (CAT5e or higher).

   a. Connect one end of the cable to the RJ-45 port labeled "Input" on the composite asset strip.

   b. Connect the other end of the cable to the FEATURE port on the EMX device.

2. Affix an asset tag to the IT device. Then connect this asset tag to the composite asset strip by plugging the tag connector into the tag port on the composite asset strip. For details, see *Connecting Regular Asset Strips to the EMX* (on page 28).

3. If necessary, daisy chain additional composite asset strips to track more IT devices.

   a. Get a standard network patch cable that is within 2 meters.

b. Connect one end of the network cable to the RJ-45 connector labeled "Output" on the previous composite asset strip.

c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on the subsequent composite asset strip.

d. Repeat the above steps to connect more composite asset strips. See *Daisy-Chain Limitations of Composite Asset Strips* (on page 36) for the maximum number of composite asset strips supported per chain.

e. It is highly recommended using the cable ties to help hold the weight of all connecting cables.
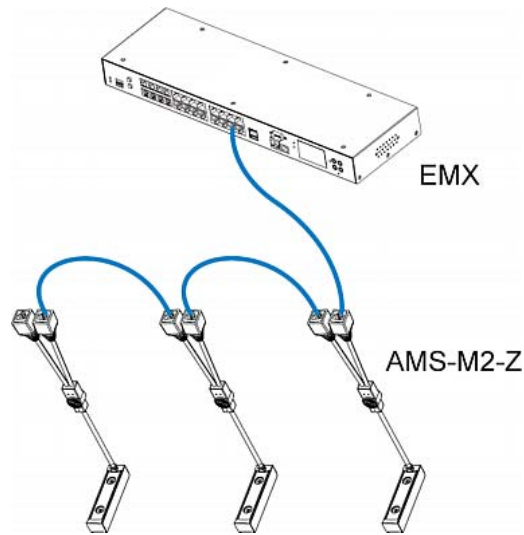
4. Repeat Step 2 to connect IT devices to the other composite asset strips in the chain.

Daisy-Chain Limitations of Composite Asset Strips

There are some limitations when daisy chaining composite asset strips "AMS-Mx-Z," where x is a number.

- The maximum cable length between composite asset strips is 2 meters, but the total cable length cannot exceed 10 meters.
- The maximum number of composite asset strips that can be daisy chained depend on the Raritan product you purchased.

Raritan devices	Maximum strips per chain
EMX2-111, PX2 PDUs, BCM1 (NOT BCM2 series)	Up to 4 composite asset strips are supported.

Raritan devices	Maximum strips per chain
EMX2-888, PX3 PDUs, PX3TS transfer switches PMC (BCM2 series)	Up to 6 composite asset strips are supported.

Tip: To increase the maximum number of composite asset strips attached to a Raritan PX2 PDU, EMX2-111 or BCM1, use Raritan's X cable to enhance the power supply to the asset strip chain. See **Using an X Cable** *(on page 37).*

Important: Different types of composite asset strips can be mixed in a chain as of release 3.3.0.

Using an X Cable

Raritan's EMX2-111 products support a maximum of four composite asset strips in a chain. For details, see *Daisy-Chain Limitations of Composite Asset Strips* (on page 36).

If you need to exceed the daisy-chain limitation, use Raritan's X cable to connect composite asset strips. This allows you to expand the maximum number of composite asset strips from four units per chain to six units per chain.

An X cable is a combination of two male RJ-45 connectors, one Raritan-defined male phone connector, and one female RJ-12 sensor port.

The X cable supplies 12V voltage from the SENSOR port of the EMX2-111 to the connected composite asset strips.

Note: An X cable does not help enhance the power supply to asset strips connected to Raritan's EMX2-888, so do not use this cable with these models.

▶ **To connect composite asset strips via an X cable:**

1. Plug the male RJ-45 connector at the shorter end of the X cable into the FEATURE port on the EMX2-111 device.

2. Plug the male RJ-12 phone connector at the shorter end of the X cable into the RJ-12 SENSOR port on the EMX2-111 device. **This step is required for enhancing the power supply to asset strips.**
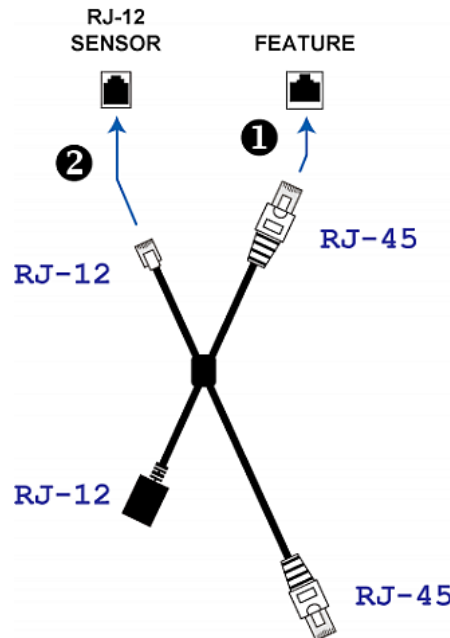
3. Plug the male RJ-45 connector at the longer end of the X cable into the RJ-45 port labeled "Input" on the composite asset strips.

   ▪ A maximum of 5 additional composite asset strips can be connected to the first composite asset strip being attached to the X cable. See *Connecting Composite Asset Strips (AMS-Mx-Z)* (on page 35) for step-by-step instructions.

4. Connect any Raritan environmental sensor package or sensor hub to the female RJ-12 sensor port of the X cable if environmental sensor packages are needed. Note that a DX or DPX3 sensor requires an RJ-12 to RJ-45 adapter to connect the X cable. See *Connecting Environmental Sensor Packages* (on page 39).
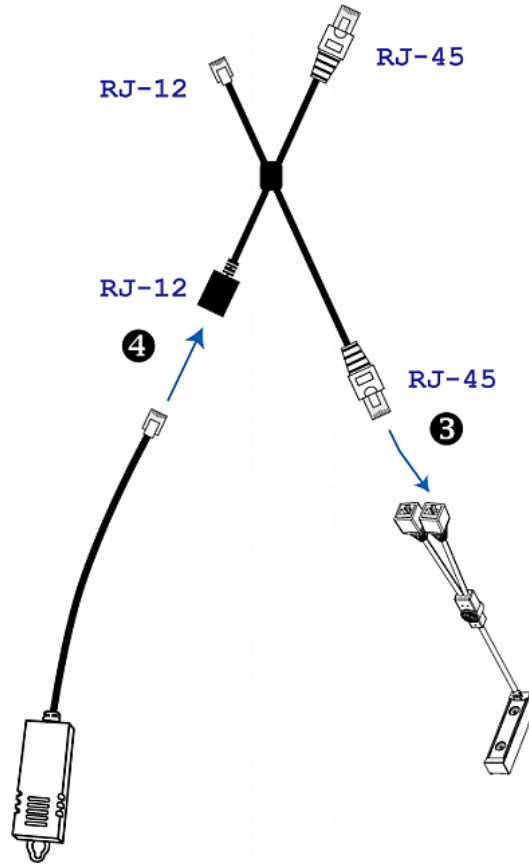
Connecting Environmental Sensor Packages

The EMX supports all types of Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages. For detailed information on each sensor package, refer to the Environmental Sensors Guide or Online Help on the Raritan website's *Support page* (*http://www.raritan.com/support/*).

An environmental sensor package may comprise sensors only or a combination of sensors and actuators. The supported maximum cabling distance is 98 feet (30 m), except for DPX sensor packages.

Each SENSOR port on the EMX can manage a maximum of 32 sensors and/or actuators, but the total number of sensors and/or actuators that an EMX supports varies based on the model you purchased.

Model	Supported maximum number of sensors/actuators
EMX2-111	This model has only one SENSOR port so it can manage up to 32 sensors and/or actuators.
EMX2-888	This model has 8 SENSOR ports, which can manage up to 128 sensors and/or actuators in total.
	In addition, it has two built-in contact closure terminals to connect two contact closure sensors. Therefore, the total number of sensors and actuators it supports is 130.

For information on connecting different types of sensor packages, see:

- *DPX Sensor Packages* (on page 40)
- *DPX2 Sensor Packages* (on page 46)
- *DPX3 Sensor Packages* (on page 48)
- *DX Sensor Packages* (on page 51)

DPX Sensor Packages

Most DPX sensor packages come with a factory-installed sensor cable, whose sensor connector is RJ-12.
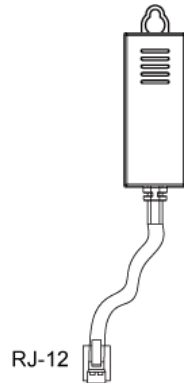
For the cabling length restrictions, see *Supported Maximum DPX Sensor Distances* (on page 45).

> Warning: For proper operation, wait for 15-30 seconds between each connection operation or each disconnection operation of environmental sensor packages.

▶ **To connect a DPX sensor package with a factory-installed sensor cable:**

- Plug the sensor cable's RJ-12 connector into the RJ-12 SENSOR port on the EMX.

▶ **To connect a DPX differential air pressure sensor:**

1. Plug one end of a Raritan-provided phone cable into the IN port of a differential air pressure sensor.

2. Plug the other end of this phone cable into the RJ-12 SENSOR port on the EMX.

3. If intended, connect one DPX sensor package to the OUT port of the differential air pressure sensor. It can be any DPX sensor package, such as a DPX-T3H1.
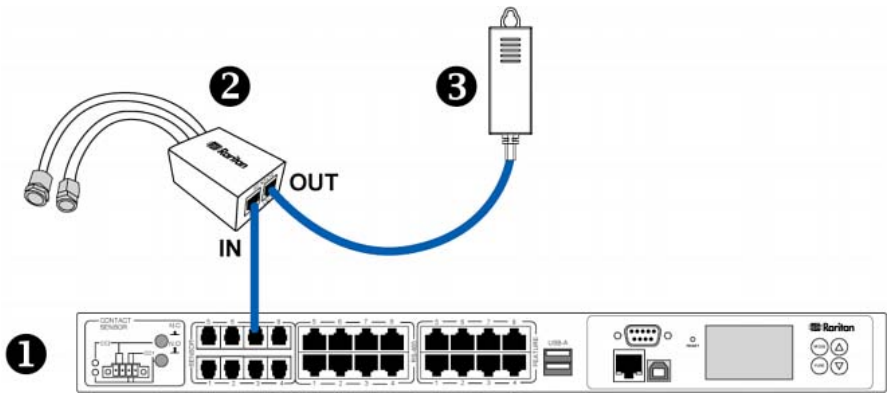
❶	The EMX device
❷	Raritan differential air pressure sensors
❸	One DPX sensor package (optional)

Using an Optional DPX-ENVHUB4 Sensor Hub

Optionally, you can connect a Raritan *DPX-ENVHUB4* sensor hub to the EMX. This allows you to connect up to four DPX sensor packages to the EMX via the hub.

This sensor hub supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

DPX-ENVHUB4 sensor hubs CANNOT be cascaded. You can connect only one hub to each SENSOR port on the EMX.

Tip: The Raritan sensor hub that supports ALL types of Raritan environmental sensor packages is DPX3-ENVHUB4. *See* **Using an Optional DPX3-ENVHUB4 Sensor Hub** *(on page 53).*

▶ **To connect DPX sensor packages via the DPX-ENVHUB4 hub:**

1. Connect the DPX-ENVHUB4 sensor hub to the EMX.

    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 of the cable into the RJ-12 SENSOR port of the EMX.

2. Connect DPX sensor packages to any of the four OUT ports on the hub.

    This diagram illustrates a configuration with a sensor hub connected.
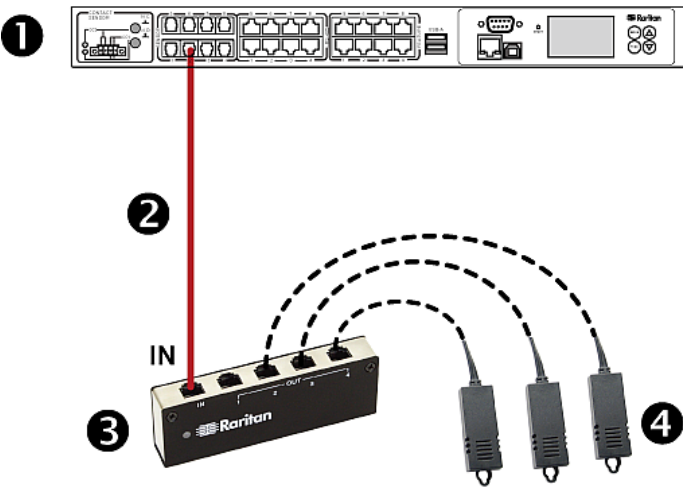
❶	The EMX device
❷	Raritan-provided phone cable
❸	DPX-ENVHUB4 sensor hub

❹	DPX sensor packages

Using an Optional DPX-ENVHUB2 cable

A Raritan *DPX-ENVHUB2* cable doubles the number of connected environmental sensors per SENSOR port.

This cable supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

▶ **To connect DPX sensor packages via the DPX-ENVHUB2 cable:**

1. Plug the connector of this cable directly into the EMX device's RJ-12 SENSOR port.
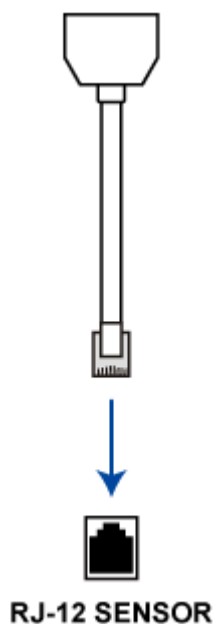
RJ-12 SENSOR

2. The cable has two RJ-12 sensor ports. Connect DPX sensor packages to the cable's sensor ports.
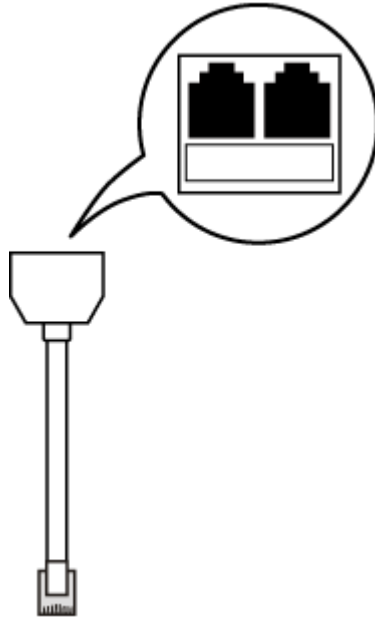
3. Repeat the above steps if there are additional SENSOR ports on your EMX.

Supported Maximum DPX Sensor Distances

When connecting the following DPX sensor packages to the EMX, you must follow two restrictions.

- DPX-CC2-TR
- DPX-T1
- DPX-T3H1
- DPX-AF1
- DPX-T1DP1

▶ **Sensor connection restrictions:**

- Connect a DPX sensor package to the EMX using the sensor cable pre-installed (or provided) by Raritan. You MUST NOT extend or modify the sensor cable's length by using any tool other than the Raritan's sensor hubs.
- If using a DPX-ENVHUB4 sensor hub, the cabling distance between the EMX and the sensor hub is up to 33' (10 m).

▶ **Maximum Distance Illustration:**

The following illustrates the maximum distance when connecting DPX sensor packages with a maximum 16' (5 m) sensor cable to an EMX via a sensor hub.

- The sum of a DPX-T3H1 sensor cable's length is 16' (5 m).
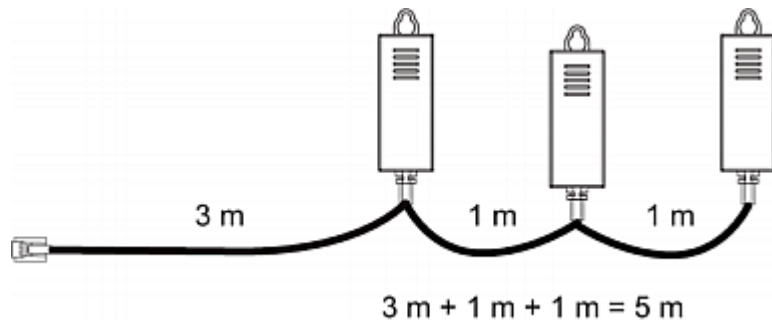
- The total cabling length between the EMX and one DPX-T3H1 is 49' (15 m) as illustrated below.

    Note that the length 16' (5 m) is the length of each DPX-T3H1 sensor cable, which is defined in the above diagram.

EMX2-888 → 33' (10 m) cable → Up to 8 hubs → 16' (5 m) cable → Up to 32 DPX-T3H1 sensor packages

| EMX2-111 | → | 33' (10 m) cable | → | Up to 1 hub | → | 16' (5 m) cable | → | Up to 4 DPX-T3H1 sensor packages |

DPX2 Sensor Packages

A DPX2 sensor cable is shipped with a DPX2 sensor package. This cable is made up of one RJ-12 connector and one to three head connectors. You have to connect DPX2 sensor packages to the sensor cable.

For more information on DPX2 sensor packages, access the Environmental Sensors Guide or Online Help on Raritan website's *Support page* (*http://www.raritan.com/support/*).
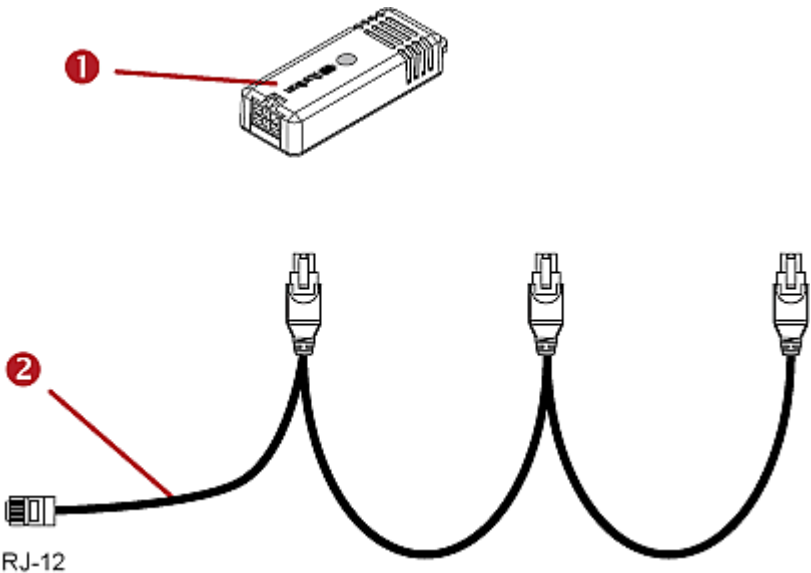
Item	
❶	DPX2 sensor package
❷	DPX2 sensor cable with one RJ-12 connector and three head connectors

The following procedure illustrates a DPX2 sensor cable with three head connectors. Your sensor cable may have fewer head connectors.

Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor package with a DPX2 sensor package.

▶ **To connect DPX2 sensor packages to the EMX:**

1. Connect a DPX2 sensor package to the first head connector of the DPX2 sensor cable.
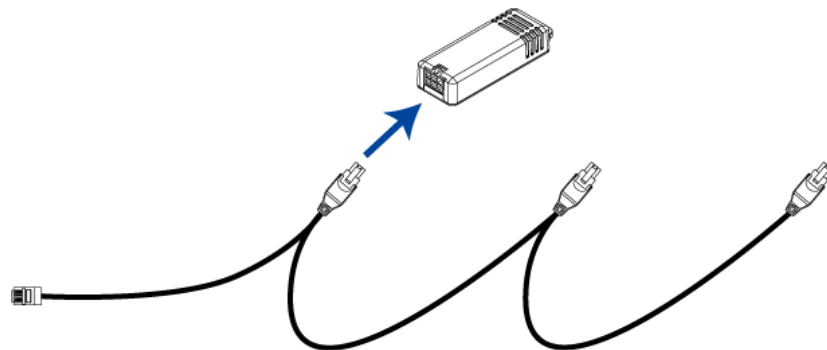
2. Connect remaining DPX2 sensor packages to the second and then the third head connector.
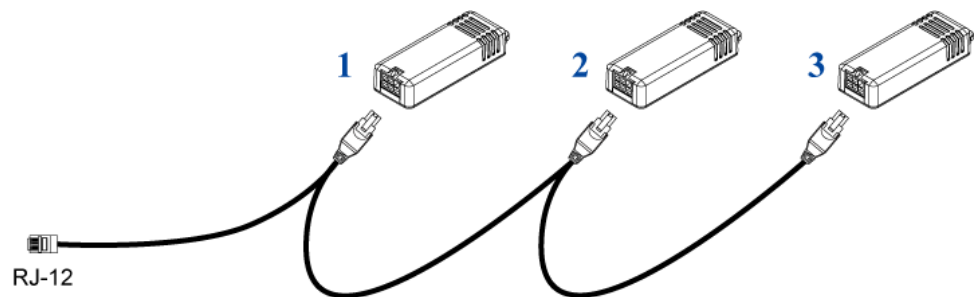
Tip: If the number of sensors you are connecting is less than the number of head connectors on your sensor cable, connect them to the first one or first two head connectors to ensure that there are NO free head connectors prior to the final DPX2 sensor package attached.

3. Plug the RJ-12 connector of the DPX2 sensor cable into the RJ-12 SENSOR port on the EMX.
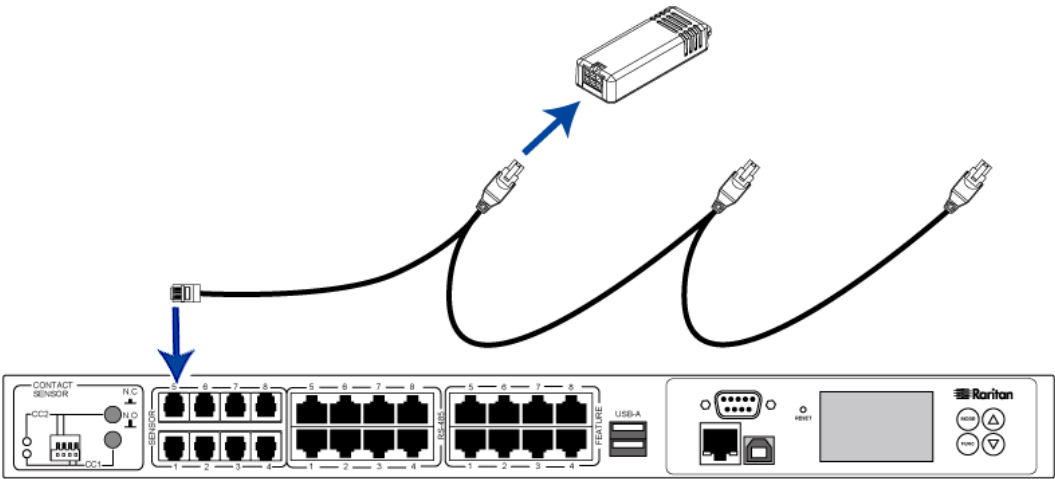
OR you can directly connect the DPX2 sensor package to a DX sensor chain without using any RJ-12 to RJ-45 adapter. See *Connecting a DPX2 Sensor Package to DX* (on page 52).

DPX3 Sensor Packages

A DPX3 sensor package features the following:

• Its connection interface is RJ-45.

• You can cascade a maximum of 12 DPX3 sensor packages.
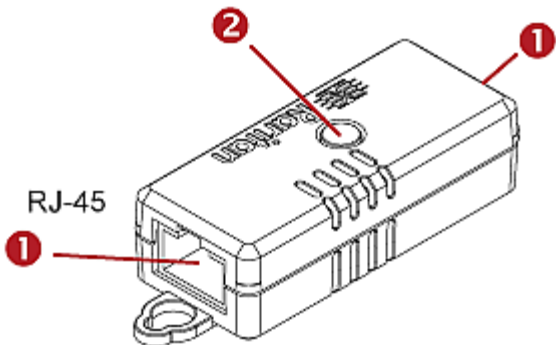
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
❷	LED for indicating the sensor status.

▶ **To connect DPX3 sensor packages to the EMX:**

1. Connect an RJ-12 to RJ-45 adapter cable to the DPX3 sensor package.

   ▪ Connect the adapter's RJ-45 connector to either RJ-45 port of the DPX3 sensor package.

2. If you want to cascade DPX3 sensor packages, get an additional standard network patch cable (CAT5e or higher) and then:

   a. Plug one end of the cable into the remaining RJ-45 port on the prior DPX3.

   b. Plug the other end into either RJ-45 port on an additional DPX3.

   Repeat the same steps to cascade more DPX3 sensor packages.
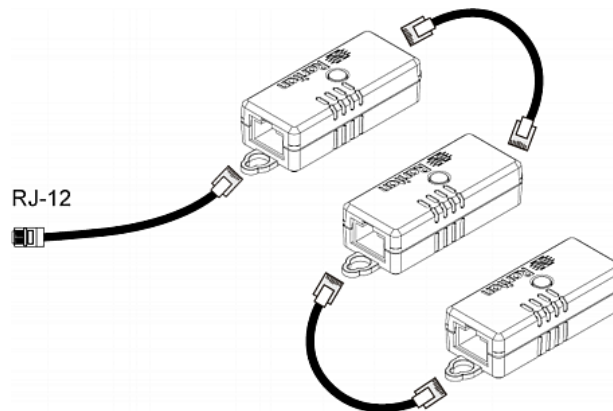
3. Connect the first DPX3 sensor package to the EMX.

   ▪ Plug the adapter cable's RJ-12 connector into the RJ-12 SENSOR port on the EMX.

Connecting a DPX2 Sensor Package to DPX3

You can connect only one DPX2 sensor package to the "end" of a DPX3 sensor chain. It is strongly recommended to use an RJ-12 to RJ-45 adapter for connecting the DPX2 to the final DPX3 in the chain.

The maximum number of DPX3 sensor packages in the chain must be less than 12 when a DPX2 sensor package is involved.

▶ **When connecting a DPX2 sensor package containing three DPX2 sensors:**

A maximum of nine DPX3 sensor packages can be cascaded because 12-3=9.
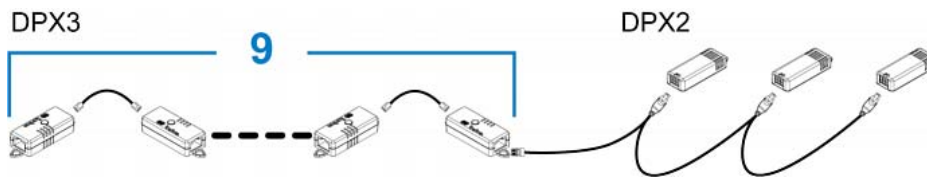
▶ **When connecting a DPX2 sensor package containing two DPX2 sensors:**

A maximum of ten DPX3 sensor packages can be cascaded because 12-2=10.
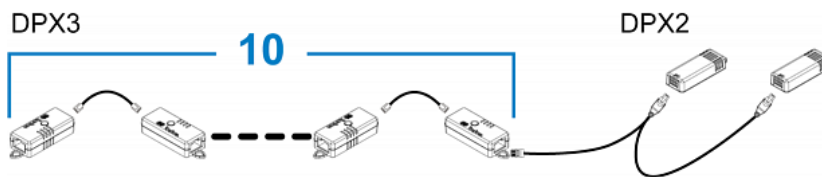
▶ **When connecting a DPX2 sensor package containing one DPX2 sensor:**

A maximum of eleven DPX3 sensor packages can be cascaded because 12-1=11.
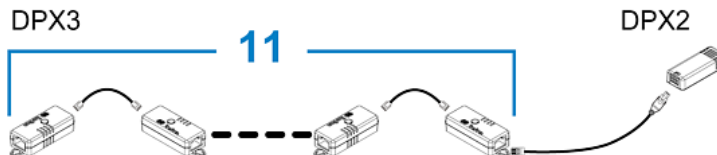
DX Sensor Packages

Most DX sensor packages contain terminals for connecting detectors or actuators. For information on connecting actuators or detectors to DX terminals, refer to the Environmental Sensors Guide or Online Help on Raritan website's *Support page* (*http://www.raritan.com/support/*).

You can cascade up to 12 DX sensor packages.

When cascading DX, remember that the EMX only supports a maximum of 32 sensors and/or actuators.

If there are more than 32 sensors and/or actuators connected, every sensor and/or actuator after the 32nd one is NOT managed by the EMX.

For example, if you cascade 12 DX packages, and each package contains 3 functions (a function is a sensor or actuator), the EMX does NOT manage the last 4 functions because the total 36 (12*3=36) exceeds 32 by 4.

Tip: To manage the last 4 functions, you can release 4 "managed" sensors or actuators, and then manually bring the last 4 functions into management. See **Peripherals** *(on page 101).*
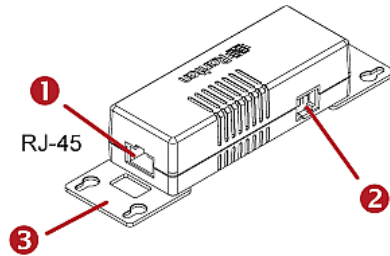
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DX sensor package.
❷	RJ-12 port, which is reserved for future use and now blocked.
❸	Removable rackmount brackets.

▶ **Connect DX to the EMX:**

1. Connect an RJ-12 to RJ-45 adapter cable which is shipped with a DX sensor package to the DX.

   - Connect the adapter's RJ-45 connector to either RJ-45 port of the DX.

2. If you want to cascade DX packages, get an additional standard network patch cable (CAT5e or higher) and then:

a. Plug one end of the cable into the remaining RJ-45 port on the prior DX package.

b. Plug the other end into either RJ-45 port on an additional DX package.

Repeat the same steps to cascade more DX packages.
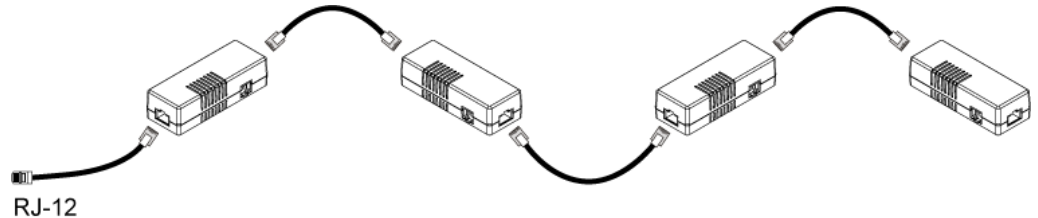
RJ-12

3. Connect the first DX sensor package to the EMX.

   - Plug the adapter cable's RJ-12 connector into the RJ-12 SENSOR port of the EMX.

4. If needed, connect a DPX2 sensor package to the end of the DX chain. See *Connecting a DPX2 Sensor Package to DX* (on page 52).

Connecting a DPX2 Sensor Package to DX

You can connect only one DPX2 sensor package to the "end" of a DX sensor chain. It is strongly recommended to use an RJ-12 to RJ-45 adapter for connecting the DPX2 to the final DX in the chain.

The maximum number of DX sensor packages in the chain must be less than 12 when a DPX2 sensor package is involved.

▶ **When connecting a DPX2 sensor package containing three DPX2 sensors:**

A maximum of nine DX sensor packages can be cascaded because 12-3=9.
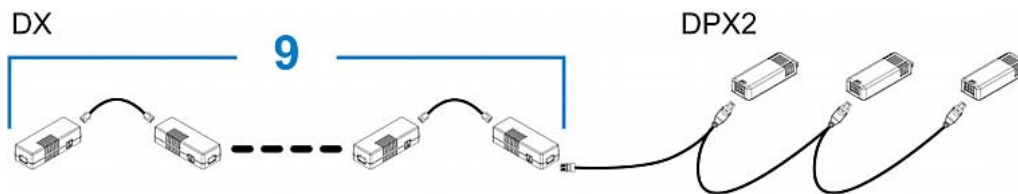
► **When connecting a DPX2 sensor package containing two DPX2 sensors:**

A maximum of ten DX sensor packages can be cascaded because 12-2=10.
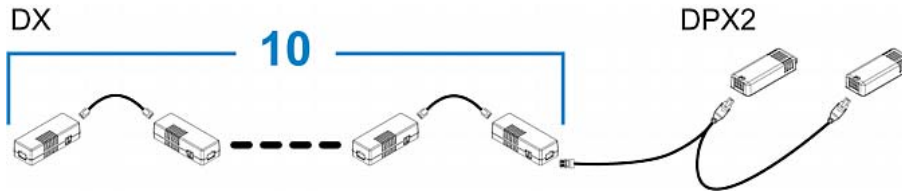
► **When connecting a DPX2 sensor package containing one DPX2 sensor:**

A maximum of eleven DX sensor packages can be cascaded because 12-1=11.
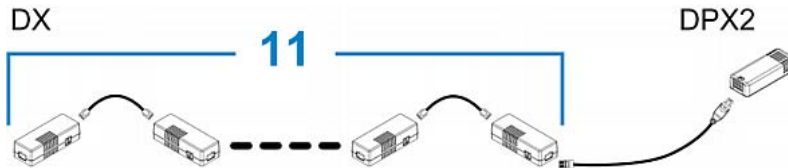
Using an Optional DPX3-ENVHUB4 Sensor Hub

A Raritan DPX3-ENVHUB4 sensor hub is physically and functionally similar to the DPX-ENVHUB4 sensor hub, which increases the number of sensor ports for the EMX, except for the following differences:

- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages.
- To connect diverse types of sensor packages to this sensor hub, you must follow the combinations shown in the section titled *Mixing Diverse Sensor Types* (on page 55).

► **To connect DPX3 sensor packages via the DPX3-ENVHUB4 hub:**

1. Connect the DPX3-ENVHUB4 sensor hub to the EMX using an RJ-12 to RJ-45 adapter cable.

   a. Plug the RJ-45 connector of this cable into the IN port (Port 1) of the hub.

   b. Plug the RJ-12 connector of this cable into the RJ-12 SENSOR port of the EMX.

2. Connect the Raritan sensor packages to any of the four OUT ports on the hub.

    ▪ An RJ-12 to RJ-45 adapter is required for connecting a DPX or DPX2 sensor package to the hub.

    This diagram illustrates a configuration with a sensor hub connected.
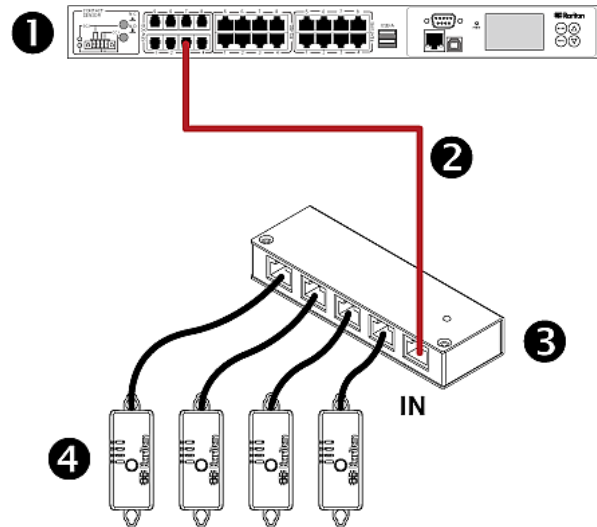
❶	The EMX
❷	RJ-12 to RJ-45 adapter cable
❸	DPX3-ENVHUB4 sensor hub
❹	Any Raritan sensor packages

Mixing Diverse Sensor Types

You can mix DPX, DPX2, DPX3 and DX sensor packages on any sensor port of the EMX2-888 or EMX2-111 according to the following sensor combinations. In some scenarios, the DPX3-ENVHUB4 sensor hub is required.

When mixing different sensor types, remember that each sensor port supports a maximum of 32 sensors/actuators. For the total number of supported sensors/actuators for your EMX model, see *Connecting Environmental Sensor Packages* (on page 39).

▶ **"1 DX + 1 DPX" per sensor port:**

- An RJ-12 to RJ-45 adapter cable is required for connecting the DX sensor package to the EMX.
- It is strongly recommended to use an RJ-12 to RJ-45 adapter to connect the DPX sensor package to the DX sensor package.
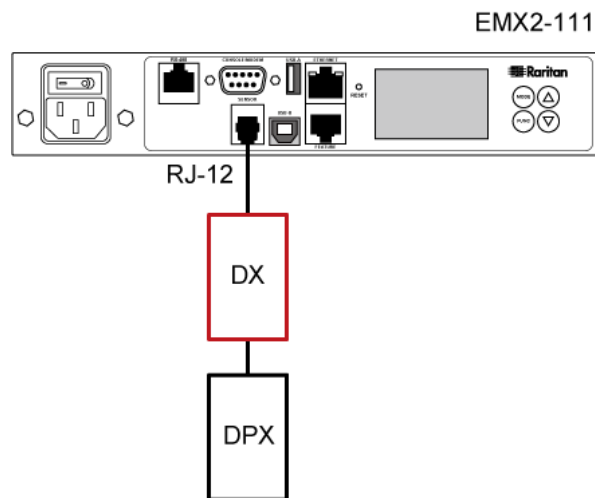
▶ **Diverse combinations via the DPX3-ENVHUB4 sensor hub:**

- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - A DX sensor package
  - A chain of DX sensor packages
  - A DPX3 sensor package
  - A chain of DPX3 sensor packages
  - A DPX2 sensor package
  - A DPX sensor package

- An RJ-12 to RJ-45 adapter is recommended to connect a DPX or DPX2 sensor package to DPX3-ENVHUB4.

- In the following diagrams, the sensor package in "green" can be replaced by a DPX2 sensor package. The sensor package in "blue" can be one DPX2, DPX3 or DX sensor package.

- An RJ-12 to RJ-45 adapter cable MUST be used for connecting the DPX3-ENVHUB4 to the EMX.

This section only illustrations the following three combinations, but actually there are tens of different combinations by using the DPX3-ENVHUB4 sensor hub.
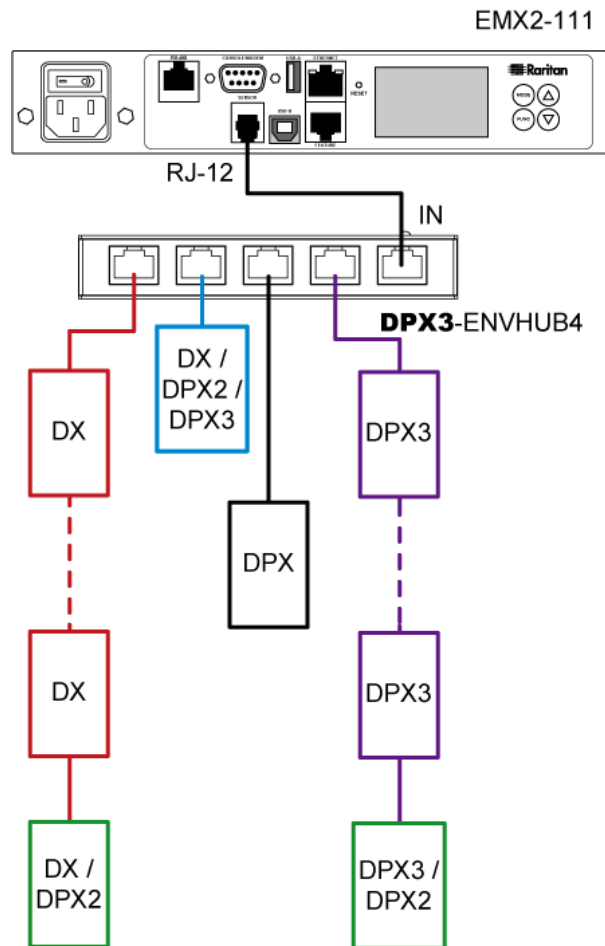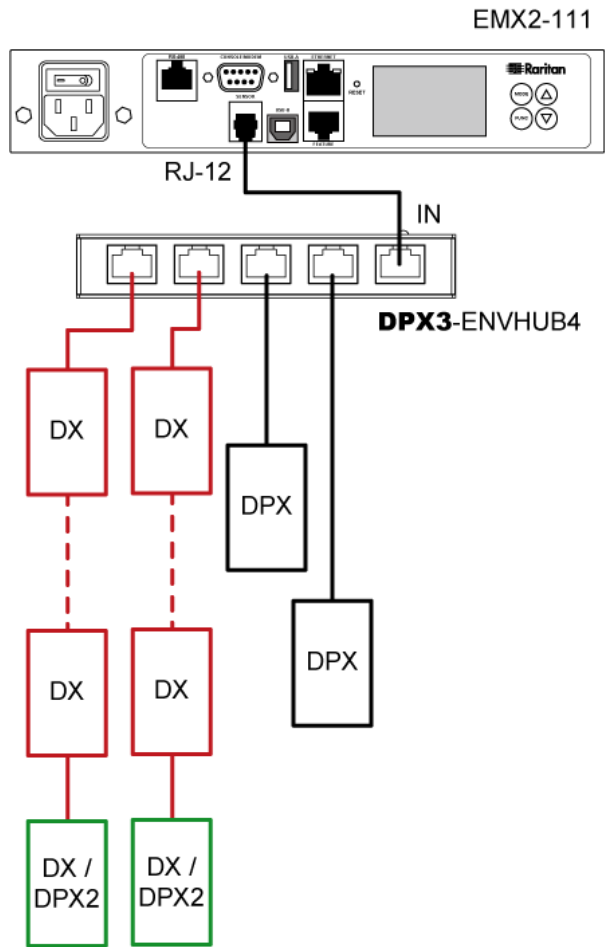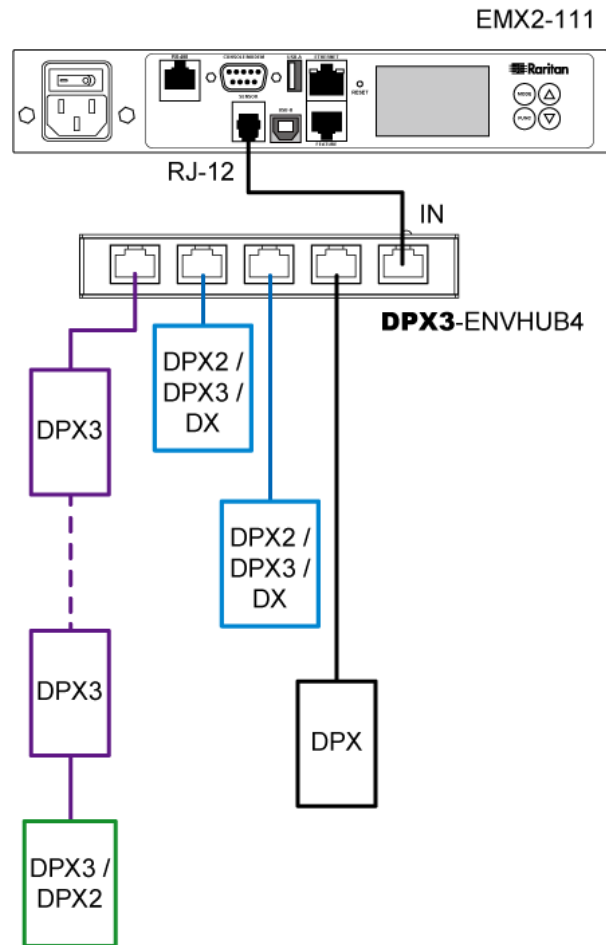
▶ **Mix DPX3 and DX in a sensor chain:**

Any DX sensor package in a chain can be replaced by a DPX3 sensor package, or vice versa. The total number of sensor packages in this chain cannot exceed 12.

For example, the following diagram shows a sensor chain comprising both DX and DPX3 sensor packages.

You can add a DPX2 sensor package to the end of such a sensor-mixing chain if intended. See *Connecting a DPX2 Sensor Package to DPX3* (on page 50) or *Connecting a DPX2 Sensor Package to DX* (on page 52).

Connecting a Logitech Webcam

Connect webcams to EMX in order to view videos or snapshots of the webcam's surrounding area.

The following USB Video Class (UVC) compliant webcam is supported:

- Logitech® Webcam® Pro 9000, Model 960-000048

Other UVC-compliant webcams may also work. However, Raritan has neither tested them nor claimed that they will work properly.

Tip: You can easily find a list of UVC-compliant webcams on the Internet.

The EMX supports up to two webcams. You can use a "powered" USB hub to connect webcams if needed.

After connecting a webcam, you can retrieve visual information from anywhere through the EMX web interface. If your webcam supports audio, audio is available with videos.

For more information on the Logitech 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.

Important: If a USB hub is used to connect the webcam, make sure it is a "powered" hub.

Snapshots or videos captured by the webcam are immediately displayed in the EMX web interface after the connection is complete. See *Configuring Webcams and Viewing Live Images* (on page 279).

Connecting a GSM Modem

The following Cinterion® GSM modems can be connected to the EMX in order to send SMS messages containing event information.

- MC52iT
- MC55iT
- EHS6

See *Available Actions* (on page 219) for more information on SMS messages.

Note: EMX cannot receive SMS messages.

▶ **To connect the GSM modem:**

1. Connect the GSM modem to the serial port labeled CONSOLE / MODEM on the EMX.
2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.
3. Configure the GSM modem settings in the EMX to specify the modem's SIM PIN number and the recipient phone number. See *Configuring the Serial Port* (on page 253).

Connecting an Analog Modem

The EMX supports remote dial-in communications to access the CLI through an analog modem. This dial-in feature provides an additional alternative to access the EMX when the LAN access is not available. To dial in to the EMX, the remote computer must have a modem connected and dial the correct phone number.

Below are the analog modems that the EMX supports for sure:

- NETCOMM IG6000 Industrial Grade SmartModem
- US Robotics 56K modem

The EMX may also support other analog modems which Raritan did not test.

Note that the EMX does NOT support dial-out or dial-back operations via the modem.

▶ **To connect an analog modem:**

1. Plug a telephone cord into the phone jack of the supported modem.
2. Plug the modem's RS-232 cable into the serial port labeled CONSOLE / MODEM on the EMX.

You need to enable the modem dial-in support to take advantage of this feature, see *Configuring the Serial Port* (on page 253).

Connecting an External Beeper

The EMX supports the use of an external beeper for audio alarms.

External beepers that are supported include but may not be limited to the following:

• Mallory Sonalert MODEL SNP2R

After having an external beeper connected, you can create event rules for the EMX to switch on or off the external beeper when specific events occur. See *Event Rules and Actions* (on page 204).

▶ **To connect an external beeper:**

1. Connect a standard network patch cable to the FEATURE port of the EMX.

2. Plug the other end of the cable into the external beeper's RJ-45 socket.

   The beeper can be located at a distance up to 330 feet (100 m) away from the EMX.

Connecting a Schroff LHX/SHX Heat Exchanger

To remotely monitor and administer the Schroff® LHX-20, LHX-40 and SHX-30 heat exchangers through the EMX device, connect the heat exchanger to the EMX.

You can connect as many LHX-20 or LHX-40 heat exchangers to your EMX device as there are RS-485 ports or Feature ports on your EMX model.

Note that the SHX-30 requires an adapter cable to connect to the RS-485 port on the EMX. Contact Schroff to purchase this cable.

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

▶ **To connect an LHX-20 or LHX-40 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.

▶ **To connect an SHX-30 heat exchanger:**

1. Plug one end of the Schroff adapter cable into the RS-485 port on the Schroff SHX heat exchanger.

2. Plug the other end of the adapter cable into one of available RS-485 ports on your EMX.

▶ **To connect an LHX/SHX heat exchanger to the FEATURE port using a Schroff serial cable:**

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

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

See *Schroff LHX/SHX* (on page 130) for how to monitor and administer the heat exchanger using the EMX.

Connecting the Schneider Electric PowerLogic PM710

The Schneider Electric PowerLogic® PM710 power meter is connected to the EMX RS485 port. Once it is connected and the EMX detects it, the PM710 is viewed in the EMX web interface.

This device is only supported when plugged into the RS485 port using a PM710 supported cable (not provided by Raritan with the EMX). A maximum of one PM710 can be connected to each RS485 port. You cannot daisy chain PM710 units because the EMX does not support a PM710 daisy chain.

Note: Refer to your Schneider Electric PowerLogic PM710 documentation for information on the pinouts for the meter and any sensor-specific configuration required.

From the EMX, you can remotely reset the PM710 energy accumulators, and the PM710 minimum and maximum reading values. Additionally, you can create event rules and actions for PM710, such as emailing or sending an SMS message when thresholds are reached, and so on. See *Event Rules and Actions* (on page 204).

The PM710 line speed, parity and address, as well as the thresholds for PM710 numeric sensors, can be configured on the PM710. These settings need to be the match in EMX. For example, if the address is 42 in the PM710 it must also be 42 in EMX.

All settings are configured on a per port basis. If you disconnect a PM710 from one EMX port and connect it to another, you must reconfigure the settings. However, if you disconnect a PM710 from a port and then plug it back in to the same port, the already configured settings still apply.

Note: PM710 meters are not supported through SNMP or the command line interface (CLI).

Connecting a Modbus RTU Device or Bus

If connecting the Modbus RTU devices to the EMX and enabling the Modbus Gateway feature, the Modbus TCP clients on your network will be able to communicate with those Modbus RTU devices attached to the EMX.

▶ **To use the Modbus Gateway feature:**

1. Connect a Modbus RTU device, or a Modbus bus with multiple RTU devices, to the EMX via two adapters described below.

   a. Connect an isolated RS485-to-RS232 adapter to the Modbus RTU device or Modbus bus.

b. Connect an RS232-to-USB adapter (using FTDI's FT232 chip) to the RS485-to-RS232 adapter.

c. Connect the RS232-to-USB adapter to the USB-A port on the EMX.

Note: DO NOT connect the Modbus RTU device or Modbus bus to the RS485 ports on the EMX, which is NOT supported.

2. On the EMX, enable and properly configure the Modbus Gateway feature. See *Changing Modbus Settings* (on page 176).

▶ **Communications between Modbus TCP and RTU devices:**

- The EMX acts only as a message gateway for the Modbus TCP client.

  Messages from the Modbus TCP client(s) are passed through the EMX to the connected Modbus RTU devices or Modbus bus.

- The Modbus RTU devices on the bus are identified with their Modbus RTU addresses using the Modbus unit identifier addresses in the Modbus TCP protocol.

  If the Modbus TCP client does not support unit identifier addressing, refer to *Changing Modbus Settings* (on page 176).

- The EMX supports communications to multiple Modbus RTU devices. Note that the connected Modbus RTU devices are invisible to the EMX.

Chapter 5 Using the EMX

In This Chapter

Power Switch

A power switch turns on or off the EMX.

EMX2-111 front panel power switch:
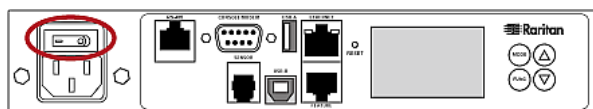
EMX2-888 rear panel power switch:
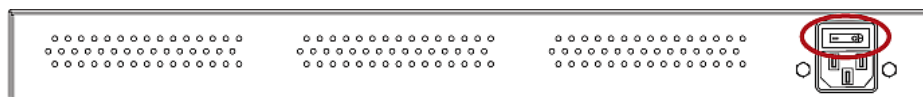
To power cycle the EMX, turn off the device, **wait at least 10 seconds** and turn it back on.

Note that a minimum of 10-second power-off period is required, or the device may not boot up properly.

Connection Ports

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

The following images and table explain the function of each port.

EMX2-111

EMX2-888

No.	Port	Used for...
1	SENSOR (RJ-12)	Connection to one of the following devices: ▪ Raritan's environmental sensor package(s). ▪ Raritan's sensor hub, which expands the number of a sensor port to four ports.
2	RS-485	Connection to an electrical device with the RS-485 interface. Currently the EMX supports the Schroff® LHX-20, LHX-40 and SHX-30 heat exchangers. *Note: The SHX-30 requires an adapter cable to connect to the RS-485 port on the EMX. Contact Schroff to purchase this cable.*
3	FEATURE	Connection to one of the following devices: ▪ A Raritan asset management strip, which allows you to track the locations of IT devices on the rack. ▪ A Schroff® LHX-20, SHX-30 or LHX-40 device, using an RJ-45 to RS-232 cable provided by Schroff. ▪ An external beeper with the RJ-45 socket. *Note: The EMX supplies power to the connected asset management sensor.*
4	USB-A	**This is a "host" port, which is powered, per USB 2.0 specifications.** • Connecting a USB device, such as a Logitech® webcam or wireless LAN adapter. • Cascading the EMX devices for sharing a network connection. See *Cascading the EMX via USB* (on page 22).
5	CONSOLE/MODEM	Establishing a serial connection between the EMX and a computer or modem. 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 to the computer.

No.	Port	Used for...
6	ETHERNET	Connecting the EMX to your company's network via a standard network patch cable (Cat5e/6). This connection is necessary to administer or access the EMX remotely.
		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 if wireless connection is preferred, or if the EMX is a slave device in the USB-cascading configuration. See **Cascading the EMX via USB** *(on page 22).*
7	USB-B	• Cascading the EMX devices for sharing a network connection.
		• Establishing a USB connection between a computer and the EMX for using the command line interface or performing the disaster recovery. For disaster recovery instructions, contact Raritan Technical Support.

LCD Display Panel

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

It consists of:

• A character LCD display

• Control buttons

Overview of the LCD Display

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

Section	Information shown
❶	The selected mode and target, such as SENSOR 8, SENSOR 36, 1 SENSOR 28, CA (cascading mode), or the number of the FEATURE port.
❷	The following information is displayed: • Readings, data or state of the selected target. • During the firmware upgrade, "FUP" is displayed.
❸	The "ALARM" status of the selected target. Examples: ▪ A numeric sensor enters the warning or critical level. ▪ A discrete (on/off) sensor enters the alarmed state. ▪ NO asset tag is detected on the selected rack unit. *Note: For the Raritan asset sensor, a rack unit refers to a tag port.*
❹	The measurement unit of the displayed data, such as % or °C.
❺	This section indicates: • The Asset Strip mode if an asset strip has been connected to the EMX. • The device's USB-cascading state - *MASTER* or *SLAVE*. If it is a standalone device, neither MASTER nor SLAVE is displayed.

Control Buttons

There are four control buttons.
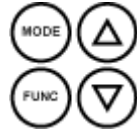
- Up and Down buttons for selecting a specific target, which can be an environmental sensor's ID number or an asset sensor's port number
- MODE button for switching between various modes, including:

   - Sensor mode

   - Asset Sensor mode, indicated by the word ASSET, for showing the asset sensor information

   - Device mode

   See *Overview of the LCD Display* (on page 69).

- FUNC (Function) button for switching between different data of the selected target, such as sensor readings, position information and serial number of an environmental sensor package

Operating the LCD Display

After powering on or resetting this product, the LCD display panel shows the first environmental sensor listed on the EMX web interface before you select a different target.

Environmental Sensor Information

The environmental sensor mode is displayed as "SENSOR" on the LCD display. Basic information about a specific environmental sensor is available, including the sensor's reading or state, X, Y, Z coordinates and its serial number.

Below illustrates the environmental sensor information.

Number	Example information
❶	The selected target is the environmental sensor whose ID number is 9 (SENSOR 9).
❷	The selected environmental sensor's reading is 22 °C .
❸	The word "MASTER" indicates the EMX is the master device in a cascading configuration. For a slave device, it shows "SLAVE" instead. *Note: As of release 3.3.10, the "MASTER/SLAVE" information is no longer available in the bridging mode, but remains available in the port forwarding mode.*
❹	The measurement unit is °C (degrees in Celsius).

▶ **To display the environmental sensor information:**

1. Press the MODE button until this product enters the Sensor mode, as indicated by "SENSOR" at the top of the LCD display.

2. Press the Up or Down button until the desired environmental sensor's ID number is displayed.

   For example, "SENSOR 1" refers to the sensor #1 listed on the EMX web interface. "1 SENSOR 24" refers to the #124 sensor.

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

   ▪ When showing a numeric sensor's reading, the appropriate measurement unit is displayed to the right of the reading.

Measurement units	Sensor types
%	A relative humidity sensor
°C	A temperature sensor
m/s	An air flow sensor
Pa	An air pressure sensor
NO measurement units	For an "absolute" humidity sensor, the measurement unit is g/m^3, which cannot be displayed on the LCD.

   ▪ Available states for a state sensor:

States	Description
nor	Normal state.
ALA	Alarmed state. ▪ This state is accompanied with the word "ALARM" below it.

▪ Available states for a dry contact signal actuator (DX sensor series):

States	Description
On	The actuator is turned on.
Off	The actuator is turned off.

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while state sensors show sensor states only to indicate state changes.

4. Press the FUNC button to show the sensor's port position. There are two types of information.

   ▪ *P:n* (where n is the SENSOR port's number): This information indicates the SENSOR port number. The port number for onboard contact closure sensor is displayed as *CC1* or *CC2*.

   ▪ *C:x* (where x is the sensor's position in a sensor chain): This information indicates the sensor's position in a chain, which is available for DPX2, DPX3 and DX sensors only. The LCD display will cycle between the port information (*P:n*) and chain position information (*C:x*).

   Note that if the DPX3-ENVHUB4 sensor hub is used to connect the DPX2, DPX3 or DX sensors, the chain position information (C:x) is displayed twice - the first one indicates the sensor hub's chain position, which is always *C:1*, and the second one indicates the sensor's chain position.

5. Press the FUNC button to display the X, Y and Z coordinates of the sensor respectively.

   ▪ X coordinate is shown as "x:NN," where NN are the first two numeric digits entered for the X coordinate in the web interface.

   ▪ Y coordinate is shown as "y:NN," where NN are the first two numeric digits entered for the Y coordinate in the web interface.

   ▪ Z coordinate is shown as "z:NN," where NN 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, these alphabetical characters are replaced with dashes (-).

6. Press the FUNC button 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

Note: Some alphabets cannot be properly displayed due to the LCD display restriction. For example, Q looks like 9, Z looks like 2, and M looks like $\equiv$. Check the sensor's label or the web interface when you have doubts.

Asset Sensor Information

The LCD display can show 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.

Below illustrates the asset strip information.

Section	Example information
❶	"1" refers to the asset strip connected to the first FEATURE port.
❷	This symbol ◇ indicates that you can switch between diverse rack units now by pressing the Up or Down button.
❸	"30" indicates that the selected target is the 30th rack unit.

Section	Example information
❹	The word "MASTER" indicates the EMX is the master device in a cascading configuration. For a slave device, it shows "SLAVE" instead.
	Note: As of release 3.3.10, the "MASTER/SLAVE" information is no longer available in the bridging mode, but remains available in the port forwarding mode.
❺	"ASSET" means that the LCD display enters the Asset Strip mode.

► **To display the asset management information:**

1. Press the MODE button until the EMX enters the Asset Strip mode, as indicated by "ASSET" to the right of the LCD.

2. Press the Up or Down button until the desired FEATURE port number is displayed at the top of the LCD display.

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

3. Press the FUNC button. When a blinking double-arrow symbol ◇ appears to the left of the LCD display, press the Up or Down button to select the desired rack unit on the asset strip. The rack unit number appears in the middle of the LCD display.

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

   ▪ If the word "ALARM" appears below the rack unit number, it means no asset tag is physically connected to that rack unit.

   ▪ If the word "ALARM" does NOT appear, it means a connected asset tag is detected on the rack unit.

IPv4 Address

The IP address is available in the Device mode, which is indicated by the alphabet 'd' shown at the top of the LCD display. Note that the LCD display only shows the IPv4 address (if available).

Below illustrates the IP address information.

Section	Example information
❶	"d" means the LCD display has entered the Device mode.
❷	The LCD display is showing 192, which is one of the four IP address octets. It will cycle through four octets.
❸	"i4" indicates that the IP address shown on the LCD display is an IPv4 address.
❹	The word "MASTER" indicates the EMX is the master device in a cascading configuration. For a slave device, it shows "SLAVE" instead. *Note: As of release 3.3.10, the "MASTER/SLAVE" information is no longer available in the bridging mode, but remains available in the port forwarding mode.*

If you connect your EMX to the wireless network, a Wi-Fi icon is displayed at the bottom-right corner.

▶ **To display the IPv4 address:**

1. Press the MODE button to enter the Device mode, indicated by an alphabet "d" at the top left of the display.

2. The LCD display cycles between the four octets of the IPv4 address, indicated by "i4" at the upper right corner of the display.

   For example, 192.168.84.4 cycles in this sequence:

   192 --> 168 --> 84 --> 4

MAC Address

This product's MAC address is retrievable by operating the LCD display.

Below illustrates the MAC address information.

Section	Example information
❶	"d" means the LCD display has entered the Device mode.
❷	"M" indicates that the displayed information is the MAC address.
❸	The word "MASTER" indicates the EMX is the master device in a cascading configuration. For a slave device, it shows "SLAVE" instead. *Note: As of release 3.3.10, the "MASTER/SLAVE" information is no longer available in the bridging mode, but remains available in the port forwarding mode.*
❹	The LCD display is showing "03," which is part of the MAC address.

▶ **To display the MAC address:**

1. Press the MODE button to enter the Device mode, indicated by a 'd' in at the top left of the display.

2. Press the FUNC button until the MAC address is displayed. The character "M" appears in the left side of the LCD display.

3. 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 that 'M' is NOT followed by the colon symbol when showing the first two digits of the MAC address.

USB-Cascaded Device's Position

Note: As of release 3.3.10, the following cascading information is no longer available in the bridging mode, but remains available in the port forwarding mode.

A cascaded device's position is available by operating the LCD display.

Below illustrates a slave device's position.
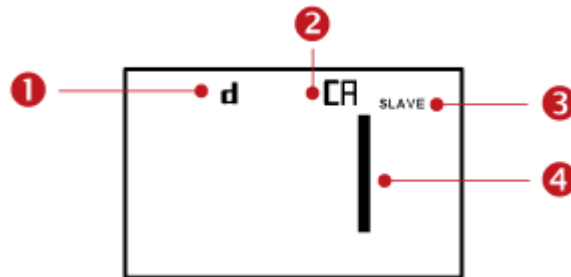
Section	Example information
❶	"d" means the LCD display has entered the Device mode.
❷	"CA" indicates that the cascading information is being displayed.
❸	"SLAVE" indicates that this EMX is a slave device. *Note: For a master device, it shows the word "MASTER" instead.*
❹	The number 1 means the device position is Slave 1.

▶ **To retrieve the device's USB-cascading position information:**

1. Press the MODE button to enter the Device mode, indicated by a 'd' in at the top left of the display.

2. Press the FUNC button until "CA" is displayed at the top right of the display.

3. The device's position is represented by any number defined below:

Number	Device position
0	Master device
1	Slave 1
2	Slave 2
3	Slave 3
4	Slave 4
5	Slave 5
6	Slave 6
7	Slave 7

As of release 3.3.10, the port forwarding mode supports up to 15 slave devices so the numbers 8 to 15 may be shown in this mode.

Raritan.
A brand of Legrand

EMX2-888 Contact Closure Sensor Termination

An EMX2-888 model contains two built-in contact closure (CC) sensor channels, each of which comprises two termination points.

EMX2-888 is designed to use a detachable terminal module for CC sensor termination, which makes installation of contact closure sensors more convenient.

Connect third-party detectors/switches to the CC sensor termination on your EMX2-888.

Exception: Older EMX2-888 models have the "spring-loaded" CC sensor termination built into EMX2-888 so they do not use a detachable terminal module. See **Connecting Contact Closure Sensors to OLD EMX2-888** *(on page 534).*
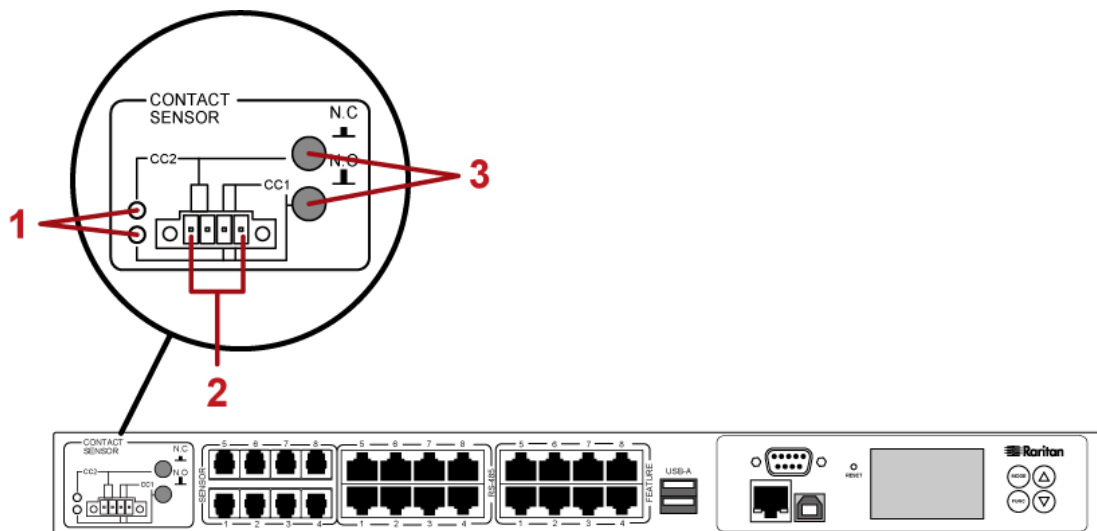
Numbers	Components
1	Two LEDs for indicating the status of two CC sensor channels: ▪ The upper LED is for CC2. ▪ The lower LED is for CC1.
2	Four termination points for two CC sensor channels.

Numbers	Components
3	Two buttons to configure the normal settings of the built-in CC sensor channels. ▪ The upper button is for CC2. ▪ The lower button is for CC1. ▶ **To adjust the normal settings:** ▪ To set to Normally Closed (N.C), press the button to turn it down. ▪ To set to Normally Open (N.O), press the button to turn it up.

Tip: Alternatively, third-party CC switches can be connected to Raritan's DPX-CC2-TR or DX sensor package, which is then connected to a SENSOR port on the EMX. For sensor information, refer to the Environmental Sensors Guide or Online Help on the Raritan's website's **Support page** *(* **http://www.raritan.com/support/** *).*

Connecting Contact Closure Sensors to EMX2-888

Follow the steps below to connect contact closure detectors/switches to the built-in contact closure sensor terminals on your EMX2-888.

Note: For connecting detectors/switches to old EMX2-888 with spring-loaded contact closure sensor terminals, see **Connecting Contact Closure Sensors to OLD EMX2-888** *(on page 534).*

The built-in contact closure sensor terminals comprise two parts as shown below.
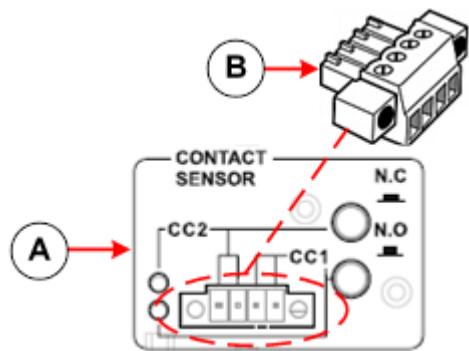
A	Contact closure sensor panel
B	Removable terminal module

The two termination points to the right are associated with channel 1 (CC1 as indicated in the panel), and the two to the left are associated with channel 2 (CC2).

With this design, there are two ways to plug discrete detectors/switches:

- Connect the discrete detectors/switches while the terminal module is attached to the EMX.
- Connect the discrete detectors/switches while the terminal module is separated from the EMX.

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

▶ **To make connections when the terminal module is attached to the EMX:**

1. Strip the insulation around 12 mm from the end of each wire of discrete detectors/switches.

2. Fully insert each wire of both 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 the other detector/switch into the two termination points to the right.
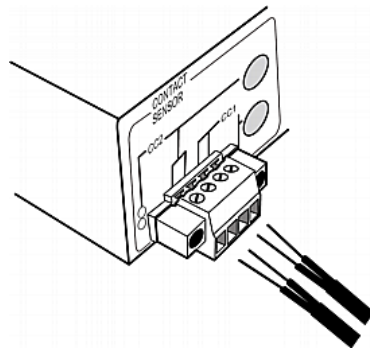
3. Use a screwdriver with a 2.5 mm wide shaft to tighten the screws above each termination point to secure the wires, using a torque of 0.196 N·m (2 kgf·cm).
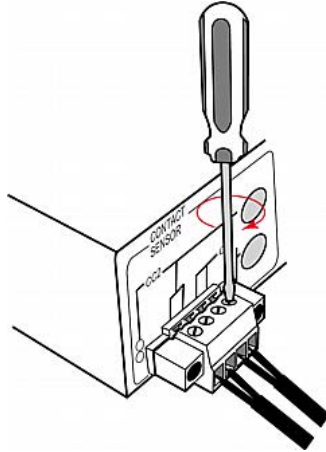
▶ **To make connections when the terminal module is separated from the EMX:**

1. Loosen the two screws on each side of the terminal module.

   Note: The two screws are not removable, so just loosen them.
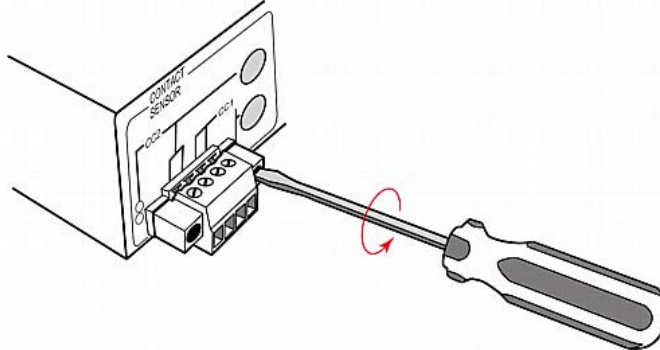
2. Remove the terminal module from the EMX.
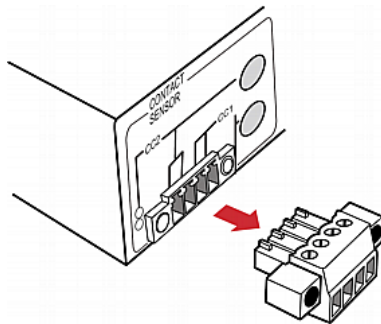
3. Strip the insulation and insert each wire of both detectors/switches into each termination point.
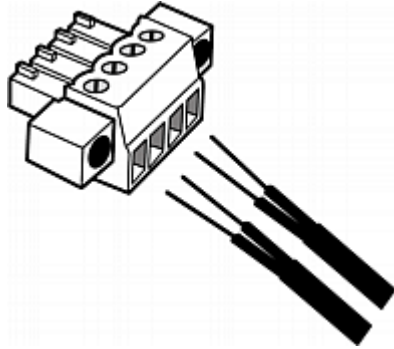
4. Use a screwdriver with a 2.5 mm wide shaft to tighten the screws above each termination point to secure the wires, using a torque of 0.196 N·m (2 kgf·cm).
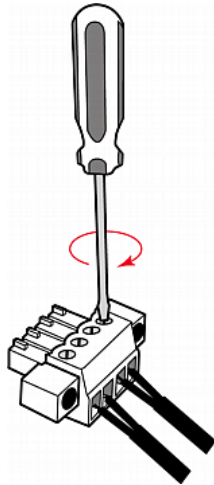
5. Plug the terminal module back into the EMX.
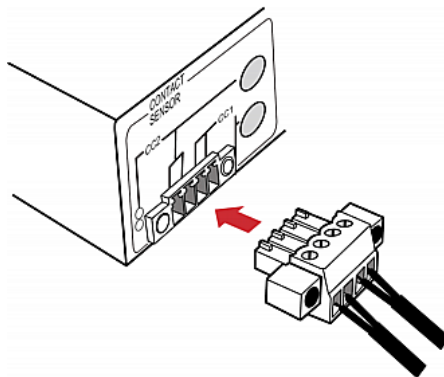
6. Tighten the two screws on two sides of the module to secure it.
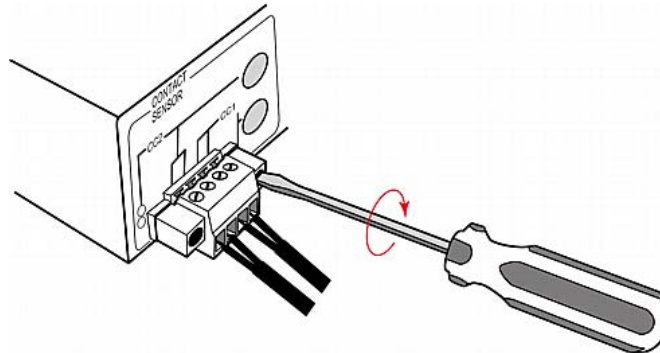
EMX2-888 Contact Closure Sensor LEDs

Two LEDs that show the states of corresponding CC sensor channels are located on the leftmost of the EMX2-888 panel.

• The upper LED is for CC2.
• The lower LED is for CC1.
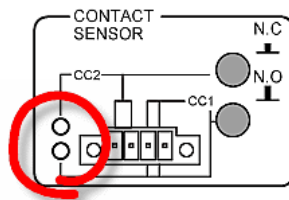
The LED is lit when the associated detector/switch enters the "alarmed" state.

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

• **When the Normal state is set to Normally Closed (N.C):**

LED	Sensor state
Off	Closed
Lit	Open

• **When the Normal state is set to Normally Open (N.O):**

LED	Sensor state
Off	Open
Lit	Closed

For Raritan's DPX water sensors, the Normal state must be set to Normally Open (N.O). The following is the correct LED behavior based on proper dip switch settings.

LED	Sensor state
Off	No water detected
Lit	Water detected

Reset Button

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

The EMX can be reset to its factory default values using this button when a serial connection is available. See *Resetting to Factory Defaults* (on page 465).

Without the serial connection, pressing this reset button only restarts the EMX software.

Beeper

The EMX includes an internal beeper, which can issue an audible alarm.

Note that the beeper does NOT sound an alarm unless an event rule involving the internal beeper has been created and turned on the internal beeper accordingly. See *Event Rules and Actions* (on page 204).

Tip: To remotely check this beeper's state via the web interface, see **EMX** *(on page 98).*

Chapter 6   Using the Web Interface

This chapter explains how to use the web interface to administer a EMX.

In This Chapter

Supported Web Browsers

- Internet Explorer® 11
- Windows Edge
- Firefox® 25 and later
- Safari® (Mac)
- Google® Chrome® 52 and later
- Android 4.2 and later
- iOS 7.0 and later

Note: Depending on the browser you use, spin controls similar to
may or may not appear in the numeric input fields. Clicking these adjusts
numeric values by 1.

Login, Logout and Password Change

The first time you log in to the EMX, use the factory default "admin" user credentials. For details, see the Quick Setup Guide accompanying the product.

After login, you can create user accounts for other users. See *Creating Users* (on page 138).

Login

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

▶ **To log in to the web interface:**

1. Open a browser and type the IP address of the EMX.

    ▪ If the link-local addressing has been enabled, you can type
      pdu.local instead of an IP address. See *APIPA and Link-Local
      Addressing* (on page 4).
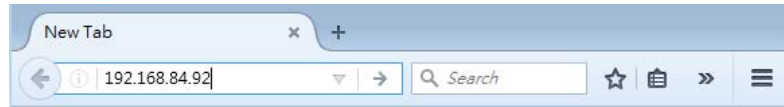
    *Tip: You can also enter the desired page's URL so that you can
    immediately go to that page after login. See* **Quick Access to a
    Specific Page** *(on page 93).*

2. If any security alert message appears, accept it.

3. The login screen displays. Type your user name and password. User
    credentials are case sensitive.
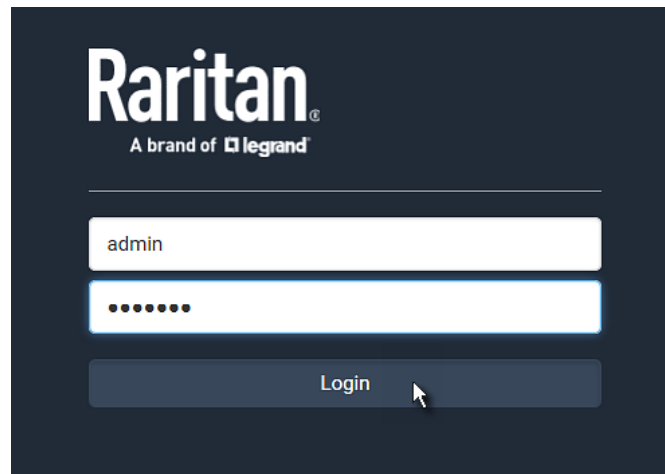
4. (Optional) If a security agreement is displayed, accept it. Otherwise,
    you cannot log in.

    ▪ To select the agreement checkbox using the keyboard, first press
      Tab to go to the checkbox and then Enter.

    Note: To configure the security agreement, see **Enabling the
    Restricted Service Agreement** *(on page 201).*

5. Click Login or press Enter. The EMX web interface opens.

Note: The address to access a slave device in the port forwarding mode via non-standard ports is a combination of a protocol (http:// or https://), an IP address and a port number. See **Port Forwarding Examples** *(on page 166).*

Changing Your Password

You must have the Change Own Password permission to change your own password. See *Creating Roles* (on page 143).

You must have Administrator Privileges to change other users' passwords. See *Editing or Deleting Users* (on page 142).

▶ **Password change request on first login:**

On *first login*, if you have both the Change Local User Management and Change Security Settings permissions, you can choose to either change your password or ignore it.

• *Not Now* ignores the request for this time only.
• *Do not ask again* ignores the request permanently. If you select this checkbox, then click *Not Now*.
• Or enter the new password and click Ok.

Users without permissions listed must change password.

Note: This password change request also appears if the 'force password change' is enabled in the user account setting. See **Creating Users** *(on page 138).*

▶ **To change your password via the Change Password command:**

1. Choose User Management > Change Password.
2. First type the current password, and then the new password twice. Passwords are case sensitive.
   ▪ A password comprises 4 to 64 characters.

Remembering User Names and Passwords

The EMX supports the password manager of common web browsers, including:

- Microsoft Internet Explorer®
- Mozilla Firefox®
- Google Chrome®

You can save the login name and password when these browsers ask whether to remember them.

For information on how to activate a web browser's password manager, see the user documentation accompanying your browser.

The EMX does NOT support other browser password managers.

Logout

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

▶ **To log out without closing the web browser:**

- Click "Logout" on the top-right corner.

  -- OR --

- Close the EMX tab while there are other tabs available in the browser.

▶ **To log out by closing the web browser:**

- Click ⊠ on the top-right corner of the window.

  -- OR --

- Choose File > Close, or File > Exit.

Web Interface Overview

The web interface consists of four areas as shown below.

▶ **Operation:**

1. Click any menu or submenu item in the area of ❶.
2. That item's data/setup page is then opened in the area of ❷.
3. Now you can view or configure settings on the opened page.

4. To return to the main menu and the Dashboard page, click ![Raritan A brand of legrand] on the top-left corner.

Number	Web interface element
❶	*Menu* (on page 91)
❷	Data/setup page of the selected menu item
❸	▪ Left side: 　- EMX device name 　*Note: To customize the device name, see* **EMX** *(on page 98).* ▪ Right side: 　- Your login name, which you can click to view your user account settings 　- Logout button

Number	Web interface element

❹	From top to bottom --
	
	 ▪ Your EMX model
	 ▪ Current firmware version
	 ▪ **Online Documentation**: link to the EMX online help.
	   - See *Browsing through the Online Help* (on page 540).
	 ▪ **Raritan Support**: link to the Raritan Technical Support webpage.
	 ▪ Date and time of your user account's last login
	   - Click **Last Login** to view your login history.
	 ▪ EMX system time
	   - Click **Device Time** to open the Date/Time setup page.

Menu

Depending on your model and hardware configuration, the menu of your EMX may look the same or similar to the following.
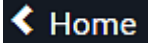
Menu	Information shown
Dashboard	Summary of the EMX status, which shows a list of alerted sensors and alarms, if any. See *Dashboard* (on page 94).
EMX	Device data and settings, such as the device name and MAC address. See *EMX* (on page 98).
Peripherals	Status and settings of Raritan environmental sensor packages, if connected. See *Peripherals* (on page 101).
Feature Port(s) On the EMX2-111, the name 'Fature Port' will be replaced with one of the device names listed to the right	Status and settings of the device connected to the Feature port(s), which can be one of the following. - Asset Strip - External Beeper - LHX 20 - SHX 30 - LHX 40 See *Feature Port(s)* (on page 119).
Auxiliary Port(s)	Status and settings of the device connected to the Auxiliary port(s), which can be one of the following. - LHX 20 - SHX 30 - LHX 40 - PowerLogic PM710 See *Auxiliary Port(s)* (on page 133).
Webcam, Webcam Snapshots	The webcam-related menu items appear only when there are webcam(s) connected to the EMX. Webcam live snapshots/video and webcam settings. See *Webcam Management* (on page 279).
User Management	Data and settings of user accounts and groups, such as password change. See *User Management* (on page 138).
Device Settings	Device-related settings, including network, security, system time, event rules and more. See *Device Settings* (on page 147).

Raritan.
A brand of Legrand

Menu	Information shown
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset. See *Maintenance* (on page 260).

If a menu item contains the submenu, the submenu is shown after clicking that item.

▶ **To return to the previous menu list, do any below:**

- Click the topmost link with the symbol **>**. For example, click
  .

- Press Backspace on the keyboard.

- OR click on the top-left corner to return to the main menu.

Quick Access to a Specific Page

If you often visit a specific page in the EMX web interface, you can note down its URL or bookmark it with your web browser. Next time, you can simply enter its URL in the address bar of the browser prior to login. After login, the EMX immediately shows the desired page rather than the Dashboard page.

If needed, you can even send the URL to other users so that they can immediately see that page after login, using their own user credentials.

▶ **URL examples:**

In the following examples, it is assumed that the IP address of the EMX is 192.168.84.118.

Page	URL
Peripherals	https://192.168.84.118/#/peripherals
Event Log	https://192.168.84.118/#/maintenance/eventLog/0

Sorting a List

If any list displays this arrow ▲ in one of its column headers, you are allowed to resort the list by clicking any column header. The list will be resorted in the ascending or descending order based on the selected column.

▶ **Example:**

1. By default, the Firmware Update History is sorted in the ascending order based on the Timestamp column. Therefore, the arrow ▲ is displayed adjacent to the Timestamp header.

2. To have it resorted in the descending order based on the same column, click the Timestamp header.

3. The arrow turns to ▼, indicating the list is sorted in the "descending" order.

Timestamp ▼

4. To resort the list based on a different column, click a different column header.

5. The arrow ▲ now appears adjacent to the selected column header, indicating the list is sorted in the ascending order based on that column.

Dashboard

The Dashboard page contains two sections.

Number	Section	Information shown
❶	**Alerted Sensors**	▪ When no sensors enter the alarmed state, this section shows the message "No Alerted Sensors." ▪ When any sensor enters the alarmed state, this section lists all of them. See *Dashboard - Alerted Sensors* (on page 95).
❷	**Alarms**	This section can show data only after you have set event rules requiring users to take the acknowledgment action. ▪ When there are no unacknowledged events, this section shows the message "No Alarms." ▪ When there are unacknowledged events, this section lists all of them. See *Dashboard - Alarms* (on page 97).

Dashboard - Alerted Sensors

When any internal sensors or environmental sensor packages connected to the EMX enter an abnormal state, the Alerted Sensors section in the Dashboard show them for alerting users.

To view detailed information or configure each alerted sensor, you can click each sensor's name to go to individual sensor pages. See *Individual Sensor/Actuator Pages* (on page 114).

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

▶ **Summary in the section title:**

Information in parentheses adjacent to the title is the total number of alerted sensors.

For example:

- **1 Critical**: 1 sensor enters the critical or alarmed state.
  - Numeric sensors enter the critical state.

- State sensors enter the alarmed state.

- **1 Warned**: 1 'numeric' sensor enters the warning state.

▶ **List of alerted sensors:**

Two icons are used to indicate various sensor states.

Icons	Sensor states
⚠	For numeric sensors: ▪ above upper warning ▪ below lower warning
🔺	For numeric sensors: ▪ above upper critical ▪ below lower critical
	For state sensors: ▪ alarmed state

For details, see *Sensor/Actuator States* (on page 108).

Dashboard - Alarms

If configuring any event rules which require users to take the acknowledgment action, the Alarms section will list any event which no one acknowledges yet since event occurrence.

Note: For information on event rules, see **Event Rules and Actions** *(on page 204).*

Only users with the Acknowledge Alarms permission can manually acknowledge an alarm.

▶ **To acknowledge an alarm:**

- Click Acknowledge, and that alarm then disappears from the Alarms section.
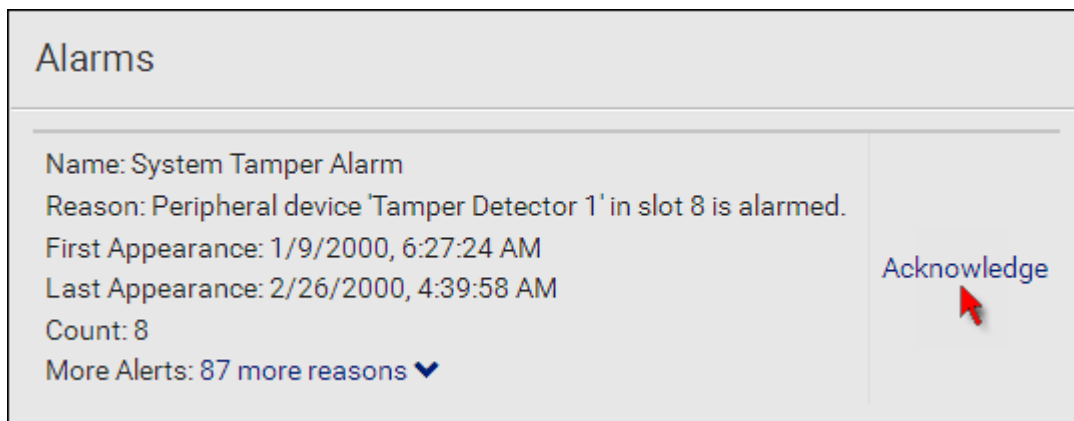
This table explains each column of the alarms list.

Field	Description
Name	The customized name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	The date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	The date and time when the event indicated in the Reason column occurred for the last time.
Count	The number of times the event indicated in the Reason column has occurred.

Field	Description
More Alerts	This field appears only when there are more than one type of events triggering this alert.
	If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events triggering this alert.

EMX

The EMX device's generic information and device-level global settings are available on the EMX page. To open this page, click 'EMX' in the *Menu* (on page 91).

▶ **Device information shown:**
- Firmware version
- MAC address
- *Internal beeper state* (on page 99)

▶ **To configure global settings:**
1. Click Edit Settings.

2. Now you can configure the fields.
   - Click ⬆⬇ to select an option.
   - Select or deselect the checkbox.
   - Adjust the numeric values.

Field	Function	Note
Name	Customizes the device name.	

Field	Function	Note
Peripheral Device Z Coordinate Format	Determines how to describe the vertical locations (Z coordinates) of Raritan environmental sensor packages. ▪ *Options: Rack-Units and Free-Form* See *Z Coordinate Format* (on page 100).	To specify the location of any sensor/actuators in the data center, see *Individual Sensor/Actuator Pages* (on page 114).
Peripheral Device Auto Management	Enables or disables the automatic management feature for Raritan environmental sensor packages. ▪ *The default is to enable it.*	See *How the Automatic Management Function Works* (on page 100).
Altitude	Specifies the EMX device's altitude above sea level when a Raritan's DPX differential air pressure sensor is attached. ▪ *Range: 0 to 3000 meters (0 to 9842 feet)*	▪ The device's altitude is associated with the altitude correction factor. See *Altitude Correction Factors* (on page 532). ▪ The default altitude measurement unit is meter. See *Setting Default Measurement Units* (on page 146). ▪ You can have the measurement unit vary between meter and foot according to user credentials. See *Setting Your Preferred Measurement Units* (on page 146).

3. Click Save.

Internal Beeper State

The EMX page indicates the internal beeper state.

▶ **Available beeper states:**

States	Description
Off	The beeper is turned off.

States	Description
Active	The beeper is turned on.
	"Activation Reason" is displayed, indicating why the beeper sounds an alarm.
	For example, if the beeper is turned on because of a specific event rule "XXX," the activation reason looks like:
	`Event Action triggered by rule: XXX`

See *Event Rules and Actions* (on page 204).

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 and actuators, which are configured on the *Individual Sensor/Actuator Pages* (on page 114).

The Z coordinate format is determined on *EMX* (on page 98). For a Z coordinate example, see *Sensor/Actuator Location Example* (on page 118).

▶ **Available Z coordinate formats:**

* 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 or actuators.
* Free-Form: Any alphanumeric string can be used for specifying the Z coordinate. The value can be 0 to 24 characters long.

How the Automatic Management Function Works

This setting is configured on *EMX* (on page 98).

▶ **After enabling the automatic management function:**

When the total number of managed sensors and actuators has not reached the upper limit yet, the EMX automatically brings newly-connected environmental sensors and actuators under management after detecting them.

  ▪ EMX2-111 can manage up to 32 sensors/actuators per unit.
  ▪ EMX2-888 can manage up to 32 sensors/actuators per sensor port, but the total CANNOT exceed 130 per unit.

▶ **After disabling the automatic management function:**

The EMX no longer automatically manages any newly-added environmental sensors and actuators, and therefore neither ID numbers are assigned nor sensor readings or states are available for newly-added ones.

You must manually manage new sensors/actuators. See *Peripherals* (on page 101).

Peripherals

If there are Raritan environmental sensor packages connected to the EMX, they are listed on the Peripherals page. See *Connecting Environmental Sensor Packages* (on page 39).

An environmental sensor package comprises one or some of the following sensors/actuators:

- Numeric sensors: Detectors that show both readings and states, such as temperature sensors.
- State sensors: Detectors that show states only, such as contact closure sensors.
- Actuators: An actuator controls a system or mechanism so it shows states only.

The EMX communicates with *managed* sensors/actuators only and retrieves their data. It does not communicate with unmanaged ones. See *Managed vs Unmanaged Sensors/Actuators* (on page 107).

When the number of "managed" sensors/actuators has not reached the maximum, the EMX automatically brings newly-detected sensors/actuators under management by default.

- EMX2-111 can manage up to 32 sensors/actuators per unit.
- EMX2-888 can manage up to 32 sensors/actuators per sensor port, but the total CANNOT exceed 130 per unit.

Note: To disable the automatic management function, go to **EMX** *(on page 98). You need to manually manage a sensor/actuator only when it is not under management.*

When any sensor/actuator is no longer needed, you can unmanage/release it.

Open the Peripherals page by clicking Peripherals in the *Menu* (on page 91). Then you can:

- **Perform actions on multiple sensors/actuators by using the control/action icons on the top-right corner.**

- **Go to an individual sensor's or actuator's data/setup page by clicking its name.**

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

▶ **Sensor/actuator overview on this page:**

If any sensor enters the alarmed state, it is highlighted in yellow or red. See *Yellow- or Red-Highlighted Sensors* (on page 106). An actuator is never highlighted.

Column	Description
Name	By default the EMX assigns a name comprising the following two elements to a newly-managed sensor/actuator. ▪ Sensor/actuator type, such as "Temperature" or "Dry Contact." ▪ Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on. You can customize the name. See *Individual Sensor/Actuator Pages* (on page 114).
Reading	Only managed 'numeric' sensors show this data, such as temperature and humidity sensors.
State	The data is available for all sensors and actuators. See *Sensor/Actuator States* (on page 108).
Type	Sensor or actuator type.
Serial Number	This is the serial number printed on the sensor package's label. It helps to identify your Raritan sensors/actuators. See *Finding the Sensor's Serial Number* (on page 110).
Position	The data indicates where this sensor or actuator is located in the sensor chain. See *Identifying the Sensor Position and Channel* (on page 111).
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ✔ is shown.

▶ **To release or manage sensors/actuators:**

When the total of managed sensors/actuators reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace any managed ones. To replace a managed sensor/actuator, see *Managing One Sensor or Actuator* (on page 112). To release any one, follow this procedure.
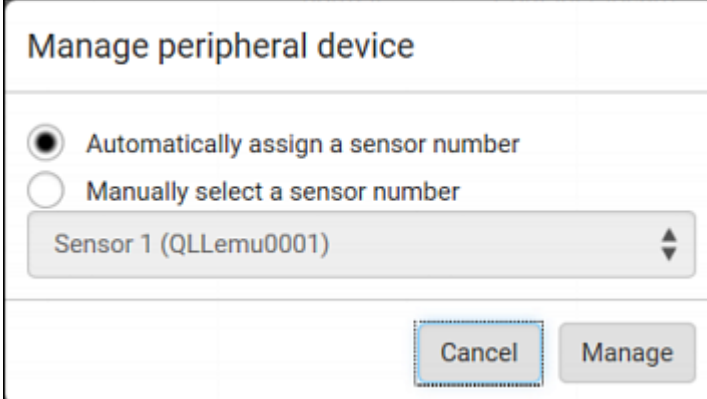
1. Click   to make checkboxes appear in front of sensors/actuators.

   Tip: To perform the desired action on only one sensor/actuator, simply click that sensor/actuator without making the checkboxes appear.

2. Select multiple sensors/actuators.
   - To release sensors/actuators, you must only select "managed" ones. See *Sensor/Actuator States* (on page 108).
   - To manage sensors/actuators, you must only select "unmanaged" ones.
   - To select ALL sensors/actuators, select the topmost checkbox in the header row.

3. To release selected ones, click   > Release.

   To manage them, click   > Manage.
   - The management action triggers a "Manage peripheral device" dialog. Simply click Manage if you are managing *multiple* sensors/actuators.

   - If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number." See *Managing One Sensor or Actuator* (on page 112).
4. Now released sensors/actuators become "unmanaged."

Managed ones show one of the managed states.

▶ **To configure default threshold settings:**

Note that any changes made to default threshold settings not only re-determine the initial threshold values applying to newly-added sensors but also the threshold values of the already-managed sensors where default thresholds are being used. See *Individual Sensor/Actuator Pages* (on page 114).

1. Click ⚙ > Default Threshold Setup.
2. **Click the desired sensor type** (required), and then click Edit Thresholds.

Peripherals Default Thresholds				
				Edit Thresholds
Sensor Type	**Lower Critical**	**Lower Warning**	**Upper Warning**	**Upper Critical**
Absolute Humidity	2 g/m³	4 g/m³	20 g/m³	22 g/m³
Air Flow	0.4 m/s	0.8 m/s	2.6 m/s	3.2 m/s
Air Pressure	---	---	80 Pa	100 Pa
Relative Humidity	10 %	15 %	85 %	90 %
Temperature	10 °C	15 °C	30 °C	35 °C
Vibration	---	---	0.05 g	0.1 g

3. Make changes as needed.
   - To enable any threshold, select the corresponding checkbox.
   - Type a new value in the accompanying text box.

   For concepts of thresholds, deassertion hysteresis and assertion timeout, see *Sensor Threshold Settings* (on page 523).
4. Click Save.

Tip: To customize the threshold settings on a per-sensor basis, go to **Individual Sensor/Actuator Pages** *(on page 114).*

▶ **To turn on or off any actuator(s):**

1. Select one or multiple actuators which are *in the same status* - on or off.
   - To select multiple actuators, click 🗹 to make checkboxes appear and then select desired actuators.
2. Click the desired button.

: Turn ON.
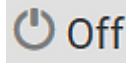
: Turn OFF.

3. Confirm the operation when prompted.

Yellow- or Red-Highlighted Sensors

The EMX highlights those sensors that enter the abnormal state with a yellow or red color. Note that numeric sensors can change colors only after you have enabled their thresholds.

Tip: When an actuator is turned ON, it is also highlighted in red for drawing attention.

For concepts of thresholds, deassertion hysteresis and assertion timeout, see *Sensor Threshold Settings* (on page 523).

# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	25.0 °C	above upper critical	Temperature	AEH2A51454	Port 1	
2	Absolute Humidity 1	10.8 g/m³	normal	Absolute Humidity	AEI1750551	Port 4	
3	Absolute Humidity 2	11.0 g/m³	above upper warning	Absolute Humidity	AEI2850240	Port 4	
4	Temperature 2	25.8 °C	above upper critical	Temperature	AEI2A50775	Port 1	
5	Relative Humidity 1	44 %	normal	Humidity	AEI2A50775	Port 1	

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

Sensor status	Color	States shown in the interface	Description
Unknown		unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed. See *Managed vs Unmanaged Sensors/Actuators* (on page 107).
Normal		normal	▪ Numeric or state sensors are within the normal range. -- OR -- ▪ No thresholds have been enabled for numeric sensors.
Warning		above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold

Sensor status	Color	States shown in the interface	Description
Critical		above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold
Alarmed		alarmed	State sensors enter the abnormal state.

If you have connected a Schroff® LHX/SHX heat exchanger, when any sensor implemented on that device fails, it is also highlighted in red.

Managed vs Unmanaged Sensors/Actuators

To manually manage or unmanage/release a sensor or actuator, see *Peripherals* (on page 101).

▶ **Managed sensors/actuators:**

- The EMX communicates with managed sensors/actuators and retrieves their data.
- Managed sensors/actuators are always listed on the Peripheral Devices page no matter they are physically connected or not.
- They have an ID number as illustrated below.

Peripheral Devices	
# ▲	**Name**
1	On/Off 1
2	On/Off 2
3	Temperature 1
4	Absolute Humidity 1
5	Relative Humidity 1

- They show one of the managed states. See *Sensor/Actuator States* (on page 108).
- For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

▶ **Unmanaged sensors/actuators:**

- The EMX neither communicates with unmanaged sensors/actuators nor retrieves their data.
- Unmanaged sensors/actuators are listed only when they are physically connected to the EMX. They disappear when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

Sensor/Actuator States

An environmental sensor or actuator shows its real-time state after being managed.

Available sensor states depend on the sensor type -- numeric or state sensors. For example, a contact closure sensor is a state sensor so it switches between three states only -- *unavailable*, *alarmed* and *normal*.

Sensors will be highlighted in yellow or red when they enter abnormal states. See *Yellow- or Red-Highlighted Sensors* (on page 106).

An actuator's state is marked in red when it is turned on.

▶ **Managed sensor states:**

In the following table, "R" represents any numeric sensor's reading. The symbol <= means "smaller than" or "equal to."

State	Description
normal	▪ For numeric sensors, it means the readings are within the normal range. ▪ For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"

State	Description
alarmed	The state sensor enters the abnormal state.
unavailable	▪ The communication with the managed sensor is lost. -- OR -- ▪ DPX2, DPX3 or DX sensor packages are upgrading their sensor firmware.

Note that for a contact closure sensor, the normal state depends on the normal setting you have configured. Refer to the Environmental Sensors Guide or Online Help for detailed information, which is available on Raritan's *Support page* (*http://www.raritan.com/support/*).

▶ **Managed actuator states:**

State	Description
on	The actuator is turned on.
off	The actuator is turned off.
unavailable	▪ The communication with the managed actuator is lost. -- OR -- ▪ DX sensor packages are upgrading their sensor firmware.

▶ **Unmanaged sensor/actuator states:**

State	Description
unmanaged	Sensors or actuators are physically connected to the EMX but not managed yet.

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the EMX. To manage a sensor/actuator, go to **Peripherals** *(on page 101).*

Finding the Sensor's Serial Number

A DPX environmental sensor package includes a serial number tag on the sensor cable.

A DPX2, DPX3 or DX sensor package has a serial number tag attached to its rear side.

The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the EMX. Match the serial number from the tag to those listed in the sensor table.

Identifying the Sensor Position and Channel

Raritan has developed four types of environmental sensor packages - DPX, DPX2, DPX3 and DX series. Only DPX2, DPX3 and DX sensor packages can be daisy chained.

The EMX can indicate where each sensor or actuator is connected on the Peripheral Devices page.

- DPX series only shows the sensor port number only.

  For example, *Port 1*.

- DPX2, DPX3 and DX series show both the sensor port number and its position in a sensor chain.

  For example, *Port 1, Chain Position 2*.

- If a Raritan DPX3-ENVHUB4 sensor hub is involved, the hub port information is also indicated for DPX2, DPX3 and DX series, but NOT indicated for DPX series.

  For example, *Hub Port 3*.

- If a sensor/actuator contains channels, such as a contact closure or dry contact sensor, the channel information is included in the position information.

  For example, *Channel 1*.

▶ **Sensor/actuator position examples:**

Example	Physical position
Port 1	Connected to the sensor port #1.
Port 1, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is the 2nd channel of the sensor package.
Port 1, Chain Position 4	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 4th sensor package of the sensor chain.
Port 1, Chain Position 3, Channel 2	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain. ▪ It is the 2nd channel of the sensor package.

Port 1,
 	
Chain Position 1,
 	
Hub Port 2,
 	
Chain Position 3
	▪ Connected to the sensor port #1.
	▪ Connected to the 2nd port of the DPX3-ENVHUB4 sensor hub, which shows the following two pieces of information:
	  ▪ The hub's position in the sensor chain -- "Chain Position 1"
	  ▪ The hub port where this particular sensor package is connected -- "Hub Port 2"
	▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain connected to the hub's port 2.

Managing One Sensor or Actuator

If you are managing only one sensor or actuator, you can assign the desired ID number to it. Note that you cannot assign ID numbers when you are managing multiple sensors/actuators at a time.

Tip: When the total of managed sensors/actuators reaches the maximum (32), you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace any managed ones. To replace a managed one, assign an ID number to it by following this procedure. To release any one, see **Peripherals** *(on page 101).*

▶ **To manage only one sensor/actuator:**

1. From the list of "unmanaged" sensors/actuators, click the one you want to manage.

2. The "Manage peripheral device" dialog appears.

- To let the EMX randomly assign an ID number to it, select "Automatically assign a sensor number."

  This method does not release any managed sensor or actuator.

- To assign the desired ID number to it, select "Manually select a sensor number." Then click [⬆⬇] to select an ID number.

  This method may release a managed sensor/actuator if the number you selected has been assigned to a specific sensor/actuator.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to a sensor or actuator. If it has been assigned to a sensor or actuator, it shows its serial number. Otherwise, it shows the word "unused."

3. Click Manage.

▶ **Special note for a Raritan humidity sensor:**

A Raritan humidity sensor is able to provide two measurements - relative and absolute humidity values.

- A relative humidity value is measured in percentage (%).
- An absolute humidity value is measured in grams per cubic meter (g/m^3).

However, only relative humidity sensors are "automatically" managed if the automatic management function is enabled. You must "manually" manage absolute humidity sensors as needed.

Note that relative and absolute values of the same humidity sensor do NOT share the same ID number though they share the same serial number and position.

Individual Sensor/Actuator Pages

A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page. See *Peripherals* (on page 101).

Note that only a numeric sensor has threshold settings, while a state sensor or actuator has no thresholds.

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. See *Yellow- or Red-Highlighted Sensors* (on page 106). In addition, you can have the EMX automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 204).

▶ **To configure a numeric sensor's threshold settings:**

1. Click Edit Thresholds.

2. Select or deselect Use Default Thresholds according to your needs.

- To have this sensor follow the default threshold settings configured for its sensor type, select the Use Default Thresholds checkbox.

  The default threshold settings are configured on the page of *Peripherals* (on page 101).

- To customize the threshold settings for this particular sensor, deselect the Use Default Thresholds checkbox, and then modify the threshold fields below it.

Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** *(on page 523).*

3. Click Save.

► **To set up a sensor's or actuator's physical location and additional settings:**

1. Click Edit Settings.

2. Make changes to available fields, and then click Save.

Fields	Description
Binary Sensor Subtype	This field is available for a contact closure sensor only.
	Determine the sensor type of your contact closure detector.
	▪ *Contact Closure* detects the door lock or door open/closed status.
	▪ *Smoke Detection* detects the appearance of smoke.
	▪ *Water Detection* detects the appearance of water on the floor.
	▪ *Vibration* detects the vibration of the floor.
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See *Sensor/Actuator Location Example* (on page 118).
	If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. Note that the Z coordinate's format is determined on the page of *EMX* (on page 98).
Alarmed to Normal Delay	This field is available for the DX-PIR presence detector only.
	It determines the wait time before the EMX announces that the presence detector is back to normal after it actually returns to normal.
	Adjust the value in seconds.

▶ **To view a numeric sensor's readings waveform:**

This sensor's data within the past tens of minutes is shown in the waveform diagram. Note that only a numeric sensor has this diagram. State sensors and actuators do not show such data.
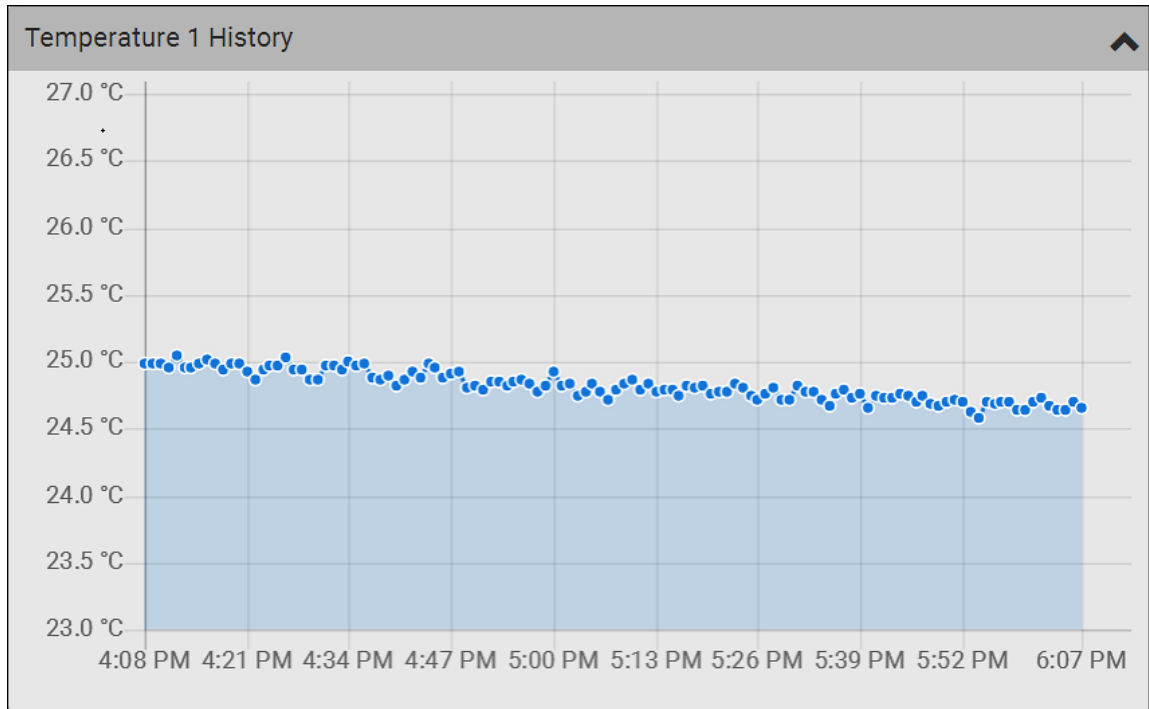
▶ **To turn on or off an actuator:**

1. Click the desired control button.

: Turn ON.

: Turn OFF.

2. Confirm the operation on the confirmation message. An actuator's state is marked in red when it is turned on.

▶ **Other operations:**

You can go to another sensor's or actuators's data/setup page by clicking the selector [⬆⬇] on the top-left corner.

Details	
Peripheral Device ID	1
Position	Port 1
Serial Number	AEH2A51454
Type	Temperature

Sensor/Actuator Location Example

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center. See *Individual Sensor/Actuator Pages* (on page 114).

The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. Therefore, you can use non-measurement values.

▶ **Example:**

X = Brown Cabinet Row

Y = Third Rack

Z = Top of Cabinet

▶ **Values of the X, Y and Z coordinates:**

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.
- Z: When the Z coordinate format is set to *Rack Units*, it can be any number ranging from 0 to 60. When its format is set to *Free-Form*, it can be any alphanumeric value comprising 0 to 24 characters. See *EMX* (on page 98).

Feature Port(s)

One FEATURE port supports connection to the following devices.

Device	Description
Asset Strip	Raritan asset strips
External Beeper	An external beeper with the RJ-45 socket.
LHX 20	Schroff® LHX-20 heat exchanger.
SHX 30	Schroff® SHX-30 heat exchanger.
LHX 40	Schroff® LHX-40 heat exchanger.

Open the Feature Port(s) page by clicking it in the *Menu* (on page 91). From this page, you can enable or disable this port's detection capability, or force it to show a specific device's data/settings even though no device is detected. See *Asset Strip* (on page 121), *External Beeper* (on page 129), and *Schroff LHX/SHX* (on page 130).

Note: You must enable the LHX/SHX support for the EMX to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See **Miscellaneous** *(on page 260).*

▶ **EMX2-111 Feature Port mode configuration:**

When the EMX detects the connection of any listed device, it replaces 'Feature Port' in the menu with that device's name and shows that device's data/settings instead.

When no devices are detected, the EMX displays the name 'Feature Port" and the Feature Port page shows the message "No device is currently connected."

1. Click ⚙ on the top-right corner. The Feature Port Setup dialog appears.

   Feature Port Setup

   Port: 1
   Device Type: Asset Strip
   Detection Mode:

   Auto ⬍

   Cancel   Save

2. Click the Detection Mode field, and select one mode.

3. Mode	Description
Auto	Enable the port to automatically detect the device connection.
Disabled	Disable the port's detection capability.
Asset Strip, Raritan asset strips, LHX 20, SHX 30, LHX 40	Force the EMX to show the selected device's data/setup page regardless of the physical connection status.

Note: 'LHX 20', 'SHX 30', and 'LHX 40' are not available when the support of LHX/SHX heat exchangers is disabled. See **Miscellaneous** *(on page 260).*

▶ **EMX2-888 Feature Port mode configuration:**

1. On the Feature Ports page, click the 'Mode' column of the port that you want to configure.

   Note: To configure a connected device, click that port's 'Device Name' column instead.

Feature Ports

Port ▲	Device Name	Mode	Device Type	Status
1	**Asset Strip (1)**	Auto	Asset Strip	connected
2		Auto		not connected
3		Auto		not connected
4		Auto		not connected
5		Auto		not connected
6	**Asset Strip (6)**	Auto	Asset Strip	connected
7		Auto		not connected
8		Auto		not connected

2. The Feature Port Setup dialog appears. For a list of available modes, see the above table.

Note: The Mode column shows 'Pinned' if you select a specific device in the Detection Mode field.

Asset Strip

After connecting and detecting Raritan asset management strips (asset strips), the EMX shows the name 'Asset Strip.'

- EMX2-888 shows 'Asset Strip' for those ports where asset strips are physically connected on the Feature Ports page.
- EMX2-111 shows 'Asset Strip' in place of 'Feature Port' in the *Menu* (on page 91).
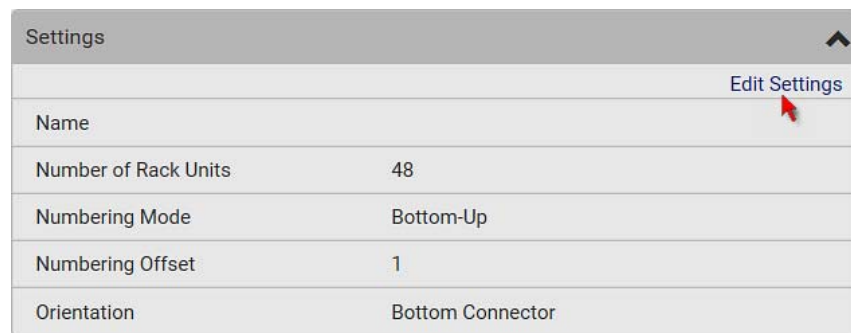
Note: For connection instructions, see **Connecting Asset Management Strips** *(on page 25).*

To open the desired Asset Strip page, click it. On this page, you can configure the rack units of asset strips and asset tags. A rack unit refers to a tag port on the asset strips. The "Change Asset Strip Configuration" permission is required.

For the Feature Port's mode configuration, see *Feature Port(s)* (on page 119).

▶ **To configure asset strip and rack unit settings:**

1. Click Edit Settings.

Settings		⌃
		Edit Settings
Name		
Number of Rack Units	48	
Numbering Mode	Bottom-Up	
Numbering Offset	1	
Orientation	Bottom Connector	

2. Make changes to the settings by directly typing a new value, or clicking that field to select a different option.
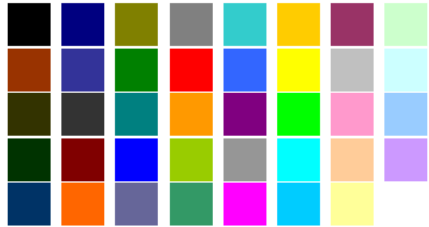
Field	Description
Name	Name for this asset strip assembly.

Field	Description
Number of Rack Units	Total of available tag ports on this asset strip assembly, ranging between 8 and 64. ▪ For the current generation of asset strips, which show the suffix "G3" on its hardware label, the EMX automatically detects the number of its tag ports (rack units), and you *cannot* change this value. ▪ For old "non-G3" asset strips, there is no automatic detection for them so you must manually adjust this value.
Numbering Mode	The rack unit numbering method in a rack/cabinet. ▪ *Top-Down*: The numbering starts from the highest rack unit of a rack/cabinet. ▪ *Bottom-Up*: The numbering starts from the lowest rack unit of a rack/cabinet.
Numbering Offset	The start number in the rack unit numbering. For example, if this value is set to 3, then the first number is 3, the second number is 4, and so on.
Orientation	The asset strip's orientation by indicating the location of its RJ-45 connector. ▪ *Top Connector*: The RJ-45 connector is located on the top. ▪ *Bottom Connector*: The RJ-45 connector is located on the bottom. Asset strips can detect their strip orientation and show it in this field. You need to adjust this value only when your asset strips are the oldest ones without tilt sensors implemented.
Color with connected tag	Click this field to determine the LED color denoting the presence of an asset tag. ▪ Default is green.
Color without connected tag	Click this field to determine the LED color denoting the absence of an asset tag. ▪ Default is red.

For color settings, there are two ways to set the color.

Raritan.

- Click a color in the color palette.
- Type the hexadecimal RGB value of the color, such as #00FF00.

Enter a color
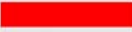
Color code

#00FF00

Cancel   Ok

3. Click Ok. The rack unit numbering and LED color settings are immediately updated on the Rack Units list illustrated below.

- The 'Index' number is the physical tag port number printed on the asset strip, which is not configurable. However, its order will change to reflect the latest rack unit numbering.

Rack Units

Program Asset IDs

Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B914BB	Auto	On	
2	2			000015B9152E	Auto	On	
3	3			000015B9158C	Auto	On	
4	4				Auto	On	
5	5			000015B91600	Auto	On	
6	6			000015B91546	Auto	On	

- A blade extension strip and a *programmable* tag are marked with the word 'programmable' in the Asset/ID column. You can customize their Asset IDs. For instructions, refer to this section's last procedure below.
- If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

> ▶ **To customize a single rack unit's settings:**

You can make a specific rack unit's LED behave differently from the others on the asset strip, including the LED light and color.

1. Click the desired rack unit on the Rack Units list. The setup dialog for the selected one appears.

Setup of Rack Unit 3

Name

Operation Mode

Auto (based on Tag)   ▲▼

LED Mode

On   ▲▼

LED Color

Cancel   Save

2. Make changes to the information by typing a new value or clicking that field to select a different option.

Field	Description
Name	Name for this rack unit. For example, you can name it based on the associated IT device.
Operation Mode	Determine whether this rack unit's LED behavior automatically changes according to the presence and absence of the asset tag. ▪ *Auto*: The LED behavior varies, based on the asset tag's presence. ▪ *Manual Override*: This option differentiates this rack unit's LED behavior.

Raritan.
A brand of Legrand

Field	Description
LED Mode	This field is configurable only after the Operation Mode is set to Manual Override. Determine how the LED light behaves for this particular rack unit. ▪ *On*: The LED stays lit. ▪ *Off*: The LED stays off. ▪ *Slow blinking*: The LED blinks slowly. ▪ *Fast blinking*: The LED blinks quickly.
LED Color	This field is configurable only after the Operation Mode is set to Manual Override. Determine what LED color is shown for this rack unit if the LED is lit.

▶ **To expand a blade extension strip:**

A blade extension strip, like an asset strip, has multiple tag ports. An extension strip is marked with a grayer color on the Asset Strip page, and its tag ports list is collapsed by default.
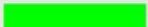
Note: If you need to temporarily disconnect the blade extension strip from the asset strip, wait at least 1 second before re-connecting it back, or the EMX device may not detect it.

1. Locate the rack unit (tag port) where the blade extension strip is connected. Click its slot number, whose format is similar to **1-N ∧**, where N is the total number of its tag ports.

2. All tag ports of the blade extension strip are listed below it. Their port numbers are displayed in the Slot column.

Rack Units							
							Program Asset IDs
Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B914BB	Auto	On	
2	2	1-16 ⌄		0000ABC12345 (programmable)	Auto	On	
	Extension	1		000015B9160A			
	Extension	2		000015B91610			
	Extension	3		000015B91622			
	Extension	4		000015B9158C			
	Extension	5		000015B91600			
	Extension	6		000015B91546			
	Extension	7					
	Extension	8					
	Extension	9					
	Extension	10					
	Extension	11					
	Extension	12					
	Extension	13					
	Extension	14					
	Extension	15					
	Extension	16					
3	3			000015B9152E	Auto	On	
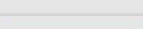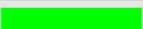
▪ To hide the blade extension slots list, click 1-N ⌄.

▶ **To customize asset IDs on programmable asset tags:**

You can customize asset IDs only when the asset tags are "programmable" ones. Non-programmable tags do not support this feature. In addition, you can also customize the ID of a blade extension strip.

If a barcode reader is intended, connect it to the computer you use to access the EMX.

1. Click Program Asset IDs.

Rack Units							
							Program Asset IDs
Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	16				Auto	On	
2	15				Auto	On	
3	14				Auto	On	
4	13				Auto	On	
5	12				Auto	On	
6	11				Auto	On	
7	10			(programmable)	Auto	On	
8	9			(programmable)	Auto	On	
9	8			(programmable)	Auto	On	
10	7			00001492BD47	Auto	On	
11	6			00001492CB50	Auto	On	

2. In the Asset/ID column, enter the customized asset IDs by typing values or scanning the barcode.
   - When using a barcode reader, first click the desired rack unit, and then scan the asset tag. Repeat this step for all desired rack units.

▪ An asset ID contains up to 12 characters that comprise only numbers and/or UPPER CASE alphabets. Lower case alphabets are NOT accepted.

Rack Units				
				Rack Units
Rack unit ▲	**Index**	**Slot**	**Name**	**Asset / ID**
1	16			Tag ID
2	15			Tag ID
3	14			Tag ID
4	13			Tag ID
5	12			Tag ID
6	11			Tag ID
7	10			WINDOWS
8	9			LINUX
9	8			ROUTER ✕
10	7			00001492BD47

3. Verify the correctness of customized asset IDs and modify as needed.

4. Click Apply at the bottom of the page or Rack Units (see below) to save changes.

Rack Units				
				Rack Units
Rack unit ▲	**Index**	**Slot**	**Name**	**Asset / ID**
1	16			Tag ID
2	15			Tag ID

Raritan.
A brand of Legrand

Asset Strip Automatic Firmware Upgrade

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

During the firmware upgrade, the following events take place:

- The asset strip is completely lit up, with the blinking LEDs cycling through diverse colors.
- A firmware upgrade process is indicated in the EMX web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

External Beeper

After connecting and detecting a supported external beeper, the EMX shows the name 'External Beeper.'

- EMX2-888 shows 'External Beeper' for those ports where external beepers are physically connected on the Feature Ports page.
- EMX2-111 shows 'External Beeper' in place of 'Feature Port' in the *Menu* (on page 91).

Note: For connection instructions, see **Connecting an External Beeper** *(on page 61).*

To open the desired External Beeper page, click it. This page shows an external beeper's status, including:

- Number of the FEATURE port where this external beeper is connected
- Its device type
- Its connection status
- The beeper's state - off or active

For the Feature Port's mode configuration, see *Feature Port(s)* (on page 119).

Schroff LHX/SHX

You must enable the LHX/SHX support for the EMX to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See *Miscellaneous* (on page 260).

After enabling the LHX/SHX support and connecting the supported Schroff® LHX/SHX heat exchanger, the EMX shows the LHX or SHX name -- LHX 20, LHX 40 or SHX 30.

- EMX2-888 shows the LHX or SHX name for those ports where LHX/SHX heat exchangers are physically connected on the Feature Ports page.
- EMX2-111 shows the LHX or SHX name in place of 'Feature Port' in the *Menu* (on page 91).

Note: For connection instructions, see **Connecting a Schroff LHX/SHX Heat Exchanger** *(on page 61).*

To open the LHX/SHX page, click its name. Then you can monitor and administer the connected LHX/SHX device with the following.

- Name the heat exchanger
- Monitor LHX/SHX built-in sensors and device states
- Configure the air outlet temperature setpoint
- Configure the default fan speed
- Configure the air temperature/fan speed thresholds (for alert generation)
- Request maximum cooling using the fan speed and opening the cold water valve
- Acknowledge alerts or errors remotely, such as failed LHX/SHX sensors or emergency cooling activation
- Accumulative operating hours
- Indicate the number of power supplies present and whether a condenser pump is present

Available information/operation is model dependent. For example, only LHX devices can show sensor alerts. See your LHX/SHX user documentation for details.

Important: The LHX/SHX settings are stored on the port where the LHX/SHX device is connected, and are lost if that device is re-connected to a different EMX port.

For the Feature Port's mode configuration, see *Feature Port(s)* (on page 119).

▶ **To view the LHX/SHX device state:**

The Operation State field indicates whether the device is operating fine, and the Switch State field indicates its power status.

If the device does not operate properly, such as some sensor failure, it shows "critical" and the symbol ⚠.

▶ **To turn on or off the LHX/SHX device:**

1. Click the desired power-control button on the top-right corner.

⏻ On : Power ON.
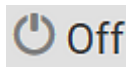
⏻ Off : Power OFF.

2. Confirm the operation on the confirmation message.

▶ **To configure LHX/SHX settings:**

1. Click Edit Settings.
2. Configure the settings as needed.
   - Provide a customized name.
   - Specify the desired air outlet setpoint temperature.
   - Specify the default fan speed.
3. Click Save.

▶ **To view all sensor data and configure thresholds:**

1. Locate the Sensors section, which lists all air outlet/inlet temperatures and fan speeds, and indicates the door closed/open status of the LHX/SHX device.
2. To set the thresholds for any temperature or fan speed sensor implemented on the LHX/SHX device:
   a. Click the desired sensor.
   b. Click Edit Thresholds.
   c. Enable and set the desired thresholds and deassertion hysteresis.

   Note that assertion timeout is NOT available on LHX/SHX.
   d. Click Save.
3. After thresholds are enabled, sensors may be highlighted in yellow or red if they enter the warning or critical range. See *Yellow- or Red-Highlighted Sensors* (on page 106).

Tip: You can also create event rules to notify you of the warning or critical levels. See **Event Rules and Actions** *(on page 204).*

▶ **To view sensor alerts and LHX event log:**

Remote alert acknowledgment is supported by the LHX-20 and LHX-40. The SHX-30 does not support this feature.

1. Locate the Alert States section.
2. If any LHX sensors fail, they are indicated. Click Acknowledge to acknowledge the sensor failure.
3. To view the history of LHX events, click Show Event Log to go to the Event Log page.

▶ **Operation time statistics:**

This section indicates the accumulative operation hours of the LHX/SHX device and its fans since the device is connected to the EMX and turned on.

Available time units in the statistics --

- h: hour(s)
- d: day(s)

▶ **Request maximum cooling:**

Only SHX 30 supports this feature. See *SHX Request Maximum Cooling* (on page 132).

SHX Request Maximum Cooling

The EMX allows you to remotely activate the Schroff SHX 30's maximum cooling feature. Both LHX 20 and LHX 40 do not support remote activation of maximum cooling.

The Request Maximum Cooling feature is available only after the EMX detects SHX 30. For additional information on the SHX 30 maximum cooling feature, see the SHX 30 documentation.

▶ **To perform maximum cooling:**

- Go to the SHX page, and click Request Maximum Cooling.

  Then the SHX 30 enters into emergency cooling mode and runs at its maximum cooling level of 100% in order to cool the device.

  When maximum cooling is requested for an SHX 30, the message "Maximum cooling requested" is displayed.

▶ **To stop maximum cooling:**

- Click Cancel Maximum Cooling.

Auxiliary Port(s)

One Auxiliary port supports connection to the following devices.

Device	Description
LHX 20	Schroff® LHX-20 heat exchanger.
SHX 30	Schroff® SHX-30 heat exchanger.
LHX 40	Schroff® LHX-40 heat exchanger.
PowerLogic PM710	Schneider Electric PowerLogic PM710.

Open the Auxiliary Port(s) page by clicking it in the *Menu* (on page 91). From this page, you can enable or disable this port's detection capability, or force it to show a specific device's data/settings even though no device is detected. See *Schroff LHX/SHX* (on page 130) and *Schneider Electric PowerLogic PM710* (on page 135).

Note: You must enable the LHX/SHX support for the EMX to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See **Miscellaneous** *(on page 260).*

▶ **EMX2-111 Auxiliary Port mode configuration:**

When EMX2-111 detects the connection of any listed device, it replaces 'Auxiliary Port' in the menu with that device's name and shows that device's data/settings instead.

When no devices are detected, EMX2-111 displays the name 'Auxiliary Port" and the Auxiliary Port page shows the message "No device is currently connected."

1. Click ⚙ on the top-right corner. The Auxiliary Port Setup dialog appears.

Auxiliary Port Setup

Port: 1
Device Type: None
Detection Mode:

Auto ⬍

Cancel   Save

2. Click the Detection Mode field, and select one mode.

Mode	Description
Auto	Enable the port to automatically detect the device connection.
Disabled	Disable the port's detection capability.
LHX 20, SHX 30, LHX 40, PowerLogic PM710	Force the EMX to show the selected device's data/setup page regardless of the physical connection status.

*Note: 'LHX 20', 'SHX 30', and 'LHX 40' are not available when the support of LHX/SHX heat exchangers is disabled. See **Miscellaneous** (on page 260).*

▶ **EMX2-888 Auxiliary Port mode configuration:**

1. On the Auxiliary Ports page, click the 'Mode' column of the port that you want to configure.

   Note: To configure a connected device, click that port's 'Device Name' column instead.

Auxiliary Ports

Port ▲	Device Name	Mode	Device Type	Status
1		Auto		not connected
2		Auto		not connected
3		Auto		not connected
4		Auto		not connected
5		Auto		not connected
6		Auto		not connected
7		Auto		not connected
8		Auto		not connected

2. The Auxiliary Port Setup dialog appears.
3. Click the Detection Mode field, and select one mode. For a list of available modes, see the above table.

Note: The Mode column shows 'Pinned' if you select a specific device in the Detection Mode field.

Schneider Electric PowerLogic PM710

All settings are configured on a per port basis. If you disconnect a PM710 from one EMX port and connect it to another EMX port, you must reconfigure the settings. However, if you disconnect a PM710 from an EMX port and then plug it back into the same port, the already-configured settings still apply.

The PM710 saves readings when they reach their highest and lowest value. The highest value and lowest value are the minimum and maximum values, which can be reset as needed. Besides, it also saves energy accumulator values, which can be also reset. Refer to your PM710 documentation for additional information.

▶ **PM710 information shown:**

The following PM710-related information is shown on this page.

- PM710-related device data, including device type and operational state.
- All sensor readings and power quality values gathered by PM710.

  For some readings followed by the symbol "^", such as

  RMS Current Average ⌃ , you need to click it to view its details.

▶ **To configure the PM710:**

1. On the PowerLogic PM710 page, click Edit Settings.

Settings	⌃
	Edit Settings
Device Name	
Address	1
Line Speed	19200
Parity	Even

2. Enter a name for the sensor.
3. Leave the device address, line speed and parity as is so it matches the PM710 settings.
4. Click Save.

▶ **To configure threshold settings for PM710:**

1. Click the Thresholds title bar at the bottom of the page to display a list of sensor thresholds.

Thresholds	⌄

2. **Click the desired sensor** (required), and then click Edit Thresholds.

Thresholds				⌃
				Edit Thresholds
Sensor ▲	**Lower Critical**	**Lower Warning**	**Upper Warning**	**Upper Critical**
Active Energy	---	---	---	---
Active Power L1	---	---	---	---
Active Power L2	---	---	---	---
Active Power L3	---	---	---	---
Active Power Total	---	---	---	---
Apparent Energy	---	---	---	---
Apparent Power L1	---	---	---	---
Apparent Power L2	---	---	---	---
Apparent Power L3	---	---	---	---

3. Make changes as needed.

 ▪ To enable any threshold, select the corresponding checkbox.

▪ Type a new value in the accompanying text box.

For concepts of thresholds, deassertion hysteresis and assertion timeout, see *Sensor Threshold Settings* (on page 523).

4. Click Save.

▶ **To reset the PM710 minimum and maximum values:**

1. At the bottom of the Sensors section, click

.

2. Confirm it on the confirmation message. All values are reset.

▶ **To clear the PM710 energy accumulator values:**

1. At the bottom of the Sensors section, click

.

2. Confirm it on the confirmation message. All values are clear.

User Management

User Management menu deals with user accounts, permissions, and preferred measurement units on a per-user basis.

The EMX is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administrator. You can neither delete 'admin' nor change its permissions.

A "role" determines the tasks/actions a user is permitted to perform on the EMX so you must assign one or multiple roles to each user.

Click 'User Management' in the *Menu* (on page 91), and the following submenu displays.

Submenu command	Refer to...
Users	*Creating Users* (on page 138)
Roles	*Creating Roles* (on page 143)
Change Password	*Changing Your Password* (on page 88)
Preferences	*Setting Your Preferred Measurement Units* (on page 146)
Default Preferences	*Setting Default Measurement Units* (on page 146)

Creating Users

All users must have a user account, containing the login name and password. Multiple users can log in simultaneously using the same login name.

To add users, choose User Management > Users > .

Note that you must enter information in the fields showing the message 'required.'

▶ **User information:**

Field/setting	Description
User Name	The name the user enters to log in to the EMX. ▪ 4 to 32 characters ▪ Case sensitive ▪ Spaces are NOT permitted.
Full Name	The user's first and last names.
Password, Confirm Password	▪ 4 to 64 characters ▪ Case sensitive ▪ Spaces are permitted.
Telephone Number	The user's telephone number
eMail Address	The user's email address ▪ Up to 64 characters ▪ Case sensitive
Enable	When selected, the user can log in to the EMX.
Force password change on next login	When selected, a password change request automatically appears when next time the user logs in. For details, see *Changing Your Password* (on page 88).

▶ **SSH:**

You need to enter the SSH public key only if the public key authentication for SSH is enabled. See *Changing SSH Settings* (on page 175).

1. Open the SSH public key with a text editor.
2. Copy and paste all content in the text editor into the SSH Public Key field.

▶ **SNMPv3:**

The SNMPv3 access permission is disabled by default.

Field/setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user. *Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See* **Configuring SNMP Settings**

Field/setting	Description
	(on page 172).
Security Level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

- **Authentication Password**: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Same as User Password	Select this checkbox if the authentication password is identical to the user's password. To specify a different authentication password, disable the checkbox.
Password, Confirm Password	Type the authentication password if the 'Same as User Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- **Privacy Password**: This section is configurable only when 'Authentication & Privacy' is selected.

Field/setting	Description
Same as Authentication Password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.
Password, Confirm Password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

- **Protocol**: This section is configurable only when 'Authentication' or 'Authentication & Privacy' is selected.

Field/setting	Description
Authentication	Click this field to select the desired authentication protocol. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)
Privacy	Click this field to select the desired privacy protocol. Two protocols are available: ▪ DES (default) ▪ AES-128

▶ **Preferences:**

This section determines the measurement units displayed in the web interface and command line interface for this user.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

Note: Users can change the measurement units at any time by setting their own preferences. See **Setting Your Preferred Measurement Units** *(on page 146).*

▶ **Roles:**

Select one or multiple roles to determine the user's permissions. To select all roles, select the top-most checkbox in the header row.

If the built-in roles do not satisfy your needs, add new roles by clicking

New Role . See *Creating Roles* (on page 143).

The Operator role is assigned to a newly-created user account by default.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change EMD Configuration • View Event Settings • View Local Event Log

Note: With multiple roles selected, a user has the union of all roles' permissions.

Editing or Deleting Users

To edit or delete users, choose User Management > Users to open the Users page, which lists all users.

In the Enabled column:

- ✔ : The user is enabled.
- ✖ : The user is disabled.

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

▶ **To edit or delete a user account:**

1. On the Users page, click the desired user. The Edit User page for that user opens.

2. Make changes as needed.

   ▪ For information on each field, see *Creating Users* (on page 138).

- ▪ To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.

- ▪ To delete this user, click ![trash icon], and confirm the operation.

3. Click Save.

► **To delete multiple user accounts:**

1. On the Users page, click ![checkbox icon] to make checkboxes appear in front of user names.

   Tip: To delete only one user, you can simply click that user without making the checkboxes appear. See the above procedure.

2. Select one or multiple users.

   - ▪ To select all roles, except for the admin role, select the top-most checkbox in the header row.

3. Click ![trash icon].

4. Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.

The EMX provides two built-in roles. The Operator role is assigned to a newly-created user account per default. See *Creating Users* (on page 138).

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change EMD Configuration • View Event Settings • View Local Event Log

If the two do not satisfy your needs, add new roles.

▶ **To create a role:**

1. Choose User Management > Roles > ![icon].

2. Assign a role name.
   - 1 to 32 characters long
   - Case sensitive
   - Spaces are permitted as of release 3.3.0

3. Type a description for the role in the Description field.

4. Select the desired privilege(s).
   - The 'Administrator Privileges' includes all privileges.
   - The 'Unrestricted View Privileges' includes all 'View' privileges.

5. To select any privilege requiring the argument setting, click ![icon] to select the desired arguments.
   - For example, you can specify the actuators that are allowed to be switched on/off for the 'Switch Actuator' privilege as shown below.

6. Click Save.

Now you can assign the role to any user. See *Creating Users* (on page 138) or *Editing or Deleting Users* (on page 142).

Editing or Deleting Roles

Choose User Management > Roles to open the Roles page, which lists all roles.

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

The Admin role is not user-configurable so the lock icon ![lock] displays, indicating that you are not allowed to configure it.

▶ **To edit a role:**

1. On the Roles page, click the desired role. The Edit Role page opens.
2. Make changes as needed.
    -   The role name cannot be changed.
    -   To delete this role, click ![trash], and confirm the operation.
3. Click Save.

▶ **To delete any roles:**

1. On the Roles page, click ![checkbox] to make checkboxes appear in front of roles.

    Tip: To delete only one role, you can simply click that user without making the checkboxes appear. See the above procedure.

2. Select one or multiple roles.
    -   To select all roles, except for the Admin role, select the top-most checkbox in the header row.
3. Click ![trash] on the top-right corner.
4. Click Delete on the confirmation message.

Setting Your Preferred Measurement Units

You can change the measurement units shown in the EMX user interface according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users on the Edit User page. See **Editing or Deleting Users** *(on page 142).*

Measurement unit changes only apply to the web interface and command line interface.

Setting your own preferences does not change the default measurement units. See *Setting Default Measurement Units* (on page 146).

▶ **To select the measurement units you prefer:**

1. Choose User Management > Preferences.
2. Make changes as needed.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

3. Click Save.

Setting Default Measurement Units

Default measurement units are applied to all EMX user interfaces across all users, including users accessing the EMX via external authentication servers. For a list of affected user interfaces, see *User Interfaces Showing Default Units* (on page 147).

Note: The preferred measurement units set by any individual user or by the administrator on a per-user basis will override the default units in the web interface and command line interface. See **Setting Your Preferred Measurement Units** *(on page 146) or* **Creating Users** *(on page 138).*

▶ **To set up default user preferences:**

1. Click User Management > Default Preferences.

2. Make changes as needed.

Field	Description
Temperature Unit	Preferred units for temperatures -- °C (Celsius) or °F (Fahrenheit).
Length Unit	Preferred units for length or height -- Meter or Feet.
Pressure Unit	Preferred units for pressure -- Pascal or Psi. ▪ Pascal = one newton per square meter ▪ Psi = pounds per square inch

3. Click Save.

User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or information:

- Web interface for "newly-created" local users when they have not configured their own preferred measurement units. See *Creating Users* (on page 138).
- Web interface for users who are authenticated via LDAP/Radius servers.
- The sensor report sent because of the "Send Sensor Report" action. See *Send Sensor Report* (on page 227).
- Front panel LCD display.

Device Settings

Click 'Device Settings' in the *Menu* (on page 91), and the following submenu displays.

Menu command	Submenu command	Refer to...
Network		*Configuring Network Settings* (on page 149)
Network Services	HTTP	*Changing HTTP(S) Settings* (on page 171)
	SNMP	*Configuring SNMP Settings* (on page 172)
	SMTP Server	*Configuring SMTP Settings* (on page 173)
	SSH	*Changing SSH Settings* (on page 175)
	Telnet	*Changing Telnet Settings* (on page 175)
	Modbus	*Changing Modbus Settings* (on page 176)
	Server Advertising	*Enabling Service Advertising* (on page 178)
Security	IP Access Control	*Creating IP Access Control Rules* (on page 179)
	Role Access Control	*Creating Role Access Control Rules* (on page 182)
	SSL Certificate	*Setting Up an SSL/TLS Certificate* (on page 184)
	Authentication	*Setting Up External Authentication* (on page 189)
	Login Settings	*Configuring Login Settings* (on page 198)
	Password Policy	*Configuring Password Policy* (on page 200)
	Service Agreement	*Enabling the Restricted Service Agreement* (on page 201)
Date/Time		*Setting the Date and Time* (on page 201)
Event Rules		*Event Rules and Actions* (on page 204)
Data Logging		*Setting Data Logging* (on page 245)
Data Push		*Configuring Data Push Settings* (on page 247)
Server Reachability		*Monitoring Server Accessibility* (on page 249)
Serial Port		*Configuring the Serial Port* (on page 253)
Lua Scripts		*Lua Scripts* (on page 255)
Miscellaneous		*Miscellaneous* (on page 260)

Configuring Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after *connecting the EMX to your network* (on page 10).

You can enable both the wired and wireless networking on the EMX so that it has multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface. This also applies when the EMX enters the port forwarding mode so that the EMX has more than one IPv4 or IPv6 address in the port forwarding mode.

However, the EMX in the BRIDGING mode obtains "only one" IP address for wired networking. Wireless networking is NOT supported in this mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

▶ **To set up the network settings:**

1. Choose Device Settings > Network.

2. To use DHCP-assigned DNS servers and gateway instead of static ones, go to step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section. See *Common Network Settings* (on page 151).

   ▪ Static routes and cascading mode are in this section. You need to configure them only when there are such local requirements. See *Setting the Cascading Mode* (on page 162) and *Static Route Examples* (on page 158).

3. To configure IPv4/IPv6 settings for a *wired* network, click the ETHERNET or BRIDGE section. See *Wired Network Settings* (on page 150).

   ▪ If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings.

4. To configure IPv4/IPv6 settings for a *wireless* network, click the WIRELESS section. See *Wireless Network Settings* (on page 153).

   ▪ You must connect a USB wireless LAN adapter to the EMX for wireless networking.

   Note: If the device's cascading mode is set to 'Bridging' or its role is set to 'Slave' in the port forwarding mode, the wireless settings will be disabled.

5. To configure the ETHERNET interface settings, see *Ethernet Interface Settings* (on page 152).

6. Click Save.

▶ **After enabling either or both Internet protocols:**

After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

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

Note: The EMX supports TLS 1.0, 1.1 and 1.2.

Wired Network Settings

On the Network page, click the ETHERNET section to configure IPv4/IPv6 settings.

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings. See *Setting the Cascading Mode* (on page 162).

▶ **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETHERNET section, but not available in the BRIDGE section.

| Enable Interface | ✔ |

▶ **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP Auto Configuration	Select the method to configure IPv4 settings. ▪ DHCP: Auto-configure IPv4 settings via DHCP servers.

Field/setting	Description
	▪ Static: Manually configure the IPv4 settings.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - ▪ 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
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
  Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. ▪ Automatic: Auto-configure IPv6 settings via DHCPv6. ▪ Static: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".
  Example: *fd07:2fa:6cff:1111::0/128*

Common Network Settings

Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

Field	Description
Cascading Mode	Leave it to the default "None" unless you are establishing a cascading chain. For more information, refer to: ▪ *Cascading Multiple EMX Devices for Sharing Ethernet Connectivity* (on page 21) ▪ *Setting the Cascading Mode* (on page 162)

Field	Description
DNS Resolver Reference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 Address: Use the IPv4 addresses. ▪ IPv6 Address: Use the IPv6 addresses.
DNS Suffixes (optional)	Specify a DNS suffix name if needed.
First/Second/Third DNS Server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the EMX will use DHCP-assigned DNS servers.
IPv4/IPv6 Routes	You need to configure these settings only when your local network contains two subnets, and you want EMX to communicate with the other subnet. If so, make sure IP forwarding has been enabled in your network, and then you can click 'Add Route' to add static routes. See *Static Route Examples* (on page 158).

Ethernet Interface Settings

By default the Ethernet interface is enabled.

▶ **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETHERNET section, but not available in the BRIDGE section.

▶ **Other Ethernet settings:**

Field	Description
Speed	Select a LAN speed.

Field	Description
	• Auto: System determines the optimum LAN speed through auto-negotiation. • 10 MBit/s: Speed is always 10 Mbps. • 100 MBit/s: Speed is always 100 Mbps.
Duplex	Select a duplex mode. • 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.
Current State	Show the LAN's current status, including the current speed and duplex mode.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the EMX to NON-Auto values, which may result in a duplex mismatch.

Wireless Network Settings

If the device's cascading mode is set to 'Bridging' or its role is set to 'Slave' in the port forwarding mode, the wireless settings will be disabled. See *Setting the Cascading Mode* (on page 162).

By default the wireless interface is disabled. You should enable it if wireless networking is wanted.

▶ **Interface Settings:**

Field/setting	Description
Enable Interface	Enable or disable the wireless interface. When disabled, the wireless networking fails.
Hardware State	Check this 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.
SSID	Type the name of the wireless access point (AP)
Force AP BSSID	If the BSSID is available, select this checkbox

Field/setting	Description
BSSID	Type the MAC address of an access point
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. ▪ No Authentication: No authentication data is required. ▪ PSK: A Pre-Shared Key is required. ▪ EAP - PEAP: Use Protected Extensible Authentication Protocol. Only MSCHAPv2 is supported. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string
Identity	This field appears only when 'EAP - PEAP' is selected. Type your user name.
Password	This field appears only when 'EAP - PEAP' is selected. Type your password.
CA Certificate	This field appears only when 'EAP - PEAP' is selected. A third-party CA certificate may or may not be needed. If needed, follow the steps below.

- **Available settings for the CA Certificate:**

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the EMX to verify the validity of the TLS certificate that will be installed. ▪ For example, the EMX will check the certificate's validity period against the system time.

Raritan.
A brand of Legrand

25

Field/setting	Description
Browse…	Click this button to install a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow wireless connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the EMX system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the EMX has once been powered off for a long time.

▶ **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP Auto Configuration	Select the method to configure IPv4 settings. ▪ DHCP: Auto-configure IPv4 settings via DHCP servers. ▪ Static: Manually configure the IPv4 settings.

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - 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

- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".

  Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP Auto Configuration	Select the method to configure IPv6 settings. ▪ Automatic: Auto-configure IPv6 settings via DHCPv6. ▪ Static: Manually configure the IPv6 settings.

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

  Example: *fd07:2fa:6cff:1111::0/128*

▶ **(Optional) To view the wireless LAN diagnostic log:**

- Click Show WLAN Diagnostic Log. See *Wireless LAN Diagnostic Log* (on page 156).

Wireless LAN Diagnostic Log

The EMX provides a diagnostic log for inspecting connection errors that occurred over the wireless network interface. The information is useful for technical support.

Note that the WLAN Diagnostic Log shows data only after the Network Interface is set to Wireless.

Each entry in the log consists of:

- ID number
- Date and time
- Description

▶ **To view the log:**

1. Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log. See *Configuring Network Settings* (on page 149).
2. To go to other pages of the log, click the pagination bar at the bottom of the page.

▪ If there are more than 5 pages and the page numbers displayed

in the bar does not show the desired one, click [...] to have it
show the next or previous five page numbers, if available.

First	Previous	1	2	3	4	5	...	Next	Last

3. To refresh the diagnostic, click ↻ **Refresh** on the top-right
corner.

4. If wanted, you can resort the list by clicking the desired column
header. See *Sorting a List* (on page 94).

▶ **To clear the diagnostic log:**

1. On the top-right corner of the log, click ⋮ > 🗑 Clear Log.

2. Click Clear Log on the confirmation message.

Static Route Examples

This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and EMX devices in the examples use static IP addresses.

Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

Note: If Interface is selected, you should select an interface name instead of entering an IP address. See **Interface Names** *(on page 161).*

▶ **IPv4 example:**
- Your EMX: *192.168.100.64*
- Two NICs: *192.168.200.75* and *192.168.100.88*
- Two networks: *192.168.200.0* and *192.168.100.0*
- Subnet mask: *24*
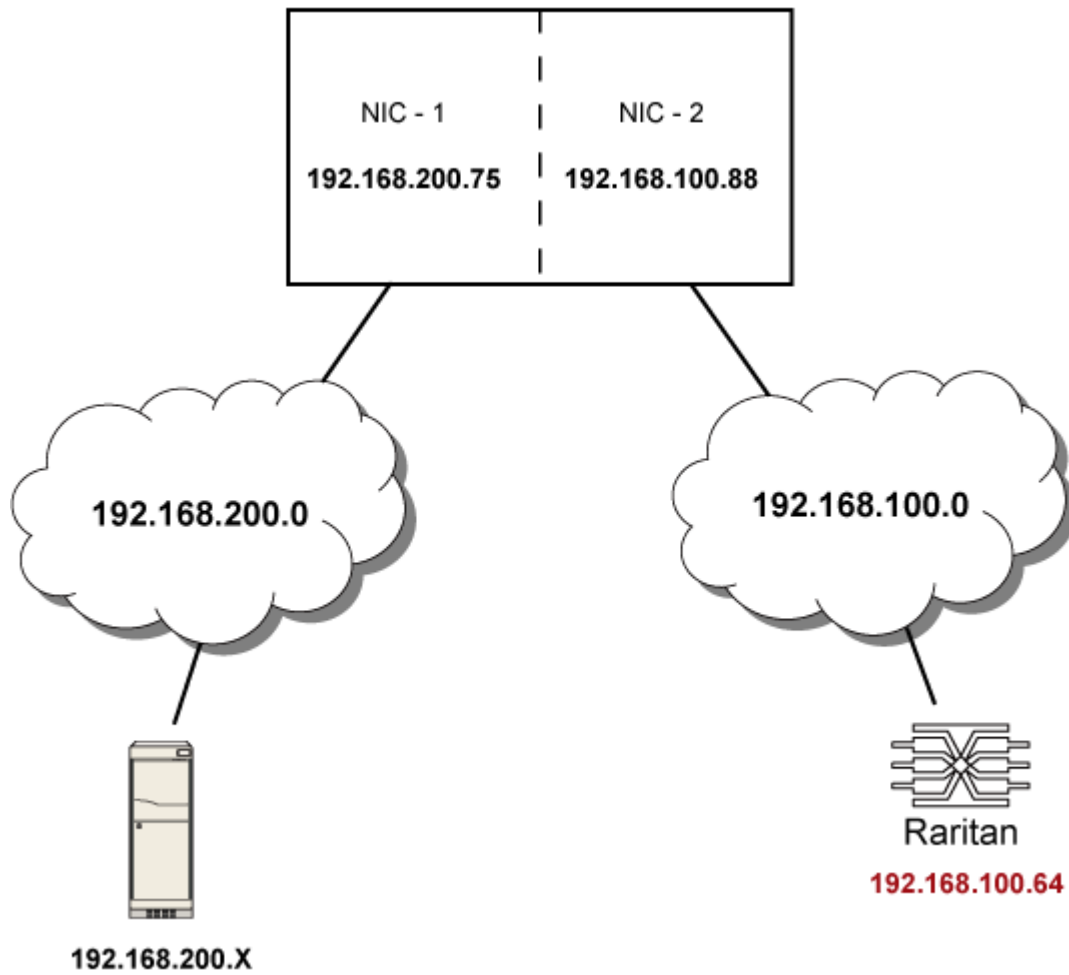
In this example, NIC-2 (192.168.100.88) is the next hop router for your EMX to communicate with any device in the other subnet 192.168.200.0. In the IPv4 "Static Routes" section, you should specify:

1	192.168.200.0/24	Gateway	192.168.100.88	↑ ↓ 🗑

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use [↑] or [↓] to re-sort the priority, or click [🗑] to delete it.

▶ **IPv6 example:**
- Your EMX: *fd07:2fa:6cff:2405::30*
- Two NICs: *fd07:2fa:6cff:1111::50* and *fd07:2fa:6cff:2405::80*
- Two networks: *fd07:2fa:6cff:1111::0* and *fd07:2fa:6cff:2405::0*
- Prefix length: *64*

Raritan.
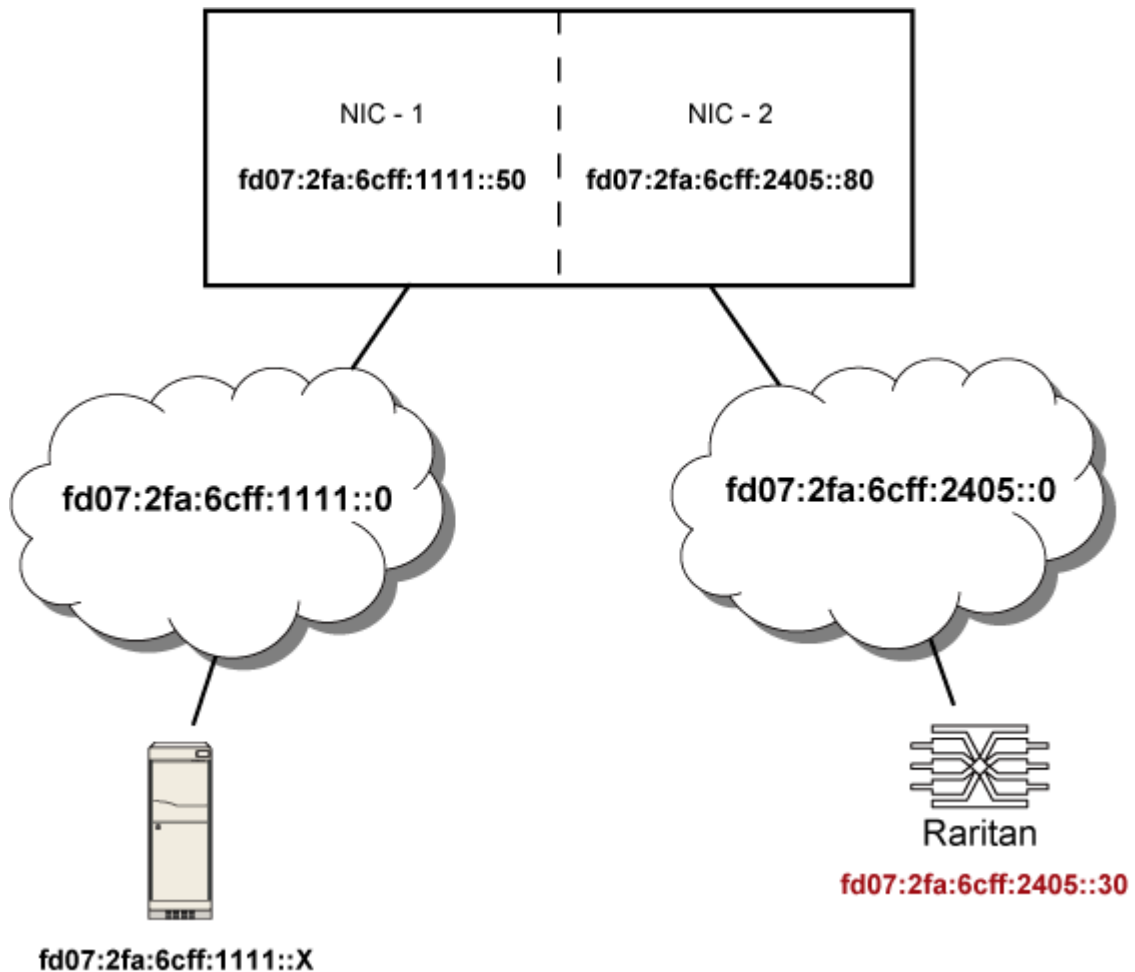
In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your EMX to communicate with any device in the other subnet fd07:2fa:6cff:1111::0. In the IPv6 "Static Routes" section, you should specify:

| 1 | fd07:2fa:6cff:2405::0/64 | Gateway | fd07:2fa:6cff:2405::80 ✕ | ⬆ ⬇ 🗑 |

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ⬆ *or* ⬇ *to re-sort the priority, or click* 🗑 *to delete it.*

Interface Names

When your local multiple networks are "directly reachable", you should select Interface for static routes. Then choose the interface where another network is connected.

192.168.200.0/24	Interface	BRIDGE
		ETHERNET
		WIRELESS

Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your EMX, and your EMX has been set to the bridging mode, select this interface name instead of the Ethernet interface.
ETHERNET	When another wired network is connected to the Ethernet port of your EMX, select this interface name.
WIRELESS	When another wireless network is connected to your EMX, select this interface name.

Setting the Cascading Mode

A maximum of 16 EMX devices can be cascaded to share one Ethernet connection. See *Cascading Multiple EMX Devices for Sharing Ethernet Connectivity* (on page 21).

The cascading mode configured on the master device determines the Ethernet sharing method, which is either network bridging or port forwarding. See *Overview of the Cascading Modes* (on page 163).

Only a user with the Change Network Settings can configure the cascading mode.

Note: The EMX in the Port Forwarding mode does not support APIPA. See **APIPA and Link-Local Addressing** *(on page 4).*

▶ **To configure the cascading mode:**

1. Connect the device that you will cascade to the LAN and find its IP address, or connect it to a computer.

    ▪ For the computer connection instructions, see *Connecting the EMX to a Computer* (on page 12).

    ▪ To find the IP address, see *IPv4 Address* (on page 75).

2. Log in to its web interface.

3. Choose Device Settings > Network.

4. Select the preferred mode in the Cascading Mode field.

    ▪ None: No cascading mode is enabled. This is the default.

    ▪ Bridging: Each device in the cascading chain is accessed with a different IP address.

    ▪ Port Forwarding: Each device in the cascading chain is accessed with the same IP address but with a different port number assigned. For details on port numbers, see *Port Number Syntax* (on page 165).

    Tip: If selecting Port Forwarding, the Device Information page will show a list of port numbers for all cascaded devices.

5. For the port forwarding mode, one to two more fields have to be configured. Note that if either setting is incorrectly configured, a networking issue occurs.

    ▪ Role: Master or Slave. This is to determine which device is the master and which ones are slave devices.

    ▪ Downstream interface: USB or Ethernet. This is to determine which port of the master device is connected to Slave 1. Always select USB.

6. Now you can configure the network settings.

   ▪ Bridging mode: Click the BRIDGE section on the same page.

   ▪ Port forwarding mode: Click the ETHERNET or WIRELESS section on the same page, depending on the networking method you prefer.

7. Click Save.

For information on accessing each cascaded device in the Port Forwarding mode, see *Port Forwarding Examples* (on page 166).

For information on wired or wireless network settings, see *Wired Network Settings* (on page 150) or *Wireless Network Settings* (on page 153).

▶ **Online USB-cascading information:**

For more information on the USB-cascading configuration, see the *Cascading Guide*, which is available from Raritan website's *Support page* (*http://www.raritan.com/support/*).

Overview of the Cascading Modes

You must apply a cascading mode to the cascading configuration. See *Setting the Cascading Mode* (on page 162).

▶ **Overview:**

- The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.

- All cascading modes support a maximum of 16 devices in a chain.

- All cascading modes support both DHCP and static IP addressing.

- In the Bridging mode, each cascaded device has a unique IP address. In the Port Forwarding mode, all cascaded devices share the same IP address.

- Each cascaded device can be remotely accessed through the network regardless of the cascading mode.

▶ **Illustration:**

In the following diagrams, it is assumed that users enable the DHCP networking in the cascading configuration comprising four devices. "M" is the master device and "S" is the slave device.

- **"Bridging" mode:**

  In this mode, the DHCP server communicates with every cascaded device respectively and assigns four *different* IP addresses. Each device has its own IP address. The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.
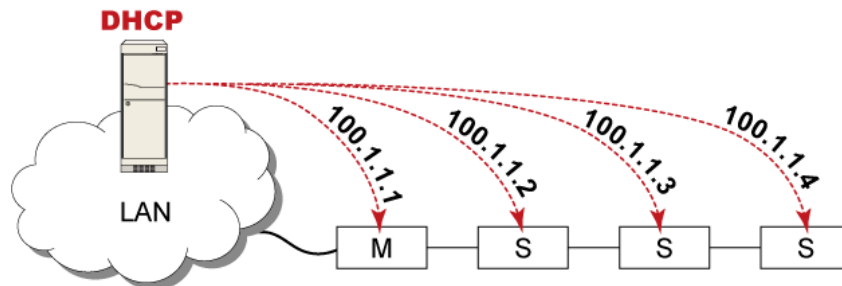
- **"Port Forwarding" mode:**

  In this mode, the DHCP server communicates with the master device alone and assigns only one IP address. All slave devices share the same IP address as the master device. You must specify a 5XXXX port number (where X is a number) when remotely accessing any slave device via the shared IP address. See *Port Number Syntax* (on page 165).
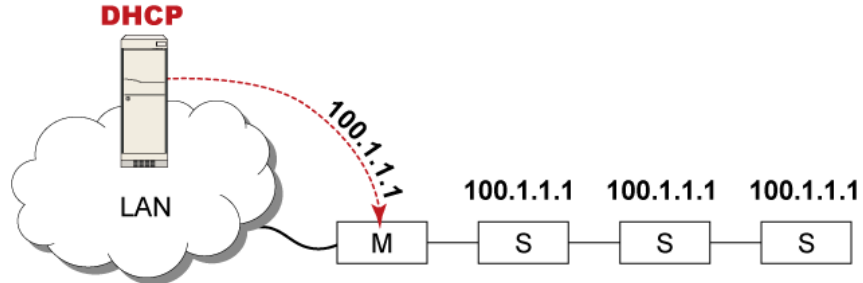
Port Number Syntax

In the Port Forwarding mode, all devices in the USB-cascading configuration share the same IP address. To access any cascaded device, you must assign an appropriate port number to it.

- Master device: The port number is either *5NNXX* or the standard TCP/UDP port.
- Slave device: The port number is *5NNXX*.

▶ **5NNXX port number syntax:**

- NN is a two-digit number representing the network protocol as shown below:

Protocols	NN
HTTPS	00
HTTP	01
SSH	02
TELNET	03
SNMP	05
MODBUS	06

- XX is a two-digit number representing the device position as shown below.

  The following table only lists 7 slave devices, but the port forwarding supports up to 15 slave devices.

Position	XX
Master device	00
Slave 1	01
Slave 2	02
Slave 3	03
Slave 4	04
Slave 5	05
Slave 6	06
Slave 7	07

For example, to access the Slave 4 device via Modbus/TCP, the port number is 50604. See *Port Forwarding Examples* (on page 166) for further illustrations.

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. Choose Maintenance > Device Information > Port Forwarding.

▶ **Standard TCP/UDP ports:**

The master device can be also accessed through standard TCP/UDP ports as listed in the following table.

Protocols	Port Numbers
HTTPS	443
HTTP	80
SSH	22
TELNET	23
SNMP	161
MODBUS	502

In the Port Forwarding mode, the EMX does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet and Modbus/TCP.

Port Forwarding Examples

To access a cascaded device in the Port Forwarding mode, assign a port number to the IP address.

- Master device: Assign proper 5NNXX port numbers or standard TCP/UDP ports. See *Port Number Syntax* (on page 165) for details.
- Slave device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a USB-cascading configuration comprising three Raritan devices. The IP address is 192.168.84.77.*

▶ **Master device:**

Position code for the master device is '00' so each port number is 5NN00 as listed below.

Protocols	Port numbers
HTTPS	50000

Protocols	Port numbers
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

Examples using "5NN00" ports:

- To access the master device via HTTPS, the IP address is:

  https://192.168.84.77:50000/

- To access the master device via HTTP, the IP address is:

  http://192.168.84.77:50100/

- To access the master device via SSH, the command is:

  ssh -p 50200 192.168.84.77

Examples using standard TCP/UDP ports:

- To access the master device via HTTPS, the IP address is:

  https://192.168.84.77:443/

- To access the master device via HTTP, the IP address is:

  http://192.168.84.77:80/

- To access the master device via SSH, the command is:

  ssh -p 22 192.168.84.77

▶ **Slave 1 device:**

Position code for Slave 1 is '01' so each port number is 5NN01 as shown below.

Protocols	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

Examples:

- To access Slave 1 via HTTPS, the IP address is:

  https://192.168.84.77:50001/

- To access Slave 1 via HTTP, the IP address is:

  http://192.168.84.77:50101/

- To access Slave 1 via SSH, the command is:

  ssh -p 50201 192.168.84.77

▶ **Slave 2 device:**

Position code for Slave 2 is '02' so each port number is 5NN02 as shown below.

Protocols	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502
MODBUS	50602

Examples:

- To access Slave 2 via HTTPS, the IP address is:

  https://192.168.84.77:50002/

- To access Slave 2 via HTTP, the IP address is:

  http://192.168.84.77:50102/

- To access Slave 2 via SSH, the command is:

  ssh -p 50202 192.168.84.77

Adding, Removing or Swapping Cascaded Devices

Change the cascading mode first before adding any device to a cascading chain, or before disconnecting a cascaded device from the chain.

If you only want to change the cascading mode of an existing chain, or swap the master and slave device, always start from the slave device.

Note: If the following procedures are not followed, a networking issue occurs. When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain. See **Cascading Troubleshooting** *(on page 535).*

▶ **To add a device to an existing chain:**

1. Connect the device that you will cascade to the LAN and find its IP address, or connect it to a computer.

2. Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode. See *Setting the Cascading Mode* (on page 162).

3. Connect it to the chain, using either USB or Ethernet cable.

▶ **To remove a device from the chain:**

1. Log in to the desired cascaded device, and change its cascading mode to None.

   Exception: If you are going to connect the removed device to another cascading chain, set its cascading mode to be the same as the cascading mode of another chain.

2. Now disconnect it from the cascading chain.

▶ **To swap the master and slave device:**

- In the bridging mode, you can swap the master and slave devices by simply disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.

- In the port forwarding mode, you must follow the procedure below:

   a. Access the slave device that will replace the master device, and set its role to 'Master', and correctly set the downstream interface.

   b. Access the master device, set its role to 'Slave'.

   c. Swap the master and slave device now. You must disconnect ALL cascading cables connected to the two devices first before swapping them and reconnecting cascading cables.

▶ **To change the cascading mode applied to a chain:**

1. Access the last slave device, and change its cascading mode.

   ▪ If the new cascading mode is 'Port Forwarding', you must also set its role to 'Slave'.

2. Access the second to last, third to last and so on until the first slave device to change their cascading modes one by one.

3. Access the master device, and change its cascading mode.

   ▪ If the new cascading mode is 'Port Forwarding', you must also set its role to 'Master', and correctly select the downstream interface.

Configuring Network Services

The EMX supports the following network communication services.

HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface. See *Using the Command Line Interface* (on page 291).

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.

Submenu command	Refer to
HTTP	*Changing HTTP(S) Settings* (on page 171)
SNMP	*Configuring SNMP Settings* (on page 172)
SMTP Server	*Configuring SMTP Settings* (on page 173)
SSH	*Changing SSH Settings* (on page 175)
Telnet	*Changing Telnet Settings* (on page 175)
Modbus	*Changing Modbus Settings* (on page 176)
Service Advertising	*Enabling Service Advertising* (on page 178)

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Raritan.
A brand of Legrand

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the EMX so it is a more secure protocol than HTTP. The EMX supports TLS *1.0*, *1.1* and *1.2*.

By default, any access to the EMX via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

▶ **To change HTTP or HTTPS port settings:**

1. Choose Device Settings > Network Services > HTTP.
2. Enable either or both protocols by selecting the corresponding 'Enable' checkbox.
3. To use a different port for HTTP or HTTPS, type a new port number.

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

4. To redirect the HTTP access to the EMX to HTTPS, select the "Redirect HTTP connections to HTTPS."

   ▪ The redirection checkbox is configurable only when both HTTP and HTTPS have been enabled.

Special note for AES ciphers:

The EMX device's SSL/TLS-based protocols, including HTTPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the EMX and the client (such as a web browser), which is impacted by the cipher priority of the EMX and the client's cipher availability/settings.

Tip: If intending to force the EMX to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the Firefox via the "about:config" command.

Configuring 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 and even control the power status of each outlet.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See *Event Rules and Actions* (on page 204).

▶ **To configure SNMP communication:**

1. Choose Device Settings > Network Services > SNMP.

2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.

   - The SNMP v1/v2c read-only access is enabled by default. The default Read Community String is 'public.'

   - To enable read-write access, type the Write Community String. Usually the string is 'private.'

3. Enter the MIB-II system group information, if applicable.

   - sysContact - the contact person in charge of the system

   - sysName - the name assigned to the system

   - sysLocation - the location of the system

4. To configure SNMP notifications:

   a. Select the Enable SNMP Notifications checkbox.

   b. Select a notification type -- SNMPv2c Trap, SNMPv2c Inform, SNMPv3 Trap, and SNMPv3 Inform.

   c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:

      - *SNMPv2c Notifications* (on page 285)

      - *SNMPv3 Notifications* (on page 286)

   Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** *(on page 219). To add more than three SNMP destinations, you can create new SNMP notification actions. See* **Send an SNMP Notification** *(on page 230).*

5. You must download the SNMP MIB for your EMX to use with your SNMP manager.

a. Click the Download MIBs title bar to show the download links.

Download MIBs ⌄

b. Click the EMD-MIB download link. See *Downloading SNMP MIB* (on page 287).

6. Click Save.

Configuring SMTP Settings

The EMX can be configured to send alerts or event messages to a specific administrator by email. See *Event Rules and Actions* (on page 204).

To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 268).

▶ **To set SMTP server settings:**

1. Choose Device Settings > Network Services > SMTP Server.

2. Enter the information needed.

Field	Description
Server Name	Type the name or IP address of the mail server.
Port	Type the port number. ▪ Default is 25
Sender Email Address	Type an email address for the sender.
Number of Sending Retries	Type the number of email retries. ▪ Default is 2 retries
Time Between Sending Retries	Type the interval between email retries in minutes. ▪ Default is 2 minutes.
Server Requires Authentication	Select this checkbox if your SMTP server requires password authentication.

Field	Description
User Name, Password	Type a user name and password for authentication after selecting the above checkbox. ▪ The length of user name and password ranges between 4 and 64. Case sensitive. ▪ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

- **Settings for the CA Certificate:**

Field/setting	Description
Browse...	Click this button to install a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

3. Now that you have set the SMTP settings, you can test it to ensure it works properly.

   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.

   c. Check if the recipient(s) receives the email successfully.

4. Click Save.

Raritan.

▶ **Special note for AES ciphers:**

The EMX device's SSL/TLS-based protocols, including SMTP over StartTLS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the EMX and the client (such as a web browser), which is impacted by the cipher priority of the EMX and the client's cipher availability/settings.

Tip: If intending to force the EMX to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

▶ **To change SSH settings:**

1. Choose Device Settings > Network Services > SSH.
2. To enable or disable the SSH access, select or deselect the checkbox.
3. To use a different port, type a port number.
4. Select one of the authentication methods.
   - Password authentication only: Enables the password-based login only.
   - Public key authentication only: Enables the public key-based login only.
   - Password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click Save.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See *Creating Users* (on page 138).

Changing Telnet Settings

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

▶ **To change Telnet settings:**

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.

3. To use a different port, type a new port number.

4. Click Save.

Changing Modbus Settings

The EMX supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

▶ **Modbus/TCP Access:**

You can enable or disable the Modbus/TCP access to the EMX, set it to the read-only mode, or change the TCP port.

1. Choose Device Settings > Network Services > Modbus.

2. To enable the Modbus/TCP access, select the "Modbus/TCP Access" checkbox.

3. To use a different port, type a new port number.

4. To enable the Modbus read-only mode, select the checkbox of the "Read-only mode" field. To enable the read-write mode, deselect it.

▶ **Modbus Gateway:**

If connecting the Modbus RTU devices to the EMX and enabling the Modbus Gateway feature, the Modbus TCP clients on your network will be able to communicate with those Modbus RTU devices attached to the EMX. See *Connecting a Modbus RTU Device or Bus* (on page 63).

1. To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the EMX, select the Modbus Gateway checkbox.

Modbus Gateway	
Modbus Gateway	✔ Enable
TCP Port	503
Parity	Even ⬍
Line Speed	19200 ⬍
Default Address	1

2. Now configure the fields shown.

Field	Description
TCP Port	Use the default port 503, or assign a different port. Valid range is 1 to 65535.
	Note: Port 502 is the default Modbus/TCP port for EMX, so you cannot use that port for the Modbus Gateway.
Parity, Line Speed	Use the default values, or update if the Modbus RTU devices are using different communication parameters.
Default Address	If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address. If you must provide a unit identifier address: ▪ Only one Modbus RTU device is supported. ▪ The unit identifier address you provide is applied to the Modbus RTU device connected to the EMX. Note that each Modbus RTU device's unit identifier address must be unique.
	Warning: If the connected Modbus RTU device's address does not match the address entered in this field, communications between the Modbus TCP clients and Modbus RTU device fail.

Enabling Service Advertising

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

By default, this feature is enabled.

Enabling this feature also enables Link-Local Multicast Name Resolution (LLMNR) and/or MDNS, which are required for resolving APIPA host names. See *APIPA and Link-Local Addressing* (on page 4).

The service advertisement feature supports both IPv4 and IPv6 protocols.

If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where <preferred_host_name> is the preferred host name you have specified for EMX. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

Note: For information on configuring IPv4 and/or IPv6 network settings, see **Wired Network Settings** *(on page 150).*

▶ **To enable or disable service advertising:**

1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
   - To advertise via MDNS, select the Multicast DNS checkbox.
   - To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.
3. Click Save.

Configuring Security Settings

The EMX provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports the SHA-2 certificate.

Tip: To force all HTTP accesses to the EMX to be redirected to HTTPS, see **Changing HTTP(S) Settings** *(on page 171).*

Submenu command	Refer to
IP Access Control	*Creating IP Access Control Rules* (on page 179)
Role Access Control	*Creating Role Access Control Rules* (on page 182)
SSL Certificate	*Setting Up an SSL/TLS Certificate* (on page 184)
Authentication	*Setting Up External Authentication* (on page 189)
Login Settings	*Configuring Login Settings* (on page 198)
Password Policy	*Configuring Password Policy* (on page 200)
Service Agreement	*Enabling the Restricted Service Agreement* (on page 201)

Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the EMX, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- **Rule order is important.**

    When traffic reaches or is sent from 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.

- **Subnet mask is required.**

    When typing the IP address, you must specify BOTH the address and a subnet mask. 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 IPv4 addresses range from 0.0.0.0 through 255.255.255.255.

▶ **To configure IPv4 access control rules:**

1. Choose Device Settings > Security > IP Access Control.
2. Select the Enable IPv4 Access Control checkbox to enable IPv4 access control rules.
3. Determine the IPv4 default policy.
    - 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.
4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.
    - Inbound rules control the data sent to the EMX.
    - Outbound rules control the data sent from the EMX.
5. Create rules. See the tables for different operations.

ADD a rule to the end of the list

- Click Append.
- Type an IP address and subnet mask in the IP/Mask field.
- Select an option in the Policy field.
    - Accept: Accepts traffic from/to the specified IP address(es).
    - Drop: Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
    - Reject: Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

INSERT a rule between two 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 Above.
- Type an IP address and subnet mask in the IP/Mask field.
- Select Accept, Drop or Reject in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

6. When finished, the rules are listed.

- You can select any existing rule and then click ⬆ or
  ⬇ to change its priority.

7. Click Save. The rules are applied.

▶ **To configure IPv6 access control rules:**

1. On the same page, select the Enable IPv6 Access Control checkbox to enable IPv6 access control rules.

2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

▶ **To modify or delete a rule:**

1. Choose Device Settings > Security > IP Access Control.

2. Go to the IPv4 or IPv6 section.

3. Select the desired rule in the list.

   - Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot edit or delete any rule.

4. Perform the desired action.

   - Make changes to the selected rule, and then click Save. For information on each field, see *Creating IP Access Control Rules* (on page 179).

   - Click ⬚ to remove it.

   - To resort its order, click ⬆ or ⬇ .

5. Click Save.

   - IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.

   - IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Creating Role Access Control Rules

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

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

▶ **To create IPv4 role-based access control rules:**

1. Choose Device Settings > Security > Role Access Control.

2. Select the "Enable Role Based Access Control for IPv4" checkbox to enable IPv4 access control rules.

3. Determine the IPv4 default policy.

   ▪ 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.

4. Create rules. See the tables for different operations.

ADD a rule to the end of the list
▪ Click Append. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in the Role field. This rule applies to members of this role only. ▪ Select an option 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

INSERT a rule between two 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 Above. ▪ Type a starting IP address in the Start IP field. ▪ Type an ending IP address in the End IP field. ▪ Select a role in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny in the Policy field. See the above for their descriptions.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.

   ▪ You can select any existing rule and then click ⬆ or ⬇ to change its priority.

6. Click Save. The rules are applied.

▶ **To configure IPv6 access control rules:**

1. On the same page, select the "Enable Role Based Access Control for IPv6" checkbox to enable IPv6 access control rules.

2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting Role Access Control Rules

You can modify existing rules to update their roles/IP addresses, or or delete them when they are no longer needed.

▶ **To modify a role-based access control rule:**

1. Choose Device Settings > Security > Role Access Control.

2. Go to the IPv4 or IPv6 section.

3. Select the desired rule in the list.
   ▪ Ensure the IPv4 or IPv6 checkbox has been selected, or you cannot select any rule.

4. Perform the desired action.
   ▪ Make changes to the selected rule, and then click Save. For information on each field, see *Creating Role Access Control Rules* (on page 182).

- Click to remove it.

- To resort its order, click or .

5. Click Save.

    - IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.

    - IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Setting Up an SSL/TLS Certificate

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

▶ **To obtain a CA-signed certificate:**

1. Create a Certificate Signing Request (CSR) on the EMX. See *Creating a CSR* (on page 185).

2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.

3. Install the CA-signed certificate onto the EMX. See *Installing a CA-Signed Certificate* (on page 186).

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

▶ **A CSR is not required in either scenario below:**

- Make the EMX create a *self-signed* certificate. See *Creating a Self-Signed Certificate* (on page 187).

- Appropriate, valid certificate and key files are already available, and you just need to install them. See *Installing or Downloading Existing Certificate and Key* (on page 188).

Creating a CSR

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

Note that you must enter information in the fields showing the message 'required.'

▶ **To create a CSR:**

1. Choose Device Settings > Security > SSL Certificate.
2. Provide the information requested.
   - **Subject:**

Field	Description
Country	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.

Warning: If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

   - **Key Creation Parameters:**

Field	Do this
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the EMX device's response. ▪ Only 2048 is available now.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**

Field	Do this
Challenge, Confirm Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

3. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.

4. Click Download Certificate Signing Request to download the CSR to your computer.

    a. You are prompted to open or save the file. Click Save to save it onto your computer.

    b. Submit it to a CA to obtain the digital certificate.

    c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.

5. To store the newly-created private key on your computer, click Download Key in the **New SSL Certificate** section.

    Note: The Download Key button in the Active SSL Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.

    ▪ You are prompted to open or save the file. Click Save to save it onto your computer.

6. After getting the CA-signed certificate, install it. See *Installing a CA-Signed Certificate* (on page 186).

Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See *Creating a CSR* (on page 185).

After receiving the CA-signed certificate, install it onto the EMX.

▶ **To install the CA-signed certificate:**

1. Choose Device Settings > Security > SSL Certificate.

2. Click [Browse...] to navigate to the CA-signed certificate file.

3. Click Upload to install it.

4. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

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.

Note that you must enter information in the fields showing the message 'required.'

required

▶ **To create and install a self-signed certificate:**

1. Choose Device Settings > Security > SSL Certificate.
2. Enter information.

Field	Description
Country	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.
Key Length	Select an available key length (bits). A larger key length enhances the security, but slows down the EMX device's response. ▪ Only 2048 is available now.
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 will be valid.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear.

3. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.

4. Once complete, do the following:

    a. Double check the data shown in the New SSL Certificate section.

    b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

    Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

    If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New SSL Certificate section.

    ▪ You are prompted to open or save the file. Click Save to save it onto your computer.

    Note: The Download Key button in the Active SSL Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.
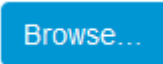
Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any EMX for backup or file transfer. For example, you can install the files onto a replacement EMX device, add the certificate to your browser and so on.

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

Note: If you are using a certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

▶ **To download active key and certificate files from the EMX:**

1. Choose Device Settings > Security > SSL Certificate.

2. In the *Active SSL Certificate* section, click Download Key and Download Certificate respectively.

    Note: The Download Key button in the New SSL Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.

3. You are prompted to open or save the file. Click Save to save it onto your computer.

▶ **To install available key and certificate files onto the EMX:**

1. Choose Device Settings > Security > SSL Certificate.
2. Select the "Upload Key and Certificate" checkbox at the bottom of the page.
3. The Key File and Certificate File fields appear. Click ![Browse...] to select the key and/or certificate file.
4. Click Upload. The selected files are installed.
5. To verify whether the certificate has been installed successfully, check the data shown in the Active SSL Certificate section.

Setting Up External Authentication

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

- Local user database on the EMX
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (Radius) protocol

By default, the EMX is configured for local authentication. If you stay with this method, you only need to create user accounts. See *Creating Users* (on page 138).

If you prefer external authentication, you must provide the EMX with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user accounts on the EMX in addition to providing the external AA server data.

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

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 268).

Note that only users who have both the "Change Authentication Settings" and "Change Security Settings" permissions can configure or modify the authentication settings.

▶ **To enable external authentication:**

1. Collect external AA server information. See *Gathering LDAP/Radius Information* (on page 191).
2. Enter required data for external AA server(s) on the EMX. See *Adding LDAP/LDAPS Servers* (on page 192) or *Adding Radius Servers* (on page 195).
   - For illustrations, see *LDAP Configuration Illustration* (on page 468) or *Radius Configuration Illustration* (on page 483).
3. If both the external and local authentication is needed, or you have to return to the local authentication only, see *Managing External Authentication Settings* (on page 197).

▶ **Special note about the AES cipher:**

The EMX device's SSL/TLS-based protocols, including LDAPS, support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between the EMX and the client (such as a web browser), which is impacted by the cipher priority of the EMX and the client's cipher availability/settings.

Tip: If intending to force the EMX to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Gathering LDAP/Radius Information

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

▶ **Information needed for LDAP authentication:**

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) 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)

▶ **Information needed for Radius authentication:**

- The IP address or host name of the Radius server
- Authentication protocol used by the Radius server
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

Adding LDAP/LDAPS Servers

To use LDAP authentication, enable it and enter the information you have gathered.
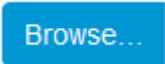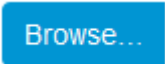
Note that you must enter information in the fields showing the message 'required.'

required

▶ **To add LDAP/LDAPS servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the LDAP Servers section.
3. Enter information.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your LDAP/LDAPS server. ▪ Important: Without the 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 encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the EMX. To duplicate any existing AA server's settings, refer to the duplicating procedure below.

Field/setting	Description
Type of LDAP Server	Choose one of the following options: ▪ OpenLDAP ▪ Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the EMX to communicate securely with the LDAPS server. Three options are available: ▪ StartTLS ▪ TLS ▪ None
Port (None/StartTLS)	The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.
Enable verification of LDAP Server Certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the EMX prior to the connection. If the certificate validation fails, the connection is refused.
CA Certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click [Browse...] to select and install the certificate file. ▪ Click Show to view the installed certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous Bind	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.

Field/setting	Description
Bind DN	**Required after deselecting the Anonymous Bind checkbox.** Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind Password, Confirm Bind Password	**Required after deselecting the Anonymous Bind checkbox.** Enter the Bind password.
Base DN for Search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. ▪ Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. ▪ Usually it is the `uid`.
User Entry Object Class	The object class for user entries. ▪ Usually it is `inetOrgPerson`.
User Search Subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory Domain	The name of the Active Directory Domain. ▪ Example: `testradius.com`

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the EMX can connect to the new server successfully.

Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 197).*

5. Click Add Server. The new LDAP server is listed on the Authentication page.
6. To add more servers, repeat the same steps.
7. **In the Authentication Type field, select LDAP.** Otherwise, the LDAP authentication does not work.
8. Click Save. The LDAP authentication is now in place.

Raritan.

▶ **To duplicate LDAP/LDAPS server settings:**

If you have added any LDAP/LDAPS server to the EMX, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

1. Repeat Steps 1 to 2 in the above procedure.
2. Select the "Copy settings from existing LDAP server" checkbox.
3. Click the "Select LDAP Server" field to select the LDAP/LDAPS server whose settings you want to copy.
4. Modify the IP Address/Hostname field.
5. Click Add Server.

Note: If the EMX clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the EMX and the LDAP server to use the same NTP server(s).

Adding Radius Servers

To use Radius authentication, enable it and enter the information you have gathered.

Note that you must enter information in the fields showing the message 'required.'

required

▶ **To add Radius servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the Radius section.
3. Enter information.

Field/setting	Description
IP Address / Hostname	The IP address or hostname of your Radius server.
Type of RADIUS Authentication	Select an authentication protocol. ■ PAP (Password Authentication Protocol) ■ CHAP (Challenge Handshake Authentication Protocol) CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.

Field/setting	Description
Authentication Port, Accounting Port	The default are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared Secret, Confirm Shared Secret	The shared secret is necessary to protect communication with the Radius server.

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the EMX can connect to the new server successfully.

Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 197).*

5. Click Add Server. The new Radius server is listed on the Authentication page.

6. To add more servers, repeat the same steps.

7. **In the Authentication Type field, select Radius.** Otherwise, the Radius authentication does not work.

8. Click Save. Radius authentication is now in place.

Managing External Authentication Settings

Choose Device Settings > Security > Authentication to open the Authentication page, where you can:

- Enable both the external and local authentication
- Edit or delete a server
- Resort the access order of servers
- Test the connection to a server
- Disable external authentication without removing servers

▶ **To test, edit or delete a server, or resort the server list:**

1. Select a server in the list.

Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	None	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	None	389	Microsoft Active Directory

2. Perform the desired action.
   - Click Edit to edit its settings, and click Modify Server to save changes. For information on each field, see *Adding LDAP/LDAPS Servers* (on page 192) or *Adding Radius Servers* (on page 195).
   - Click Delete to delete the server, and then confirm the operation.
   - Click Test Connection to test the connection to the selected server. User credentials may be required.
   - Click [▲] or [▼] to change the server order, which determines the access priority, and click Save Order to save the new sequence.

   Note: Whenever the EMX is successfully connected to one external authentication server, it STOPS trying to access the remaining servers in the authentication list regardless of the user authentication result.

▶ **To enable both the external and local authentication:**

1. In the Authentication Type field, select the external authentication you want -- LDAP or Radius.

2. Select the following checkbox. Then the EMX always tries external authentication first. Whenever the external authentication fails, the EMX switches to local authentication.

☑ Use Local Authentication if Remote Authentication is not available

3. Click Save.

▶ **To disable external authentication:**

1. In the Authentication Type, select Local.

2. Click Save.

Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

- Configure the user blocking feature.

  Note: The user blocking function applies only to local authentication instead of external authentication through AA servers.

- Determine the timeout period for any inactive user.

- Prevent simultaneous logins using the same login name.

▶ **To configure user blocking:**

1. To enable the user blocking feature, select the "Block user on login failure" checkbox.

2. In the "Maximum number of failed logins" field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the EMX.

3. In the "Block timeout" field, type a value or click [⬆⬇] to select a time option. This setting determines how long the user is blocked.

   ▪ If you type a value, the value must be followed by a time unit, such as '4 min.' See *Time Units* (on page 199).

4. Click Save.

*Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection. See **Unblocking a User** (on page 415).*

▶ **To set limitations for login timeout and use of identical login names:**

1. In the "Idle timeout period" field, type a value or click [⬍] to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.
   ▪ If you type a value, the value must be followed by a time unit, such as '4 min.' See *Time Units* (on page 199).
   ▪ 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.
2. Select the "Prevent concurrent login with same username" checkbox if intending to prevent multiple persons from using the same login name simultaneously.
3. Click Save.

Time Units

If you choose to type a new value in the time-related fields, such as the "Idle timeout period" field, you must add a time unit after the numeric value. For example, you can type '15 min' for 15 minutes.

Note that different fields have different range of valid values.

▶ **Time units:**

Unit	Time
min	minute(s)
h	hour(s)
d	day(s)

Configuring Password Policy

Choose Device Settings > Security > Password Policy to open the Password Policy page, where you can:

- Force users to use strong passwords.
- Force users to change passwords at a regular interval -- that is, password aging.

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the EMX device.

▶ **To configure password aging:**

1. Select the 'Enabled' checkbox of Password Aging.

2. In the Password Aging Interval field, type a value or click [▲▼] to select a time option. This setting determines how often users are requested to change their passwords.

   - If you type a value, the value must be followed by a time unit, such as '10 d.' See *Time Units* (on page 199).

3. Click Save.

▶ **To force users to create strong passwords:**

1. Select the 'Enabled' checkbox of Strong Passwords 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 forbidden previous passwords	= 5

   Note: The maximum password length accepted by the EMX is 64 characters.

2. Make changes to the default settings as needed.

3. Click Save.

Enabling the Restricted Service Agreement

The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the EMX.

Users must accept the agreement, or they cannot log in.

An event notifying you if a user has accepted or declined the agreement can be generated. See *Default Log Messages* (on page 210)

▶ **To enable the service agreement:**

1. Click Device Settings > Security > Service Agreement.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit or paste the content as needed.
   - A maximum of 10,000 characters can be entered.
4. Click Save.

▶ **Login manner after enabling the service agreement:**

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

  Tip: To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting the Date and Time

Set the internal clock on the EMX device manually, or link to a Network Time Protocol (NTP) server.

*Note: If you are using Sunbird's Power IQ to manage the EMX, you must configure Power IQ and the EMX to have the same date/time or NTP settings.*

▶ **To set the date and time:**

1. Choose Device Settings > Date/Time.
2. Click the Time Zone field to 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. Select the method for setting the date and time.

Customize the date and time

- Select User Specified Time.

- Type values in the Date field using the yyyy-mm-dd format, or click [calendar icon] to select a date. For details, see *Calendar* (on page 203).

- Type values in the Time field using the hh:mm:ss format, or click [up arrow] [down arrow] to adjust values.

  - The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM or PM button.

12	:	00	:	00	AM

Use the NTP server

- Select "Synchronize with NTP Server."

- There are two ways to assign the NTP servers:

  - To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second NTP Server.

    DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.

  - To use the manually-specified NTP servers, specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.

    Click Check NTP Servers to verify the validity and accessibility of the manually-specified NTP servers.

5. Click Save.

   The EMX follows the NTP server sanity check per the IETF RFC. If your EMX has problems synchronizing with a Windows NTP server, see *Windows NTP Server Synchronization Solution* (on page 203).

Calendar

The calendar icon in the Date field is a convenient tool to select a custom date. Click it and a calendar appears.

Button	Function
arrows	Switch between months.
dates (01-31)	Click a date.
Today	Select today.
Clear	Clear the entry, if any, in the Date field.
Close	Close the calendar.

Windows NTP Server Synchronization Solution

The NTP client on the EMX follows the NTP RFC so the EMX rejects any NTP servers whose root dispersion is more than one second. An NTP server with a dispersion of more than one second is considered an inaccurate NTP server by the EMX.

Note: For information on NTP RFC, visit **http://tools.ietf.org/html/rfc4330 http://tools.ietf.org/html/rfc4330** *to refer to section 5.*

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the EMX. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

▶ **To change the Windows NTP's root dispersion settings:**

1. Access the registry settings associated with the root dispersion on the Windows NTP server.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

2. *AnnounceFlags* must be set to 0x05 or 0x06.
   - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
   - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

> *Note: Do NOT use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and then gradually decreases to one second or lower.*

3. *LocalClockDispersion* must be set to 0.

Event Rules and Actions

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

An event rule consists of two parts:

- Event: This is the situation where the EMX or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.
- Action: This is the response to the event. For example, the EMX notifies the system administrator of the event via email.

If you want the EMX to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, you can make the EMX email the temperature report every hour.

Note that you need the Administrator Privileges to configure event rules.

▶ **To create an event rule:**

1. Choose Device Settings > Event Rules.
2. If the needed action is not available yet, create it by clicking ✚ New Action .
    a. Assign a name to this action.
    b. Select the desired action and configure it as needed.
    c. Click Create.
    For details, see *Available Actions* (on page 219).
3. Click ✚ New Rule to create a new rule.
    a. Assign a name to this rule.
    b. Make sure the Enabled checkbox is selected, or the new event rule does not work.
    c. In the Event field, select the event to which you want the EMX to react.
    d. In the Available Actions field, select the desired action(s) to respond to the selected event.
    e. Click Create.
    For details, see *Built-in Rules and Rule Configuration* (on page 205).

▶ **To create a scheduled action:**

1. If the needed action is not available yet, create it by clicking
    ➕ New Action. See above.

    Note: When creating scheduled actions, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

2. Click **➕ New Scheduled Action** to schedule the desired action.

    a. Assign a name to this scheduled action.

    b. Make sure the Enabled checkbox is selected, or the EMX does not perform this scheduled action.

    c. Set the interval time, which ranges from every minute to yearly.

    d. In the Available Actions field, select the desired action(s).

    e. Click Create.

    For details, see *Scheduling an Action* (on page 235).

Built-in Rules and Rule Configuration

The EMX is shipped with four built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

▶ **Built-in rules:**

*   *System Event Log Rule:*

    This causes ANY event occurred to the EMX to be recorded in the internal log. It is enabled by default.

    Note: For the default log messages generated for each event, see **Default Log Messages** *(on page 210).*

*   *System SNMP Notification Rule:*

    This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the EMX. It is disabled by default.

*   *System Tamper Detection Alarmed:*

    This causes the EMX to send alarm notifications if a DX tamper sensor has been connected and the EMX detects that the tamper sensor enters the alarmed state. It is enabled by default.
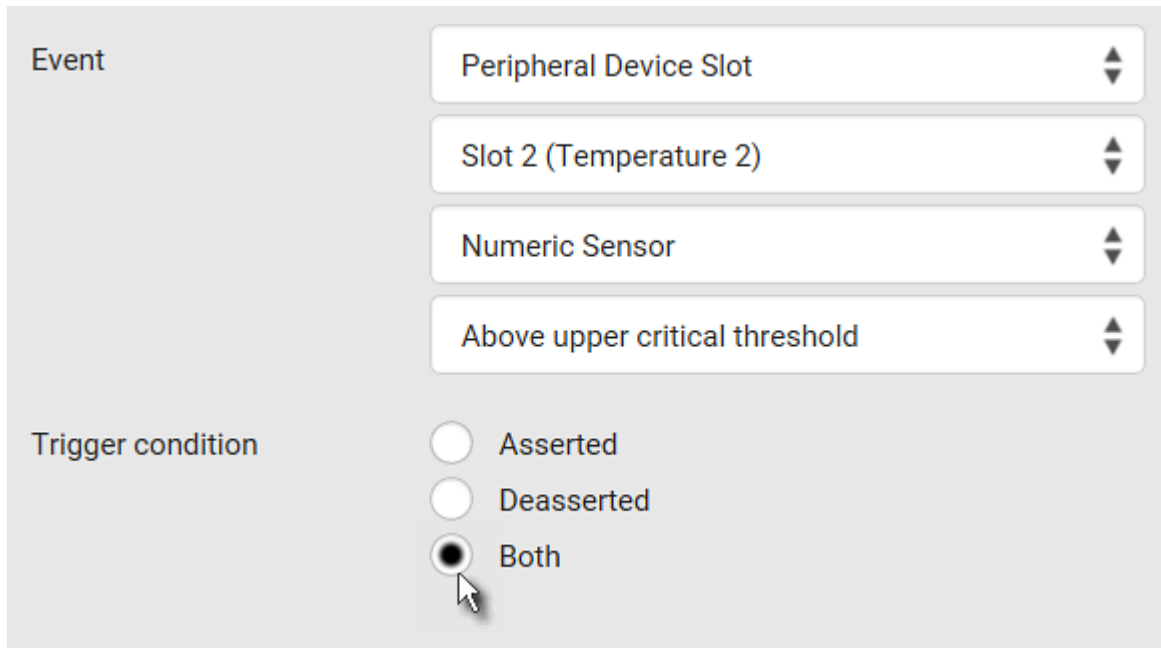
- *System Tamper Detection Unavailable:*

  This causes the EMX to send alarm notifications if a DX tamper sensor was once connected or remains connected but then the EMX does not detect the presence of the tamper sensor. It is enabled by default.

▶ **Event rule configuration illustration:**

1. Choose Device Settings > Event Rules > .
2. Click the Event field to select an event type.

   - <Any sub-event> means all events shown on the list.

   - <Any Numeric Sensor> means all numeric sensors of the EMX, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.

3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.

4. In this example, sensor ID 2 (Slot 2) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.

5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.

6. In this example, 'Above upper critical threshold' is selected because we want the EMX to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.

7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.

   ▪ If needed, you may refer to event rule examples in the section titled *Sample Event Rules* (on page 242).

8. To select any action(s), select them one by one from the Available Actions list.

   ▪ To select all available actions, click Select All.

9. To remove any action(s) from the Selected Actions field, click that action's ✖.

   ▪ To remove all actions, click Deselect All.

▶ **Radio buttons for different events:**

According to the event you select, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The EMX takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: The EMX takes the action only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. ▪ Both: The EMX takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: The EMX takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: The EMX takes the action only when the chosen sensor returns to the normal, closed, or off state. ▪ Both: The EMX takes the action whenever the chosen sensor switches its 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	▪ 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	▪ 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.
Restricted service agreement	▪ Accepted: The EMX takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: The EMX takes the action only when the specified user rejects the restricted service agreement. ▪ Both: The EMX takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	▪ 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	▪ 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.
Device connection or disconnection, such as a USB-cascaded slave device	▪ Connected: The EMX takes the action only when the selected device is physically connected to it. ▪ Disconnected: The EMX takes the action only when the selected device is physically disconnected from it. ▪ Both: The EMX takes the action both when the selected device is physically connected to it and when it is disconnected.

Default Log Messages

Following are default log messages recorded internally and emailed to specified recipients when EMX events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See *Send Email* (on page 226) for information configuring email messages to be sent when specified events occur.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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]').

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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 occurred 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]').	
Card Reader Management > Card inserted	Card Reader with id '[CARDREADERID]' connected.	
Card Reader Management > Card Reader attached	Card Reader with id '[CARDREADERID]' disconnected.	
Card Reader Management > Card Reader detached	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted.	
Card Reader Management > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed.	
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]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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 failed	Firmware upgrade failed from version '[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 > Device settings saved	Device settings saved from host '[USERIP]'	
Device > Device settings restored	Device settings restored from host '[USERIP]'.	
Device > Data push failed	Data push to URL [DATAPUSH_URL] failed. [ERRORDESC].	
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 > Peripheral Device Firmware Update	Firmware update for peripheral device [EXTSENSORSERIAL] from [OLDVERSION] to [VERSION] [SENSORSTATENAME].	
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	

Raritan.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	
Device > Sending Syslog message failed	Sending Syslog message to server [SYSLOGSERVER]:[SYSLOGPORT] ([SYSLOGTRANSPORTPROTO]) failed. [ERRORDESC].	
Device > Sending SMS message failed	Sending SMS message to '[PHONENUMBER]' failed.	
Device > An LDAP error occurred	An LDAP error occurred: [LDAPERRORDESC].	
Device > An Radius error occurred	An Radius error occurred: [RADIUSERRORDESC].	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > WLAN authentication over TLS with incorrect system clock	Established connection to wireless network '[SSID]' via Access Point with BSSID '[BSSID]' using '[AUTHPROTO]' authentication with incorrrect system clock.	
Peripheral Device Slot > * > Numeric Sensor > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > Numeric Sensor > Above upper critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning' at [READING].

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Peripheral Device Slot > * > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning' at [READING].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical' at [READING].	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical' at [READING].
Peripheral Device Slot > * > State Sensor/Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor/Actuator > Alarmed/Open/On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Modem > Dial-in link established	An incoming call from caller '[CALLERID]' was received.	The incoming call from caller '[CALLERID]' was disconnected: [CALLENDREASON].
Modem > Modem attached	A [MODEMTYPE] modem was attached.	
Modem > Modem detached	A [MODEMTYPE] modem was removed.	
Power Logic Device > * > Connected	PowerLogic Device has been connected to [PORTTYPE] port [PORTID].	PowerLogic Device has been disconnected from [PORTTYPE] port [PORTID].
Power Logic Device > * > Alarm	PowerLogic Device connected to [PORTTYPE] port [PORTID] entered an alarm condition.	PowerLogic Device connected to [PORTTYPE] port [PORTID] left an alarm condition.
Power Logic Device > * > Sensor > * > Unavailable	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' unavailable.	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' available.
Power Logic Device > * > Sensor > * > Above upper critical	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' asserted 'above upper critical' at [SENSORREADING]	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical' at

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
	[SENSORREADINGUNIT].	[SENSORREADING] [SENSORREADINGUNIT].
Power Logic Device > * > Sensor > * > Above upper warning	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].
Power Logic Device > * > Sensor > * > Below lower warning	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
Power Logic Device > * > Sensor > * > Below lower critical	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].")
Server Monitoring > * > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]	
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.
Server Monitoring > * > Unrecoverable	Connection to server '[MONITOREDHOST]' could not be restored.	
User Activity > * > User logon state	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 accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.
User Activity > * > User blocked	User '[USERNAME]' from host	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
	'[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
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 '[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam detached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') removed from port '[WEBCAMUSBPORT]'.	
Webcam Management > Webcam settings changed	Webcam '[WEBCAMNAME]' settings changed by user '[USERNAME]'.	
LHX/SHX > * > Connected	LHX has been connected to [PORTTYPE] port [PORTID].	LHX has been disconnected from [PORTTYPE] port [PORTID].
LHX/SHX > * > Operational State	LHX connected to [PORTTYPE] port [PORTID] has been switched on.	LHX connected to [PORTTYPE] port [PORTID] has been switched off.

Raritan.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
LHX/SHX > * > Sensor > Unavailable	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available.
LHX/SHX > * > 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/SHX > * > 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/SHX > * > 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/SHX > * > 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/SHX > * > Base Electronics Failure	The base electronics on LHX at [PORTTYPE] port '[PORTID]' failed.	
LHX/SHX > * > Condenser Pump Failure	The condenser pump on LHX at [PORTTYPE] port '[PORTID]' failed.	The condenser pump on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX/SHX > * > Emergency Cooling	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated.	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated.
LHX/SHX > * > 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/SHX > * > Parameter Data Loss	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > * > ST-Bus Communication Error	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > * > Collective fault	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > * > Door Contact	The door of LHX at [PORTTYPE] port '[PORTID]' was opened.	The door of LHX at [PORTTYPE] port '[PORTID]' was closed.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
LHX/SHX > * > Sensor Failure	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'.	
LHX/SHX > * > Fan Failure	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'.	
LHX/SHX > * > Power Supply Failure	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'.	
LHX/SHX > * > Threshold Air Inlet	The air inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > * > Threshold Air Outlet	The air outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > * > Threshold Water Inlet	The water inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > * > Threshold Water Outlet	The water outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > * > Voltage Low	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is low.	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX/SHX > * > 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/SHX > * > External Water Cooling Failure	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > * > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Available Actions

The EMX comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

▶ **Built-in actions:**

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

  Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action** *(on page 241). Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See* **Configuring SNMP Settings** *(on page 172).*

- *System Tamper Alarm:*

  This action causes the EMX to show the alarm for the DX tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see *Dashboard - Alarms* (on page 97).

▶ **Actions you can create:**

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Click the Action field to select an action type from the list.
3. Below is the list of available actions.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See *Alarm* (on page 221).
Execute an action group	Creates a group of actions comprising existing actions. See *Action Group* (on page 222).

Action	Function
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See *External Beeper* (on page 223).
Internal beeper	Turns on or off the internal beeper. See *Internal Beeper* (on page 223).
Log event message	Records the selected events in the internal log. See *Log an Event Message* (on page 223).
Push out sensor readings	Sends internal sensor log, environmental sensor log or asset management strip data to a remote server using HTTP POST requests. See *Push Out Sensor Readings* (on page 224).
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See *Record Snapshots to Webcam Storage* (on page 224).
Request LHX/SHX maximum cooling	Applies the maximum cooling to the LHX/SHX device. See *Request LHX/SHX Maximum Cooling* (on page 225). This option is available only when the Schroff LHX/SHX support has been enabled.
Send email	Emails a textual message. See *Send Email* (on page 226).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See *Send Sensor Report* (on page 227).
Send SMS message	Sends a message to a mobile phone. See *Send SMS Message* (on page 229).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See *Send Snapshots via Email* (on page 230).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See *Send an SNMP Notification* (on page 230).

Action	Function
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the EMX, and have the EMX automatically perform or stop the script in response to an event. See *Start or Stop a Lua Script* (on page 232).
Switch LHX/SHX	Switches on or off the LHX/SHX device. See *Switch LHX/SHX* (on page 233). This option is available only when the Schroff LHX/SHX support has been enabled.
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See *Switch Peripheral Actuator* (on page 233).
Syslog message	Makes the EMX automatically forward event messages to the specified syslog server. See *Syslog Message* (on page 234).

4. Enter the information as needed and click Create.

5. Then you can assign the newly-created action to an event rule or schedule it. See *Event Rules and Actions* (on page 204).

Alarm

The Alarm is an action that requires users to acknowledge an alert. This helps ensure that the user is aware of the alert.

If the Alarm action has been included in a specific event rule and no one acknowledges that alert after it occurs, the EMX resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent.

For information on acknowledging an alert, see *Dashboard* (on page 94).

▶ **Operation:**

1. Choose Device Settings > Event Rules > New Action .

2. Select Alarm from the Action list.

3. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:

- External beeper
- Syslog message
- Send email
- Send SMS message
- Internal beeper

If no appropriate actions are available, create them first.

a. To select any methods, select them one by one in the Available field.

   To add all available methods, simply click Select All.

b. To delete any methods, click a method's ✖ in the Selected field.

   To remove all methods, simply click Deselect All.

4. To enable the notification-resending feature, select the "Enable Re-scheduling of Alarm Notifications" checkbox.

5. In the "Re-scheduling Period" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.

6. In the "Re-scheduling Limit" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.

7. **(Optional)** You can instruct the EMX to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications field. Available methods are identical to those for generating alarm notifications.

a. In the Available field, select desired methods one by one, or click Select All. See step 3 for details.

b. In the Selected field, click any method's ✖ to remove unnecessary ones, or click Deselect All.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first. See *Available Actions* (on page 219).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Execute an action group" from the Action list.

3. To select any action(s), select them one by one from the Available Actions list.

   ▪ To select all available actions, click Select All.

4. To remove any action(s) from the Selected Actions field, click that action's ![x] .

   ▪ To remove all actions, click Deselect All.

External Beeper

If an external beeper is connected to the EMX, the EMX can change the beeper's behavior or status to respond to a certain event.

▶ **To control the connected external beeper:**

1. Choose Device Settings > Event Rules > ![New Action].

2. Select "External beeper" from the Action list.

3. In the Beeper Port field, select the port where the external beeper is connected. This port is the FEATURE port.

4. In the Beeper Action field, select an action for the external beeper to carry out.

   ▪ Alarm: Causes the external beeper to sound an alarm cycle every 20 seconds - stays on for 0.7 seconds and then off for 19.3 seconds.

   ▪ On: Turns on the external beeper so that it buzzes continuously.

   ▪ Off: Turns off the external beeper so that it stops buzzing.

Warning: If you create an event rule for the external beeper but disconnect it when an event causes it to beep, the beeper no longer beeps after it is re-connected even though the event triggering the beeping action remains asserted.

Internal Beeper

You can have the built-in beeper of the EMX turned on or off when a certain event occurs.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action].

2. Select "Internal beeper" from the Action list.

3. Select an option from the Operation field.

   ▪ Turn Beeper On: Turns on the internal beeper to make it buzz.

   ▪ Turn Beeper Off: Turns off the internal beeper to make it stop buzzing.

Log an Event Message

The option "Log event message" records the selected events in the internal log.

The default log message generated for each type of event is available in the section titled *Default Log Messages* (on page 210).

Push Out Sensor Readings

You can configure the EMX to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

If you have connected Raritan's asset strips to the EMX, you can also configure the EMX to push the data to a server.

Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page. See *Configuring Data Push Settings* (on page 247).

Tip: To send the data at a regular interval, schedule this action. See **Scheduling an Action** *(on page 235). Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.*

▶ **Operation:**

1. Choose Device Settings > Event Rules > 　 **New Action**.
2. Select "Push out sensor readings" from the Action list.
3. Select a server or host which receives the asset strip data or sensor log in the Destination field.
   ▪ If the desired destination is not available yet, go to the Data Push page to specify it.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the EMX. You can specify a remote server to store snapshots. See *Viewing Saved Snapshots and Managing Storage* (on page 282).

▶ **Operation:**

1. Choose Device Settings > Event Rules > 　 **New Action**.
2. Select "Record snapshots to webcam storage" from the Action list.
3. Select a webcam in the Webcam field.
4. Select the action to perform - "Start recording" or "Stop recording."

If "Start recording" is selected, adjust the values of the following:

- Number of Snapshots - the number of snapshots to be taken when the event occurs.

  The maximum amount of snapshots that can be stored on the EMX is 10. If you set it for a number greater than 10 and the storage location is on the EMX, after the 10th snapshot is taken and stored, the oldest snapshots are overwritten. Storing snapshots on a remote server does not have such a limitation.

- Time Before First Snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.

- Time Between Snapshots - the amount of time in seconds between when each snapshot is taken.

Request LHX/SHX Maximum Cooling

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See *Miscellaneous* (on page 260).

The "Request LHX/SHX Maximum Cooling" action applies the maximum cooling to the SHX-30 device only. The LHX-20 and LHX-40 devices do not support this feature.

In the maximum cooling mode, an SHX-30 device runs at 100% fan speed and the cold water valve is open 100%.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Request LHX/SHX Maximum Cooling" from the Action list.

3. In the Available LHX/SHX field, select the desired SHX-30 device one by one, or click Select All.

4. To remove any SHX-30 device from the Selected LHX/SHX field, click that device's ✖ or click Deselect All.

Send Email

You can configure emails to be sent when an event occurs and can customize the message.

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:

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

translates to

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

For a list and definition of available variables, see *Email and SMS Message Placeholders* (on page 239).

▶ **Operation:**

1. Choose Device Settings > Event Rules > **New Action**.

2. Select "Send email" from the Action list.

3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

4. To use the SMTP server specified on the SMTP Server page, make sure the "Use custom SMTP Server" checkbox is NOT selected.

   To use a different SMTP server, select this checkbox. The fields for customized SMTP settings appear. For information on each field, see *Configuring SMTP Settings* (on page 173).

   Default messages are sent based on the event. For a list of default log messages and events that trigger them, see *Default Log Messages* (on page 210).

5. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.

   ▪ When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see *Email and SMS Message Placeholders* (on page 239).

   ▪ To start a new line in the text box, press Enter.

   ▪ If needed, you can resize the text box by dragging the bottom-right corner.

Send Sensor Report

You may set the EMX so that it automatically reports the latest readings or states of one or multiple sensors by sending a message or email or simply recording the report in a log. These sensors can be either internal or environmental sensors as listed below.

- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the EMX, such as temperature or humidity sensors.

An example of this action is available in the section titled *Send Sensor Report Example* (on page 238).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Send sensor report" from the Action list.

3. In the Destination Actions section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

   The messaging action types include:

   ▪ Log event message
   ▪ Syslog message
   ▪ Send email
   ▪ Send SMS message

   a. If no messaging actions are available, create them now. See *Available Actions* (on page 219).

   b. To select any methods, select them one by one in the Available field.

      To add all available methods, simply click Select All.

   c. To delete any methods, click a method's ✖ in the Selected field.

      To remove all methods, simply click Deselect All.

4. In the Available Sensors field, select the desired target's sensor.

   a. Click the first ⬍ to select a target component from the list.

⬍ Peripheral Devices   ⬍ Temperature 1   ⊕   ⊖
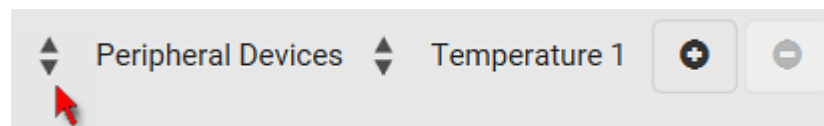
b. Click the second ⬍ to select the specific sensor for the target from the list.

Peripheral Devices   Temperature 1   ⊕   ⊖
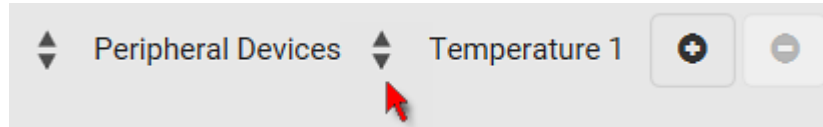
c. Click ⊕ to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

5. To report additional sensors simultaneously, repeat the above step to add more sensors.

▪ To remove any sensor from the Report Sensors list box, select it and click ⊖. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

6. To immediately send out the sensor report, click Send Report Now.

Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Email and SMS Message Placeholders** *(on page 239).*

Send SMS Message

You can configure SMS messages to be sent when an event occurs and can customize the message.

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

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged into the EMX in order to send SMS messages. See *Connecting a GSM Modem* (on page 60).

Note: The EMX cannot receive SMS messages.

For example:

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

translates to

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

For a list and definition of available variables, see *Email and SMS Message Placeholders* (on page 239).

► **Operation:**

1. Choose Device Settings > Event Rules > New Action.
2. Select "Send SMS message" from the Action list.
3. In the Recipient Phone Number field, specify the phone number of the recipient.
4. Select the Use Custom Log Message checkbox, and then create a custom message in the provided text box.
   - When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just click the desired placeholder. For details, see *Email and SMS Message Placeholders* (on page 239).
   - To start a new line in the text box, press Enter.
   - If needed, you can resize the text box by dragging the bottom-right corner.

Note: Only the 7-bit ASCII charset is supported for SMS messages.

Send Snapshots via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select "Send snapshots via email" from the Action list.
3. In the "Recipient Email Addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. To use the SMTP server specified on the SMTP Server page, make sure the "Use custom SMTP Server" checkbox is NOT selected.

    To use a different SMTP server, select this checkbox. The fields for customized SMTP settings appear. For information on each field, see *Configuring SMTP Settings* (on page 173).
5. Select the webcam that is capturing the images you want sent in the email.
6. Adjust the values of the following:
    -   Number of Snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
    -   Snapshots per Mail - the number of snapshots to be sent at one time in the email.
    -   Time Before First Snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.
    -   Time Between Snapshots - the amount of time in seconds between when each snapshot is taken.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action .
2. Select "Send SNMP notification" from the Action list.
3. Select the type of SNMP notification. See either procedure below according to your selection.

▶ **To send SNMP v2c notifications:**

1. In the Notification Type field, select SNMPv2c Trap or SNMPv2c Inform.

2. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.

4. In the Port fields, enter the port number used to access the device(s).

5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the EMX and all SNMP management stations.

Tip: An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

▶ **To send SNMP v3 notifications:**

1. In the Notification Type field, select SNMPv3 Trap or SNMPv3 Inform.

2. For SNMP TRAPs, the engine ID is prepopulated.

3. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the Number of Retries field, specify the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

a. Host name

b. Port number

c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.

d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the EMX, you can have that script automatically run or stop in response to a specific event.

For instructions on creating or loading a Lua script into this product, see *Lua Scripts* (on page 255).

▶ **To automatically start or stop a Lua script:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Start/stop Lua script" from the Action list.

3. In the Operation field, select Start Script or Stop Script.

4. In the Script field, select the script that you want it to be started or stopped when an event occurs.

- No script is available if you have not created or loaded it into the EMX.

5. To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.

   a. Click ![Add argument] .

   b. Type the key and value.

   c. Repeat the same steps to enter more arguments as needed.

      - To remove any existing argument, click ![-] adjacent to it.

Switch LHX/SHX

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See *Miscellaneous* (on page 260).

Use this action to switch the LHX/SHX on or off when, for example, temperature thresholds are reached.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action] .
2. Select "Switch LHX/SHX" from the Action list.
3. In the Operation field, select Turn LHX/SHX On or Turn LHX/SHX Off.
4. In the Available LHX/SHX field, select the LHX/SHX device to be turned on or off. To select all available LHX/SHX devices, click Select All.
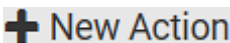
   To remove any LHX/SHX device from the Selected LHX/SHX field, click that device's ![x]. To remove all devices, click Deselect All.

Switch Peripheral Actuator

If you have any actuator connected to the EMX, you can set up the EMX so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

Note: For information on connecting actuators, see **DX Sensor Packages** *(on page 51).*

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action] .
2. Select "Switch peripheral actuator" from the Action list.

3. In the Operation field, select an operation for the selected actuator(s).

    ▪   Turn On: Turns on the selected actuator(s).

    ▪   Turn Off: Turns off the selected actuator(s).

4. To select the actuator(s) where this action will be applied, select them one by one from the Available Actuators list.

    ▪   To add all actuators, click Select All.

5. To remove any selected actuator from the Selected Actuators field, click that actuator's ✖.

    ▪   To remove all actuators, click Deselect All.

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

The EMX may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log. See *Viewing or Clearing the Local Event Log* (on page 268).

▶   **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select "Syslog message" from the Action list.

3. In the Syslog Server field, specify the IP address to which the syslog is forwarded.

4. In the Transport Protocol field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	▪ In the UDP Port field, type an appropriate port number. Default is 514. ▪ Select the "Legacy BSD Syslog Protocol" checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the TCP Port field.

Transport protocols	Next steps

TCP+TLS	A TLS certificate is required. Do the following:
	
	a. Type an appropriate port number in the "TCP Port" field. Default is 6514.
	
	b. In the CA Certificate field, click ![Browse...] to select a TLS certificate. After installing the certificate, you may:
	
	  ▪ Click Show to view its contents.
	  ▪ Click Remove to delete it if it is inappropriate.
	
	c. Determine whether to select the "Allow expired and not yet valid certificates" checkbox.
	
	  ▪ To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox.
	
	  ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

Scheduling an Action

An action can be regularly performed at a preset time interval instead of being triggered by a specific event. For example, you can make the EMX report the reading or state of a specific sensor regularly by scheduling the "Send Sensor Report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

If the needed action is not available yet, create it first. See *Available Actions* (on page 219).

▶ **Operation:**

1. Choose Device Settings > Event Rules > **✚ New Scheduled Action**.

2. To select any action(s), select them one by one from the Available Actions list.

  ▪ To select all available actions, click Select All.

3. To remove any action(s) from the Selected Actions field, click that action's ✖.

- To remove all actions, click Deselect All.

4. Select the desired frequency in the Execution Time field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	Type values or click . The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ▪ Days range from Sunday to Saturday. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ▪ The dates range from 1 to 31. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.

Execution time	Frequency settings
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Day of month - 1 to 31. ▪ Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

An example of the scheduled action is available in the section titled *Send Sensor Report Example* (on page 238).

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

▶ **Steps:**

1. Click ✚ New Action to create a 'Send email' action that sends an email to the desired recipient(s). For details, see *Send Email* (on page 226).

   ▪ In this example, this action is named *Email a Sensor Report*.
   ▪ If intended, you can customize the email messages in this action.

2. Click ✚ New Action to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action. For details, see *Send Sensor Report* (on page 227).

   ▪ In this example, this action is named *Send Temperature Sensor Readings*.
   ▪ You can specify more than one temperature sensor as needed in this action.

3. Click ✚ New Scheduled Action to create a timer for performing the 'Send Temperature Sensor Readings' action hourly. For details, see *Scheduling an Action* (on page 235).

   ▪ In this example, the timer is named *Hourly Temperature Sensor Reports*.
   ▪ To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.

Then the EMX will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the EMX to stop sending the temperature report, simply deselect the Enabled checkbox in the timer.

Email and SMS Message Placeholders

Actions of "Send email" and "Send SMS message" allow you to customize event messages. See *Send Email* (on page 226) or *Send SMS Message* (on page 229).

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

To make the Event Context Information disappear, click anywhere outside its window.

Following are placeholders that can be used in custom messages.

Placeholder	Definition
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on

Placeholder	Definition
[DEVICENAME]	The name of the device, the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[EXTSENSOR]	The peripheral device identifier
[IFNAME]	The human readable name of a network interface
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[MONITOREDHOST]	The name or IP address of a monitored host
[OLDVERSION]	The firmware version the device is being upgraded from
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The phone number an SMS was sent to
[PLSENSORNAME]	The Power Logic Device sensor name
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[RADIUSERRORDESC]	A Radius error occurred
[ROMCODE]	The rom code of an attached peripheral device
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to

Placeholder	Definition
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SysContact as configured for SNMP
[SYSLOCATION]	SysLocation as configured for SNMP
[SYSNAME]	SysName as configured for SNMP
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[UMTARGETROLE]	The name of a user management role, an action was applied on
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. Besides, you cannot delete built-in rules and actions. See **Built-in Rules and Rule Configuration** *(on page 205) or* **Available Actions** *(on page 219).*

▶ **To edit or delete an event rule, action or scheduled action:**

1. Choose Device Settings > Event Rules.
2. Click the desired one in the list of rules, actions or scheduled actions. Its setup page opens.
3. Perform the desired action.
   - To modify settings, make necessary changes and then click Save.
   - To delete it, click 🗑 Delete on the top-right corner. Then click Delete on the confirmation message.

Sample Event Rules

Sample Asset-Management-Level Event Rule

In this example, we want the EMX to record in the internal log when the network link is up to 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 the EMX device, and we want the EMX to respond to the event related to physical connections and/or disconnections from the network.
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 Asset-Management-Level Event Rule

In this example, we want the EMX to record the connection and disconnection events of a specific asset tag in the internal log. The event rule is set like this:

- Event: Asset Management > Feature Port 1 > Rack Unit > Index 3 > Tag Connected
- Trigger condition: Both
- Actions: System Event Log Action

▶ **To create the above event rule:**

1. Select "Asset Management" in the Event field to indicate we are specifying an event regarding the asset strips and/or tags.
2. If you are using EMX2-888, it is necessary to select a Feature port number. Select "Feature Port 1" from the submenu because the desired asset tag is attached to the asset strip connected to Feature Port 1.
3. Select "Rack Unit" for events related to rack units (tag ports) of an asset strip.
4. Select "Index 3" becasue the desired asset tag is connected to the tag port #3 of the asset strip.

5. Select "Tag Connected" as the events we want to record are related to physical tag connections or disconnections.

6. Select the Both radio button since we want both connection and disconnection actions to be recorded when either event occurs.

7. 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 to send a notification email when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

▶ **Step 1: create a new action for sending an email**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. In this illustration, assign the name "Send a Notification" to the new action.

3. In the Action field, select "Send email."

4. In the Recipient Email Addresses field, type one or multiple recipients' email addresses.

5. (Optional) Specify the SMTP settings and custom log message if needed.

6. Click Create to finish the creation.

After the new action is created, follow the procedure below to create an event rule that sends a notification email when the contact closure sensor enters the alarmed state. This event rule involves the following:

• Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On

• Trigger condition: Alarmed

• Action: Send a Notification

▶ **Step 2: create the contact closure-triggered email event rule**

1. Click ➕ New Rule on the Event Rules page.

2. In this illustration, assign the name "Contact Closure Triggered Email" to the new rule.

3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.

4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

Note: ID numbers of all sensors/actuators are available on the Peripherals page. See **Peripherals** *(on page 101).*

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.

6. Select "Alarmed" since we want the EMX to respond when the selected contact closure sensor changes its state related to the "alarmed" state.

7. In the "Trigger condition" field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.

8. Select "Send a Notification" from the Available Actions list.

A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the EMX keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

Example 1

This example illustrates an event rule which continuously causes the EMX to send out email messages.

Event selected	Action included
Device > Sending SMTP message failed	Send email

Example 2

This example illustrates an event rule which continuously causes the EMX to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

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 *"To De-assert" and Deassertion Hysteresis* (on page 528).

Raritan.
A brand of Legrand

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 EMX internal sensors are measured every 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 the log gets overwritten.

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 device's SNMP agent must be enabled for this feature to work. See **Enabling and Configuring SNMP** *(on page 284). In addition, using an NTP time server ensures accurately time-stamped measurements.*

By default, data logging is enabled. You must have the "Administrator Privileges" or "Change EMD Configuration" permissions to change the setting.

▶ **To configure the data logging feature:**

1. Choose Device Settings > Data Logging.
2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.

   Tip: Type a large number in this field when there are a large number of environmental sensors connected. This is because the sensor update interval becomes longer. See **Information about Update Interval** *(on page 246).*

4. Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.
   - You can also click the topmost checkbox labeled "Logging Enabled" in the header row of each section to select all sensors of the same type.

- If any section's number of sensors exceeds 35, the remaining sensors are listed on next page(s). If so, a pagination bar similar to the following diagram displays in this section, which you can click any button to switch between pages.

| First | Previous | 1 | 2 | 3 | 4 | 5 | ... | Next | Last |

5. Click Save. This button is located at the bottom of the page.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the EMX, it is NOT recommended to do so.

Information about Update Interval

Though the environmental sensors are measured per second, their readings may not be updated per second. The update interval varies depending on the total number of environmental sensors connected to the EMX and the sensor type. The more the environmental sensors are connected, the longer the update interval is. It is strongly recommended to type a larger value in the Measurements Per Log Entry field when there are a lot of environmental sensors connected. See *Setting Data Logging* (on page 245).

Raritan environmental sensors can be divided into two categories according to the update interval of the sensor reading or sensor state.

- *Normal type*: Sensor readings or states are updated at a longer interval, which ranges 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 at a shorter interval, which is less than or equal to 3 seconds. Raritan contact closure sensors belong to this type.

Configuring Data Push Settings

You can push the sensor or asset strip data to a remote server for data synchronization. The data will be sent in JSON format using HTTP POST requests. You need to set up the destination and authentication for data push on the EMX.

For instructions on connecting asset strips, see *Connecting Asset Management Strips* (on page 25).

After configuring the destination and authentication settings, do either or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action. See *Event Rules and Actions* (on page 204).

▶ **To configure data push settings:**

1. Choose Device Settings > Data Push.
2. To specify a destination, click New Destination.
3. Do the following to set up the URL field.

   a. Click to select *http* or *https*.

   b. Type the URL or host name in the accompanying text box.

4. If selecting https, a CA certificate is required for making the connection. Click Browse… to install it. Then you can:

   ▪ Click Show to view the certificate's content.

   ▪ Click Remove to delete the installed certificate if it is inappropriate.

5. If the destination server requires authentication, select the Use Authentication checkbox, and enter the following data.

   ▪ User name

   ▪ Password

6. In the Entry Type field, determine the data that will be transmitted.

   ▪ Asset management tag list: Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes those on blade extension strips, if any.

- Asset management log: Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.

- Sensor log: Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page. See *Setting Data Logging* (on page 245).

7. If "Asset management tag list" is selected in the above step, specify the asset strip(s) whose information to send. For EMX with only one FEATURE port, only one asset strip is available.

- To specify the asset strip(s), select them one by one from the Available AMS Ports list. Or click Select All to add all.

- To remove the asset strip(s), click that asset strip's ![x] in the Selected AMS Ports field. Or click Deselect All to remove all.

8. Click Create.

9. Repeat the same steps for additional destinations.

▶ **To modify or delete data push settings:**

1. On the Data Push page, click the one you want in the list.

2. Perform either action below.

- To modify settings, make necessary changes and then click Save.

- To delete it, click ![Delete], and then confirm it on the confirmation message.

Monitoring 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.

EMX can monitor the accessibility of any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

Tip: To make the EMX automatically log, send notifications or perform other actions for any server monitoring events, you can create event rules. See **Event Rules and Actions** *(on page 204). An example is available in* **Example: Ping Monitoring and SNMP Notifications** *(on page 251).*

▶ **To add IT equipment for ping monitoring:**

1. Choose Device Settings > Server Reachability.
2. Click ➕ **Monitor New Server**.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time 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 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).

Field	Description
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the EMX resumes pinging after the monitored equipment is declared "Unreachable." Valid range is 1 to 1200 (seconds).
Number of consecutive failures before disabling feature (0 = unlimited)	The number of times the monitored equipment is declared "Unreachable" consecutively before the EMX disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click Create.

6. To add more IT devices, repeat the same steps.

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before the EMX can declare that the monitored device is reachable or unreachable.

▶ **To check the server monitoring states and results:**

1. After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.

2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.

3. The column labeled "Status" indicates the accessibility of each monitored equipment.

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

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

▶ **To modify or delete any monitored IT device:**

1. Choose Device Settings > Server Reachability.
2. Click the desired one in the list.
3. Perform the desired action.
   - To modify settings, make necessary changes and then click Save. For information on each field, see *Monitoring Server Accessibility* (on page 249).
   - To delete it, click ![trash icon] on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your EMX to make sure that PDU is properly operating all the time, and the EMX must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your EMX and the monitored PDU.

This requires the following two steps.

▶ **Step 1: Set up the ping monitoring for the target PDU**

1. Choose Device Settings > Server Reachability.
2. Click ![plus icon] **Monitor New Server**.
3. Ensure the "Enable ping monitoring for this server" checkbox is selected.
4. Enter the data shown below.
   - Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

   - To make the EMX declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3

Field	Data entered
Wait time after successful ping	5

- To make the EMX declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

- To make the EMX stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the EMX will re-ping the target PDU, enter the following data.

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

▶ **Step 2: Create an event rule to send SNMP notifications for the target PDU**

1. Choose Device Settings > Event Rules.

2. Click ➕ New Rule.

3. Select the Enabled checkbox to enable this new rule.

4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the EMX react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Editing or Deleting a Rule/Action** *(on page 241).*

Configuring the Serial Port

You can change the bit rate of the serial port labeled CONSOLE / MODEM on the EMX. The default bit rate for both console and modem operation is 115200 bps.

The EMX supports using the following devices via the serial interface:

- A computer or Raritan KVM product for console management.
- An analog modem for remote dial-in and access to the CLI.
- A GSM modem for sending out SMS messages to a cellular phone.

Bit-rate adjustment may be necessary. Change the bit rate before connecting the supported device to the EMX through the serial port, or there are communication problems.

Note: The serial port bit-rate change is required when the EMX works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

You can set diverse bit-rate settings for console and modem operations. Usually the EMX can detect the device type, and automatically apply the preset bit rate.

The EMX will indicate the detected device in the Port State section of the Serial Port page. For example, if an analog modem is detected, the Port State section looks similar to the following.

To configure serial port or modem settings, choose Device Settings > Serial Port.

▶ **To change the serial port baud rate settings:**

1. Click the "Connected device" field to make the serial port enter an appropriate state.

Options	Description
Automatic detection	The EMX automatically detects the type of the device connected to the serial port. Select this option unless your EMX cannot correctly detect the device type.

Options	Description
Force console	The EMX attempts to recognize that the connected device is set for the console mode.
Force analog modem	The EMX attempts to recognize that the connected device is an analog modem.
Force GSM modem	The EMX attempts to recognize that the connected device is a GSM modem.

2. Click the Console Baud Rate field to select the baud rate intended for console management.

   Note: For a serial RS-232 or USB connection between a computer and the EMX, leave it at the default (115200 bps).

3. Click the Modem Baud Rate field to select the baud rate for the modem connected to the EMX.

The following modem settings/fields appear in the web interface after the EMX detects the connection of an analog or GSM modem.

▶ **To configure the analog modem:**

1. Select the "Answer incoming calls" checkbox to enable the remote access via a modem. Otherwise, deselect it.

2. Type a value in the "Number of rings before answering" field to determine the number of rings the EMX must wait before answering the call.

▶ **To configure the GSM modem:**

1. Enter the SIM PIN code.

2. Select the "Use custom SMS center number" checkbox if a custom SMS center will be used.

   ▪ Enter the SMS center number in the "SMS center" field.

3. If needed, click Advanced Information to view detailed information about the modem, SIM and mobile network.

4. To test whether the EMX can successfully send out SMS messages with the modem settings:

   a. Enter the number of the recipient's phone in the Recipient Phone field.

   b. Click Send SMS Test to send a test SMS message.

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the EMX to control its behaviors.

Raritan also provides some Lua scripts examples, which you can load as needed.

Note: Not all Raritan Lua script examples can apply to your EMX model. You should read each example's introduction before applying them.
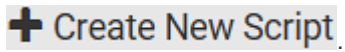
You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the EMX.

Tip: If you can no longer enter or load a new script after reaching the upper limit, you can either delete any existing script or simply modify/replace an existing script's codes. See **Modifying or Deleting a Script** *(on page 259).*

▶ **To write or load a Lua script:**

1. Choose Device Settings > Lua Scripts > .
2. Type a name for this script. Its length ranges between 1 to 63 characters.

   The name must contain the following characters only.
   - Alphanumeric characters
   - Underscore (_)
   - Minus (-)
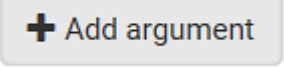
   Note: Spaces are NOT permitted.

3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the EMX reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.

   a. Click .

b. Type the key and value.

c. Repeat the same steps to enter more arguments as needed.

> ▪ To remove any existing argument, click [−] adjacent to it.

Note: Default arguments are overridden by the new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule. See **Manually Starting or Stopping a Script** *(on page 257) or* **Start or Stop a Lua Script** *(on page 232).*

5. In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

> ▪ To write a Lua script, type the codes in the Source Code section.

Source Code

📥 Load Local File	📖 Load Example

☑ Enable Syntax Highlighting

```
-- Type your codes here.
```

> ▪ To load an existing Lua script file, click Load Local File.
> ▪ To use one of Raritan's Lua script examples, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

6. If you chose to load a script or Raritan's example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.

7. Click Create.

Raritan.
A brand of Legrand

▶ **Next steps:**

- To execute the newly-added script now, click ▶ Start, or

  click ⋮ > Start with Arguments. See *Manually Starting or Stopping a Script* (on page 257).

- To add more scripts, return to the scripts list by clicking "Lua Scripts" again in the *Menu* (on page 91), and then repeat the above steps.

Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.
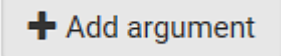
Tip: To have the EMX automatically start or stop a script in response to an event, create an event rule. See **Event Rules and Actions** *(on page 204) and* **Start or Stop a Lua Script** *(on page 232).*

▶ **To manually start a script:**

1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.

Lua Scripts			➕ Create New Script
Name	**State**	**Autostart**	**Restart**
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

2. Click the desired script whose state is either 'Terminated' or 'New.' For details, see *Checking Lua Scripts States* (on page 259).

3. To start with default arguments, click ▶ Start.

   To start with new arguments, click ⋮ > Start with Arguments. Newly-assigned arguments will override default ones.

4. If you chose "Start with Arguments" in the above step, enter the key and value in the Start Lua Script dialog.

- Click **+ Add argument** if needing additional arguments.

Start Lua Script

Key	Value	
		–

+ Add Argument

Cancel   Start

5. Click Start.

6. The script output will be shown in the Script Output section.

- If needed, click **◇ Clear** to delete the existing output data.

▶ **To manually stop a script:**

1. Choose Device Settings > Lua Scripts.

2. Click the desired script whose state is either 'Running' or 'Restarting.' For details, see *Checking Lua Scripts States* (on page 259).

3. Click **■ Stop** on the top-right corner.

4. Click Stop on the confirmation message.

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.

Lua Scripts			✚ Create New Script
Name	**State**	**Autostart**	**Restart**
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

▶ **State:**

Four script states are available.

- *New*: The script is never executed since the device boot.
- *Running*: The script is currently being executed.
- *Terminated*: The script was once executed, but stops now.
- *Restarting*: The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

▶ **Autostart:**

This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled. See *Writing or Loading a Lua Script* (on page 255).

▶ **Restart:**

This column indicates whether the checkbox labeled "Restart after termination" is enabled. See *Writing or Loading a Lua Script* (on page 255).

Modifying or Deleting a Script

You can edit an existing script's codes or even replace it with a new script. Or you can simply remove a unnecessary script from the EMX.

▶ **To modify or replace a script:**

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.

3. Click > Edit Script.

4. Make changes to the information shown, except for the script's name, which cannot be revised.

  ▪ To replace the current script, click Load Local File or Load Example to select a new script.

▶ **To delete a script:**

1. Choose Device Settings > Lua Scripts.

2. Click the desired one in the scripts list.

3. Click > Delete.

4. Click Delete on the confirmation message.

Miscellaneous

By default, the support for Schroff LHX/SHX heat exchangers is disabled.

Support needs to be enabled for the LHX/SHX information to appear in the EMX web interface. Besides, Schroff LHX/SHX support must be enabled in order for the LHX-MIB to be accessible through SNMP.

To enable this feature, choose Device Settings > Miscellaneous.

▶ **To enable the support for Schroff LHX/SHX:**

1. Select the Schroff LHX/SHX Support checkbox.

2. Click Save in the *Features* section.

3. Click Apply on the confirmation message.

4. The EMX reboots.

Maintenance

Click 'Maintenance' in the *Menu* (on page 91), and the following submenu displays.

Submenu command	Refer to...
Device Information	*Device Information* (on page 262)
Connected Users	*Viewing Connected Users* (on page 267)
Event Log	*Viewing or Clearing the Local Event Log* (on page 268)
Update Firmware	*Updating the EMX Firmware* (on page 269)
Firmware History	*Viewing Firmware Update History* (on page 271)
Bulk Configuration	*Bulk Configuration* (on page 272)

Submenu command	Refer to...
Backup/Restore	*Backup and Restore of Device Settings* (on page 274)
Network Diagnostic	*Network Diagnostics* (on page 275)
Download Diagnostic	*Downloading Diagnostic Information* (on page 276)
Unit Reset	▪ *Rebooting the EMX Device* (on page 277) ▪ *Resetting All Settings to Factory Defaults* (on page 277)
About iPDU	*Retrieving Software Packages Information* (on page 278)

Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your EMX.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

▶ **To display device information:**

1. Choose Maintenance > Device Information.

2. Click the desired section's title bar to show that section's information. For example, click the Network section.

The number of available sections is model dependent.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so on. Note that the download link of LHX-MIB is available only after enabling the Schroff LHX/SHX support. See *Miscellaneous* (on page 260).
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. This tab also indicates whether the EMX is part of a cascading configuration. See *Identifying Cascaded Devices* (on page 263).
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected environmental sensor packages.
Asset Management	Each asset strip's ID, boot version, application version and protocol version.

Identifying Cascaded Devices

For information on how to cascade EMX devices, see *Cascading Multiple EMX Devices for Sharing Ethernet Connectivity* (on page 21).

This section explains how to identify a cascaded device on the Device Information page.

Note: For more information on the USB-cascading configuration, see the Cascading Guide, *which is available from Raritan website's* Support page (http://www.raritan.com/support/).

▶ **To identify the USB-cascading status:**

1. Choose Maintenance > Device Information.
2. Click the Network title bar.

▪ If the information shown on this page does not match the latest status, press F5 to reload it.

▶ **Cascading information in the Bridging mode:**

• The Common section contains two read-only fields for indicating the cascading status. Note that the cascading position is NOT available in the bridging mode.

Fields	Description
Port Forwarding	Indicates the Port Forwarding is disabled. See *Setting the Cascading Mode* (on page 162).
BRIDGE section	Indicates the device is in the bridging mode and its IP address.

▶ **Cascading information in the Port Forwarding mode:**

• The Common section contains three read-only fields for indicating the cascading status.

Fields	Description
Port Forwarding	Indicates the Port Forwarding is enabled. See *Setting the Cascading Mode* (on page 162).

Fields	Description
Cascade Position	Indicates the position of the EMX in the cascading configuration. ▪ 0 (zero) represents the master device. ▪ A non-zero number represents a slave device. 1 is Slave 1, 2 is Slave 2, 3 is Slave 3 and so on.
Cascaded Device Connected	Indicates whether a slave device is detected on the USB-A or Ethernet port. ▪ yes: Connection to a slave device is detected. ▪ no: NO connection to a slave device is detected.

▪ A master device shows *0* (zero) in the Cascade Position field and *yes* in the Cascaded Device Connected field.

Network

Common

DNS Servers	192.168.80.249, 192.168.80.19
DNS Suffixes	rgp.raritan.com.
DNS Resolver Preference	IPv6 Address
IPv4 Routes	192.168.84.0/24 dev ETH1 default via 192.168.84.254 (ETH1)
IPv6 Routes	none
Port Forwarding	enabled
Cascade Position	0 (Master)
Cascaded Device Connected	yes

▪ A slave device in the middle position shows a non-zero number which indicates its exact position in the Cascade Position field and *yes* in the Cascaded Device Connected field.

The following diagram shows 1, indicating it is the first slave - Slave 1.

Network	⌃
Common	
DNS Servers	192.168.80.249, 192.168.80.19
DNS Suffixes	rgp.raritan.com.
DNS Resolver Preference	IPv6 Address
Port Forwarding	enabled
Cascade Position	**1 (Slave)**
Cascaded Device Connected	**yes**

▪ The final slave device shows a non-zero number which indicates its position in the Cascade Position field and *no* in the Cascaded Device Connected field.

The following diagram shows 2, indicating it is the second slave - Slave 2. The Cascaded Device Connected field shows *no*, indicating that it is the final one in the chain.

Network	⌃
Common	
DNS Servers	192.168.80.249, 192.168.80.19
DNS Suffixes	rgp.raritan.com.
DNS Resolver Preference	IPv6 Address
Port Forwarding	enabled
Cascade Position	**2 (Slave)**
Cascaded Device Connected	**no**

● For a list of port numbers required for accessing each cascaded device in the port forwarding mode, click the Port Forwarding title bar on the same page.

Port Forwarding	⌄

Viewing Connected Users

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

▶ **To view and manage connected users:**

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

   If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

Column	Description
User name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <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 web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user is connected to the CLI. - Serial: The local connection, such as the serial RS-232 or USB connection. - SSH: The SSH connection. - Telnet: The Telnet connection. ▪ Webcam Live Preview: Refers to the live webcame image sessions. See below.
Idle Time	The length of time for which a user remains idle.

2. To disconnect any user, click the corresponding ⬛ Disconnect .
   a. Click Disconnect on the confirmation message.
   b. The disconnected user is forced to log out.

▶ **If there are live webcam sessions:**

All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window of the sender and two sessions of the remote recipients, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all of the three sessions of a specific URL.

The IP address refers to the IP address of the host where the Primary Standalone Live Preview window exists, NOT the IP address of the other two associated sessions.

For more webcam information, see *Webcam Management* (on page 279).

Viewing or Clearing the Local Event Log

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

You can view over 2000 historical events that occurred on the EMX in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

▶ **To display the local log:**

1. Choose Maintenance > Event Log.

   Each event entry consists of:
   - ID number of the event
   - Date and time of the event
   - Event type
   - A description of the event

2. To view a specific type of events only, select the desired event type in the Filter Event Class field.
   - To refresh the data, press F5 as needed.

3. To go to other pages of the log, click the pagination bar at the bottom of the page.
   - If there are more than 5 pages and the page numbers displayed in the bar does not show the desired one, click [...] to have it show the next or previous five page numbers, if available.

First	Previous	1	2	3	4	5	...	Next	Last

4. If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

▶ **To clear the local log:**

1. Click on the top-right corner.

2. Click Clear Log on the confirmation message.

Updating the EMX Firmware

Firmware files are available on Raritan website's *Support page* (*http://www.raritan.com/support/*).

You must be the administrator or a user with the Firmware Update permission to update the EMX firmware.
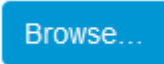
Before starting the upgrade, read the release notes downloaded from the Raritan website's *Support page* (*http://www.raritan.com/support/*). If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Note that firmware upgrade via some mobile devices, such as iPad, requires the use of a file manager app.

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

Important: If you are upgrading an existing USB-cascading chain from a firmware version older than 3.3.10, you must follow specific guidelines to avoid networking issues. See *Upgrade Guidelines for Existing USB-Cascading Chains* (on page 270).

▶ **To update the firmware:**

1. Choose Maintenance > Update Firmware.

2. Click to select an appropriate firmware file.

3. Click Upload. A progress bar appears to indicate the upload process.

4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.

   ▪ If anything is incorrect, click Discard Upload.

5. To proceed with the update, click Update Firmware.

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

6. During the firmware update:

   ▪ A progress bar appears on the web interface, indicating the update status.

- The front panel display shows the firmware upgrade message. Three digits are displayed: FUP. See *Overview of the LCD Display* (on page 69).
- No users can successfully log in to the EMX.
- Other users' operation, if any, is forced to suspend.

7. When the update is complete, the EMX resets, and the Login page re-appears.
  - Other logged-in users are logged out when the firmware update is complete.

Important: If you are using the EMX with an SNMP manager, download its MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using. See *Using SNMP* **(on page 284).**

▶ **Alternatives:**

To use a different method to update the firmware, refer to:

- *Firmware Update via SCP* (on page 421)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 442)
- *Firmware Upgrade via USB* (on page 440)

Upgrade Guidelines for Existing USB-Cascading Chains

- Firmware version 3.3.10 is NOT compatible with old firmware versions in terms of the USB-cascading feature so all devices in a chain must be running version 3.3.10 or later. Otherwise, a networking issue occurs.

  Alternative: You can also choose to have an existing USB-cascading chain keep on running the old firmware without upgrading any device to 3.3.10 or later.

- When upgrading an existing USB-cascading chain from **any version prior to 3.3.10**, the upgrade must start from the last slave device, then the second to last, the third to last, and so on until the master device. Any upgrade without following this sequence results in the networking failure of some cascaded devices.

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/7/10 and Linux. In addition, an appropriate EMX firmware file is required in the recovery procedure.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the EMX. It remains available even though you perform a device reboot or any firmware update.

▶ **To view the firmware update history:**

1. Choose Maintenance > Firmware History.

    Each firmware update event consists of:

    ▪ Update date and time

    ▪ Previous firmware version

    ▪ Update firmware version

    ▪ Update result

2. If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 94).

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured EMX device to your computer. You can use this configuration file to copy common settings to other EMX devices of the same model and firmware version.

Note that **NO device-specific data is saved** to the bulk configuration file, such as environmental sensors or certain network settings. For a list of device-specific settings that are *not* saved, see *Device-Specific Settings NOT Included* (on page 273).

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.

Tip: To back up or restore "all" settings of a particular EMX device, use the Backup/Restore feature instead. See **Backup and Restore of Device Settings** *(on page 274).*

▶ **To save a bulk configuration file:**

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

1. Log in to the EMX whose settings you want to copy.
2. Choose Maintenance > Bulk Configuration.
3. Click Download Bulk Configuration.
4. When prompted to open or save the configuration file, click Save.
   - The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

▶ **To perform bulk configuration:**

You must have the Administrator Privileges to upload the configuration.

1. Log in to another EMX of the same model running the same firmware.
2. Choose Maintenance > Bulk Configuration.
3. Click [Browse...] to select the configuration file.
4. Click 'Upload & Restore Bulk Configuration' to copy it.
5. A message appears, prompting you to confirm the operation and enter the admin password.

Enter the admin password, and click Restore.

6. Wait until the EMX device resets and the login page re-appears.

Note: On startup, the EMX performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

▶ **The last configuration-copying record:**

If you once copied any bulk configuration or device backup file to the EMX, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

▶ **Alternatives:**

To use a different method to perform bulk configuration, refer to:

*   *Bulk Configuration via SCP* (on page 422)
*   *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 442)
*   *Configuration or Firmware Upgrade with a USB Drive* (on page 430)

Device-Specific Settings NOT Included

The settings saved in the bulk configuration file include user and role configurations, thresholds, event rules, security settings, date/time and so on.

Note: 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.

The bulk configuration file does NOT contain device-specific information, including:

*   Device name
*   SNMP system name, contact and location
*   Network settings (IP address, gateway, netmask and so on)
*   Device logs
*   Names, states and values of environmental sensors and actuators
*   TLS certificate
*   Server monitoring entries
*   Asset strip names and rack unit names

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and network settings. To back up or restore a EMX device's settings, you should perform the Backup/Restore feature.

All EMX information is captured in the XML backup file except for the device logs and TLS certificate.

Note: To perform bulk configuration among multiple EMX devices, use the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 272).*

► **To download a backup EMX XML file:**

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

1. Choose Maintenance > Backup/Restore.
2. Click Download Device Settings. Save the file to your computer.
   - The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

► **To restore the EMX using a backup XML file:**

You must have the Administrator Privileges to restore the device settings.

1. Choose Maintenance > Backup/Restore.
2. Click [Browse…] to select the backup file.
3. Click 'Upload & Restore Device Settings' to upload the file.
   - A message appears, prompting you to confirm the operation and enter the admin password.
4. Enter the admin password, then click Restore.
5. Wait until the EMX device resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, the EMX performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

▶ **The last configuration-copying record:**

If you once copied any bulk configuration or device backup file to the EMX, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last Restore: 2/24/2017, 6:05:53 PM, Status: OK

▶ **Alternative:**

To use a different method to perform backup/restore, refer to:

- *Backup and Restore via SCP* (on page 423)

Network Diagnostics

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

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 416).*

Choose Maintenance > Network Diagnostics, and then perform any function below.

▶ **Ping:**

1. Type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

▶ **Trace Route:**

1. Type values in the following fields.

Field/setting	Description
Host Name	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP Packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

▶ **List TCP Connections:**

1. Click the List TCP Connections title bar to show the list.

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 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 or Unrestricted View Privileges.

▶ **To retrieve a diagnostic file:**

1. Choose Maintenance > Download Diagnostic >

   Download Diagnostic .
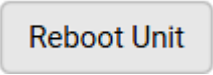
2. The system prompts you to save or open the file. Click Save.
3. E-mail this file as instructed by Raritan Technical Support.

Rebooting the EMX Device

You can remotely reboot the EMX device via the web interface.

> Warning: Rebooting the EMX deletes all webcam snapshots that are saved on the EMX locally. See *Viewing Saved Snapshots and Managing Storage* (on page 282).

▶ **To reboot the device:**

1. Choose Maintenance > Unit Reset > .
2. Click Reboot to restart 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 restart is complete, the login page opens.

Note: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the EMX to factory defaults.

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. Only firmware upgrade history is retained.

► **To reset the device to factory defaults:**

1. Choose Maintenance > Unit Reset >

   Reset to Factory Defaults .

   Factory Reset

   Do you really want to reset the device to factory defaults?
   Saying yes will clear all settings, including the network
   setup.

   Cancel   Factory Reset

2. Click Factory Reset to reset the EMX to factory defaults.

3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.

4. When the reset is complete, the login page opens.

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

► **Alternative:**

There are two more methods to reset the device to factory defaults.

- Use the "mechanical" reset button
- Perform the CLI command

For details, see *Resetting to Factory Defaults* (on page 416).

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the EMX device through the web interface.

► **To retrieve the embedded software packages information:**

1. Choose Maintenance > About iPDU. A list of open source packages is displayed.

2. You can click any link to access related information or download any software package.

Webcam Management

The webcam-related menu items appear only when there are webcam(s) connected to the EMX. See *Connecting a Logitech Webcam* (on page 59).

With a Logitech® webcam connected to the EMX, you can visually monitor the environment around the EMX via snapshots or videos captured by the webcam.

- To view snapshots and videos, you need the permission of either "Change Webcam Configuration" or "View Webcam Snapshots and Configuration."
- To configure webcam settings, you need the "Change Webcam Configuration" permission.

If your webcam supports audio transmission, audio will be available in live videos.

You can manually store snapshots taken from the webcam onto the EMX or a remote server. See *Viewing Saved Snapshots and Managing Storage* (on page 282).

Links to snapshots or videos being captured by a webcam can be sent via email or instant message. See *Sending Snapshots or Videos in an Email or Instant Message* (on page 281).

You can create event rules to trigger emails containing snapshots from a webcam. See *Available Actions* (on page 219).

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

Configuring Webcams and Viewing Live Images

To configure the webcam or view live snapshot/video sessions, choose Webcam in the *Menu* (on page 91).

▶ **Live Preview:**

1. Click the Live Preview title bar to expand it.
2. The live snapshot/video session captured by the webcam is displayed.
   - The default is to show live snapshots. Interval time and the image captured time are displayed on the top of the image.
3. To save the current image, click Save Snapshot. See *Viewing Saved Snapshots and Managing Storage* (on page 282).

4. To have the live session also displayed in a Primary Standalone Live Preview window, click New Live Preview Window.

- You can send out this window's URL to share the live image with other users. See *Sending Snapshots or Videos in an Email or Instant Message* (on page 281).

5. To switch between snapshot and video modes, see the *Settings* section below.

- In the video mode, the number of frames to take per second (fps) and the captured time are displayed on the top of the image.

▶ **Image Controls:**

1. Click the Image Controls title bar to expand it.

2. Adjust the brightness, contrast and saturation by adjusting the corresponding slide bar.

- Or click "Set to Webcam Defaults" to restore all settings to this webcam's factory defaults.

▶ **Settings:**

1. Click Edit Settings.

2. Enter a name for the webcam. Up to 64 characters are supported.

3. Type the location information in each location field if needed. Up to 63 characters are supported.

4. Select a resolution for the webcam.

- If you connect two webcams to one USB-A port using a powered USB hub, set the resolution to 352x288 or lower for optimal performance.

5. Select the webcam mode.

- Video - the webcam enters the video mode. Set the Framerate (frames per second) rate.

- Snapshot - the webcam shows static images from the webcam. Set the "Time Between Snapshots" rate as measured in seconds.

6. Click Save. The changes made to the settings are applied to the live session. See the above *Live Preview* section.

Note: The settings changes do not apply to those images captured prior to the changes.

Sending Snapshots or Videos in an Email or Instant Message

Whenever you open a Primary Standalone Live Preview window, a unique URL is generated for this window session. A URL supports a maximum of three sessions. Therefore, you can email or instant message up to two persons this URL. Recipients can then click on the provided link and view live snapshots or videos simultaneously.

Tip: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window of the sender and two sessions of the remote recipients, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all of the three sessions of a specific URL. See **Viewing Connected Users** *(on page 267).*

For explanation of this topic, the message sender is User A and the two recipients are User B and C.

User C is able to access the snapshot or video image via the link in any of the following scenarios:

- The Primary Standalone Live Preview window remains open on User A's computer. If so, even though User A logs out of the web interface or the login session times out, the link remains available.
- Another recipient's live preview session based on the same URL remains open. That is, User B's session remains. If so, even though User A has closed the Primary Standalone Live Preview window, the link remains available.
- Neither User A's Primary Standalone Live Preview window nor User B's session based on the same URL remains open, but the idle timeout period has not expired yet since the last live preview window session was closed. For information on idle timeout, see *Configuring Login Settings* (on page 198).

Tip: When the idle timeout has not expired, the <webcam> user for that live preview URL remains shown on the Connected Users page.

Best Practice

As a best practice, User A should open the live snapshot or video session using a Primary Standalone Live Preview window and keep that window open at least until User C opens the live image session via the link.

Once User C opens the live session via the link, User A can close the Primary Standalone Live Preview window.

User C should let User A know that the link has been opened.

▶ **To send a snapshot or video link via email or instant message:**

1. Open the Webcam page by clicking it in the *Menu* (on page 91).

2. Click Live Preview > New Live Preview Window. The live snapshot or video in a standalone live preview window opens. See *Configuring Webcams and Viewing Live Images* (on page 279).

3. Copy the URL from the live preview window, and send it through an email or instant message application.

4. Leave the live preview window open until the recipient opens the snapshot or video via the link.

Viewing Saved Snapshots and Managing Storage

Once a snapshot is saved, it is stored locally on the EMX by default. For instructions on saving snapshots, see *Configuring Webcams and Viewing Live Images* (on page 279).

Up to 10 images can be stored onto the EMX at once. Unless snapshots are deleted manually, the oldest snapshot is automatically overridden by the newest one when the total of snapshots exceeds 10.

To save more than 10 snapshots, you must save the images on a Common Internet File System (CIFS)/Samba.

Snapshots are saved as JPG files, and named based on the sequential numbers, such as 1.jpg, 2.jpg, 3.jpg and so on.

> Warning: Rebooting the EMX deletes all webcam snapshots that are saved on the EMX locally. See *Viewing Saved Snapshots and Managing Storage* (on page 282).

To view saved images or configure the storage settings, choose Webcam Snapshots in the *Menu* (on page 91).

▶ **To view and manage saved images:**

1. Click the snapshot you want to view from the list.

   ▪ If the list of snapshots saved in the specified CIFS/Samba server exceeds one page, you can switch between available pages by clicking the pagination bar on the top.

   If there are more than 5 pages and the page numbers displayed in the bar does not show the desired one, click [...] to have it show the next or previous five page numbers, if available.

First	Previous	1	2	3	4	5	...	Next	Last

2. The selected snapshot as well as its information, such as captured time and resolution, is displayed on the same page.

3. If the latest saved snapshot is not listed yet, click ⋮ > Refresh on the top of the list.

4. To manually delete any images:

   a. Select the checkboxes of the images you want to remove.

      ▪ To select all images, select the top-most checkbox in the header row.

   b. On the top of the list, click ⋮ > Delete Selected.

   c. Click Delete on the confirmation message.

▶ **To configure the storage settings:**

1. Click ⋮ > Settings.

2. Click the Storage Type field to select the desired storage location and configure as needed.

Storage location	Description
Local	Local means the EMX. This is default.
CIFS/Samba	Snapshots will be saved on a Common Internet File System/Samba. Configure the following fields for this server: ▪ Server - the desired CIFS/Samba server ▪ Share/Folder - this is the share drive/folder ▪ Username - for server access ▪ Password - for server access

3. In the Capacity field, type values to determine the maximum number of snapshots that can be saved on the selected storage location.

4. Click Save.

Chapter 7   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 or informs 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 and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the EMX. By default the "read-only" mode of SNMP v1/v2c is enabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the EMX.

Important: You must download the SNMP MIB for your EMX to use with your SNMP manager. See *Downloading SNMP MIB* **(on page 287).**

▶ **To enable SNMP v1/v2c and/or v3 protocols:**

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.
   - If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission. See below.

   For details, see *Configuring SNMP Settings* (on page 172).

▶ **To configure users for SNMP v3 access:**

1. Choose User Management > Users.
2. Create or modify users to enable their SNMP v3 access permission.
   - If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

   For details, see *Creating Users* (on page 138).

▶ **To enable SNMP notifications:**

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, refer to:

   ▪ *SNMPv2c Notifications* (on page 285)

   ▪ *SNMPv3 Notifications* (on page 286)

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** *(on page 219).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.

4. Select SNMPv2c Trap or SNMPv2c Inform as the notification type.

5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the EMX and all SNMP management stations.

6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.
2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.
3. In the SNMP Notifications section, make sure the Enable SNMP Notifications checkbox is selected.
4. Select SNMPv3 Trap or SNMPv3 Inform as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of Retries	Specify the number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Security Level	Three types are available. ▪ noAuthNoPriv - neither authentication nor privacy protocols are needed. ▪ AuthNoPriv - only authentication is required. ▪ authPriv - both authentication and privacy protocols are required.

Field	Description
Authentication Protocol, Authentication Passphrase, Confirm Authentication Passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. ▪ Select the authentication protocol - MD5 or SHA ▪ Enter the authentication passphrase
Privacy Protocol, Privacy Passphrase, Confirm Privacy Passphrase	The three fields are available when the security level is set to authPriv. ▪ Select the Privacy Protocol - DES or AES ▪ Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your EMX.

You can download the MIBs from two different pages of the web interface.

▶ **MIB download via the SNMP page:**

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

Download MIBs ⌄

3. Select the desired MIB file to download.
   ▪ EMD-MIB: The SNMP MIB file for EMX power management.
   ▪ ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
   ▪ LHX-MIB: The SNMP MIB file for managing the LHX/SHX heat exchanger(s).
4. Click Save to save the file onto your computer.

▶ **MIB download via the Device Information page:**

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
   - EMD-MIB
   - ASSETMANAGEMENT-MIB
   - LHX MIB
3. Click Save to save the file onto your computer.

Note: LHX-MIB is available only after the LHX/SHX support has been enabled. See **Miscellaneous** *(on page 260).*

SNMP Gets and Sets

In addition to sending notifications, 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.

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 notification when certain parameters are exceeded. See *Sensor Threshold Settings* (on page 523) 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.

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (primaryNTPServerAddressType and primaryNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondaryNTPServerAddressType and secondaryNTPServerAddress)

Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, see **Setting the Time Zone** *(on page 350). For the web interface, see* **Setting the Date and Time** *(on page 201).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 8   Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a EMX device.

CLI commands are case sensitive.

In This Chapter

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 local 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 **Changing Telnet Settings** *(on page 175).*

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

If a security login agreement has been enabled, you must accept the agreement in order to complete the login. Users are authenticated first and the security banner is checked afterwards.

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 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 determine the COM port by choosing Control Panel > System > Hardware > Device Manager, and locating the "Dominion EMX Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the EMX. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive. Then you are prompted to enter a password.

   ```
   Username: admin
   Password: _
   ```

5. Type a password and press Enter. The password is case sensitive.

After properly entering the password, the # or > system prompt appears. See *Different CLI Modes and Prompts* (on page 294) in the User Guide for more information.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the EMX.

With SSH or Telnet

You can remotely log in to the command line interface (CLI) 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 *Configuring Network Services* (on page 170) in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as: █
```

3. Type a name and press Enter. The name is case sensitive.

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.

```
login as: admin
admin@192.168.84.88's password: █
```

4. Type a password and press Enter. The password is case sensitive.
5. After properly entering the password, the # or > system prompt appears. See *Different CLI Modes and Prompts* (on page 294) in the User Guide for more information.

Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was used to log in to this product's web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the EMX.

With an Analog Modem

The EMX supports remote access to the CLI via a connected analog modem. This feature is especially useful when the LAN access is not available.

▶ **To connect to the EMX via the modem:**

1. Make sure the EMX has an analog modem connected. See *Connecting an Analog Modem* (on page 60).
2. Make sure the computer you are using has an appropriate modem connected.
3. Launch a terminal emulation program, and configure its baud rate settings according to the baud rate set for the analog modem connected to the EMX. See *Configuring the Serial Port* (on page 253).
4. Type the following AT command to make a connection with the EMX.
   ATD<modem phone number>
5. The CLI login prompt appears after the connection is established successfully. Then type the user name and password to log in to the CLI.

▶ **To disconnect from the EMX:**

1. Return to the modem's command mode using the escape code +++.
2. After the OK prompt appears, type the following AT command to disconnect from the EMX.
   ATH

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 may 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 or user mode. In this mode, the prompt changes to **config:#** or **config:>** and you can change EMX device and network configurations. See *Entering Configuration Mode* (on page 319).
- Diagnostic Mode: You can enter the diagnostic mode from the administrator or user mode. In this mode, the prompt changes to **diag:#** or **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See *Entering Diagnostic Mode* (on page 417).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a EMX device over the local connection.

When accessing or upgrading multiple EMX devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

Help Command

The help (?) command shows a list of main CLI commands available for the current mode. This is helpful when you are not familiar with CLI commands.

▶ **Help command under the administrator mode:**

```
#          ?
```

▶ **Help command under the configuration mode:**

```
config:#    ?
```

▶ **Help command under the diagnostic mode:**

```
diag:#      ?
```

Press Enter after typing the help command, and a list of main commands for the current mode is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding the help command to the end of the queried command. See **Querying Available Parameters for a Command** *(on page 296).*

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) 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:**

```
#           show ?
```

▶ **To query available parameters for the "show user" command:**

```
#           show user ?
```

▶ **To query available network configuration parameters:**

```
config:#    network ?
```

▶ **To query available role configuration parameters:**

```
config:#    role ?
```

▶ **To query available parameters for the "role create" command:**

```
config:#    role create ?
```

Showing Information

You can use the show commands to view current settings or the status of the EMX device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, user profiles, 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. See **Different CLI Modes and Prompts** *(on page 294).*

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interface's duplex mode, and the wireless interface's status/settings.

```
#       show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

Tip: To show IPv4-only and IPv6-only configuration data, see **IPv4-Only or IPv6-Only Configuration** *(on page 298).*

```
#       show network ip common
```

To show the IP-related configuration of a specific network interface, use the following command.

```
#       show network ip interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the IP-related configuration of the ETHERNET interface.
wireless	Show the IP-related configuration of the WIRELESS interface.
bridge	Show the IP-related configuration of the BRIDGE interface.

Option	Description
all	Show the IP-related configuration of all interfaces.
	You can type the CLI command without the word 'all.' For example, *show network ip interface*.

IPv4-Only or IPv6-Only Configuration

To show IPv4-only configuration or IPv6-only configuration, use any of the following commands.

Tip: To show both IPv4 and IPv6 configuration data, see **IP Configuration** *(on page 297).*

▶ **To show all IPv4 configuration:**

```
#       show network ipv4 common
```

▶ **To show all IPv6 configuration:**

```
#       show network ipv6 common
```

▶ **To show the IPv4 configuration of a specific network interface:**

```
#       show network ipv4 interface <ETH>
```

▶ **To show the IPv6 configuration of a specific network interface:**

```
#       show network ipv6 interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the IPv4 or IPv6 configuration of the ETHERNET interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces. You can type the CLI command without the word 'all.' For example, *show network ipv4 interface*.

Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
#       show network interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Option	Description
ethernet	Show the ETHERNET interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.
all	Show the non-IP settings of all interfaces. You can type the CLI command without the word 'all.' For example, *show network interface*.

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
#       show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp*, *modbus* 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.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

Device Configuration

This command shows the EMX configuration, such as the device name, firmware version and model type.

```
#       show emd
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show emd details
```

Date and Time Settings

This command shows the current date and time settings on the EMX device.

```
#       show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show time details
```

Default Measurement Units

This command shows the default measurement units applied to the EMX web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
#       show user defaultPreferences
```

Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the EMX. See **Existing User Profiles** *(on page 308) for the preferred measurement units for a specific user.*

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
```

```
External sensor 3 ('Temperature 1')
Sensor type: Temperature
Reading:     31.8 deg C (normal)

Serial number:          AEI0950133
Description:            Not configured
Location:               X Not configured
                        Y Not configured
                        Z Not configured
Position:               Port 1
Using default thresholds: yes
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of 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 Peripherals page of the EMX web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A state 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, sensor position, and X, Y, and Z coordinates.

Note: DPX sensor packages do not provide chain position information.

Environmental Sensor Package Information

Different from the "`show externalsensors`" commands, which show the reading, status and configuration of an individual environmental sensor, the following command shows the information of all connected environmental sensor packages, each of which may contain more than one sensor or actuator.

```
#      show peripheralDevicePackages
```

Information similar to the following is displayed. An environmental sensor package is a peripheral device package.

```
Peripheral Device Package 1
Serial Number:    AEI7A00022
Package Type:     DPX-T1H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available

Peripheral Device Package 2
Serial Number:    AEI7A00021
Package Type:     DPX-T3H1
Position:         Port 1
Package State:    operational
Firmware Version: Not available
```

Actuator Information

This command syntax shows an actuator's information.

```
#        show actuators <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show actuators <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all actuators.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific actuator number*	Displays the information for the specified actuator only.

* The actuator number is the ID number assigned to the actuator. The ID number can be found using the EMX web interface or CLI. It is an integer starting at 1.

Displayed information:

- Without the parameter "details," only the actuator ID, type and state are displayed.
- With the parameter "details," more information is displayed in addition to the ID number and actuator state, 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
```

```
External sensor 3 (Temperature):
Reading: 31.8 deg C
State:   normal

Active Thresholds: Sensor specific thresholds

Default Thresholds for Temperature sensors:
Lower critical threshold: 10.0 deg C
Lower warning threshold:  15.0 deg C
Upper warning threshold:  30.0 deg C
Upper critical threshold: 35.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples

Sensor Specific Thresholds:
Lower critical threshold: 8.0 deg C
Lower warning threshold:  13.0 deg C
Upper warning threshold:  28.0 deg C
Upper critical threshold: 33.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples
```

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 Peripherals 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 resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#       show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors
all	All of the above numeric sensors
	Tip: You can also type the command without adding this option "all" to get the same data.

Displayed information:

- Without the parameter "details," only the default upper and lower thresholds, deassertion hysteresis and assertion timeout settings of the specified sensor type are displayed.
- With the parameter "details," the threshold range is displayed in addition to default thresholds settings.

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, user idle timeout and front panel permissions (if supported by your model).

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, user "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 measurement units 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.

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the EMX device.

```
#        show serial
```

Asset Strip Settings

This command shows the asset strip settings, such as the total number of rack units (tag ports), asset strip 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 strip information.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific asset strip number	Displays the settings of the asset strip connected to the specified FEATURE port number.
	For the EMX device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Strip

A rack unit refers to a tag port on the asset strips. This command shows the settings of a specific rack unit or all rack units on an asset strip, 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 strip 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 strip.
	Tip: You can also type the command without adding this option "all" to get the same data.

Option	Description
A specific number	Displays the settings of the specified rack unit on the specified asset strip.
	Use the index number to specify the rack unit. The index number is available on the asset strip or 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> <slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip 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 strip. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <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.

Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

▶ **Show the last 30 entries:**

```
#        show eventlog
```

▶ **Show a specific number of last entries in the event log:**

```
#        show eventlog limit <n>
```

▶ **Show a specific type of events only:**

```
#        show eventlog class <event_type>
```

▶ **Show a specific number of last entries associated with a specific type of events only:**

```
#        show eventlog limit <n> class <event_type>
```

Variables:

- <n> is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event_type> is one of the following event types.

Event type	Description
all	All events.
device	Device-related events, such as system starting or firmware upgrade event.
userAdministration	User management events, such as a new user profile or a new role.
userActivity	User activities, such as login or logout.
sensor	Internal or external sensor events, such as state changes of any sensors.

Event type	Description
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.
assetManagement	Raritan asset management events, such as asset tag connections or disconnections.
lhx	Schroff® LHX/SHX heat exchanger events.
modem	Modem-related events.
timerEvent	Scheduled action events.
webcam	Events for webcam management, if available.
cardReader	Events for card reader management, if available.
powerLgic	Events about Power Logic PM710 if this device is connected.

Wireless LAN Diagnostic Log

This command shows the diagnostic log for the wireless LAN connection.

```
#       show wlanlog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
#       show serverReachability
```

Server Reachability Information for a Specific Server

To show the server reachability information for a certain IT device only, use the following command.

    #   `show serverReachability server <n>`

To show detailed information, add the parameter "details" to the end of the command.

    #   `show serverReachability server <n> details`

Variables:

- `<n>` is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

```
_____
 #  IP address       Enabled  Status
_____
 1  192.168.84.126   Yes      Waiting for reliable connection
 2  www.raritan.com  Yes      Waiting for reliable connection
```

Displayed information:

- Without the parameter "details," only the specified device's IP address, monitoring enabled/disabled state and current status are displayed.
- With the parameter "details," more settings for the specified device are displayed, such as number of pings and wait time prior to the next ping.

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 history commands.

```
#        show history bufferlength
```

Displayed information:

• The current history buffer length is displayed.

Reliability Data

This command shows the reliability data.

```
#        show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
#        show reliability errorlog <n>
```

Variables:

• <n> is one of the options: *0* (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log.
	Tip: You can also type the command without adding this option "0" to get all data.

Option	Description
A specific integer number	Displays the specified number of last entries in the reliability error log.

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
IPv4 access control: Disabled

IPv6 access control: Disabled

Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:    No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IPv4 access control: Disabled

IPv6 access control: Disabled


Role based access control for IPv4: Disabled

Role based access control for IPv6: Disabled

Password aging: Disabled

Prevent concurrent user login:    No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 1440 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitly authori
zed by management are unauthorized. All activities are monitored and logged. The
re is no privacy on this system. Unauthorized access and activities or any crimi
nal activity will be reported to appropriate authorities.
```

Clearing Information

You can use the clear commands to remove unnecessary data from the EMX.

After typing a "clear" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** *(on page 294).*

Clearing Event Log

This command removes all data from the event log.

```
#       clear eventlog
```

-- OR --

```
#       clear eventlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the event log or n to abort the operation.

If you type y, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Clearing WLAN Log

This command removes all data from the diagnostic log for the wireless LAN (WLAN) connection.

```
#       clear wlanlog
```

-- OR --

```
#       clear wlanlog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the WLAN log or n to abort the operation.

If you type y, a message "WLAN log was cleared successfully" is displayed to indicate all data in the WLAN log has been deleted.

Configuring the EMX Device and Network

To configure the EMX device or network settings through the CLI, it is highly recommended to log in as the administrator so that you have full permissions.

To configure any settings, enter the configuration mode. Configuration commands are case sensitive so ensure you capitalize them correctly.

Entering Configuration Mode

Configuration commands function in configuration mode only.

▶ **To enter configuration mode:**

1. Ensure you have entered administrator mode and the # prompt is displayed.

   Note: If you enter configuration mode from user mode, you may have limited permissions to make configuration changes. See **Different CLI Modes and Prompts** *(on page 294).*

2. Type `config` and press Enter.

3. The config:# prompt appears, indicating that you have entered configuration mode.

   config:# _

4. 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 Configuration Mode* **(on page 319).**

Quitting 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 # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See *Different CLI Modes and Prompts* (on page 294).

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.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Changing the Device Name

This command 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.

Enabling or Disabling Data Logging

This command 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 245).

Setting Data Logging Measurements Per Entry

This command 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 245).

Specifying the Device Altitude

This command specifies your EMX device's altitude above sea level (in meters). You must specify the EMX device's altitude above sea level if a Raritan's DPX differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See *Altitude Correction Factors* (on page 532).

```
config:#    emd deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between 1 and 3000 meters.

Setting the Z Coordinate Format for Environmental Sensors

This command 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 or actuators.

Option	Description
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 392).*

Enabling or Disabling Peripheral Device Auto Management

This command enables or disables the Peripheral Device Auto Management feature.

```
config:#   emd peripheralDeviceAutoManagement <option>
```

Variables:

- *<option> is one of the options: enable or disable.*

Option	Description
enable	Enables the automatic management feature for environmental sensor packages.
disable	Disables the automatic management feature for environmental sensor packages.

For more information, see *How the Automatic Management Function Works* (on page 100).

Network Configuration Commands

A network configuration command begins with *network*. A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv4 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 configuration mode of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 configuration mode of the BRIDGE interface (that is, bridging mode).

- <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.

Setting the IPv4 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:

```
config:#   network ipv4 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 preferred host name of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

- <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

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the EMX device.

```
config:#   network ipv4 interface <ETH> address <ip address>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv4 address of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your EMX device. Its format is "IP address/prefix". For example, *192.168.84.99/32*.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command 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.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the EMX and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see *Static Route Examples* (on page 158).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv4 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#    network ipv4 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ethernet*, *wireless* and *bridge*. Type "bridge" only when your EMX is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:#    network ipv6 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 configuration mode of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

- <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.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv6 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 preferred host name of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

- <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

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the EMX device.

```
config:#   network ipv6 interface <ETH> address <ip
           address>
```

Variables:

- <ETH> is one of the network interfaces: *ethernet*, *wireless*, *bridge* or *all*. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Interface	Description
ethernet	Determine the IPv6 address of the ETHERNET interface (that is, wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your EMX device. This value uses the IPv6 address format. Note that you must add */xx*, which indicates a prefix length of bits such as /64, to the end of this IPv6 address.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command 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.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the EMX and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see *Static Route Examples* (on page 158).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

-- OR --

```
config:#    network ipv6 staticRoutes modify <route_ID> <dest-2> interface <ETH>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the EMX belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ethernet*, *wireless* and *bridge*. Type "bridge" only when your EMX is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Configuring DNS Parameters

Use the following commands to configure DNS-related settings.

▶ **Specify the primary DNS server:**

```
config:#   network dns firstServer <ip address>
```

▶ **Specify the secondary DNS server:**

```
config:#   network dns secondServer <ip address>
```

▶ **Specify the third DNS server:**

```
config:#   network dns thirdServer <ip address>
```

▶ **Determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses:**

```
config:#   network dns resolverPreference <resolver>
```

Variables:
- <ip address> is the IP address of the DNS server.
- <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.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network ethernet*.

Enabling or Disabling the LAN Interface

This command enables or disables the LAN interface.

```
config:#   network ethernet ETHERNET enabled <option>
```

Variables:

- <option> is one of the options: *true or false*.

Option	Description
true	The specified network interface is enabled.
false	The specified network interface is disabled.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:#   network ethernet ETHERNET speed <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.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:#   network ethernet ETHERNET duplexMode <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.

Setting 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.

Setting the SSID

This command 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

Setting the Authentication Method

This command 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.

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - 8 to 63 characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Setting 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.

▶ **Determine the outer authentication protocol:**

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol:**

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

▶ **Set the EAP identity:**

```
config:#   network wireless eapIdentity <identity>
```

▶ **Set the EAP password:**

```
config:#   network wireless eapPassword
```

After performing the above command, the EMX prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a CA TLS certificate:**

```
config:#   network wireless eapCACertificate
```

After performing the above command, the system prompts you to enter the CA certificate's contents. For details, see *EAP CA Certificate Example* (on page 338).

▶ **Enable or disable verification of the TLS certificate chain:**

```
config:#   network wireless enableCertVerification <option1>
```

▶ **Allow expired and not yet valid TLS certificates:**

```
config:#   network wireless allowOffTimeRangeCerts <option2>
```

▶ **Allow wireless network connection with incorrect system time:**

```
config:#   network wireless allowConnectionWithIncorrectClock <option3>
```

Variables:

- The value of <outer_auth> is *PEAP* because EMX only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.
- The value of <inner_auth> is *MSCHAPv2* because EMX only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.
- <identity> is your user name for the EAP authentication.
- <option1> is one of the options: *true* or *false*.

Option	Description
true	Enables the verification of the TLS certificate chain.
false	Disables the verification of the TLS certificate chain.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Always make the wireless network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The wireless network connection is NOT successfully established when the TLS certificate chain contains any certificate which is outdated or not valid yet.

- <option3> is one of the options: *true* or *false*.

Option	Description
true	Make the wireless network connection successful when the EMX system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.

Option	Description
false	The wireless network connection is NOT successfully established when the EMX finds that the TLS certificate is not valid due to incorrect system time.

EAP CA Certificate 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 Configuration Mode* (on page 319).

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
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pblz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pblzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
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 as illustrated below, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljyBhbmQgU3BhY2UgQWRta
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 specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#   network <mode> enabled <option1>
```

Variables:

- <mode> is one of the following cascading modes.

Important: When enabling either cascading mode, you must make sure the other cascading mode is disabled, or the preferred

cascading mode may not be enabled successfully.

Mode	Description
bridge	The network bridging mode, where each cascaded device is assigned a unique IP address.
portForwarding	The port forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

- <option1> is one of the following options:

Option	Description
true	The selected cascading mode is enabled.
false	The selected cascading mode is disabled.

▶ **If Port Forwarding mode is enabled, you must configure two more settings to finish the configuration:**

On ALL cascaded devices, you must configure the 'role' setting one by one.

```
config:#    network portForwarding role <option2>
```

On the master device, you must configure the 'downstream interface' setting.

```
config:#    network portForwarding
            masterDownstreamInterface <option3>
```

Variables:

- <option2> is one of the following cascading roles:

Role	Description
master	The device is a master device.
slave	The device is a slave device.

- <option3> is one of the following options:

Option	Description
Ethernet	Ethernet port is the port where the 1st slave device is connected.
Usb	USB port is the port where the 1st slave device is connected.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

▶ **Change the HTTP port:**

```
config:#   network services http port <n>
```

▶ **Enable or disable the HTTP port:**

```
config:#   network services http enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.
- <option> is one of the options: *true* or *false*.

Option	Description
true	The HTTP port is enabled.
false	The HTTP port is disabled.

Setting the HTTPS Port

The commands used to configure the HTTPS port settings begin with *network services https*.

▶ **Change the HTTPS port:**

```
config:#   network services https port <n>
```

▶ **Enable or disable the HTTPS access:**

```
config:#   network services https enabled <option>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Forces any access to the EMX via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

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 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.

Option	Description
false	The Telnet service is disabled.

Changing the Telnet Port

This command 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.

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 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.

Changing the SSH Port

This command 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.

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 enter a valid SSH public key for each user profile to log in over the SSH connection. See *Specifying the SSH Public Key* (on page 380).

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 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.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command 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.

Setting the SNMP Read Community

This command 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.

Setting the SNMP Write Community

This command 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.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:#   network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:#   network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See *Enabling Service Advertising* (on page 178) for details.

```
config:#   network services zeroconfig enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The zero configuration protocol is enabled.
false	The zero configuration protocol is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Networking Mode

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Example 2 - Enabling Both IP Protocols

The following command determines that both IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Example 3 - Wireless Authentication Method

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Example 4 - Static IPv4 Configuration

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command that is used to set the NTP parameters begins with *time ntp*.

Specifying the Primary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp firstServer <first_server>
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.

Specifying the Secondary NTP Server

This command specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp secondServer <second_server>
```

Variables:

- The <second_server> is the IP address or host name of the secondary NTP server.

Overriding DHCP-Assigned NTP Servers

This command determines whether the customized NTP server settings override the DHCP-specified NTP servers.

```
config:#   time ntp overrideDHCPProvidedServer <option>
```

Variables:

- <option> is one of these options: *true* or *false*.

Mode	Description
true	Customized NTP server settings override the DHCP-specified NTP servers.
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Deleting an NTP Server

The following commands delete the primary and/or secondary time server(s).

▶ **To delete the primary time server:**

```
config:#   time ntp firstServer ""
```

▶ **To delete the secondary time server:**

```
config:#   time ntp secondServer ""
```

Setting the Time Zone

The CLI has a list of time zones to configure the date and time for the EMX.

```
config:#   time zone
```

After a list of time zones is displayed, type the index number of the time zone or press Enter to cancel.

Example

▶ **To set the time zone:**

1. Type the time zone command as shown below and press Enter.

   `config:#    time zone`

2. The system shows a list of time zones. Type the index number of the desired time zone and press Enter.

3. Type `apply` for the selected time zone to take effect.

Customizing the Date and Time

If intending to manually configure the date and time, use the following CLI commands to specify them.

Note: You shall set the time configuration method to "manual" prior to customizing the date and time. See **Determining the Time Setup Method** *(on page 349).*

▶ **Assign the date:**

   `config:#    time set date <yyyy-mm-dd>`

▶ **Assign the time:**

   `config:#    time set time <hh:mm:ss>`

Variables:

Variable	Description
<yyyy-mm-dd>	Type the date in the format of yyyy-mm-dd.
	For example, type *2015-11-30* for November 30, 2015.
<hh:mm:ss>	Type the time in the format of hh:mm:ss in the 24-hour format.
	For example, type *13:50:20* for 1:50:20 pm.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight savings time is applied to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Examples

This section illustrates several time configuration examples.

Example 1 - Time Setup Method

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Example 2 - Primary NTP Server

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Checking the Accessibility of NTP Servers

This command verifies the accessibility of NTP servers specified manually on your EMX and then shows the result. For instructions on specifying NTP servers via CLI, see *Setting NTP Parameters* (on page 349).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See *Setting NTP Parameters* (on page 349).
- Make the customized NTP servers override the DHCP-assigned ones. See *Overriding DHCP-Assigned NTP Servers* (on page 350).

This command is available either in the administrator/user mode or in the configuration mode. See *Different CLI Modes and Prompts* (on page 294).

▶ **In the administrator/user mode:**

```
#          check ntp
```

▶ **In the configuration mode:**

```
config#     check ntp
```

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 a 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 Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 firewall control feature:**

```
config:#   security ipAccessControl ipv4 enabled <option>
```

▶ **Determine the default IPv4 firewall control policy for inbound traffic:**

```
config:#   security ipAccessControl ipv4 defaultPolicyIn <policy>
```

▶ **Determine the default IPv4 firewall control policy for outbound traffic:**

```
config:#   security ipAccessControl ipv4 defaultPolicyOut <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 firewall control feature:**

```
config:#   security ipAccessControl ipv6 enabled <option>
```

▶ **Determine the default IPv6 firewall control policy for inbound traffic:**

```
config:#   security ipAccessControl ipv6 defaultPolicyIn <policy>
```

▶ **Determine the default IPv6 firewall control policy for outbound traffic:**

```
config:#   security ipAccessControl ipv6 defaultPolicyOut <policy>
```

Variables:

- *<option>* is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.

Option	Description
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.
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 412).*

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 for adding a rule varies.

- *IPv4 commands*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#   security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#   security ipAccessControl ipv4 rule add <direction> <ip_mask> <policy> <insert> <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv4 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
config:#    security ipAccessControl ipv6 rule add <direction> <ip_mask> <policy> <insert>
            <rule_number>
```

-- OR --

```
config:#    security ipAccessControl ipv6 rule add <direction> <insert> <rule_number>
            <ip_mask> <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), 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/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination 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.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command varies.

- *IPv4 commands*

▶ **Modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#   security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
           <ip_mask>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#   security ipAccessControl ipv4 rule modify <direction> <rule_number> policy
           <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#   security ipAccessControl ipv4 rule modify <direction> <rule_number> ipMask
           <ip_mask> policy <policy>
```

- *IPv6 commands*

▶ **Modify an IPv6 rule's IP address and/or prefix length:**

```
config:#   security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
           <ip_mask>
```

▶ **Modify an IPv6 rule's policy:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> policy
            <policy>
```

▶ **Modify all contents of an IPv6 existing rule:**

```
config:#    security ipAccessControl ipv6 rule modify <direction> <rule_number> ipMask
            <ip_mask> policy <policy>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <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 (or prefix length), 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/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

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 <direction> <rule_number>
```

▶   IPv6 commands

```
config:#    security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#    security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed in the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."

  Tip: To select the agreement checkbox using the keyboard, first press Tab to go to the checkbox and then Enter.

- In the CLI, type `y` when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.
2. To end the content:
   a. Press Enter.
   b. Type `--END--` to indicate the end of the content.
   c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command. See **Quitting Configuration Mode** *(on page 319).*

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 forcing a user to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify various login limitation parameters at a time. See **Multi-Command Syntax** (on page 412).

Single Login Limitation

This command 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.

Password Aging

This command 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.

Password Aging Interval

This command 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.

Raritan.

Idle Timeout

This command determines how long a user can remain idle before that user is forced to log out of the EMX web interface or CLI.

```
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).

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

You can combine multiple commands to modify the user blocking parameters at a time. See *Multi-Command Syntax* (on page 412).

▶ **Determine the maximum number of failed logins before blocking a user:**

```
config:#   security userBlocking maximumNumberOfFailedLogins <value1>
```

▶ **Determine how long a user is blocked:**

```
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 ranging from 1 to 1440 minutes (one day), or *infinite*, which blocks the user all the time until the user is unblocked manually.

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 412).

Enabling or Disabling Strong Passwords

This command 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.

Minimum Password Length

This command determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Maximum Password Length

This command determines the maximum length of the password.

```
config:#   security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Lowercase Character Requirement

This command 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.

Uppercase Character Requirement

This command 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.

Numeric Character Requirement

This command 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.

Option	Description
disable	No numeric character is required.

Special Character Requirement

This command 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.

Maximum Password History

This command 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.

Role-Based 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 Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- *IPv4 commands*

▶ **Enable or disable the IPv4 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv4 enabled <option>
```

▶ **Determine the IPv4 role-based access control policy:**

```
config:#   security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- *IPv6 commands*

▶ **Enable or disable the IPv6 role-based access control feature:**

```
config:#   security roleBasedAccessControl ipv6 enabled <option>
```

▶ **Determine the IPv6 role-based access control policy:**

```
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 412).*

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*

▶ **Add a new rule to the bottom of the IPv4 rules list:**

```
config:#   security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
           <policy>
```

▶ **Add a new IPv4 rule by inserting it above or below a specific rule:**

```
config:#   security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
           <policy> <insert> <rule_number>
```

- *IPv6 commands*

▶ **Add a new rule to the bottom of the IPv6 rules list:**

```
config:#   security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
           <policy>
```

▶ **Add a new IPv6 rule by inserting it above or below a specific rule:**

```
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.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- *IPv4 commands*

▶ **Modify a rule's IPv4 address range:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv4 rule's role:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> role <role>
```

▶ **Modify an IPv4 rule's policy:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> policy
            <policy>
```

▶ **Modify all contents of an existing IPv4 rule:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy <policy>
```

- *IPv6 commands*

▶ **Modify a rule's IPv6 address range:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

▶ **Modify an IPv6 rule's role:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> role <role>
```

▶ **Modify an IPv6 rule's policy:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

▶ **Modify all contents of an existing IPv6 rule:**

```
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

Deleting a Role-Based Access Control Rule

These commands remove 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.

Examples

This section illustrates several security configuration examples.

Example 1 - IPv4 Firewall Control Configuration

The following command sets up two parameters of the IPv4 access control feature.

```
config:#     security ipAccessControl ipv4 enabled true defaultPolicyIn accept
             defaultPolicyOut accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy for inbound traffic is set to "accept."
- The default policy for outbound traffic is set to "accept."

Example 2 - Adding an IPv4 Firewall Rule

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 to accept all packets sent from the IPv4 address 192.168.84.123.
- 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.

Example 3 - User Blocking

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.

Example 4 - Adding an IPv4 Role-based Access Control Rule

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.

User Configuration Commands

Most user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command 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.

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 412).*

Changing a User's Password

This command 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 Configuration Mode* (on page 319).
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.

Various commands can be combined to modify the parameters of a specific user profile at a time. See *Multi-Command Syntax* (on page 412).

▶ **Change a user's full name:**

```
config:#   user modify <name> fullName "<full_name>"
```

▶ **Change a user's telephone number:**

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

▶ **Change a user's email address:**

```
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.

Enabling or Disabling a User Profile

This command 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.

Forcing a Password Change

This command 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.

Modifying 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 412).

▶ **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.

▶ **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.

▶ **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.

▶ **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 8 to 32 ASCII printable characters.

▶ **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.

Raritan.
A brand of Legrand

▶ **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 8 to 32 ASCII printable characters.

▶ **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.

▶ **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.

Changing the Role(s)

This command 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. See *All Privileges* (on page 385).

Changing 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 412).

Note: The measurement unit change only applies to the web interface and command line interface.

Tip: To set the default measurement units applied to the EMX user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 382).*

▶ **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.

▶ **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.

▶ **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.

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 or change 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.

▶ **To remove an existing SSH public key:**

1. Type the same command as shown above.
2. When the system prompts you to input the contents, press Enter without typing or pasting anything.

Example

The following procedure illustrates how to change the SSH public key for the user "assistant."

1. Verify that you have entered the configuration mode. See *Entering Configuration Mode* (on page 319).
2. Type the following command and press Enter.

   `config:#   user modify assistant sshPublicKey`

3. You are prompted to enter a new SSH public key.
4. Type the new key and press Enter.

Deleting a User Profile

This command deletes an existing user profile.

`config:#   user delete <name>`

Changing Your Own Password

Every user can change their own password via this command 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 Configuration Mode* (on page 319).
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:
```

Setting Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the EMX user interfaces across all users except for those whose preferred measurement units are set differently by themselves or the administrator. Diverse measurement unit commands can be combined so that you can set all default measurement units at a time. To combine all commands, see *Multi-Command Syntax* (on page 412).

Note: The measurement unit change only applies to the web interface and command line interface.

Tip: To change the preferred measurement units displayed in the EMX user interfaces for a specific user via CLI, see **Changing Measurement Units** *(on page 379).*

▶ **Set the default temperature unit:**

```
config:#    user defaultpreferences preferredTemperatureUnit <option1>
```

Variables:

- <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.

▶ **Set the default length unit:**

```
config:#   user defaultpreferences preferredLengthUnit <option2>
```

Variables:

- <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.

▶ **Set the default pressure unit:**

```
config:#   user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <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.

Examples

This section illustrates several user configuration examples.

Example 1 - Creating a User Profile

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.

Example 2 - Modifying a User's Roles

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."

Example 3 - Default Measurement Units

The following command sets all default measurement units at a time.

```
config:#   user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
           preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command 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 385).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

All Privileges

This table lists all privileges.

Privilege	Description
acknowledgeAlarms	Acknowledge Alarms
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings

changeEmdConfiguration	Change EMD Configuration
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePowerLogicConfiguration	Change PowerLogic Configuration
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)
switchActuator**	Switch Actuator
viewEventSetup	View Event Settings
viewEverything	Unrestricted View Privileges
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

**The "switchActuator" privilege requires an argument that is separated with a colon. The argument could be:

- All actuators, that is,
  `switchActuator:all`
- An actuator's ID number. For example:
  `switchActuator:1`
  `switchActuator:2`
  `switchActuator:3`
- A list of comma-separated ID numbers of different actuators. For example:
  `switchActuator:1,3,6`

Note: The ID number of each actuator is shown in the EMX web interface. It is an integer between 1 and 32.

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

▶ **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.

▶ **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 385).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

▶ **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 385).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Deleting a Role

This command deletes an existing role.

```
config:#   role delete <name>
```

Example - Creating a Role

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).

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.

Note: To configure an actuator, see **Actuator Configuration Commands** *(on page 399).*

Changing the Sensor Name

This command 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 available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Note: To name an actuator, see **Actuator Configuration Commands** *(on page 399).*

Specifying the CC Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party or Raritan's detectors/switches. You must specify the type of connected detector/switch for proper operation. Use this command when you need to specify the sensor type.

```
config:#    externalsensor <n> sensorSubType <sensor_type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <sensor_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.

Type	Description
vibration	The connected detector/switch is for detection of the vibration.

Setting the X Coordinate

This command 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 available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Y Coordinate

This command 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 available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Setting the Z Coordinate

This command 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 available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- 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 321).*

Changing the Sensor Description

This command 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 available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Using Default Thresholds

This command determines whether default thresholds, including the deassertion hysteresis and assertion timeout, are applied to a specific environmental sensor.

```
config:#    externalsensor <n> useDefaultThresholds <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Default thresholds are selected as the threshold option for the specified sensor.
false	Sensor-specific thresholds are selected as the threshold option for the specified sensor.

Setting the Alarmed to Normal Delay for DX-PIR

This command determines the value of the Alarmed to Normal Delay setting for a DX-PIR presence detector.

```
config:#    externalsensor <n> alarmedToNormalDelay <time>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Example 1 - Environmental Sensor Naming

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Example 2 - Sensor Threshold Selection

The following command sets the environmental sensor #1 to use the default thresholds, including the deassertion hysteresis and assertion timeout, as its threshold settings.

```
config:#   externalsensor 1 useDefaultThresholds true
```

Configuring Environmental Sensors' Default Thresholds

You can set the default values of upper and lower thresholds, deassertion hysteresis and assertion timeout on a sensor type basis, including temperature, humidity, air pressure and air flow sensors. The default thresholds automatically apply to all environmental sensors that are newly detected or added.

A default threshold configuration command begins with *defaultThresholds*.

You can configure various default threshold settings for the same sensor type at a time by combining multiple commands. See *Multi-Command Syntax* (on page 412).

▶ **Set the Default Upper Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperCritical <value>
```

▶ **Set the Default Upper Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> upperWarning <value>
```

▶ **Set the Default Lower Critical Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerCritical <value>
```

▶ **Set the Default Lower Warning Threshold for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> lowerWarning <value>
```

▶ **Set the Default Deassertion Hysteresis for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> hysteresis <hy_value>
```

▶ **Set the Default Assertion Timeout for a specific sensor type:**

```
config:#   defaultThresholds <sensor type> assertionTimeout <as_value>
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

- <value> is the value for the specified threshold of the specified sensor type. Note that diverse sensor types use different measurement units.

Sensor types	Measurement units
absoluteHumidity	g/m^3 (that is, g/m^3)
relativeHumidity	%
temperature	Degrees Celsius (°C) or Fahrenheit (°F), depending on your measurement unit settings.
airPressure	Pascal (Pa) or psi, depending on your measurement unit settings.
airFlow	m/s

Raritan.
A brand of Legrand

Sensor types	Measurement units
vibration	g

- <hy_value> is the deassertion hysteresis value applied to the specified sensor type.
- <as_value> is the assertion timeout value applied to the specified sensor type. It ranges from 0 to 100 (samples).

Example - Default Upper Thresholds for Temperature

It is assumed that your preferred measurement unit for temperature is set to degrees Celsius. Then the following command sets the default Upper Warning threshold to 20 °C and Upper Critical threshold to 24 °C for all temperature sensors.

```
config:#    defaultThresholds temperature upperWarning 20
            upperCritical 24
```

Environmental Sensor Threshold Configuration Commands

You can use the sensor threshold configuration commands to set the threshold, hysteresis and assertion timeout values for any environmental sensor.

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

Threshold Configuration Commands for a Sensor

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

You can configure various environmental sensor threshold settings at a time by combining multiple commands. See *Multi-Command Syntax* (on page 412).

▶ **Set the Upper Critical threshold for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> upperCritical <option>
```

▶ **Set the Upper Warning threshold for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> upperWarning <option>
```

▶ **Set the Lower Critical threshold for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> lowerCritical <option>
```

▶ **Set the Lower Warning threshold for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> lowerWarning <option>
```

▶ **Set the deassertion hysteresis for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> hysteresis <hy_value>
```

▶ **Set the assertion timeout for an environmental sensor:**

```
config:#    sensor externalsensor <n> <sensor type> assertionTimeout <as_value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is available in the EMX web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer between 1 and 32.
- <sensor type> is one of these sensor types: *temperature*, *absoluteHumidity*, *relativeHumidity*, *airPressure*, *airFlow* or *vibration*.

  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 specified threshold for a specific environmental sensor.
disable	Disables the specified threshold for a specific environmental sensor.

Option	Description
A numeric value	Sets a value for the specified threshold of a specific environmental sensor and enables this threshold at the same time.

- <hy_value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See *"To De-assert" and Deassertion Hysteresis* (on page 528).
- <as_value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. It ranges between 1 and 100. See *"To Assert" and Assertion Timeout* (on page 526).

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
```

Actuator Configuration Commands

An actuator configuration command begins with *actuator*. You can configure the name and location parameters of an individual actuator.

You can configure various parameters for one actuator at a time. See *Multi-Command Syntax* (on page 412).

▶ **Change the name:**

```
config:#    actuator <n> name "<name>"
```

▶ **Set the X coordinate:**

```
config:#    actuator <n> xlabel "<coordinate>"
```

▶ **Set the Y coordinate:**

```
config:#    actuator <n> ylabel "<coordinate>"
```

▶ **Set the Z coordinate:**

```
config:#    actuator <n> zlabel "<z_label>"
```

▶ **Modify the actuator's description:**

```
config:#    actuator <n> description "<description>"
```

Variables:

- <n> is the ID number assigned to the actuator. The ID number can be found using the EMX web interface or CLI. It is an integer starting at 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
- There are two types of values for the <z_label> variable, depending on the Z coordinate format you set:

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.

- <description> is a sentence or paragraph comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example - Actuator Naming

The following command assigns the name "Door lock" to the actuator whose ID number is 9.

```
config:#    actuator 9 name "Door lock"
```

Server Reachability Configuration Commands

You can use the CLI to add or delete an IT device, such as a server, from the server reachability list, or modify the settings for a monitored IT device. A server reachability configuration command begins with *serverReachability*.

Adding a Monitored Device

This command adds a new IT device to the server reachability list.

```
config:#    serverReachability add <IP_host> <enable> <succ_ping>
           <fail_ping> <succ_wait> <fail_wait> <resume> <disable_count>
```

Variables:

- <IP_host> is the IP address or host name of the IT device that you want to add.
- <enable> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the newly added device.
false	Disables the ping monitoring feature for the newly added device.

- <succ_ping> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_ping> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the EMX resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive "Unreachable" declarations before the EMX disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Deleting a Monitored Device

This command removes a monitored IT device from the server reachability list.

```
config:#   serverReachability delete <n>
```

Variables:

- <n> is a number representing the sequence of the IT device in the monitored server list.

  You can find each IT device's sequence number using the CLI command of `show serverReachability` as illustrated below.

```
  _____
  #  IP address       Enabled  Status
  _____
  1  192.168.84.126   Yes      Waiting for reliable connection
  2  www.raritan.com  Yes      Waiting for reliable connection
```

Modifying a Monitored Device's Settings

The command to modify a monitored IT device's settings begins with *serverReachability modify*.

You can modify various settings for a monitored device at a time. See *Multi-Command Syntax* (on page 412).

▶ **Modify a device's IP address or host name:**

```
config:#    serverReachability modify <n> ipAddress <IP_host>
```

▶ **Enable or disable the ping monitoring feature for the device:**

```
config:#    serverReachability modify <n> pingMonitoringEnabled <option>
```

▶ **Modify the number of successful pings for declaring "Reachable":**

```
config:#    serverReachability modify <n> numberOfSuccessfulPingsToEnable
            <succ_number>
```

▶ **Modify the number of unsuccessful pings for declaring "Unreachable":**

```
config:#    serverReachability modify <n> numberOfUnsuccessfulPingsForFailure
            <fail_number>
```

▶ **Modify the wait time after a successful ping:**

```
config:#    serverReachability modify <n> waitTimeAfterSuccessfulPing
            <succ_wait>
```

▶ **Modify the wait time after a unsuccessful ping:**

```
config:#    serverReachability modify <n> waitTimeAfterUnsuccessfulPing
            <fail_wait>
```

▶ **Modify the wait time before resuming pinging after declaring "Unreachable":**

```
config:#    serverReachability modify <n> waitTimeBeforeResumingPinging
            <resume>
```

▶ **Modify the number of consecutive "Unreachable" declarations before disabling the ping monitoring feature:**

```
config:#    serverReachability modify <n> numberOfFailuresToDisable
            <disable_count>
```

Variables:

- <n> is a number representing the sequence of the IT device in the server monitoring list.
- <IP_host> is the IP address or host name of the IT device whose settings you want to modify.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the ping monitoring feature for the monitored device.
false	Disables the ping monitoring feature for the monitored device.

- <succ_number> is the number of successful pings for declaring the monitored device "Reachable." Valid range is 0 to 200.
- <fail_number> is the number of consecutive unsuccessful pings for declaring the monitored device "Unreachable." Valid range is 1 to 100.
- <succ_wait> is the wait time to send the next ping after a successful ping. Valid range is 5 to 600 (seconds).
- <fail_wait> is the wait time to send the next ping after a unsuccessful ping. Valid range is 3 to 600 (seconds).
- <resume> is the wait time before the EMX resumes pinging after declaring the monitored device "Unreachable." Valid range is 5 to 120 (seconds).
- <disable_count> is the number of consecutive "Unreachable" declarations before the EMX disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Example - Server Settings Changed

The following command modifies several ping monitoring settings for the second server in the server reachability list.

```
config:#    serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
            numberOfUnsuccessfulPingsForFailure 8
            waitTimeAfterSuccessfulPing 30
```

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset strip (if any) or the settings of LEDs on the asset strip.

Asset Strip Management

An asset strip management configuration command begins with `assetStrip`.

Naming an Asset Strip

This command syntax names or changes the name of an asset strip connected to the EMX device.

```
config:#   assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip 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.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset strip connected to the EMX device.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Note: A rack unit refers to a tag port on the asset strips.

Variables:

- <n> is the number of the FEATURE port where the selected asset strip 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 strip. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset strips 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 strip 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.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset strips connected to the EMX device.

```
config:#    assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip 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 strip. This value is an integer number.

Specifying the Asset Strip Orientation

This command syntax specifies the orientation of the asset strips connected to the EMX device. Usually you do not need to perform this command unless your asset strips do NOT come with the tilt sensor, causing the EMX unable to detect the asset strips' orientation.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip 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.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset strip #1 to indicate the presence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset strip(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.

Rack Unit Configuration

A rack unit refers to a tag port on the asset strips. 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 strip.

```
config:#    rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip 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 is available on the asset strip or 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.

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset strip 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 strip 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 is available on the asset strip or 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 *Setting LED Colors for Connected Tags* (on page 406) and *Setting LED Colors for Disconnected Tags* (on page 407). 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 409) and *Setting an LED Mode for a Rack Unit* (on page 409) to set different LED settings.

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset strip. 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 strip 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 is available on the asset strip or 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 **Setting LED Colors for Connected Tags** *(on page 406) and* **Setting LED Colors for Disconnected Tags** *(on page 407).*

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset strip. 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 strip 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 is available on the asset strip or 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.

Mode	Description
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Strip LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#   assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Example 2 - Rack Unit Naming

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"
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Baud Rates

The following commands set the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the EMX device. Change the baud rate before connecting it to the desired device, such as a computer, a Raritan's P2CIM-SER, or a modem, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the EMX or power cycle the connected device for proper communications.

▶ **Determine the CONSOLE baud rate:**

```
config:#   serial consoleBaudRate <baud_rate>
```

Note: The serial port bit-rate change is required when the EMX works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

▶ **Determine the MODEM baud rate:**

```
config:#   serial modemBaudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the baud rate options: *1200*, *2400*, *4800*, *9600*, *19200*, *38400*, *57600*, *115200*.

Forcing the Device Detection Mode

This command forces the serial port on the EMX to enter a specific device detection mode.

```
config:#   serial deviceDetectionType <mode>
```

Variables:

- <mode> is one of the detection modes: *automatic*, *forceConsole*, *forceAnalogModem*, or *forceGsmModem*.

Option	Description
automatic	The EMX automatically detects the type of the device connected to the serial port. Select this option unless your EMX cannot correctly detect the device type.

Option	Description
forceConsole	The EMX attempts to recognize that the connected device is set for the console mode.
forceAnalogModem	The EMX attempts to recognize that the connected device is an analog modem.
forceGsmModem	The EMX attempts to recognize that the connected device is a GSM modem.

Example

The following command sets the CONSOLE baud rate of the EMX device's serial port to 9600 bps.

```
config:#   serial consoleBaudRate 9600
```

Setting the History Buffer Length

This command syntax sets the history buffer length, which determines the amount of history commands that can be retained in the buffer. The default length is 25.

```
config:#   history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command to perform all of them at a time. All combined commands must belong to the same configuration type, such as commands prefixed with *network*, *user modify*, *sensor externalsensor* and so on.

A multi-command syntax looks like this:

```
<configuration type> <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 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.

Actuator Control Operations

An actuator, which is connected to a dry contact signal channel of a DX sensor, can control a mechanism or system. You can switch on or off that mechanism or system through the actuator control command in the CLI.

Perform these commands in the administrator or user mode. See *Different CLI Modes and Prompts* (on page 294).

Switching On an Actuator

This command syntax turns on one actuator.

```
#       control actuator <n> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       control actuator <n> on /y
```

Variables:

- <n> is an actuator's ID number.

  The ID number is available in the EMX web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

Switching Off an Actuator

This command syntax turns off one actuator.

```
#       control actuator <n> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       control actuator <n> off /y
```

Variables:

- <n> is an actuator's ID number.

  The ID number is available in the EMX web interface or using the show command in the CLI. It is an integer between 1 and 32.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type `y` to confirm the operation, OR
- Type `n` to abort the operation

Example - Turning On a Specific Actuator

The following command turns on the actuator whose ID number is 8.

```
#      control actuator 8 on
```

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 292).
2. When the Username prompt appears, type `unblock` and press Enter.

```
Username: unblock
```

3. When the "Username to unblock" prompt appears, type the name of the blocked user 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 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.

Note: If you are performing this command over a USB connection, re-connect the USB cable after the reset is completed, or the CLI communications are lost.

Resetting to Factory Defaults

The following commands restore all settings of the EMX device to factory defaults.

▶ **To reset EMX settings after login, use either command:**

   #   `reset factorydefaults`

       -- OR --

   #   `reset factorydefaults /y`

▶ **To reset EMX settings before login:**

   `Username:    factorydefaults`

See *Using the CLI Command* (on page 466) for details.

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 Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

▶ **To enter the diagnostic mode:**

1. Enter either of the following modes:
   ▪ Administrator mode: The # prompt is displayed.
   ▪ User mode: The > prompt is displayed.
2. Type `diag` and press Enter. The diag# or diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Quitting Diagnostic Mode

▶ **To quit the diagnostic mode, use this command:**

```
diag>        exit
```

The # or > prompt appears after pressing Enter, indicating that you have entered the administrator or user mode. See *Different CLI Modes and Prompts* (on page 294).

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying 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.

Showing 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.

Testing the Network Connectivity

This ping command 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. If not, either the host is shut down or it is not being properly 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 between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.

Options	Description
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag>      ping <host> count <number1> size <number2> timeout <number3>
```

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 - Ping Command

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
```

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.

Raritan.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

▶ **To have a command completed automatically:**

1. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.

2. Press Tab or Ctrl+i until the complete command appears.

Example 1:

Type the first word and the first letter of the second word of the "`reset factorydefaults`" command, that is, `reset f`. Then press Tab or Ctrl+i to complete the second word.

Example 2:

Type the first word and initial letters of the second word of the "`security enforceHttpsForWebAccess`" command, that is, `security enf`. Then press Tab or Ctrl+i to complete the second word.

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 administrator mode and the # prompt is displayed.

2. Type `exit` and press Enter.

Chapter 9   Using SCP Commands

You can perform a Secure Copy (SCP) command to update the EMX firmware, do bulk configuration, or back up and restore the configuration.

In This Chapter

Firmware Update via SCP

Same as any EMX firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update. For details, see *Updating the EMX Firmware* (on page 269).

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

▶ **To update the firmware via SCP:**

1. Type the following SCP command and press Enter.

   `scp <firmware file> <user name>@<device ip>:/fwupdate`

   - *<firmware file>* is the EMX firmware's filename. If the firmware file is not in the current directory, you must include the path in the filename.
   - *<user name>* is the "admin" or any user profile with the Firmware Update permission.
   - *<device ip>* is the IP address of the EMX that you want to update.

2. When the system prompts you to enter the password for the specified user profile, type it and press Enter.

3. The system transmits the specified firmware file to the EMX, and shows the transmission speed and percentage.

4. When the transmission is complete, it shows the following message, indicating that the EMX starts to update its firmware now. Wait until the upgrade completes.

   `Starting firmware update. The connection will be closed now.`

▶ **SCP command example:**

```
scp  emx-ecx-030200-42396.bin
admin@192.168.87.50:/fwupdate
```

Tip: The PSCP works in a similar way to the SCP command --
`pscp <firmware file> <user name>@<device ip>:/fwupdate`

Bulk Configuration via SCP

Like performing bulk configuration via the web interface, there are two steps with the bulk configuration using the SCP commands:

a. Save a configuration from a source EMX.

b. Copy the configuration file to one or multiple destination EMX.

For detailed information on the bulk configuration requirements, see *Bulk Configuration* (on page 272).

▶ **To save the configuration via SCP:**

1. Type the following SCP command and press Enter.
   `scp <user name>@<device ip>:/bulk_config.xml`

   - *<user name>* is the "admin" or any user profile with the administrator privileges.
   - *<device ip>* is the IP address of the EMX whose configuration you want to save.

2. Type the user password when prompted.

3. The system saves the configuration from the EMX to a file named "bulk_config.xml."

▶ **To copy the configuration via SCP:**

1. Type the following SCP command and press Enter.
   `scp bulk_config.xml <user name>@<device ip>:/bulk_restore`

   - *<user name>* is the "admin" or any user profile with the administrator privileges.
   - *<device ip>* is the IP address of the EMX whose configuration you want to copy.

2. Type the user password when prompted.

3. The system copies the configuration included in the file "bulk_config.xml" to another EMX, and displays the following message.

   ```
   Starting restore operation. The connection will be
   closed now.
   ```

▶ **SCP examples:**

- Save operation:

  ```
  scp admin@192.168.87.50:/bulk_config.xml
  ```

- Copy operation:

  ```
  scp bulk_config.xml
  admin@192.168.87.47:/bulk_restore
  ```

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- Save operation:

  ```
  pscp <user name>@<device ip>:/bulk_config.xml
  ```

- Copy operation:

  ```
  pscp bulk_config.xml <user name>@<device
  ip>:/bulk_restore
  ```

Backup and Restore via SCP

To back up ALL settings of a EMX, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

▶ **To back up the settings via SCP:**

1. Type the following SCP command and press Enter.

   ```
   scp <user name>@<device ip>:/backup_settings.xml
   ```

   - *<user name>* is the "admin" or any user profile with the administrator privileges.
   - *<device ip>* is the IP address of the EMX whose settings you want to back up.

2. Type the user password when prompted.

3. The system saves the settings from the EMX to a file named "backup_settings.xml."

▶ **To restore the settings via SCP:**

1. Type the following SCP command and press Enter.

```
scp backup_settings.xml <user name>@<device
ip>:/settings_restore
```

- ▪ *<user name>* is the "admin" or any user profile with the administrator privileges.
- ▪ *<device ip>* is the IP address of the EMX whose settings you want to restore.

2. Type the user password when prompted.

3. The system copies the configuration included in the file "backup_settings.xml" to the EMX, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

▶ **SCP examples:**

- Backup operation:

```
scp  admin@192.168.87.50:/backup_settings.xml
```

- Restoration operation:

```
scp  backup_settings.xml
admin@192.168.87.50:/settings_restore
```

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- Backup operation:

```
pscp <user name>@<device ip>:/backup_settings.xml
```

- Restoration operation:

```
pscp backup_settings.xml <user name>@<device
ip>:/settings_restore
```

Downloading Diagnostic Data via SCP

You can download the diagnostic data via SCP.

▶ **To download the diagnostic data via SCP:**

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/diag-data.tgz
```

- ▪ *<user name>* is the "admin" or any user profile with the Administrator or "Unrestricted View Privileges" privileges.
- ▪ *<device ip>* is the IP address of the EMX whose diagnostic data you want to download.

2. Type the password when the system prompts you to type it.

3. The system saves the diagnostic data from the EMX to a file named "diag-data.tgz."

▶ **SCP example:**

```
scp  admin@192.168.87.50:/diag-data.tgz
```

▶ **Windows PSCP command:**

PSCP in Windows works in a similar way to the SCP.

- ```
  pscp <user name>@<device ip>:/diag-data.tgz
  ```

Appendix A   Specifications

In This Chapter

Maximum Ambient Operating Temperature

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

EMX2-111 Feature RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground
3	+5V	—	Power for CIM (200mA, fuse protected) Warning: Pin 3 is only intended for use with Raritan devices.
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	N/C	N/C	No Connection
7	GND	—	Signal Ground

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
8	DCD	Input	Reserved

EMX2-888 Feature RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground
3	+5V	—	Fuse protected Warning: Pin 3 is only intended for use with Raritan devices.
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	+12V	—	Fuse protected
7	GND	—	Signal Ground
8	DCD	Input	Reserved

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	—	—	—

RJ-12 Pin/signal definition			
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		1-wire signal for external environmental sensor packages

Serial RS-232 "DB9" 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

RS-485 Port Pinouts

RS-485 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	—	—	—
2	—	—	—
3	D+	bi-directional	Data +
4	—	—	—
5	—	—	—

RS-485 Pin/signal definition			
6	D-	bi-direction al	Data -
7	—	—	—
8	—	—	—

Appendix B Configuration or Firmware Upgrade with a USB Drive

You can accomplish part or all of the following tasks simultaneously by plugging a USB flash drive which contains one or several special configuration files into the EMX.

- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

Tip: You can also accomplish the same tasks via the TFTP server in a DHCP network. See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 442).*

In This Chapter

System and USB Requirements

You must satisfy ALL of the following requirements prior to using a USB flash drive to perform device configuration and/or firmware upgrade.

▶ **EMX system requirements:**

- There is at least one USB-A port available on your Raritan device.
- Your EMX must be version 2.2.13 or later.

  Note that the EMX interpreted the USB drive's contents using the firmware which was running when plugging the USB drive, not the new firmware after firmware upgrade.

▶ **USB drive requirements:**

- The drive contains either a single partition formatted as a Windows FAT32 filesystem, or NO partition tables (that is, a superfloppy-formatted drive).
- The drive contains a configuration file called *fwupdate.cfg* in its root directory. See *fwupdate.cfg* (on page 432).

Configuration Files

There are three types of configuration files.

- **fwupdate.cfg:**

    This file MUST be always present for performing configuration or firmware upgrade tasks. See *fwupdate.cfg* (on page 432).

- **config.txt:**

    This file is used for configuring device settings. See *config.txt* (on page 436).

- **devices.csv:**

    This file is required only when there are device-specific settings to configure for multiple EMX devices. See *devices.csv* (on page 438).

fwupdate.cfg

The configuration file, *fwupdate.cfg*, is an ASCII text file containing key-value pairs, one per line.

Each value in the file must be separated by an equal sign (=), without any surrounding spaces. Keys are not case sensitive.

Illustration:

```
user=admin
password=raritan
logfile=log.txt
config=config.txt
device_list=devices.csv
```

This section only explains common options in the file.

Note: To use any options developed after version 2.2.13, the firmware version running on your EMX must be able to support them.

▶ **user**

- A required option.
- Specify the name of a user account with Administrator Privileges.
- For a EMX with factory default configuration, set this option to `admin`.

▶ **password**

- A required option.
- Specify the password of the specified admin user.
- For a EMX with factory default configuration, set this option to `raritan.`

▶ **logfile**

- Specify the name of a text file where the EMX will append the log messages when interpreting the USB drive contents.
- If the specified file does not exist in the USB drive, it will be automatically created.
- If this option is not set, no log message are recorded. The disadvantage is that no feedback is available if the EMX detects a problem with the USB drive contents.

▶ **firmware**

- Specify the name of a firmware binary file used to upgrade your EMX.

- The specified firmware file must be compatible with your EMX and have an official Raritan signature.
- If the specified firmware file is the same as the current firmware version of your EMX, no firmware upgrade is performed unless you have set the option "force_update" to `true`.

▶ **force_update**

- If this option is set to `true`, the firmware upgrade is always performed even though your EMX is running the same firmware version as the specified firmware file.
- This option CANNOT break other constraints like the minimum downgrade version.

▶ **config**

- Supported as of release 2.4.0.
- Specify the name of the configuration file containing device settings.
- The suggested filename is *config.txt*. See ***config.txt*** (on page 436).

▶ **device_list**

- Specify the name of the configuration file listing all EMX devices to configure and their device-specific settings.
- This file is required if any macros are used in the device configuration file "config.txt."
- The suggested filename is *devices.csv*. See ***devices.csv*** (on page 438).

▶ **match**

- Specify a match condition for identifying a line or a EMX device in the device configuration file "devices.csv."

  The option's value comprises one word and one number as explained below:

  ▪ The word prior to the colon is an identification property, which is either `serial` for serial number or `mac` for MAC address.

  ▪ The number following the colon indicates a column in the *devices.csv* file.

  For example, `mac:7` instructs the EMX to search for the MAC address in the 7th column of the "devices.csv" file.

- The default value is `serial:1`, making the EMX search for its serial number in the first column.
- This option is used only if the "device_list" option has been set.

▶ **collect_diag**

- If this option is set to `true`, the diagnostic data of the EMX is downloaded to the USB drive.
- The filename of the diagnostic data written into the USB drive varies, depending on the EMX firmware version:
  - Filename prior to version 3.0.0: *diag_ <unit-serial>.zip*, where <unit-serial> is the serial number of the EMX.
  - Filename as of version 3.0.0: *diag_ <unit-serial>.tgz*
- The EMX utters a short beep when writing the diagnostic data to the USB drive.

▶ **factory_reset**

- Supported as of release 3.0.0.
- If this option is set to `true`, the EMX will be reset to factory defaults.
- If the device configuration will be updated at the same time, the factory reset will be executed before updating the device configuration.

▶ **bulk_config_restore**

- Supported as of release 3.1.0.
- Specify the name of the bulk configuration file used to configure or restore the EMX.

Note: See **Bulk Configuration** *(on page 272) for instructions on generating a bulk configuration file.*

- Additional configuration keys set via the *config.txt* file will be applied after performing the bulk restore operation.
- This option CANNOT be used with the option "full_config_restore."
- If a firmware upgrade will be performed at the same time, you must generate the bulk configuration file based on the NEW firmware version instead of the current firmware version.

▶ **full_config_restore**

- Supported as of release 3.1.0.
- Specify the name of the full configuration backup file used to restore the EMX.

Note: See **Backup and Restore of Device Settings** *(on page 274) for instructions on generating the full configuration backup file.*

- Additional configuration keys set via the *config.txt* file will be applied after performing the configuration restore operation.
- This option CANNOT be used with the option "bulk_config_restore."
- If a firmware upgrade will be performed at the same time, you must generate the full configuration backup file based on the NEW firmware version instead of the current firmware version.

▶ **execute_lua_script**

- Supported as of release 3.3.0.
- Specify a LUA binding script file. For example:

  `execute_lua_script=my_script.lua`

- Script output will be recorded to a log file -- <BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log. Note this log file's size is limited on dhcp/tftp.
- A dhcp/tftp-located script has a timeout of 60 seconds. After that duration the script will be removed.
- If you unplug the USB drive while the LUA script is still running, the script will be removed.
- An exit handler can be used but the execution time is limited to three seconds. Note that this is not implemented on dhcp/tftp yet.
- This feature can be used to manage LuaService, such as upload, start, get output, and so on.

Raritan.

config.txt

To perform device configuration using a USB drive, you must:

- Copy the device configuration file "config.txt" to the root directory of the USB drive.
- Reference the "config.txt" file in the *config* option of the "fwupdate.cfg" file. See *fwupdate.cfg* (on page 432).

The file, *config.txt*, is a text file containing a number of configuration keys and values to configure or update.

This section only introduces the device configuration file in brief, and does not document all configuration keys, which vary according to the firmware version and your EMX model.

Tip: As of release 3.2.20, you can choose to encrypt important data in the "config.txt" file so that people cannot easily recognize it, such as the SNMP write community string. See **Data Encryption in 'config.txt'** *(on page 439).*

▶ **Regular configuration key syntax:**

- Each configuration key and value pair is in a single line as shown below:

```
key=value
```

Note: Each value in the file must be separated by an equal sign (=), without any surrounding spaces.

- As of release 3.1.0, multi-line values are supported by using the *Here Document Syntax* with a user-chosen delimiter.

  The following illustration declares a value in two lines. You can replace the delimiter `EOF` with other delimiter strings.

```
key<<EOF
value line 1
value line 2
EOF
```

Note: The line break before the closing EOF is not part of the value. If a line break is required in the value, insert an additional empty line before the closing EOF.

▶ **Special configuration keys:**

There are 3 special configuration keys that are prefixed with `magic:`.

- A special key that sets a user account's password without knowing the firmware's internal encryption/hashing algorithms is implemented as of release 2.2.13.

  Example:

  `magic:users[1].cleartext_password=joshua`

- Two special keys that set the SNMPv3 passphrases without knowing the firmware's internal encryption/hashing algorithms are implemented as of release 2.4.0.

  Examples:

  `magic:users[1].snmp_v3.auth_phrase=swordfish`

  `magic:users[1].snmp_v3.priv_phrase=opensesame`

▶ **To configure device-specific settings:**

1. Make sure the device list configuration file "devices.csv" is available in the USB drive. See *devices.csv* (on page 438)

2. In the "config.txt" file, refer each device-specific configuration key to a specific column in the "devices.csv" file. The syntax is: `${column}`, where "column" is a column number.

   Examples:

   `network.interfaces[eth0].ipaddr=${2}`

   `pdu.name=${16}`

▶ **To rename the admin user:**

As of release 3.1.0, you can rename the admin user by adding the following configuration key:

`users[0].name=new admin name`

Example:

`users[0].name=May`

Raritan.

devices.csv

If there are device-specific settings to configure, you must create a device list configuration file - *devices.csv*, to store unique data of each EMX.

This file must be:

- An excel file in the CSV format.
- Copied to the root directory.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See **fwupdate.cfg** (on page 432).

Every EMX identifies its entry in the "devicelist.csv" file by comparing its serial number or MAC address to one of the columns in the file.

▶ **Determine the column to identify EMX devices:**

- By default, a EMX searches for its serial number in the 1st column.
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

▶ **Syntax:**

- Prior to release 3.1.0, only single-line values containing NO commas are supported. A comma is considered a field delimiter.

  For example:

  ```
  Value-1,Value-2,Value-3
  ```

- As of release 3.1.0, values containing commas, line breaks or double quotes are all supported. The commas and line breaks to be included in the values must be enclosed in double quotes. Every double quote to be included in the value must be escaped with another double quote.

  For example:

  ```
  Value-1,"Value-2,with,three,commas",Value-3


  Value-1,"Value-2,""with""three""double-quotes",Valu
  e-3


  Value-1,"Value-2
  with a line break", Value-3
  ```

Data Encryption in 'config.txt'

Encryption for any settings in the file "config.txt" is supported as of release 3.2.20.

When intending to prevent people from identifying the values of any settings, you can encrypt them. Encrypted data still can be properly interpreted and performed by any EMX running firmware version 3.2.20 or later.

▶ **Data encryption procedure:**

1. Open the "config.txt" file to determine which setting(s) to encrypt.

2. Launch a terminal to log in to the CLI of any EMX running version 3.2.20 or later. See *Logging in to CLI* (on page 292).

3. Type the encryption command and the value of the setting you want to encrypt.

   ▪ The value *cannot* contain any double quotes (") or backslashes (-).

   ▪ If the value contains spaces, it must be enclosed in double quotes.

   ```
   # config encrypt <value>
   ```

   -- OR --

   ```
   # config encrypt "<value with spaces>"
   ```

4. Press Enter. The CLI generates and displays the encrypted form of the typed value.

5. Go to the "config.txt" file and replace the chosen value with the encrypted one by typing or copying the encrypted value from the CLI.

6. Add the text "encrypted:" to the beginning of the encrypted setting.

7. Repeat steps 3 to 6 for additional settings you intend to encrypt.

8. Save the changes made to the "config.txt" file. Now you can use this file to configure any EMX running version 3.2.20 or later. See *Configuration or Firmware Upgrade with a USB Drive* (on page 430).

▶ **Illustration:**

In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.

snmp.write_community=private

1. In the CLI, type the following command to encrypt "private."

   `# config encrypt private`

2. The CLI generates and shows the encrypted form of "private."

   `ZTtnYcvQUw==`

3. In the "config.txt" file, make the following changes to the SNMP write community setting.

   a. Replace the word "private" with the encrypted value that CLI shows.

   `snmp.write_community=ZTtnYcvQUw==`

   b. Add "encrypted:" to the beginning of that setting.

   `encrypted:snmp.write_community=ZTtnYcvQUw==`

Firmware Upgrade via USB

Firmware files are available on Raritan website's *Support page* (*http://www.raritan.com/support/*).

Note that if the firmware file used for firmware upgrade is the same as the firmware version running on the EMX, no firmware upgrade will be performed unless you have set the *force_update* option to true in the "fwupdate.cfg" file. See *fwupdate.cfg* (on page 432).

▶ **To use a USB drive to upgrade the EMX:**

1. Copy the configuration file "fwupdate.cfg" and an appropriate firmware file to the root directory of the USB drive.

2. Reference the firmware file in the *image* option of the "fwupdate.cfg" file.

3. Plug the USB drive into the USB-A port on the EMX.

4. The EMX performs the firmware upgrade. The firmware upgrade message "FUP" is displayed on the front panel display.

   Tip: You can remove the USB drive and plug it into another EMX for firmware upgrade when the firmware upgrade message displays.

5. It may take one to five minutes to complete the firmware upgrade, depending on your product.

6. When the firmware upgrade finishes, the front panel display indicates the firmware upgrade result.

    ▪ **Happy smiley**: Successful.

    Depending on your product, the happy smiley looks like one of the following.
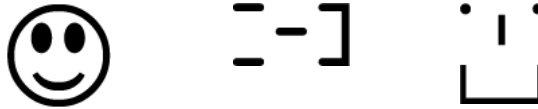
    ▪ Sad smiley: Failed. Check the log file in the USB drive or contact Raritan Technical Support to look into the failure cause.

    The sad smiley looks like one of the following.
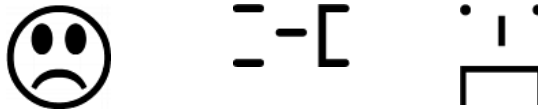
Appendix C Bulk Configuration or Firmware Upgrade via DHCP/TFTP

If a TFTP server is available, you can use it and appropriate configuration files to perform any or all of the following tasks for a large number of EMX devices in the same network.

- Initial deployment
- Configuration changes
- Firmware upgrade
- Downloading diagnostic data

This feature is drastically useful if you have hundreds or even thousands of EMX devices to configure or upgrade.

> Warning: The feature of bulk configuration or firmware upgrade via DHCP/TFTP only works on standalone EMX devices directly connected to the network. This feature does NOT work for slave devices in the USB-cascading configuration.

Tip: For the other alternative, see **Configuration or Firmware Upgrade with a USB Drive** *(on page 430).*

In This Chapter

Bulk Configuration/Upgrade Procedure

The DHCP/TFTP feature is supported as of release 3.1.0 so make sure that all EMX devices which you want to configure or upgrade are running firmware version 3.1.0 or later.

▶ **Steps of using DHCP/TFTP for bulk configuration/upgrade:**

1. Create configuration files specific to your EMX models and firmware versions. See *Configuration Files* (on page 431) or contact Raritan Technical Support to properly prepare some or all of the following files:

   - *fwupdate.cfg (always required)*

443

- *config.txt*
- *devices.csv*

Note: Supported syntax of "fwupdate.cfg" and "config.txt" may vary based on different firmware versions. If you have existing configuration files, it is suggested to double check with Raritan Technical Support for the correctness of these files prior to using this feature.

---

2. Configure your TFTP server properly. See *TFTP Requirements* (on page 443).

3. Copy ALL required configuration files into the TFTP root directory. If the tasks you will perform include firmware upgrade, an appropriate firmware binary file is also required.

4. Properly configure your DHCP server so that it refers to the file "fwupdate.cfg" on the TFTP server for your EMX.

   Click one or more of the following links for detailed DHCP configuration instructions, based on your system and the IP address type.

   - *DHCP IPv4 Configuration in Windows* (on page 444)
   - *DHCP IPv6 Configuration in Windows* (on page 454)
   - *DHCP IPv4 Configuration in Linux* (on page 461)
   - *DHCP IPv6 Configuration in Linux* (on page 463)

5. Make sure all of the desired EMX devices use DHCP as the IP configuration method and have been *directly* connected to the network.

6. Re-boot these EMX devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those EMX devices supporting DHCP in the same network.

   DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

TFTP Requirements

To perform bulk configuration or firmware upgrade successfully, your TFTP server must meet the following requirements:

- The server is able to work with both IPv4 and IPv6.

   In Linux, remove any IPv4 or IPv6 flags from */etc/xinetd.d/tftp*.

   Note: DHCP will execute the "fwupdate.cfg" commands once for IPv4 and once for IPv6 respectively if both IPv4 and IPv6 settings are configured properly in DHCP.

- All required configuration files are available in the TFTP root directory. See *Bulk Configuration/Upgrade Procedure* (on page 442).

If you are going to upload any EMX diagnostic file or create a log file in the TFTP server, the first of the following requirements is also required.

- The TFTP server supports the write operation, including file creation and upload.

  In Linux, provide the option "-c" for write support.

- **Required for uploading the diagnostic file only** - the timeout for file upload is set to one minute or larger.

DHCP IPv4 Configuration in Windows

For those EMX devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

▶ **Required Windows IPv4 settings in DHCP:**

1. Add a new vendor class for Raritan EMX under IPv4.

   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.

   b. Click Add to add a new vendor class.
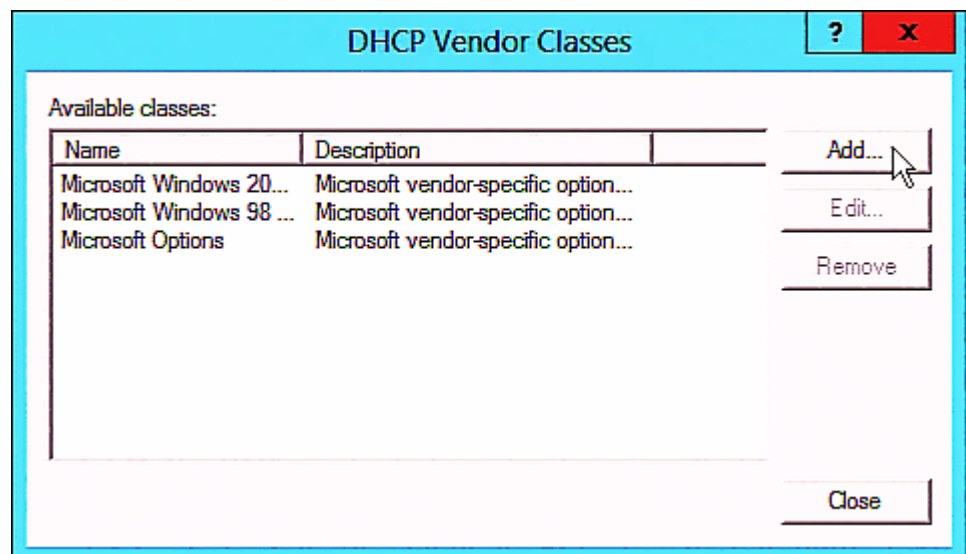
   c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.

2. Define one DHCP standard option - Vendor Class Identifier.

    a. Right-click the IPv4 node in DHCP to select Set Predefined Options.

b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.
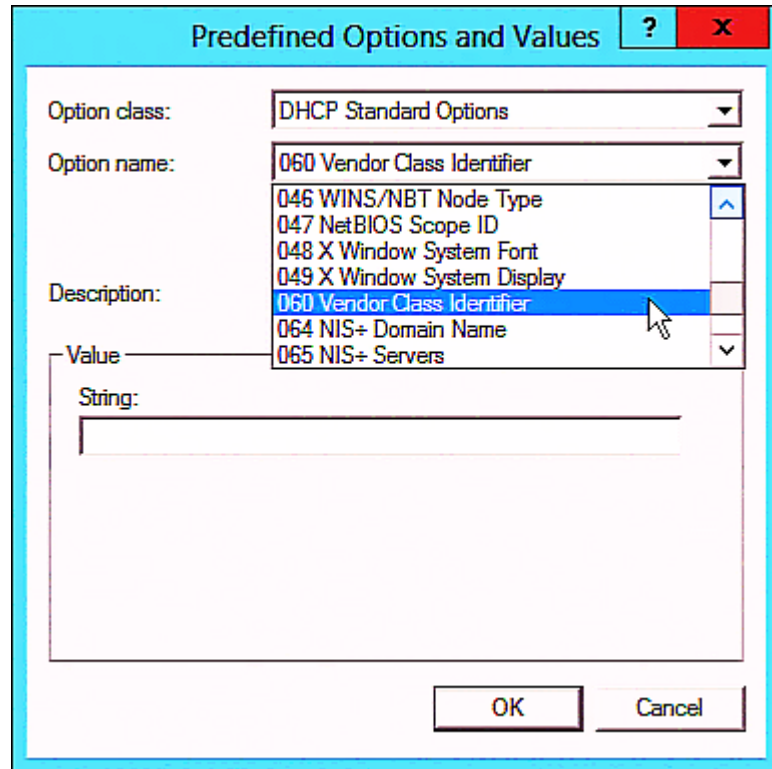
3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

a. Select Raritan PDU in the "Option class" field.

b. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.

c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

d. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

4. Create a new policy associated with the "Raritan PDU" vendor class.

a. Right-click the Policies node under IPv4 to select New Policy.

b. Specify a policy name, and click Next.

The policy is named "PDU" in this illustration.

c. Click Add to add a new condition.

d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

e. Click Next.

f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.

g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv4 address in the "IP address" field.

h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Raritan.

Important: The magic cookie is transmitted to and stored in EMX at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in EMX. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

DHCP IPv6 Configuration in Windows

For those EMX devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

▶ **Required Windows IPv6 settings in DHCP:**

1. Add a new vendor class for Raritan EMX under IPv6.

a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.
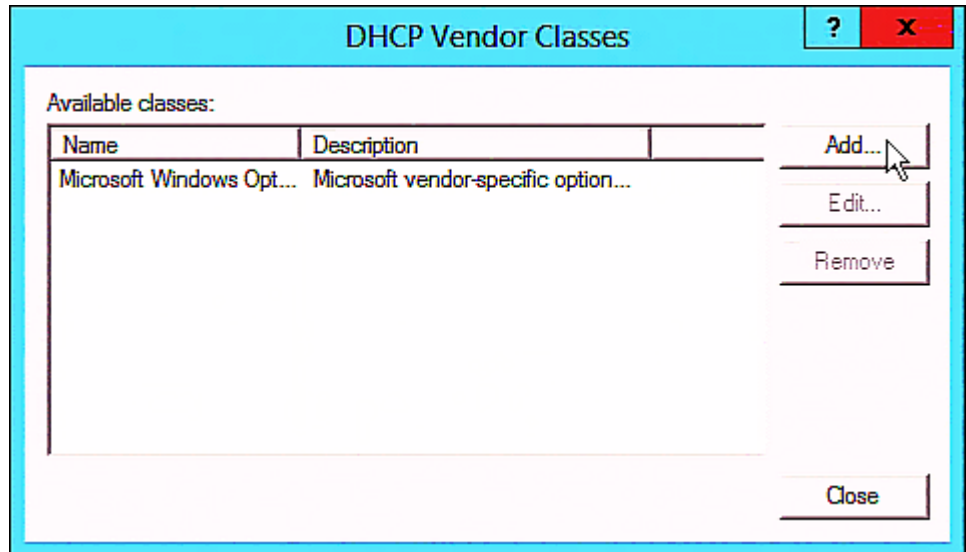
c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.

2. Add three options to the "Raritan PDU 1.0" vendor class.

    a. Right-click the IPv6 node in DHCP to select Set Predefined
        Options.

b. Select Raritan PDU 1.0 in the "Option class" field.

c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.

d. Click Add to add the second option. Type
"pdu-update-control-file" in the Name field, select String as the
data type, and type 2 in the Code field.

e. Click Add to add the third one. Type "pdu-update-magic" in the
Name field, select String as the data type, and type 3 in the Code
field.

3. Configure server options associated with the "Raritan PDU 1.0"
vendor class.

a. Right-click the Server Options node under IPv6 to select
Configure Options.

b. Click the Advanced tab.

c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv6 address in the "IPv6 address" field.

d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in EMX at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in EMX. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

DHCP IPv4 Configuration in Linux

Modify the "dhcpd.conf" file for IPv4 settings when your DHCP server is running Linux.

▶ **Required Linux IPv4 settings in DHCP:**

1. Locate and open the "dhcpd.conf" file of the DHCP server.

2. The EMX will provide the following value of the vendor-class-identifier option (option 60).

   ▪ vendor-class-identifier = "Raritan PDU 1.0"

Configure the same option in DHCP accordingly. The EMX accepts the configuration or firmware upgrade only when this value in DHCP matches.

3. Set the following three sub-options in the "vendor-encapsulated-options" (option 43).

   ▪ code 1 (pdu-tftp-server) = the TFTP server's IPv4 address

   ▪ code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"

   ▪ code 3 (pdu-update-magic) = any string

   This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

   The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in EMX at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in EMX. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

➤ **IPv4 illustration example in dhcpd.conf:**

```
[...]

set vendor-string = option vendor-class-identifier;
option space RARITAN code width 1 length width 1 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;


class "raritan" {
    match if option vendor-class-identifier = "Raritan PDU 1.0";
    vendor-option-space          RARITAN;
    option RARITAN.pdu-tftp-server 192.168.1.7;
    option RARITAN.pdu-update-control-file "fwupdate.cfg";
    option RARITAN.pdu-update-magic "20150123-0001";
    option vendor-class-identifier "Raritan PDU 1.0";
}


[...]
```

DHCP IPv6 Configuration in Linux

Modify the "dhcpd6.conf" file for IPv6 settings when your DHCP server is running Linux.

➤ **Required Linux IPv6 settings in DHCP:**

1. Locate and open the "dhcpd6.conf" file of the DHCP server.

2. The EMX will provide the following values to the "vendor-class" option (option 16). Configure related settings in DHCP accordingly.

   - 13742 (Raritan's IANA number)

   - Raritan PDU 1.0

   - 15 (the length of the above string "Raritan PDU 1.0")

3. Set the following three sub-options in the "vendor-opts" (option 17).

   - code 1 (pdu-tftp-server) = the TFTP server's IPv6 address

   - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"

Raritan.

- code 3 (pdu-update-magic) = any string

  This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

  The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in EMX at the time of executing the "fwupdate.cfg" commands. The DHCP/TFTP operation is triggered only when there is a mismatch between the magic cookie in DHCP and the one stored in EMX. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

▶ **IPv6 illustration example in dhcpd6.conf:**

```
[...]

option space RARITAN code width 2 length width 2 hash size 3;
option RARITAN.pdu-tftp-server code 1 = ip6-address;
option RARITAN.pdu-update-control-file code 2 = text;
option RARITAN.pdu-update-magic code 3 = text;
option vsio.RARITAN code 13742 = encapsulate RARITAN;

[...]

subnet6 xxxx {

[...]
        option RARITAN.pdu-tftp-server 1::2;
        option RARITAN.pdu-update-control-file "fwupdate.cfg";
        option RARITAN.pdu-update-magic "20150123-0001";
[...]

}
```

Appendix D   Resetting to Factory Defaults

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

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. Only firmware upgrade history is retained.

▶ **Alternative:**

Another method to reset it to factory defaults is to use the web interface. See *Resetting All Settings to Factory Defaults* (on page 277).

In This Chapter

Using the Reset Button

An RS-232 serial connection to a computer is required for using the reset button.

The following diagrams show the reset button on EMX2-111 and EMX2-888.

EMX2-111:
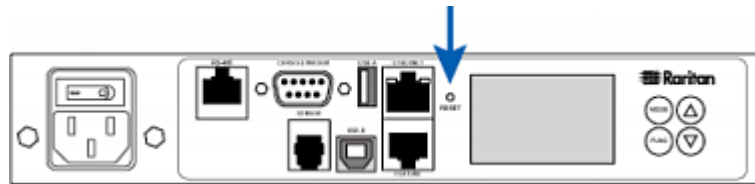
EMX2-888:
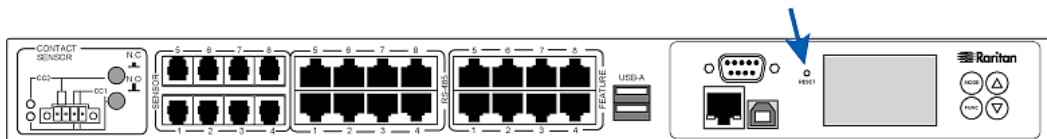
▶ **To reset to factory defaults using the reset button:**

1. Connect a computer to the EMX device. See *Connecting the EMX to a Computer* (on page 12).

2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the EMX. For information on the serial port configuration, see Step 2 of *Initial Network Configuration via CLI* (on page 15).

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.

Using the CLI Command

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* (on page 291).

▶ **To reset to factory defaults after logging in to the CLI:**

1. Connect to the EMX device. See *Logging in to CLI* (on page 292) or *Connecting the EMX to a Computer* (on page 12).

2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the EMX. For information on the serial port configuration, see Step 2 of *Initial Network Configuration via CLI* (on page 15).

3. Log in to the CLI by typing the user name "admin" and its password.

4. After the # system prompt appears, type either of the following commands and press Enter.

   #   reset factorydefaults

   　　　 -- OR --

   #   reset factorydefaults /y

5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.

6. Wait until the Username prompt appears, indicating the reset is complete.

▶ **To reset to factory defaults without logging in to the CLI:**

The EMX provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the EMX and launch a terminal emulation program as described in the above procedure.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

   ```
   Username:  factorydefaults
   ```

3. Type y on a confirmation message to perform the reset.

Appendix E 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 roles (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

Important: Raritan disables SSL 3.0 and uses TLS for releases 3.0.4, 3.0.20 and later releases due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

In This Chapter

Step A. Determine User Accounts and Roles

Determine the user accounts and roles (groups) that are authenticated for accessing the EMX. In this example, we will create two user roles with different permissions. Each role (group) will consist of two user accounts available on the AD server.

User roles	User accounts (members)
EMX_User	usera
	emxuser2
EMX_Admin	userb
	emxuser

Group permissions:

- The EMX_User role will only have read-only permissions.
- The EMX_Admin role will have full system permissions.

Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the EMX on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups (roles) 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.

Raritan.
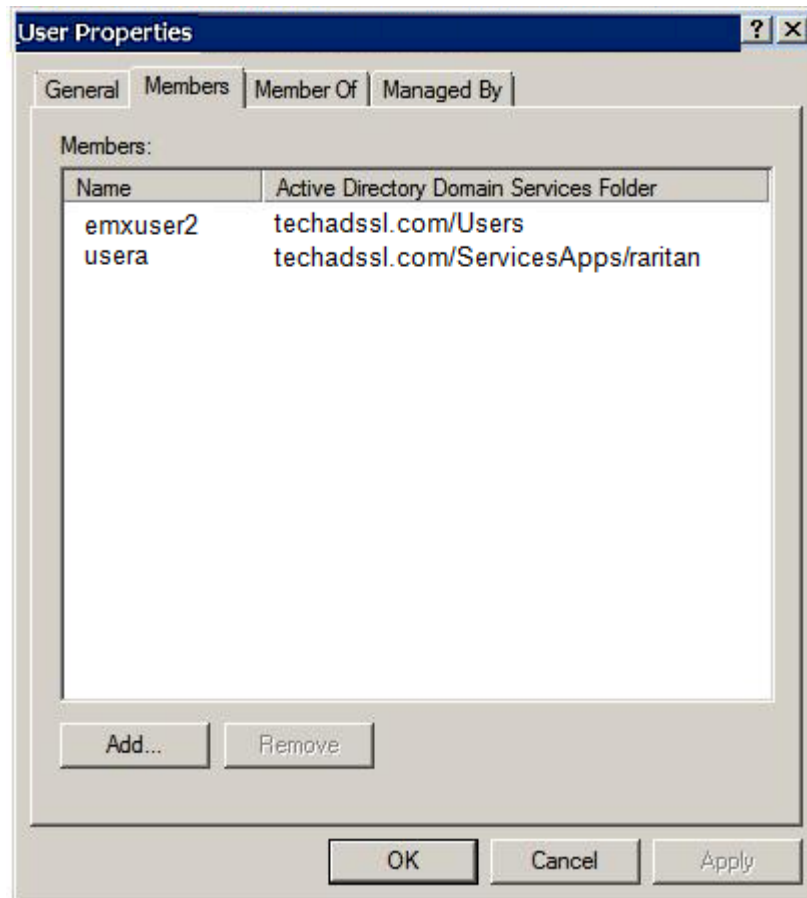
3. Add the *emxuser* and *userb* accounts to the EMX_Admin group.
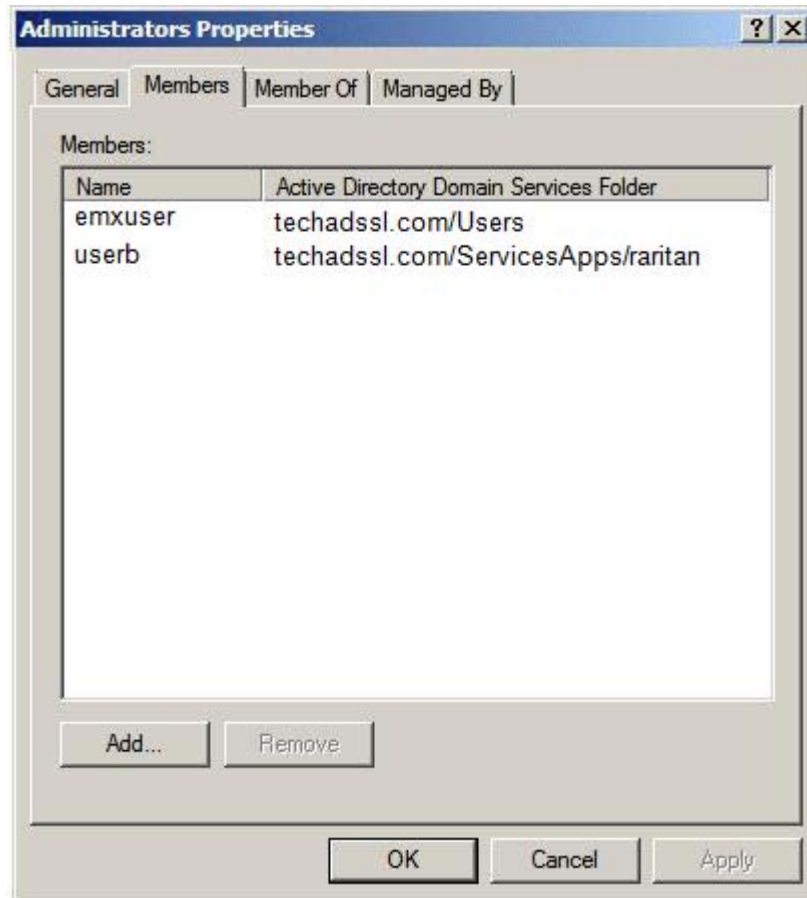
4. Verify whether each group comprises correct users.

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 *Wired Network Settings* (on page 150) and *Role of a DNS Server* (on page 535).
- 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 TLS.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

▶ **To configure LDAP authentication:**

1. Choose Device Settings > Security > Authentication.
2. In the LDAP Servers section, click New to add an LDAP/LDAPS server.
3. Provide the EMX with the information about the AD server.

Field/setting	Do this...
IP Address / Hostname	Type the domain name `techadssl.com` or IP address `192.168.56.3`. *Important: Without the 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 encryption is enabled.*
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP Server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to `389`.
Port (TLS), CA Certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous Bind	Select this checkbox because anonymous bind is used.

Field/setting	Do this...
Bind DN, Bind Password, Confirm Bind Password	Skip the three fields because of anonymous bind.
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`.

4. Click Add Server.The LDAP server is saved.
5. In the Authentication Type field, select LDAP.
6. Click Save. The LDAP authentication is activated.

Note: If the EMX clock and the LDAP server clock are out of sync, the installed TLS certificates, if any, may be considered expired. To ensure proper synchronization, administrators should configure the EMX and the LDAP server to use the same NTP server(s).

Step D. Configure Roles 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.

2. Click ![icon] to add a new role.

    a. Type `EMX_User` in the Role Name field.

    b. Type a description for the EMX_User role in the Description field. In this example, we type "View EMX settings" to describe the role.

    c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.

    d. Click Save.

3. The EMX_User role is created.

4. Keep the Roles page open to create the EMX_Admin role.

▶ **To create the EMX_Admin role with full permissions assigned:**

1. Click ![icon] to add another role.

   a. Type EMX_Admin in the Role Name field.

   b. Type a description for the EMX_Admin role in the Description field. In this example, we type "Includes all EMX privileges" to describe the role.

   c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all EMX settings.

   d. Click Save.

2. The EMX_Admin role is created.

Roles	☑ 👤+
Role Name ▲	**Description**
Admin	System defined administrator role including all privileges. 🔒
EMX_Admin	Includes all EMX privileges
EMX_User	View EMX settings
Operator	Predefined operator role.

Raritan.
A brand of Legrand

Appendix F   Updating the LDAP Schema

In This Chapter

Returning User Group Information

Use the information in this section to return User Group information (and assist with authorization) once authentication is successful.

From LDAP/LDAPS

When an LDAP/LDAPS authentication is successful, the EMX determines the permissions for a given user based on the permissions of the user's role. Your remote LDAP server can provide these user role names by returning an attribute named as follows:

rciusergroup   attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user role information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

▶ **To permit write operations to the schema:**

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.
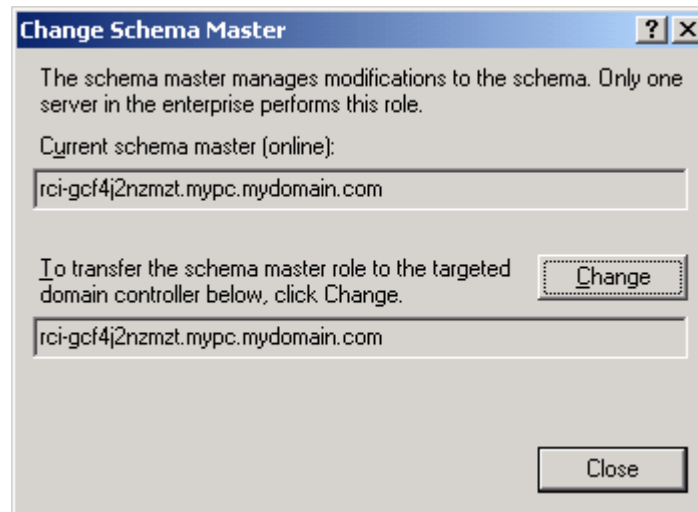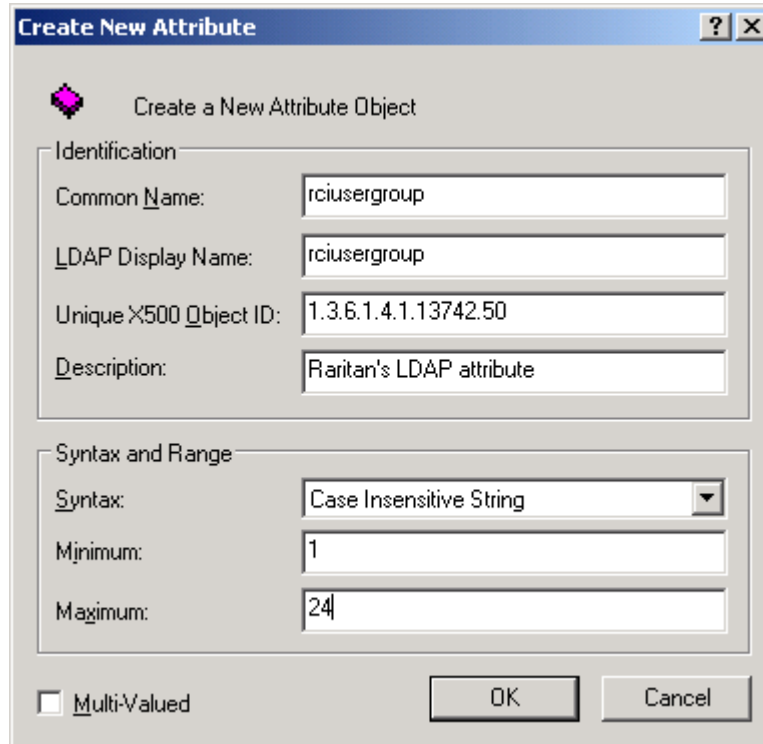
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**

3. Click OK.

Creating a New Attribute

▶ **To create new attributes for the rciusergroup class:**

1. Click the + symbol before Active Directory® Schema in the left pane of the window.

2. Right-click Attributes in the left pane.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

▶ **To add attributes to the class:**

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.
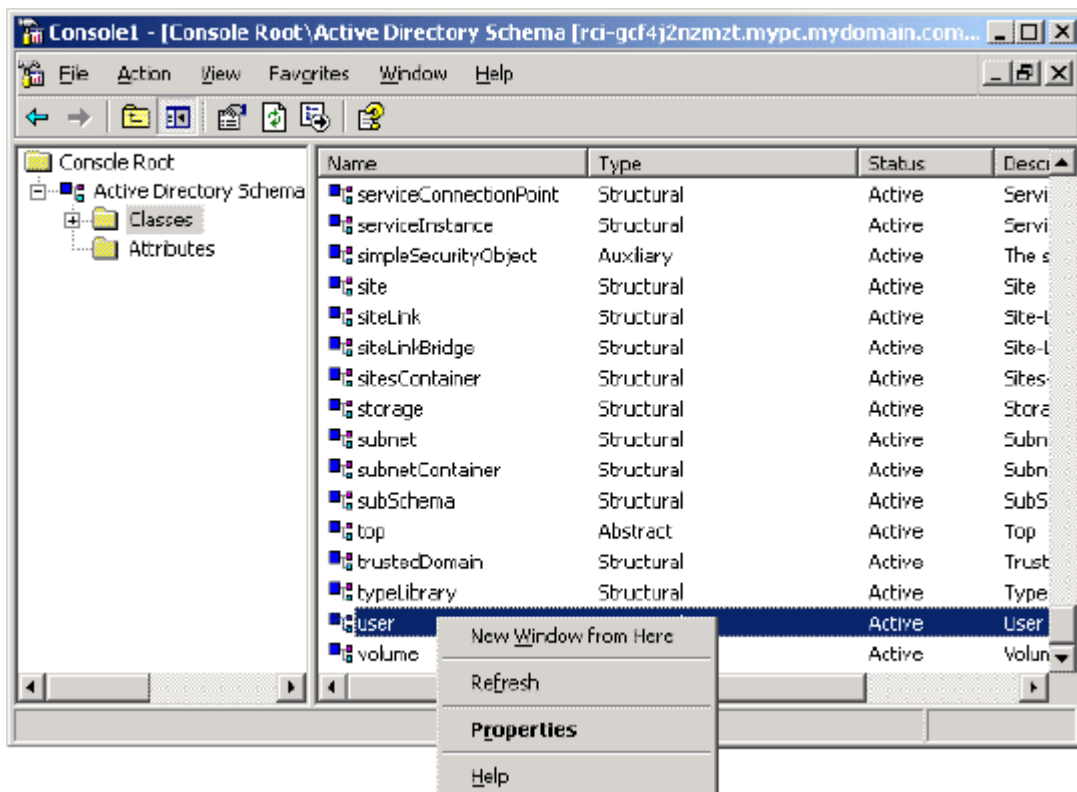
3. Choose Properties from the menu. The user Properties dialog appears.

4. Click the Attributes tab to open it.

5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.
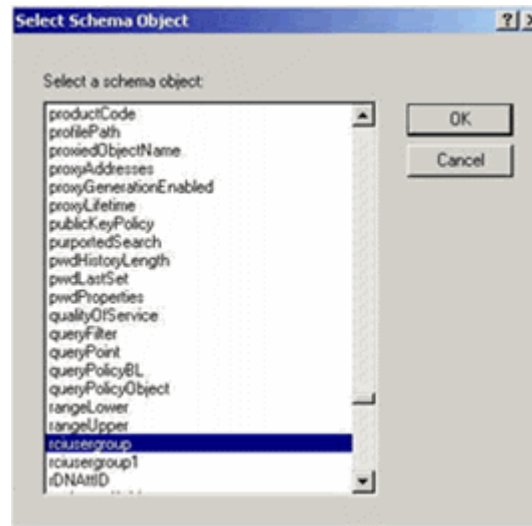
7. Click OK in the Select Schema Object dialog.
8. Click OK in the User Properties dialog.

Updating the Schema Cache

▶ **To update the schema cache:**

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.
2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

▶ **To edit the individual user attributes within the group rciusergroup:**

1. From the installation CD, choose Support > Tools.
2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.
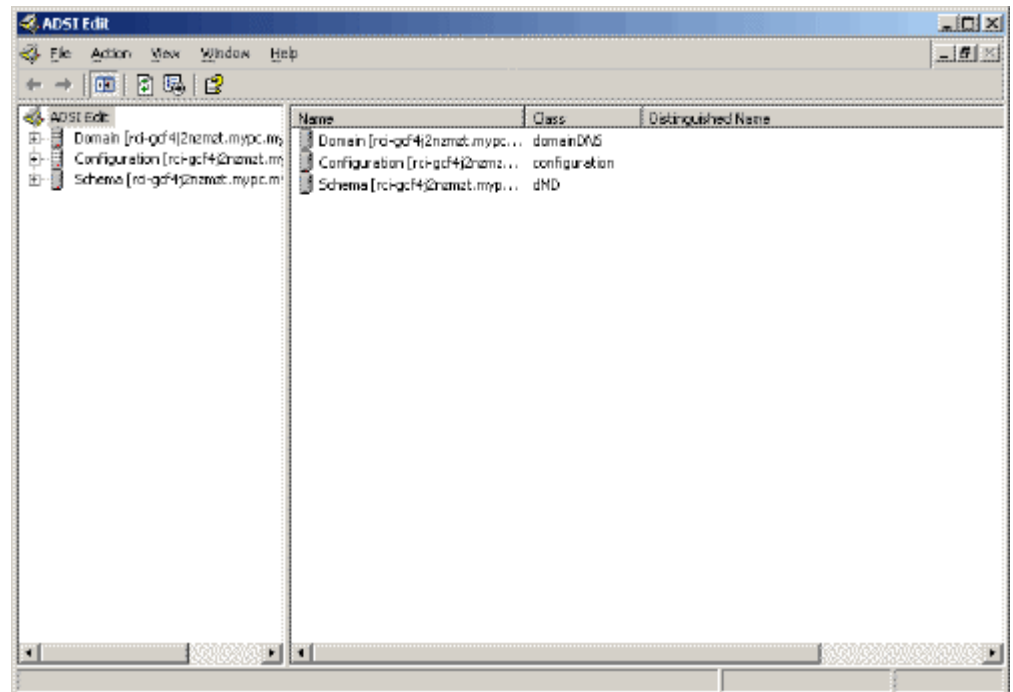
4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.
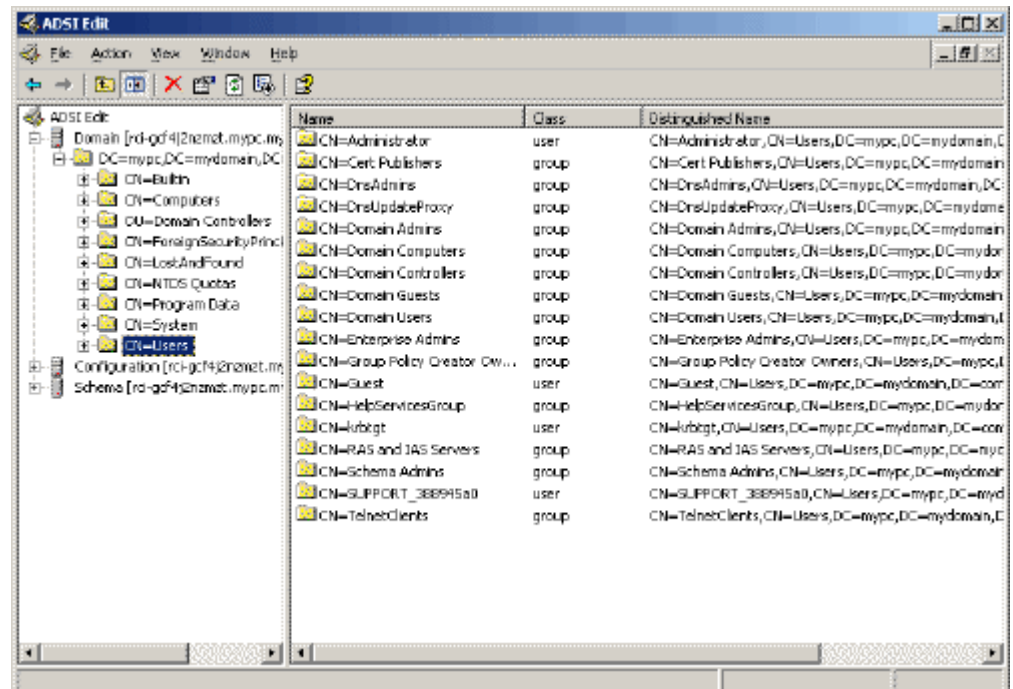
6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.
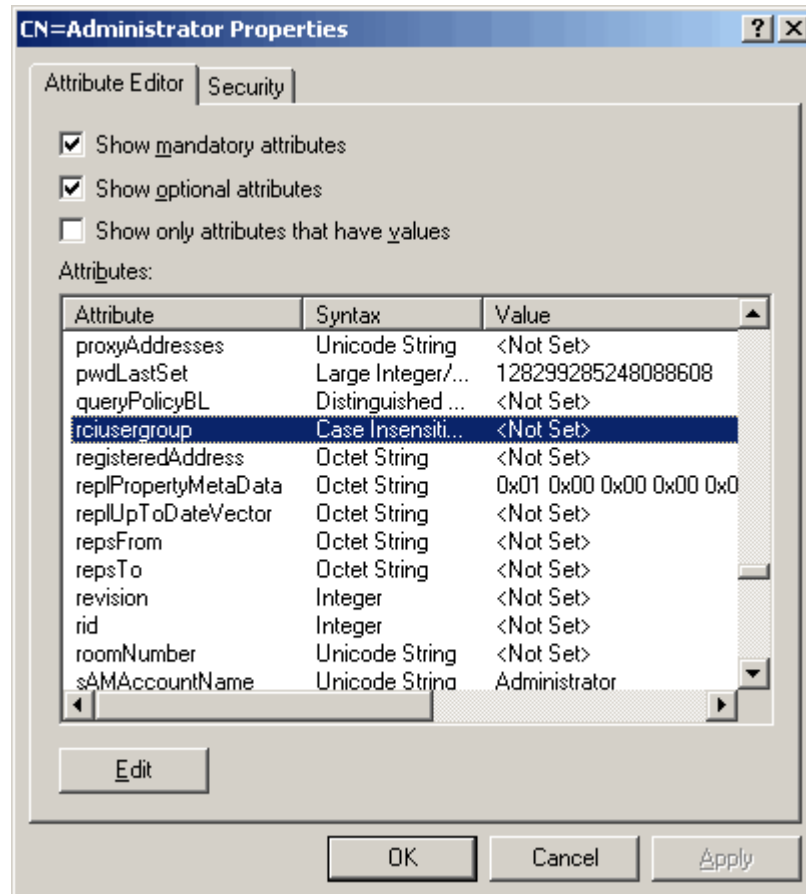
8. Click Edit. The String Attribute Editor dialog appears.

9. Type the user role (created in the EMX) in the Edit Attribute field. Click OK.
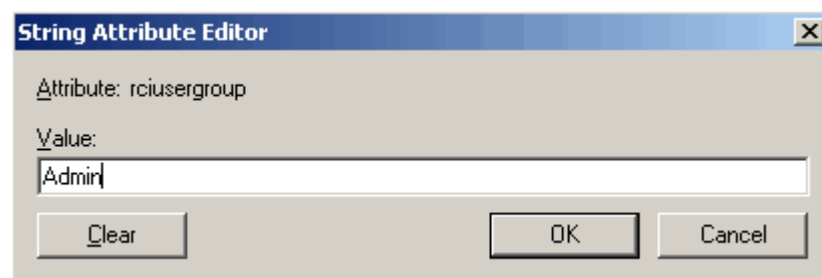
Appendix G RADIUS Configuration Illustration

This section provides illustrations for configuring RADIUS authentication. One illustration is based on the Microsoft® Network Policy Server (NPS), and the other is based on a FreeRADIUS server.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the EMX. See *Adding Radius Servers* (on page 195).
2. Configure roles on the EMX. See *Creating Roles* (on page 143).
3. Configure EMX user credentials and roles on your RADIUS server.
   - To configure using standard attributes, see *Standard Attributes* (on page 483).
   - To configure using vendor-specific attributes, see *Vendor-Specific Attributes* (on page 502).

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

In This Chapter

Standard Attributes

The RADIUS standard attribute "Filter-ID" is used to convey the group membership, that is, roles.

- If a user has multiple roles, configure multiple standard attributes for this user.
- The syntax of a standard attribute is:
  `Raritan:G{role-name}`

For configuration on NPS, see *NPS Standard Attribute Illustration* (on page 483).

For configuration on FreeRADIUS, see *FreeRADIUS Standard Attribute Illustration* (on page 501).

NPS Standard Attribute Illustration

To configure Windows 2008 NPS with the *standard attribute*, you must:

a. Add your EMX to NPS. See *Step A: Add Your EMX as a RADIUS Client* (on page 484).

b. On the NPS, configure Connection Request Policies and the standard attribute. See *Step B: Configure Connection Policies and Standard Attributes* (on page 488).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page 515).

Step A: Add Your EMX as a RADIUS Client

The RADIUS implementation on a EMX follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

▶ **Presumptions in the illustration:**

- IP address of your EMX = `192.168.56.29`
- RADIUS authentication port specified for EMX: *1812*
- RADIUS accounting port specified for EMX: *1813*

▶ **To add your EMX to the RADIUS NPS:**

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.

2. Right-click NPS (Local), and select Properties.

Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your EMX. In this example, they are 1812 and 1813. Then close this dialog.

3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.

4. Do the following to add your EMX to NPS:

   a. Verify the "Enable this RADIUS client" checkbox is selected.

   b. Type a name for identifying your EMX in the "Friendly name" field.

   c. Type *192.168.56.29* in the "Address (IP or DNS)" field.

   d. Select *RADIUS Standard* in the "Vendor name" field.

   e. Select the *Manual* radio button.

f. Type the shared secret in the "Shared secret" and "Confirm shared secret" fields. The shared secret must be the same as the one specified on your EMX.

5. Click OK.

Step B: Configure Connection Policies and Standard Attributes

You need to configure the following for connection request policies:

- IP address or host name of the EMX
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ Presumptions in the illustration:

- IP address of your EMX = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your EMX = `CHAP`
- Existing role of your EMX = `Admin`

▶ Illustration:

1. Open the NPS console, and expand the Policies folder.

2. Right-click Connection Request Policies and select New. The New
    Connection Request Policy dialog appears.

3. Type a descriptive name for identifying this policy in the "Policy
    name" field.

- You can leave the "Type of network access server" field to the
  default -- Unspecified.

4. Click Next to show the "Specify Conditions" screen. Click Add.

5. The "Select condition" dialog appears. Click Add.

6. The NAS IPv4 Address dialog appears. Type the EMX IP address --
    192.168.56.29, and click OK.

7. Click Next in the New Connection Request Policy dialog.

8. Select "Authenticate requests on this server" because a local NPS
    server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.

9. When the system prompts you to select the authentication method, select the following two options:

   ▪ Override network policy authentication settings

   ▪ CHAP -- the EMX uses "CHAP" in this example

Note: If your EMX uses PAP, then select "PAP."

10. Select Standard to the left of the dialog and then click Add.

11. Select Filter-Id from the list of attributes and click Add.
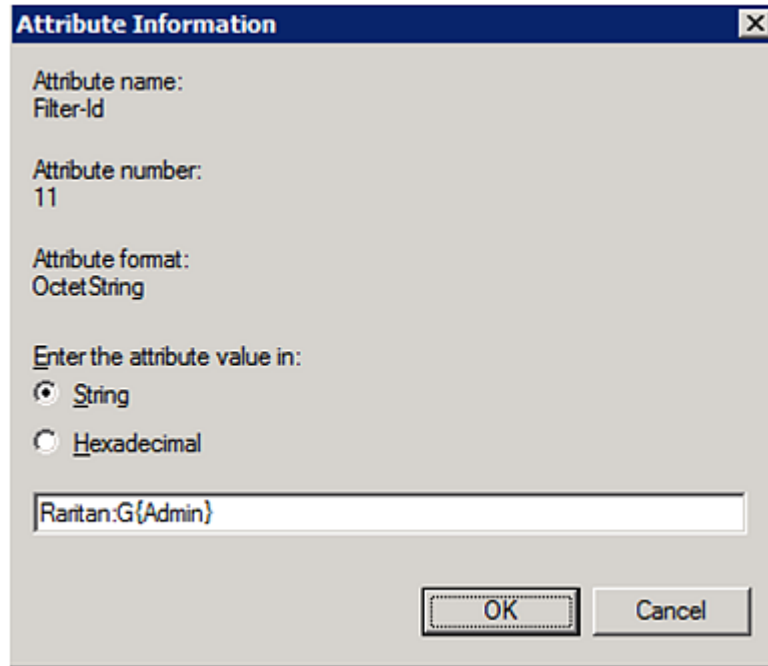
12. In the Attribute Information dialog, click Add.
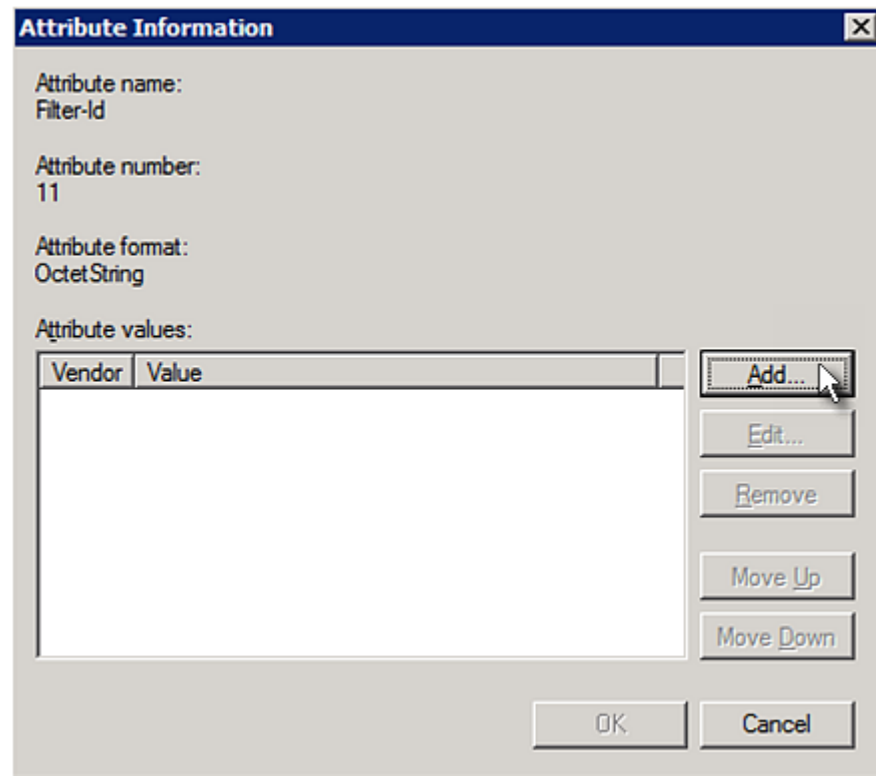
13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

Admin inside the curved brackets {} is the existing role on the EMX. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.

14. The new attribute is added. Click OK.

15. Click Next to continue.

16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.
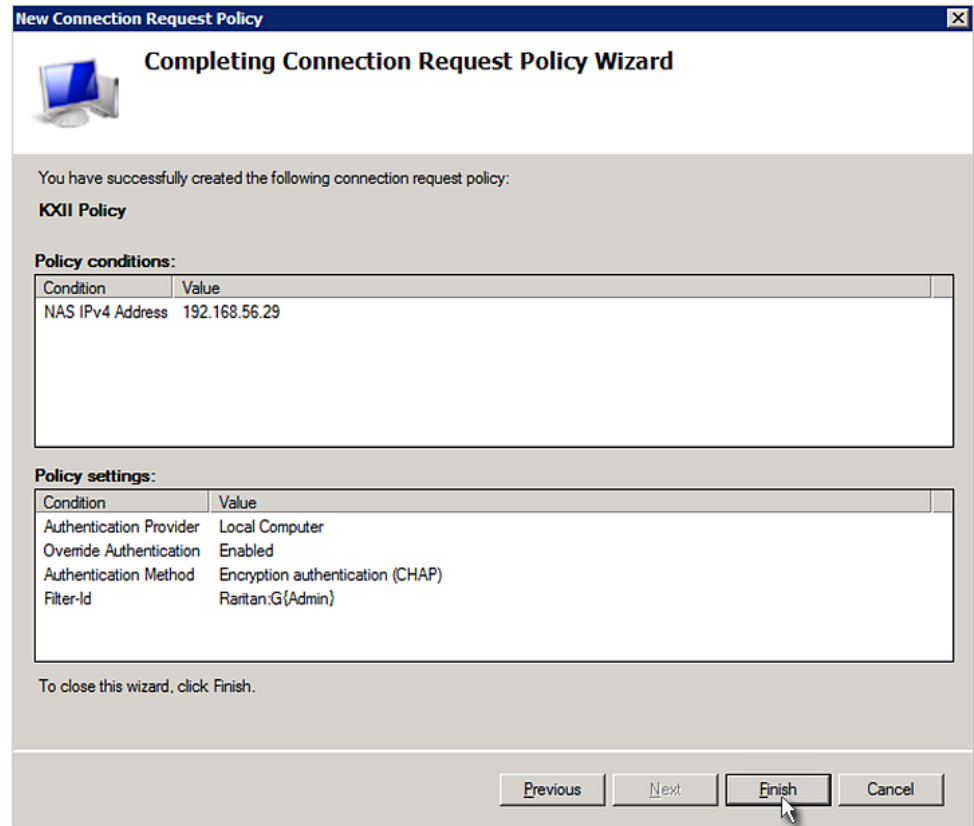
FreeRADIUS Standard Attribute Illustration

With standard attributes, NO dictionary files are required. You simply add all user data, including user names, passwords, and roles, in the following FreeRADIUS path.

`/etc/raddb/users`

▶ **Presumptions in the illustration:**

- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin` and `SystemTester`

▶ **To create a user profile for "steve" in FreeRADIUS:**

1. Go to this location: `/etc/raddb/users`.
2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Filter-ID = "Raritan:G{Admin}",
Filter-ID = "Raritan:G{SystemTester}"
```

Vendor-Specific Attributes

You must specify the following properties when using a RADIUS vendor-specific attribute (VSA).

* Vendor code = `13742`
* Vendor-assigned attribute number = `26`
* Attribute format = `String`

The syntax of the vendor-specific attribute for specifying one or multiple roles is:

`Raritan:G{role-name1 role-name2 role-name3}`

For configuration on NPS, see *NPS VSA Illustration* (on page 502).

For configuration on FreeRADIUS, see *FreeRADIUS VSA Illustration* (on page 514).

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your EMX to NPS. See *Step A: Add Your EMX as a RADIUS Client* (on page 484).

b. On the NPS, configure connection request policies and the vendor-specific attribute. See *Step B: Configure Connection Policies and Vendor-Specific Attributes* (on page 507).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page 515).

Step A: Add Your EMX as a RADIUS Client

The RADIUS implementation on a EMX follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

▶ **Presumptions in the illustration:**

- IP address of your EMX = `192.168.56.29`
- RADIUS authentication port specified for EMX: *1812*
- RADIUS accounting port specified for EMX: *1813*

▶ **To add your EMX to the RADIUS NPS:**

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.

2. Right-click NPS (Local), and select Properties.

Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your EMX. In this example, they are 1812 and 1813. Then close this dialog.

3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.

4. Do the following to add your EMX to NPS:

   a. Verify the "Enable this RADIUS client" checkbox is selected.

   b. Type a name for identifying your EMX in the "Friendly name" field.

   c. Type *192.168.56.29* in the "Address (IP or DNS)" field.

   d. Select *RADIUS Standard* in the "Vendor name" field.

   e. Select the *Manual* radio button.

f. Type the shared secret in the "Shared secret" and "Confirm shared secret" fields. The shared secret must be the same as the one specified on your EMX.

5. Click OK.

Step B: Configure Connection Policies and Vendor-Specific Attributes

You need to configure the following for connection request policies:

- IP address or host name of the EMX
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ **Presumptions in the illustration:**

- IP address of your EMX = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your EMX = `CHAP`
- Existing roles of your EMX = `Admin, User` and `SystemTester`

▶ **Illustration:**

1. Open the NPS console, and expand the Policies folder.
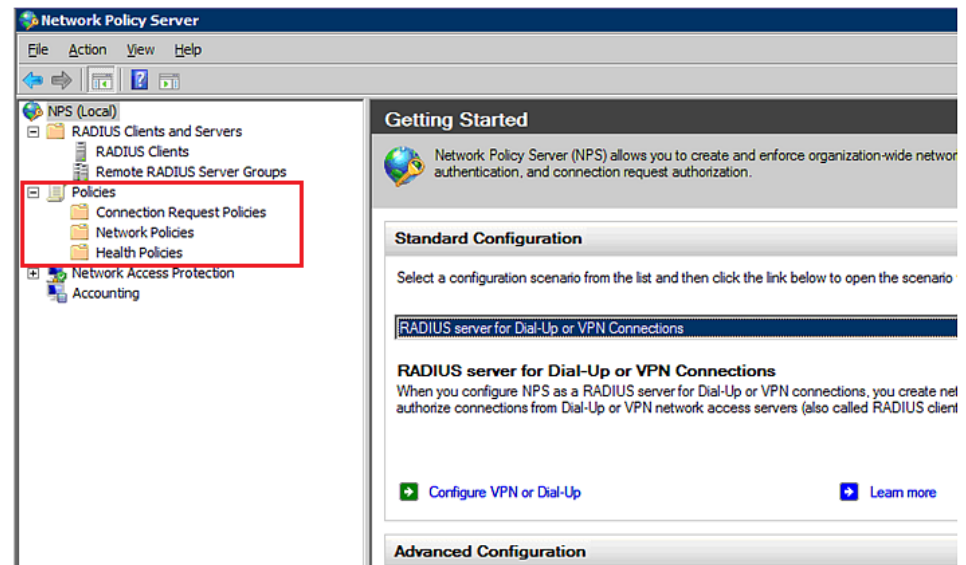
2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.
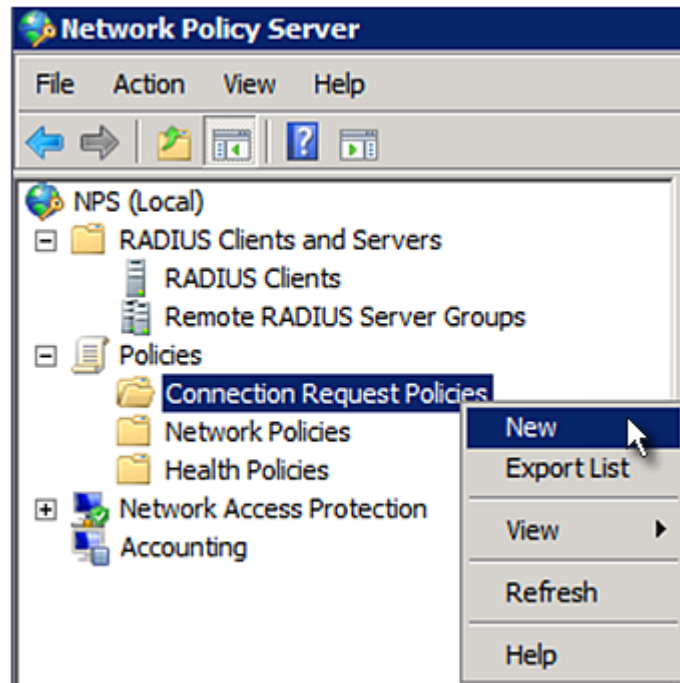
3. Type a descriptive name for identifying this policy in the "Policy name" field.

- You can leave the "Type of network access server" field to the default -- Unspecified.

New Connection Request Policy

Specify Connection Request Policy Nam

You can specify a name for your connection request policy and t applied.

Policy name:

RaritanDominionPolicy
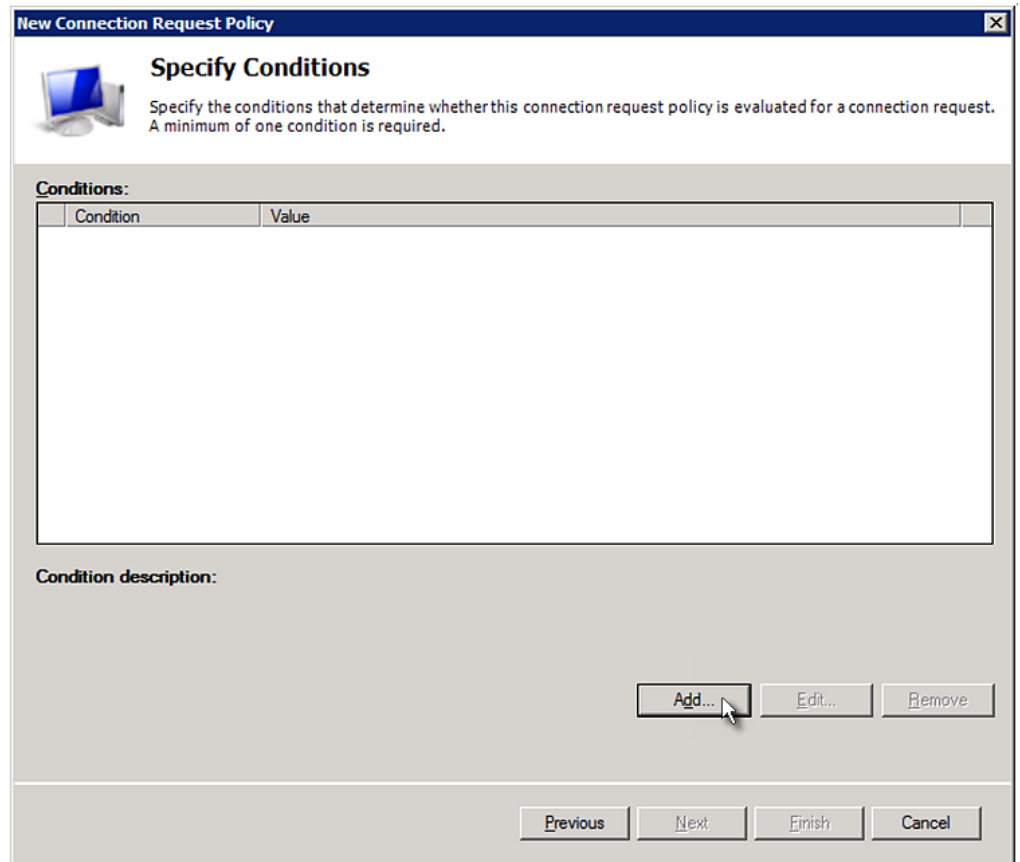
Network connection method

Select the type of network access server that sends the connection request to NPS. type or Vendor specific.

⦿ Type of network access server:

Unspecified ▾

○ Vendor specific:

10

Raritan.

4. Click Next to show the "Specify Conditions" screen. Click Add.

5. The "Select condition" dialog appears. Click Add.

6. The NAS IPv4 Address dialog appears. Type the EMX IP address --
    192.168.56.29, and click OK.

7. Click Next in the New Connection Request Policy dialog.

8. Select "Authenticate requests on this server" because a local NPS
    server is used in this example. Then click Next.

Raritan.
A brand of Legrand

Note: Connection Request Forwarding options must match your environment.

9. When the system prompts you to select the authentication method, select the following two options:

   ▪ Override network policy authentication settings

   ▪ CHAP -- the EMX uses "CHAP" in this example

Note: If your EMX uses PAP, then select "PAP."

10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.

11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.

12. Click Add, and the Vendor-Specific Attribute Information dialog appears.

13. Click "Enter Vendor Code" and type *13742*.

14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).

15. Click Configure Attribute, and then:

    a. Type *26* in the "Vendor-assigned attribute number" field.

    b. Select String in the "Attribute format" field.

    c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.

Note that multiple roles are separated with a space.
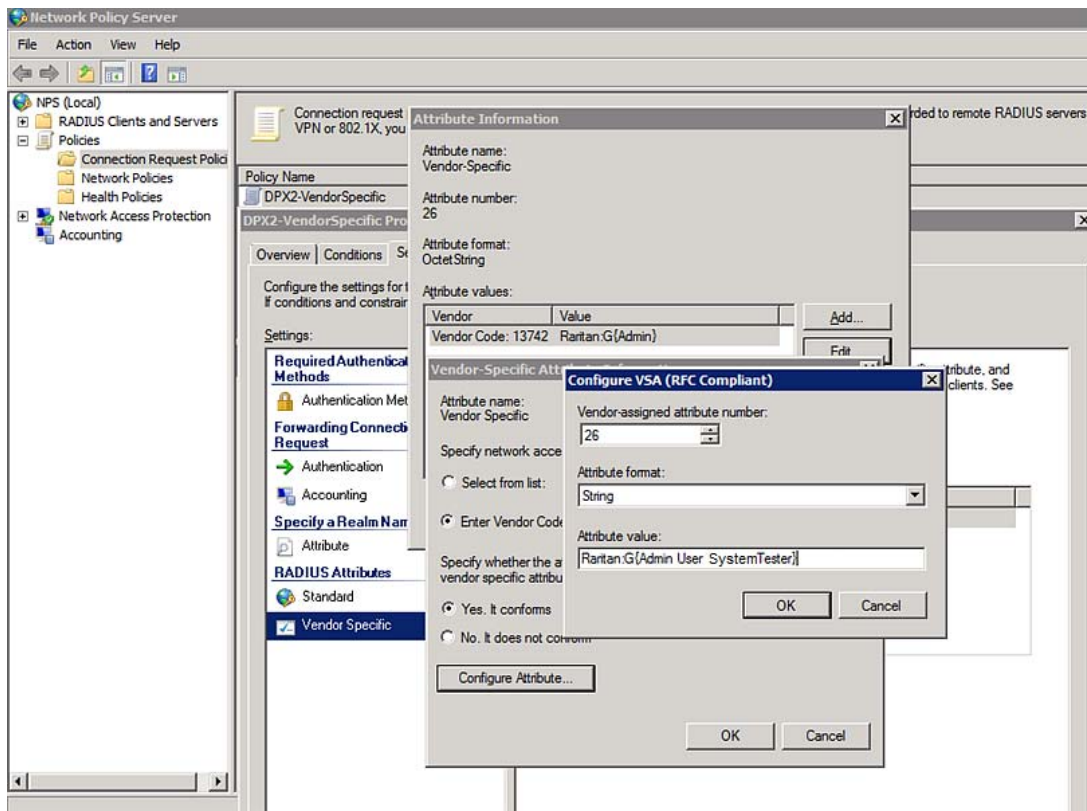
16. Click OK.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute

b. Add all user data, including user names, passwords, and roles

▶ **Presumptions in the illustration:**

- Raritan attribute = `Raritan-User-Roles`
- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin`, `User` and `SystemTester`

▶ **Step A -- define the vendor-specific attribute in FreeRADIUS:**

1. Go to this location: `/etc/raddb/dictionary`.
2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

▶ **Step B -- create a user profile for "steve" in FreeRADIUS:**

1. Go to this location: `/etc/raddb/users`.

2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

▶ **To register NPS:**

1. Open the NPS console.

2. Right-click NPS (Local) and select "Register server in Active Directory."
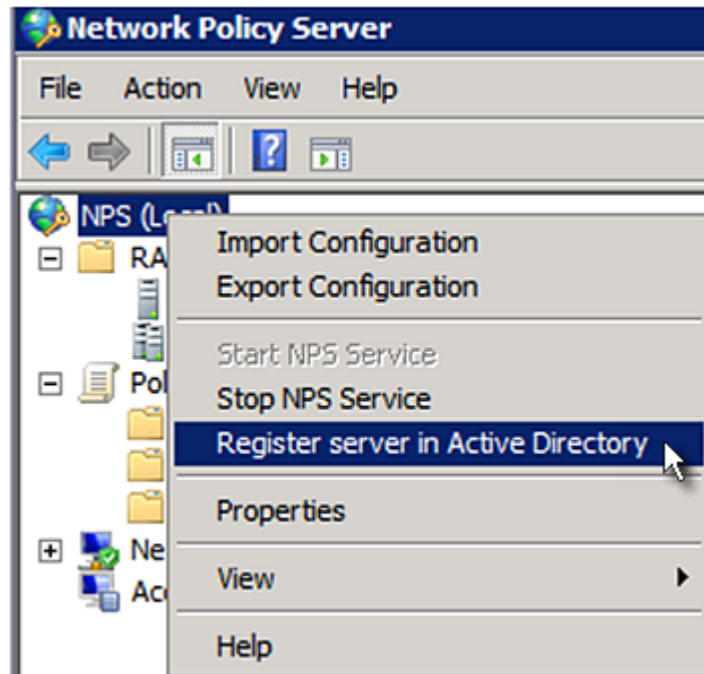
3. Click OK, and then OK again.
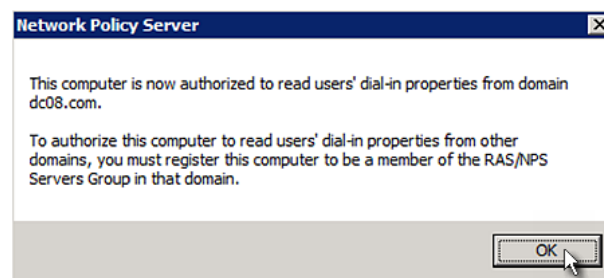
▶ **To grant EMX users remote access permission:**

1. Open Active Directory Users and Computers.

Raritan.
A brand of [] legrand®

517

2. Open the properties dialog of the user whom you want to grant the access permission.

3. Click the Dial-in tab and select the "Allow access" checkbox.

▶   **To enable reversible encryption for CHAP authentication:**

1. Open Active Directory Users and Computers.

2. Open the properties dialog of the user that you want to configure.

Raritan.

3. Click the Account tab and select the "Store password using reversible encryption" checkbox.

Appendix H Additional EMX Information

In This Chapter

Reserving IP Addresses in DHCP Servers

The EMX uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the EMX in a DHCP server, use the EMX device's serial number as the unique ID instead of the MAC address.

Since all network interfaces of the EMX can be simultaneously enabled and configured with diverse static IP addresses, the client identifier of each network interface is different. The main difference is the absence/presence of a suffix, which is the interface name added to the end of the serial number. The table below lists the client identifiers of all network interfaces.

Interface	Client Identifier
ETHERNET	serial number
WIRELESS	serial number plus the uppercase suffix "-WIRELESS"
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your EMX is set to the bridging mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of the ETHERNET and WIRELESS interfaces do NOT function.

Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

For each interface's client identifier, see *Reserving IP Addresses in DHCP Servers* (on page 519).

In the following illustration, it is assumed that the EMX serial number is PEG1A00003.

▶ **Windows IP address reservation illustration:**

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETHERNET	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, bring up the New Reservation dialog, and separate the converted ASCII codes with spaces.

   For example, to reserve the IP address of the ETHERNET interface, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. 50 45 47 31 41 30 30 30 30 33
Other fields	Configure as needed.

Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

For each interface's client identifier, see *Reserving IP Addresses in DHCP Servers* (on page 519).

In the following illustrations, it is assumed that the EMX serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

▶ **Illustration with ASCII code conversion:**

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETHERNET	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.

Interface	Client identifier conversion
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

   For example, the *converted* client identifier of the ETHERNET interface looks like the following:

   `00:50:45:47:31:41:30:30:30:30:33`

3. Now enter the converted client identifier with the following syntax.

host mypx {

option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;

fixed-address 192.168.20.1;

}

▶ **Illustration without ASCII code conversion:**

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.

2. A prefix "\000" must be added to the beginning of the client identifier.

   For example, the client identifier of the ETHERNET interface looks like the following:

   `\000PEG1A00003`

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

host mypx {

option dhcp-client-identifier = "\000PEG1A00003";

fixed-address 192.168.20.1;

}

Sensor Threshold Settings

This section explains the thresholds settings for a numeric sensor.

Thresholds and Sensor States

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.

above upper critical

Upper Critical

above upper warning

Upper Warning

normal

Lower Warning

below lower warning

Lower Critical

below lower critical
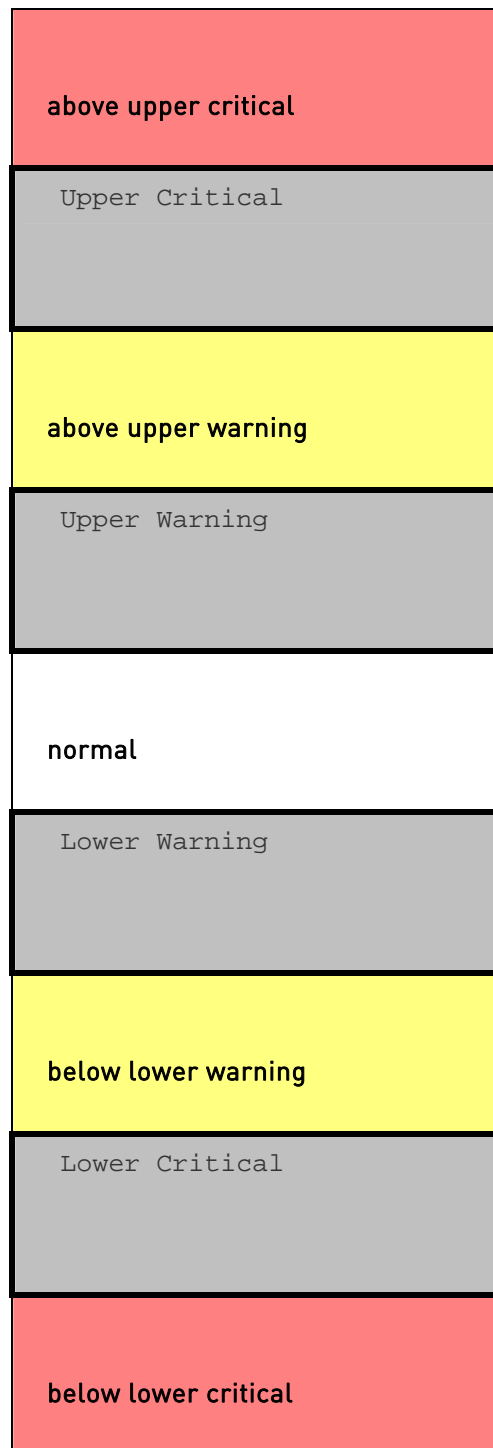
▶ Available sensor states:

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal' state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

▶ **Range of each available sensor state:**

The value of each enabled threshold determines the reading range of each available sensor state. For details, see *Yellow- or Red-Highlighted Sensors* (on page 106).

"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the EMX asserts a state for it whenever a bad state change occurs.

▶ **To assert a state:**

To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the EMX to assert.
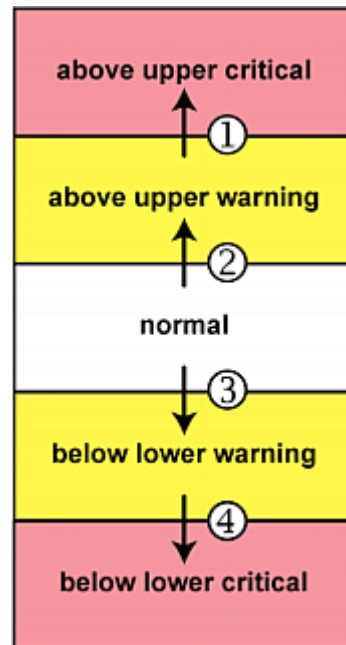
1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

▶ **Assertion Timeout:**

In the threshold settings, the Assertion Timeout field postpones or even cancels the "assertion" action. It determines how long a sensor must be in the "worse" new state before the EMX triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the EMX does NOT assert the worse state.

To disable the assertion timeout, set it to 0 (zero).

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. BCM2 is an exception to this, with a sample of 3 seconds.

▶ **How "Assertion Timeout" is helpful:**

If you have created an event rule that instructs the EMX to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's readings fluctuate around a certain threshold.

Assertion Timeout Example for Temperature Sensors

Assumption:
```
    Upper Warning threshold is enabled.
    Upper Warning = 25 (degrees Celsius)
    Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the EMX does NOT immediately announce this warning state. Instead it waits for 5 seconds, and then does either of the following:

- If the temperature remains above 25 degrees Celsius in the "above upper warning" range for 5 seconds, the EMX performs the "assertion" action to announce the "above upper warning" state.

- If the temperature drops below 25 degrees Celsius within 5 seconds, the EMX does NOT perform the "assertion" action.

"To De-assert" and Deassertion Hysteresis

After the EMX asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

▶ **To de-assert a state:**

To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the EMX to de-assert the previous state.
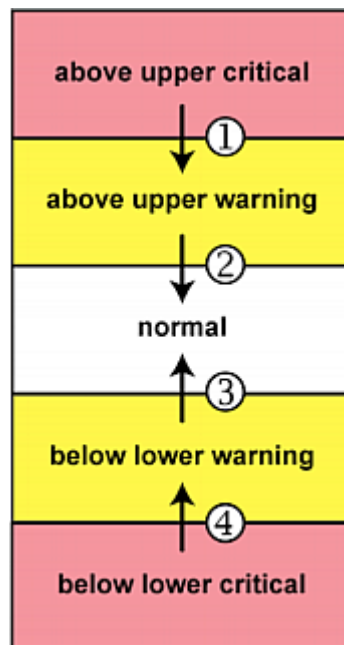
1. above upper critical --> above upper warning

2. above upper warning --> normal

3. below lower warning --> normal

4. below lower critical --> below lower warning

▶ **Deassertion Hysteresis:**

In the threshold settings, the Deassertion Hysteresis field determines a new level to trigger the "deassertion" action.

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the EMX to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then:

- Upper Critical = 33, so its "deassertion" level = 33 - 2 = 31.
- Upper Warning = 25, so its "deassertion" level = 25 - 2 = 23.
- Lower Critical = 10, so its "deassertion" level = 10 + 2 = 12.
- Lower Warning = 18, so its "deassertion" level = 18 + 2 = 20.

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

▶ How "Deassertion Hysteresis" is helpful:

If you have created an event rule that instructs the EMX to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's readings fluctuate around a certain threshold.

Deassertion Hysteresis Example for Temperature Sensors

Assumption:

```
Upper Warning threshold is enabled.
Upper Warning = 20 (degrees Celsius)
Deassertion Hysteresis = 3 (degrees Celsius)
"Deassertion"  level = 20-3 = 17 (degrees Celsius)
```

When the EMX detects that a temperature sensor's reading drops below 20 degrees Celsius, moving from the "above upper warning" range to the "normal" range, either of the following may occur:

- If the temperature falls between 20 and 17 degrees Celsius, the EMX does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the EMX performs the "deassertion" action to announce the end of the "above upper warning" state.

PDView App for Viewing the EMX

Raritan has developed an app that can turn your iOS or Android mobile device into a local display for the EMX.

This app is called PDView and it can be downloaded for free.

PDView is especially helpful when your EMX is not connected to the network but you need to check the EMX status, retrieve basic information, or even change network settings.

▶ **Requirements for using PDView:**

- The EMX is running firmware version 3.0.0 or later.
- If you are using an Android device, it must support USB "On-The-Go" (OTG).
- An appropriate USB cable is required.
  - For Android, you need an USB OTG adapter cable.
  - For iOS, use the USB cable shipped with your iOS mobile device.

▶ **To install PDView:**

1. Use your mobile device to download the PDView app from the Google Play or Apple's App Store.

2. After installing the PDView, launch it. Below illustrates the PDView screen for Android devices.
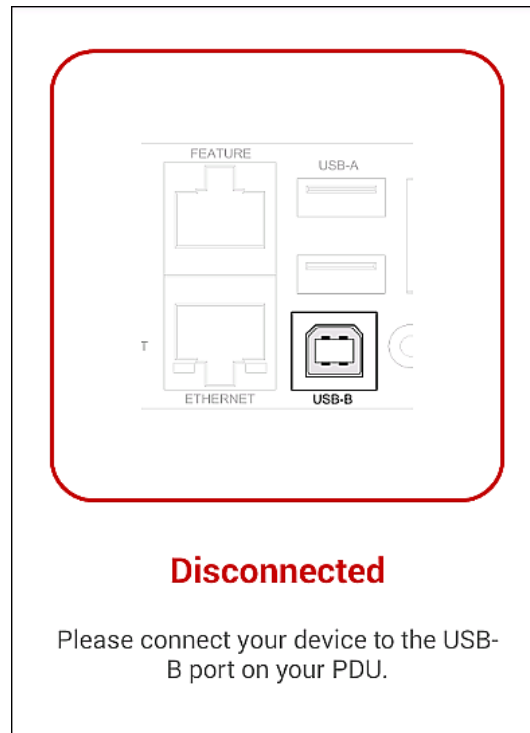
3. Connect your mobile device to the USB port of the EMX.

   Your mobile device type determines which USB port on the EMX shall be used to connect the mobile device. The PDView will automatically detect and indicate the appropriate USB port for connecting your mobile device.

The PDView shows a "Connected" message when it detects the physical connection to the EMX.

Connected

Connecting...
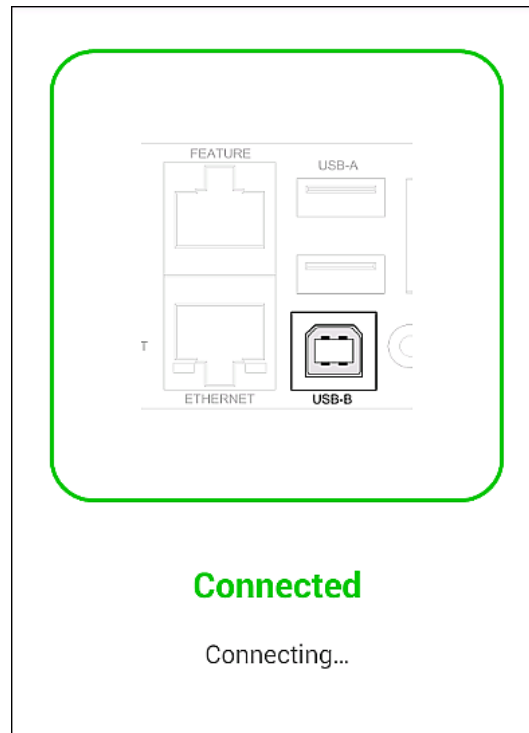
4. Log in to the PDView app at the login prompt. Now you can view limited EMX information or even change some settings.

Tip: To skip the final login step, you can click the upper right icon of PDView to save one or multiple user credentials. Next time the app automatically logs in when it detects the EMX.

Altitude Correction Factors

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

Altitude (meters)	Altitude (feet)	Correction factor
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Ways to Probe Existing User Profiles

This section indicates available ways to query existing user accounts on the EMX.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.
- Any user with the permission to view event rules can query all local existing users via JSON RPC.
- Any user with the permission to view the event log may get information about existing users from the log entries.
- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

Raritan Training Website

Raritan offers free training materials for various Raritan products on the *Raritan training website http://www.raritantraining.com*. The Raritan products introduced on this website include the intelligent PDU, dcTrack®, Power IQ, KVM, EMX, BCM and CommandCenter Secure Gateway (CC-SG). Raritan would update the training materials irregularly according to the latest development of Raritan products.

To get access to these training materials or courses, you need to apply for a username and password through the Raritan training website. After you are verified, you can access the Raritan training website anytime.

Having access to the training website could be helpful for learning or getting some ideas regarding Raritan products and making correct decisions on purchasing them. For example, you can take the dcTrack video training before implementing or using it.

Connecting Contact Closure Sensors to OLD EMX2-888

Follow the steps below to connect Raritan's or third-party contact closure detectors/switches to the termination points labeled CONTACT SENSOR if your EMX is the old EMX2-888 with a built-in spring-loaded terminal module.

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

Note: If you are using an EMX2-888 with a removable terminal module, see **Connecting Contact Closure Sensors to EMX2-888** *(on page 80).*

▶ **To connect sensors to old EMX2-888 contact closure terminals:**

1. Strip the insulation around 12 mm from the end of each wire of discrete 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.
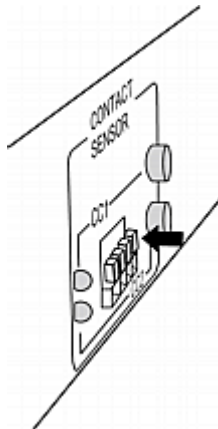
3. Fully insert each wire of both detectors/switches into each termination point.

    ▪ Plug both wires of a detector/switch into the two termination points to the left.

    ▪ Plug both wires of the other detector/switch into the two termination points to the right.
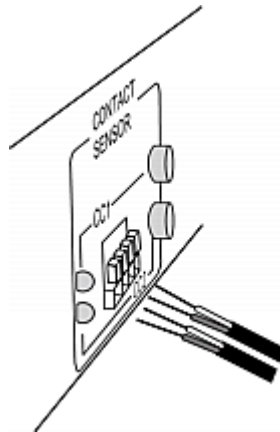
4. Release the tiny rectangular buttons after inserting the wires properly.

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.

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 external authentication. With appropriate DNS settings, the EMX can resolve the external authentication server's name to an IP address for establishing a connection. If the *SSL/TLS 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 external authentication, see *Setting Up External Authentication* (on page 189).

Cascading Troubleshooting

Any accessibility problem occurred on one of the devices in the cascading chain may result in failure to access all downstream slave devices that are connected to it.

Possible Root Causes

The following lists the network accessibility issues and possible root causes.

You can always troubleshoot the software settings by connecting the EMX to a computer if network access to that EMX fails. See *Connecting the EMX to a Computer* (on page 12).

Symptom	Probable cause
Failure to access the master device	- Network connection to the master device is lost. - No power is supplied to the master device. - The Ethernet or wireless interface on the master device is disabled. - IPv4 (or IPv6) settings are disabled on the master device. - In the port forwarding mode, the master device's role is incorrectly set to 'Slave'. - In the port forwarding mode, the interface where the network is connected is incorrectly selected as the downstream interface. - For the wireless networking, one of the following may lead to the accessibility failure: - The USB wireless LAN adapter attached to the master device is not the Raritan USB WIFI LAN adapter. See *USB Wireless LAN Adapters* (on page 11). - The wireless LAN configuration is not supported. See *Supported Wireless LAN Configuration* (on page 11). - The installed CA certificate chain contains any certificate that has expired or is not valid yet.

Symptom	Probable cause
Failure to access a slave device	• Network connection to the master device is lost. • The cascading cable connected to the slave device in question or any upstream device (if available) is loose or lost. • No power is supplied to the slave device in question or any upstream devices. • The Ethernet or wireless interface on the master device is disabled. • IPv4 (or IPv6) settings are disabled on the slave device in question. • The cascading mode of the slave device in question or any upstream device is set incorrectly. For example, the master device is set to Bridging, but one of the slave devices is set to Port Forwarding. • In the port forwarding mode, the master device's role is incorrectly set to 'Slave'. • In the port forwarding mode, the master device's downstream interface is incorrectly set. For example, you use a USB cable to connect the 1st slave device, but select the Ethernet port as the downstream interface. • In the port forwarding mode, the role of the slave device in question or any upstream device is set to 'Master' instead of 'Slave'. • In the port forwarding mode, the port number you added to the IP address is incorrect. See *Port Number Syntax* (on page 165). • The firmware version of the slave device in question or any upstream device is older than 3.3.10.

Tip: To determine which EMX may be the failure point of network, you may ping each EMX in the cascading chain, or check the slave-related events in the event log of each EMX. See **Slave Connection and Disconnection Events** *(on page 538).*

Slave Connection and Disconnection Events

In the bridging mode, events regarding connection/disconnection of a downstream slave device via USB is NOT logged.

However, in the port forwarding mode, whenever the connection or disconnection of a downstream slave device via USB is detected, the EMX at the USB-A end of the USB cable logs it in the internal log. Note that the EMX at the USB-B end of the cable does NOT log these events.

There are two slave-related events:

Event	Description
Slave connected	This log entry is generated when a EMX detects the presence of a slave device on its USB-A port.
Slave disconnected	This log entry is generated when it detects the disconnection of a slave device from its USB-A port.

The Ping Tool

The EMX provides a ping tool in the web interface and CLI so you can ping any host or EMX in your data center.

Ping via the Web Interface

To log in to the web interface, see *HTTP/HTTPS Access* (see "*Login*" on page 87).

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.
2. Type values in the following fields.

Field	Description
Network Host	The name or IP address of the host that you want to check.
Number of Requests	A number up to 20. This determines how many packets are sent for pinging the host.

3. Click Run Ping to ping the host. The Ping results are then displayed.

Ping via the CLI

You can access the CLI interface by connecting a computer to the EMX or using SSH/Telnet. See *SSH/Telnet Access* (see "*With SSH or Telnet*" on page 293) for details.

You must perform the ping command in the diagnostic mode. To enter the diagnostic mode, type the following command and press Ener.

```
#        diag
```

After the diag> or diag# prompt appears, you can perform the ping command.

This ping command 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. If not, either the host is shut down or it is not being properly 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 between 1 and 100.
size <number2>	Determines the packet size. <number2> is an integer number in bytes between 1 and 65468.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds ranging from 1 to 600.

The command looks like the following when it includes all options:

```
diag>      ping <host> count <number1> size <number2> timeout <number3>
```

Browsing through the Online Help

The EMX Online Help is accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

▶ **To use the EMX online help:**

1. Click Online Documentation. See *Web Interface Overview* (on page 89).

2. The online help opens in the default web browser.

3. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.

4. To select a different topic, do any of the following:

   - To view the next topic, click the Next icon ⊕ in the toolbar.

   - To view the previous topic, click the Previous icon ⊕.

   - To view the first topic, click the Home icon 🏠.

5. To expand or collapse a topic that contains sub-topics, do the following:

   - To expand any topic, click the white arrow ▷ prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow ◢, and sub-topics appear below the topic.

   - To collapse any expanded topic, click the black, gradient arrow ◢ prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow ▷, and all sub-topics below that topic disappear.

6. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon 🔍 to start the search.

   - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.

7. To have the left pane show the list of topics, click the Contents tab at the bottom.

8. To show the Index page, click the Index tab.

9. To email any URL link to the currently selected topic to any person, click the "Email this page" icon ![email icon] in the toolbar.

10. To email your comments or suggestions regarding the online help to Raritan, click the "Send feedback" icon ![feedback icon].

11. To print the currently selected topic, click the "Print this page" icon ![print icon].

Appendix I Integrating Asset Management Strips with Other Products

In This Chapter

Asset Management Strips and Raritan PDUs

Asset strips also work with the following Raritan power distribution units (PDUs) or transfer switches:

- PX2 PDUs
- PX3 PDUs
- PX3TS transfer switches
- Branch Circuit Monitor (BCM) series

For information on setting up asset strips to work with each product, refer to each product's User Guide or Online Help on the Raritan website's *Support page* (*http://www.raritan.com/support/*).

Asset Management Strips and dcTrack

If any asset strips are connected to the EMX, the EMX can transmit their information to Sunbird's dcTrack. All you have to do is to add the EMX to dcTrack, and also add each IT item where an asset tag is attached to dcTrack.

Note: For instructions on connecting asset strips, see **Connecting Asset Management Strips** *(on page 25).*

If SNMP is enabled, event information can be transmitted to dcTrack. Specifically, Sunbird's Power IQ detects when an asset tag is connected or disconnected from an asset strip. Power IQ then generates a connection or disconnection event. When dcTrack polls Power IQ, the connection/disconnection events are pulled into dcTrack, and displayed in the dcTrack Web Client.

▶ **To poll and display asset management events in dcTrack**

- The EMX that the asset strip is connected to must exist in dcTrack.

  EMX devices are identified as probes in dcTrack; Raritan PDUs are identified as sensors.

- Each IT item connected to the asset strip via an asset tag must exist in dcTrack.

  You do not need to manually enter the asset tag IDs for IT items that already exist in dcTrack as long as these items are in the Installed status.

  Simply, plug the item's asset tag into an asset strip that is connected to the EMX that exists in dcTrack. dcTrack automatically assigns the asset tag ID to the existing IT item.

Note: If needed, the asset tag number can be overwritten.

For more information on dcTrack as well as how asset strips work with dcTrack, contact Sunbird Professional Services and Support from the http://support.sunbirddcim.com.

Raritan.
A brand of 🔲Legrand

Index

Raritan.
A brand of Legrand

Raritan.
A brand of Legrand

Raritan.