Raritan EMX

User Guide
Release 3.2.10

EMX-0J-v3.2.10-E

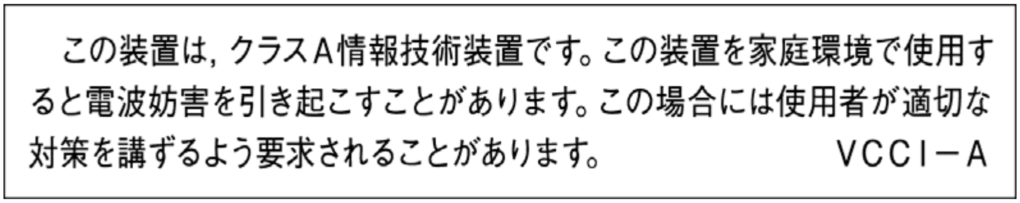
March 2016

255-80-6107-00

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.

1F61
I.T.E.

Contents

What's New in the EMX User Guide

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.

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.

Overview (on page 1)

Product Models (on page 2)

APIPA and Link-Local Addressing (on page 4)

Configuring the EMX (on page 10)

Connecting the EMX to a Computer (on page 11)

Bulk Configuration Methods (on page 21)

Cascading the EMX via USB (on page 22)

Connecting Regular Asset Sensors to the EMX (on page 28)

EMX2-111 Connection (on page 29)

EMX2-888 Connection (on page 31)

Daisy-Chain Limitations of Composite Asset Sensors (on page 36)

Connecting Environmental Sensor Packages (on page 39)

DPX Sensor Packages (on page 40)

DPX3 Sensor Packages (on page 48)

Connecting a DPX2 Sensor Package to DPX3 (on page 50)

Using an Optional DPX3-ENVHUB4 Sensor Hub (on page 53)

Mixing Diverse Sensor Types (on page 55)

Connecting an External Beeper (on page 61)

Power Switch (on page 64)

Overview of the LCD Display (on page 67)

Control Buttons (on page 68)

Environmental Sensor Information (on page 68)

Asset Sensor Information (on page 71)

IPv4 Address (on page 72)

MAC Address (on page 73)

USB-Cascaded Device's Position (on page 74)

EMX2-888 Contact Closure Sensor Termination (on page 76)

Connecting Contact Closure Sensors to EMX2-888 (on page 77)

EMX2-888 Contact Closure Sensor LEDs (on page 81)

Beeper (on page 82)

Supported Web Browsers (on page 83)

Login (on page 84)

Remembering User Names and Passwords (on page 87)

Enabling the Modbus Gateway (on page 124)

Configuring the Serial Port (on page 135)

Overview of the Cascading Modes (on page 138)

Checking the Internal Beeper State (on page 148)

Adding LDAP Server Settings (on page 180)

Creating Actions (on page 188)

Scheduling an Action (on page 211)

Send Sensor Report Example (on page 213)

Default Log Messages (on page 216)

Email and SMS Message Placeholders (on page 224)

Matching the Position (on page 242)

States of Unmanaged Sensors or Actuators (on page 255)

Unmanaging Environmental Sensors or Actuators (on page 256)

Configuring the LHX/SHX (on page 274)

Configuring Temperature and Fan Thresholds (on page 276)

Viewing the Summary (on page 277)

Downloading Diagnostic Information (on page 294)

Device Configuration (on page 318)

Event Log (on page 331)

Clearing WLAN Log (on page 337)

Specifying the Device Altitude (on page 340)

Enabling or Disabling Peripheral Device Auto Management (on page 341)

Determining the SSH Authentication Method (on page 361)

Customizing the Date and Time (on page 368)

All Privileges (on page 403)

Setting the Baud Rates (on page 430)

Forcing the Device Detection Mode (on page 430)

EMX2-111 Feature RJ-45 Port Pinouts (on page 440)

EMX2-888 Feature RJ-45 Port Pinouts (on page 441)

Configuration or Firmware Upgrade with a USB Drive (on page 443)

Bulk Configuration or Firmware Upgrade via DHCP/TFTP (on page 454)

Available SCP Commands (on page 480)

Updating the LDAP Schema (on page 493)

RADIUS Configuration Illustration (on page 501)

Reserving IP Addresses in Windows DHCP Servers (on page 528)

Sensor Threshold Settings (on page 529)

PDView App for Viewing the EMX (on page 536)

Connecting Contact Closure Sensors to OLD EMX2-888 (on page 541)

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

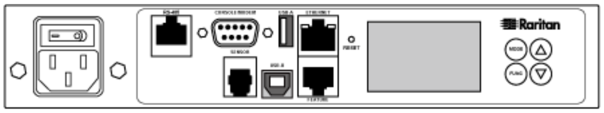
There are two EMX models:

- 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

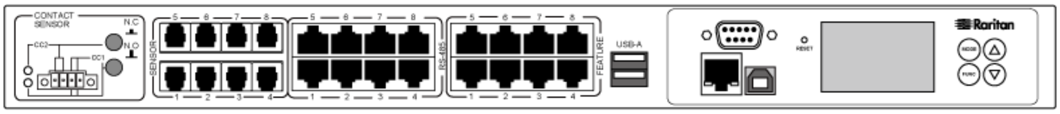


EMX2-111 has the following ports and components:

- 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 64).

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 64).

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 541) and* **Connecting Contact Closure Sensors to EMX2-888** *(on page 77), 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 sensors (optional)
- Asset tags (optional)

APIPA and Link-Local Addressing

The EMX supports Automatic Private Internet Protocol Addressing (APIPA) as of release 3.2.0.

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 136).*

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 11).*

- 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 can be obtained.

▶ 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 ***Selecting the Internet Protocol*** (on page 114).

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

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

▶ Retrieval of the link-local IPv4 address:

- See ***IPv4 Address*** (on page 72).

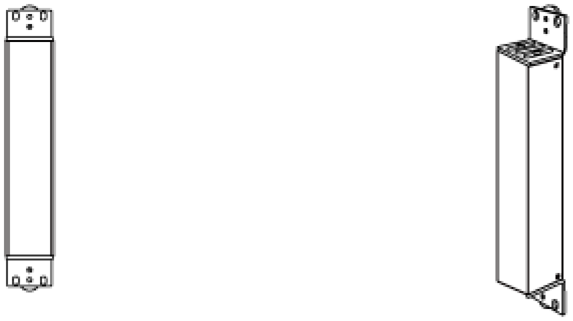
Chapter 2 Rack Mounting an EMX

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

In This Chapter

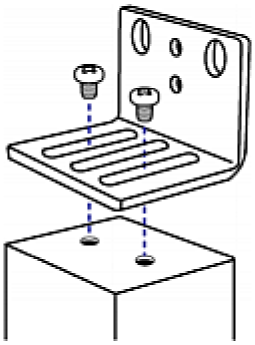
Mounting a Zero U EMX

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



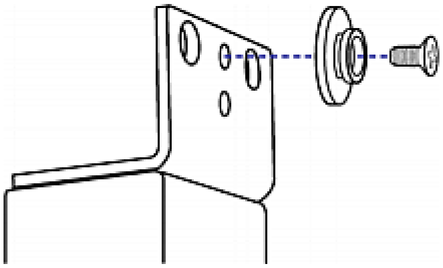
▶ To mount Zero U models using L-brackets and two buttons:

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).

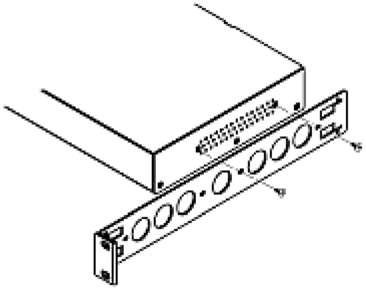


Mounting a 1U EMX

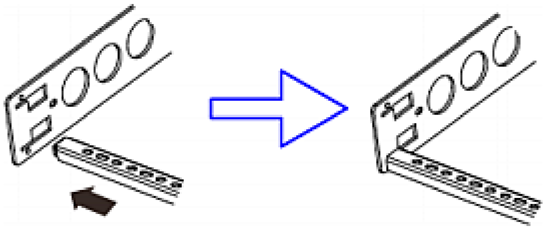
Using the appropriate brackets and tools, fasten the 1U EMX device to the rack or cabinet.

▶ **To mount the 1U EMX device:**

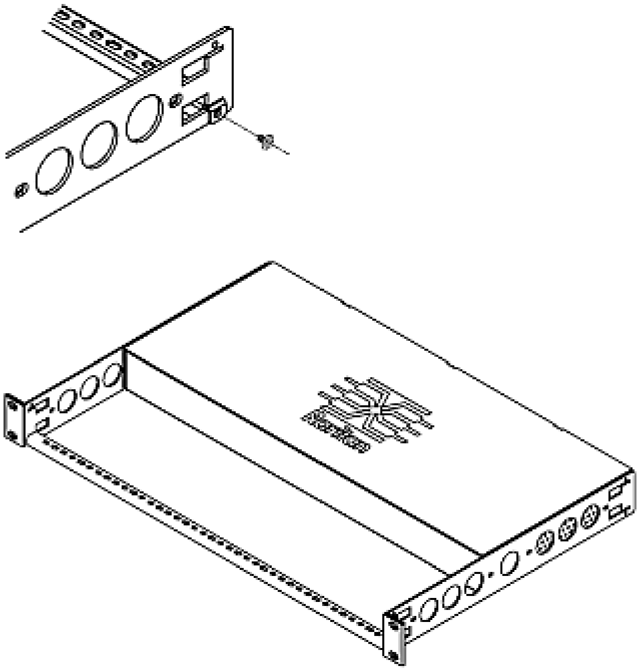
1. Attach a rackmount bracket to both sides of the EMX with the provided screws.



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 Installation and Configuration

In This Chapter

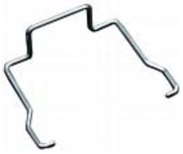
Before You Begin

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

Connecting the EMX to a Power Source

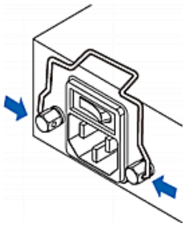
If your EMX device is designed to use a cable retention clip, install the clip before connecting a power cord. A cable retention clip prevents the connected power cord from coming loose or falling off.

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

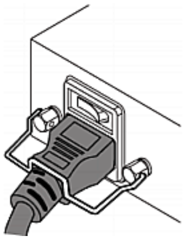


▶ To connect the EMX device to a power source:

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



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



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

Configuring the EMX

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 network. See ***Connecting the EMX to Your Network*** (on page 14).
2. Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it. See ***IPv4 Address*** (on page 72).
3. Launch a web browser to configure the EMX. See ***Login*** (on page 84).

Configuration using a connected computer:

1. Connect the EMX to a computer. See ***Connecting the EMX to a Computer*** (on page 11).
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 84). For IP address retrieval, see ***IPv4 Address*** (on page 72).

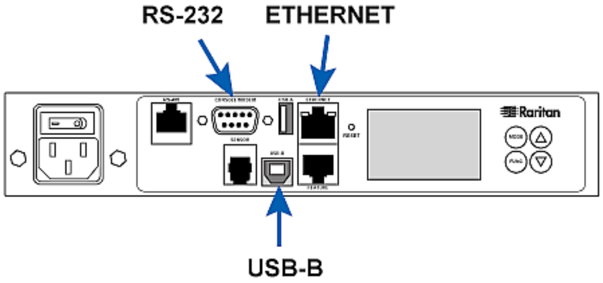
Tip: To configure a number of EMX devices quickly, see **Bulk Configuration Methods** *(on page 21).*

Connecting the EMX to a Computer

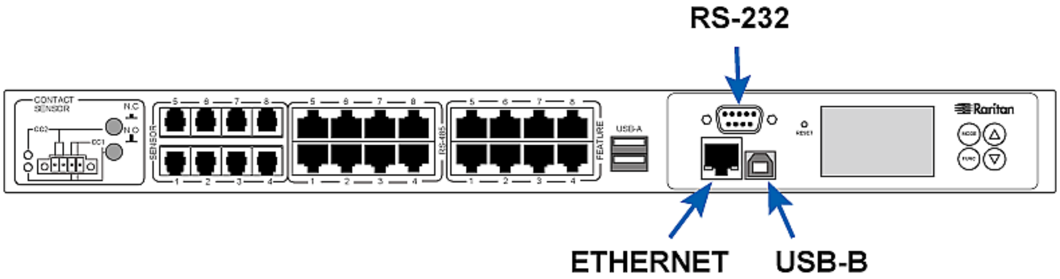
The EMX can be connected to a computer for configuration via one of the following ports.

- ETHERNET port (female)
- USB-B port (male)
- RS-232 serial port (male)

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 RS-232 connection:

1. Connect one end of the null-modem cable to the male 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 12).
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 84).

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 USB serial console driver from the Raritan website's ***Support page*** (***http://www.raritan.com/support/***). The driver contains the *dominion-serial.inf*, *dominion-serial.cat* and *dominion-serial-setup-<n>.exe* files.

Note: <n> in the filename of "dominion-serial-setup-<n>.exe" 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
```

Connecting the EMX to Your Network

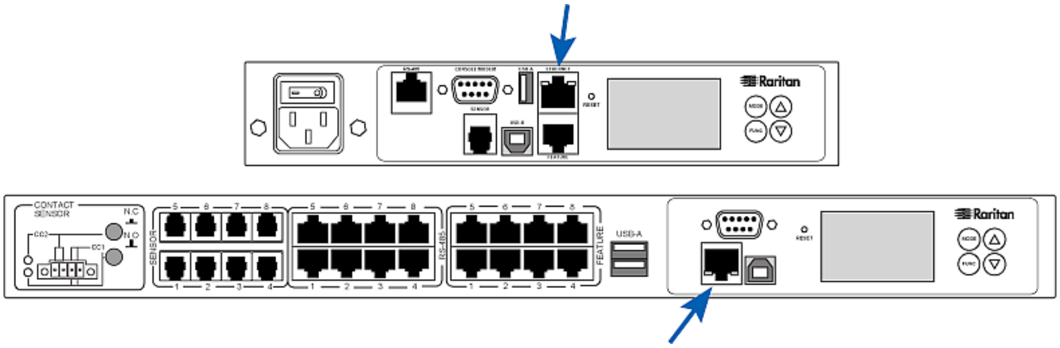
To remotely administer the EMX, you must connect the EMX to your local area network (LAN).

The EMX can be connected to a wired or wireless network.

Note: If your EMX will be used as a master device in the USB-cascading configuration where the bridging mode applies, 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 docking station to the USB-A port on the EMX. Then plug the supported USB wireless LAN adapter into the appropriate USB port on the docking station.

See ***USB Wireless LAN Adapters*** (on page 14) 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
Proxim Orinoco 8494	A/B/G

Wi-Fi LAN adapters	Supported 802.11 protocols
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 14).

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 ***Modifying the Network Configuration*** (on page 110).

▶ **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. All commands are case sensitive.
   a. To set the networking mode, type this command:

   ```
   network mode <mode>
   ```

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

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

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

Tip: You can combine multiple commands to configure multiple parameters at a time. For example,

```
network interface LANInterfaceSpeed <option>
LANInterfaceDuplexMode <mode>
```

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

To set	Use this command
SSID	`network wireless SSID <ssid>` <ssid> = SSID string

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

To set	Use this command
BSSID	`network wireless BSSID <bssid>` <bssid> = AP MAC address or *none*
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

To set	Use this command
EAP passord	`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*

d. To determine which IP protocol (IPv4 or IPv6) is enabled and which IP address (IPv4 or IPv6) returned by the DNS server is used, configure the following parameters.

To set	Use this command
IP protocol	`network ip proto <protocol>` <protocol> = *v4Only*, *v6Only* or *both*
IP address returned by the DNS server	`network ip dnsResolverPreference <resolver>` <resolver> = *preferV4* or *preferV6*

e. After enabling the IPv4 or IPv6 protocol in the earlier step, configure the IPv4 or IPv6 network parameters.

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

- Configure the preferred host name for the IPv4 DHCP or IPv6 automatic configuration.

Note: The <version> variable in all of the following commands is either ipv4 *or* ipv6*, depending on the type of the IP protocol you have enabled.*

To set	Use this command
Preferred host name (optional)	`network <version> preferredHostName <name>` <name> = preferred host name

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

```
network <version> overrideDNS <option>
```

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

- For static IP configuration, configure these parameters.

To set	Use this command
Static IPv4 or IPv6 address	`network <version> ipAddress <ip address>` <ip address> = static IP address
IPv4 subnet mask	`network ipv4 subnetMask <netmask>` <netmask> = subnet mask
IPv4 or IPv6 gateway	`network <version> gateway <ip address>` <ip address> = gateway's IP address
IPv4 or IPv6 primary DNS server	`network <version> primaryDNSServer <ip address>` <ip address> = IP address of the primary DNS server
IPv4 or IPv6 secondary DNS server (optional)	`network <version> secondaryDNSServer <ip address>` <ip address> = IP address of the secondary DNS server

9. To quit the configuration mode, type either of the following commands, and press Enter.

Command	Description
`apply`	Save all configuration changes and exit.
`cancel`	Abort all configuration changes and exit.

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

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

Command	Description
`show network`	Show network parameters.
`show network ip` all	Show all IP configuration parameters.
`show network wireless details`	Show all wireless parameters.

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

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

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 287).

▶ 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 454).

▶ Use a USB flash drive:

- Requirement: A FAT32-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 443).

Cascading the EMX via USB

You can use USB cables to cascade up to eight Raritan devices. All devices in the USB-cascading chain share the Ethernet connectivity. Different Raritan models can be cascaded as long as they are running an appropriate firmware.

The first device in the chain is the master device and all the other are slave devices.

All devices in the chain are accessible over the network, with the bridging or port-forwarding cascading mode activated on the master device. See ***Setting the Cascading Mode*** (on page 136).

Only the master device is connected to the LAN. The LAN connection method varies based on the cascading mode.

- The bridging mode supports the *wired* networking only.
- The port forwarding mode supports both the *wired* and *wireless* networking.

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

▶ To cascade the EMX devices via USB:

1. Verify that the EMX devices to be cascaded are running firmware version 2.2.0 or higher by choosing Maintenance > Device Information.

   If not, upgrade these devices. See ***Updating the EMX Firmware*** (on page 291).

   Note: Port forwarding mode over wireless LAN is supported as of release 3.1.0. You must upgrade all devices in the chain to version 3.1.0 or higher if wireless networking is preferred.

2. Select one of the devices 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.

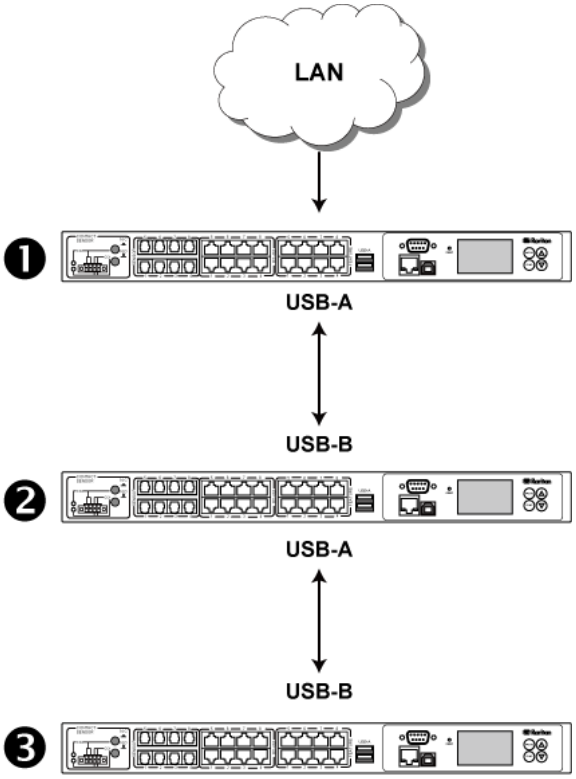
3. Connect the master device to the LAN via:

   - A standard network patch cable (CAT5e or higher) if the bridging mode is intended.
   - A standard network patch cable or a Raritan USB WIFI wireless LAN adapter if the port forwarding mode is intended.

     For information on the Raritan USB WIFI adapter, see ***USB Wireless LAN Adapters*** (on page 14).

4. 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.
5. Connect Slave 1's USB-A port to the USB-B port of an additional EMX via a USB cable. The second additional device is Slave 2.
6. Repeat the same step to connect more slave devices. You may connect up to 7 slave devices.

   Do NOT connect any slave device to the LAN. That is, there is no connection of a standard network cable or USB wireless LAN adapter to the slave devices.
7. Log in to the master device to configure the cascading mode. See ***Setting the Cascading Mode*** (on page 136) or ***Configuring the Cascading Mode*** (on page 422).
8. Configure the master and/or each slave device's networking settings.
   - Bridging mode: You need to configure each cascaded device's network settings respectively.
   - Port forwarding mode: Only the mater device's network settings must be configured.



Number	Device role
1	Master device

Number	Device role
2	Slave 1
3	Slave 2

Note: To remotely identify the master and slave devices and their positions in the USB-cascading configuration, see **Identifying Cascaded Devices** *(on page 107).*

Tip: The USB-cascading configuration can be a combination of diverse Raritan products that support the USB-cascading feature, including PX2, PX3, PX3TS, EMX and BCM. See the USB-Cascading Solution Guide *on Raritan website's* **Support page** *(***http://www.raritan.com/support/***).*

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 Sensors

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

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

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

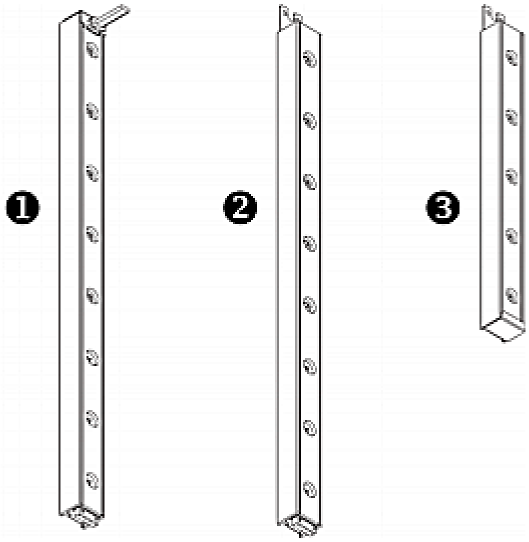
Combining Regular Asset Sensors

Each tag port on the regular asset sensor 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 sensors up to 64U long, consisting of one MASTER and multiple SLAVE asset sensors.

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

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



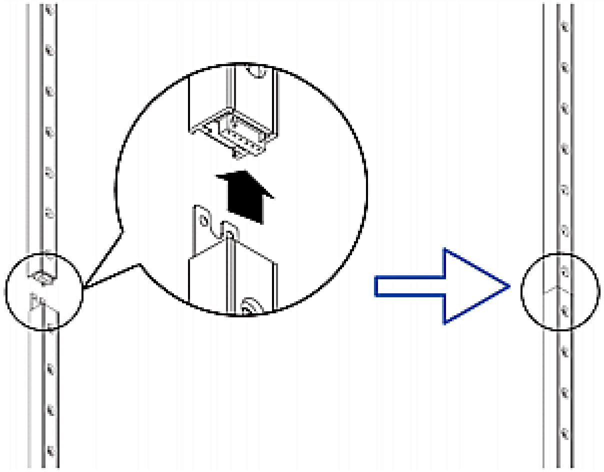
❶	8U MASTER asset sensor with 8 tag ports
❷	8U SLAVE asset sensor with 8 tag ports
❸	5U "ending" SLAVE asset sensor with 5 tag ports

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

▶ **To assemble asset sensors:**

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

- Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master asset sensor. Screw up the U-shaped sheet metal to reinforce the connection.



2. Connect another 8U slave asset sensor to the one being attached to the master asset sensor in the same manner as Step 1.
3. Repeat the above step to connect more slave asset sensors. The length of the asset sensor assembly can be up to 64U.
   - The final asset sensor can be 8U or 5U, depending on the actual height of your rack.
   - Connect the "ending" asset sensor as the final one in the assembly.
4. Vertically attach the asset sensor assembly to the rack, next to the IT equipment, making each tag port horizontally align with a rack unit.
5. The asset sensors are automatically attracted to the rack because of magnetic stripes on the back.

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

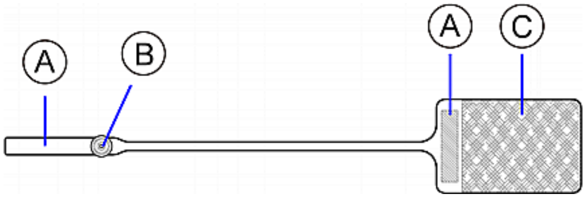
Introduction to Asset Tags

You need both asset sensors 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 sensor at the other.

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

The following diagram illustrates an asset tag.



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

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

Connecting Regular Asset Sensors to the EMX

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

The EMX supplies power to the connected asset sensors.

After powered by the EMX, all LEDs on the asset sensor may cycle through different colors if the asset sensor'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 sensors after finishing the asset sensor connection, see **Asset Management** *(on page 258).*

EMX2-111 Connection

The FEATURE port of EMX2-111 supports 5 volts of power only, which is insufficient for connecting an asset sensor at a distance between 1 and 10 meters. Therefore, the use of a Raritan X cable is required for EMX2-111 to connect an asset sensor whose cabling distance is over 1 meter.

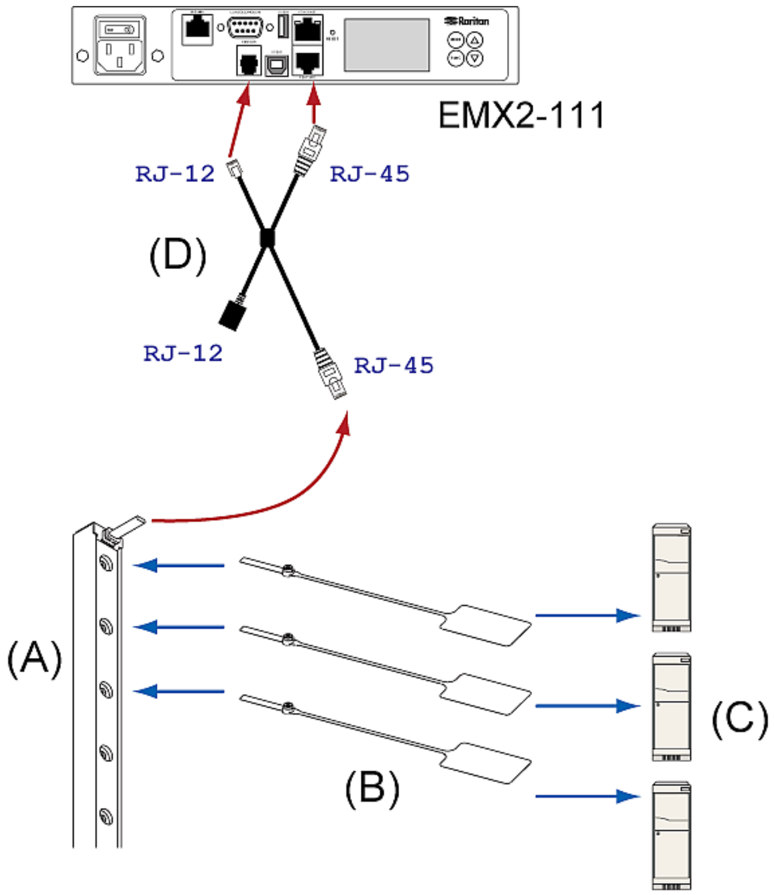
▶ **To connect a regular asset sensor assembly to EMX2-111:**

1. Assemble regular asset sensors according to your needs. See ***Combining Regular Asset Sensors*** (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 sensor.

   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 sensor'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 SENSOR port on the EMX2-111.

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



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

Note: 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

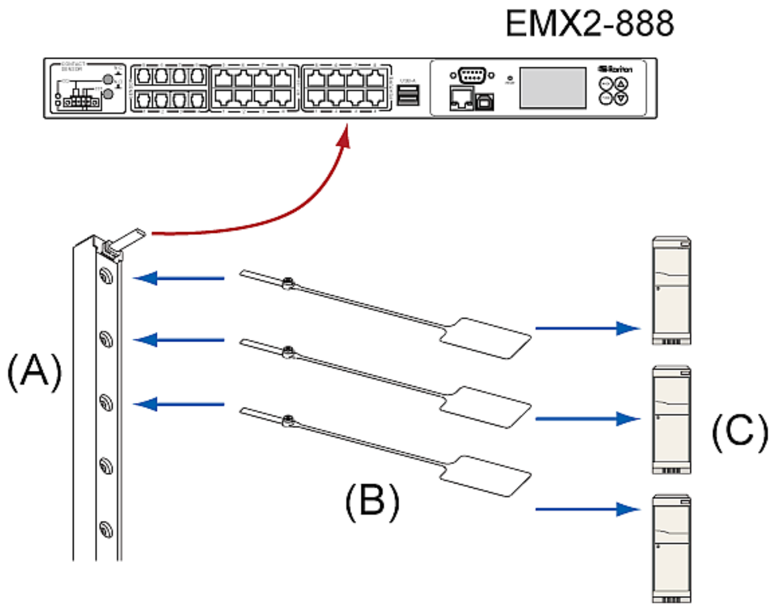
Unlike EMX2-111, EMX2-888 does NOT need to use a Raritan X cable because its FEATURE port supports 12 volts of power.

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

1. Assemble regular asset sensors according to your needs. See ***Combining Regular Asset Sensors*** (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 sensor.

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 sensor's RJ-45 connector to a FEATURE port on the EMX2-888.



(A)	MASTER asset sensor
(B)	Asset tags
(C)	IT devices

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

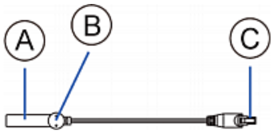
Connecting Blade Extension Strips

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 sensor but requires a tag connector cable for connecting it to a tag port on the regular or composite asset sensor. 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.

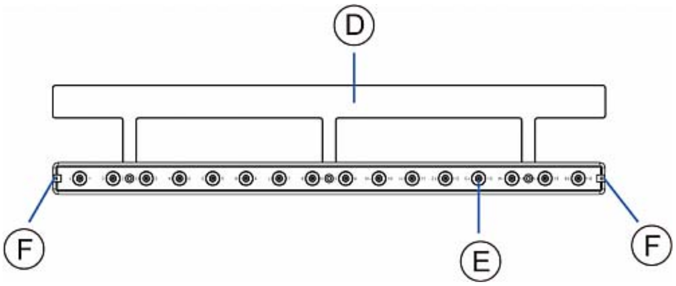
Tag connector cable



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



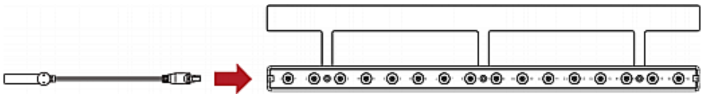
D	Mylar section with the adhesive tape

E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

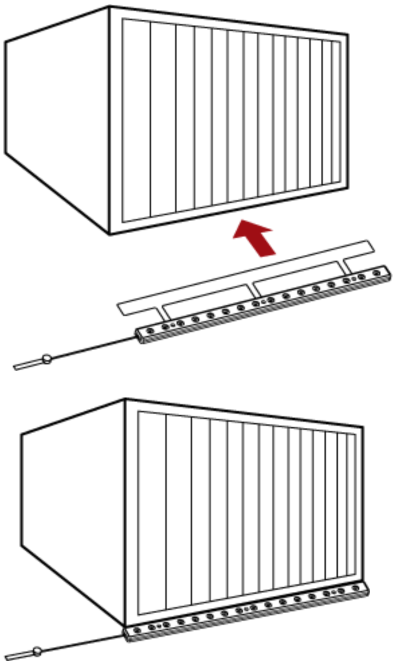
Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the EMX device's web interface.

▶ 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.



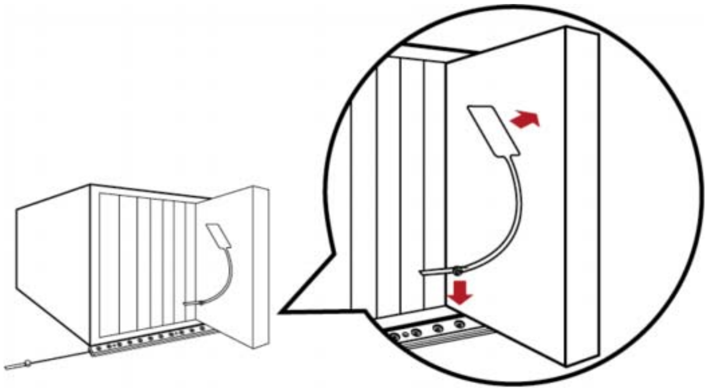
2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.



3. Connect one end of an asset tag to a blade server and the other end to the blade extension strip.

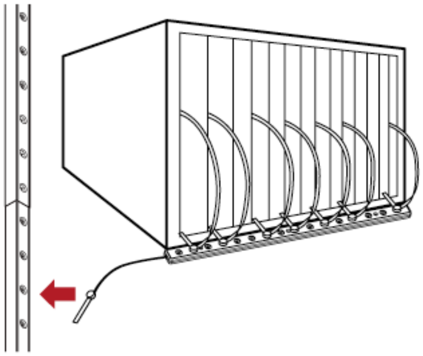
a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.

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 sensor 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 sensor, wait at least 1 second before re-connecting it back, or the EMX device may not detect it.

Connecting Composite Asset Sensors (AMS-Mx-Z)

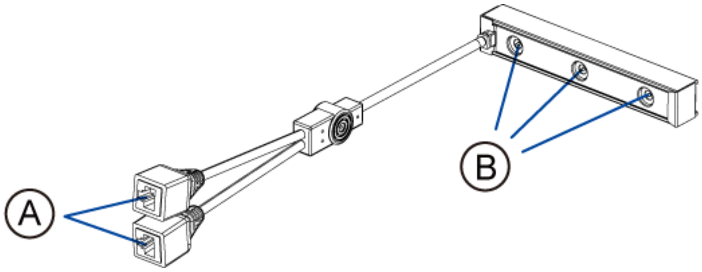
A composite asset sensor is named AMS-Mx-Z, where x is a number, such as AMS-M2-Z or AMS-M3-Z. It is a type of asset sensor that functions the same as regular MASTER asset sensors except for the following differences:

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

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

The composite asset sensor 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 sensors to the EMX device:

1. Connect a composite asset sensor 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 sensor.
   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 sensor by plugging the tag connector into the tag port on the composite asset sensor. For details, see ***Connecting Regular Asset Sensors to the EMX*** (on page 28).

3. If necessary, daisy chain *the same* type of composite asset sensors to track more IT devices.

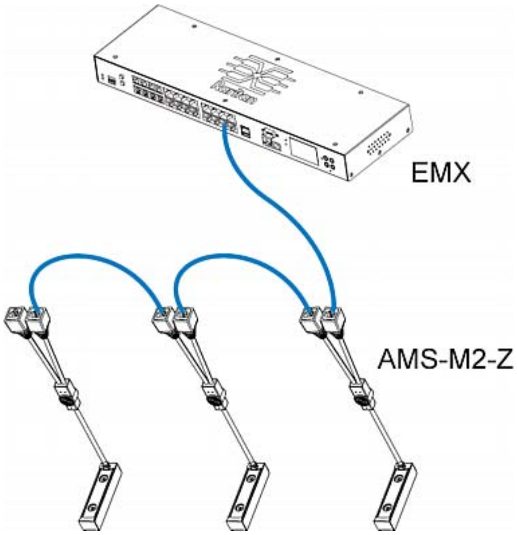
    a. Get a standard network patch cable that is within 2 meters.

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

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

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

Daisy-Chain Limitations of Composite Asset Sensors

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

- The maximum cable length between composite asset sensors is 2 meters, but the total cable length cannot exceed 10 meters.
- The maximum number of composite asset sensors that can be daisy chained vary according to the Raritan device.

Raritan devices	Maximum sensors per chain
EMX2-111,	Up to 4 composite asset sensors

Raritan devices	Maximum sensors per chain
PX2 PDUs, BCM1 (NOT BCM2 series)	are supported.
EMX2-888, PX3 PDUs, PX3TS transfer switches PMC (BCM2 series)	Up to 6 composite asset sensors are supported.

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

Important: Do NOT mix different types of composite asset sensors in a chain. For example, all in the chain are AMS-M2-Z or all are AMS-M3-Z.

Using an X Cable

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

If you need to exceed the daisy-chain limitation, use Raritan's X cable to connect composite asset sensors. This allows you to expand the maximum number of composite asset sensors 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.

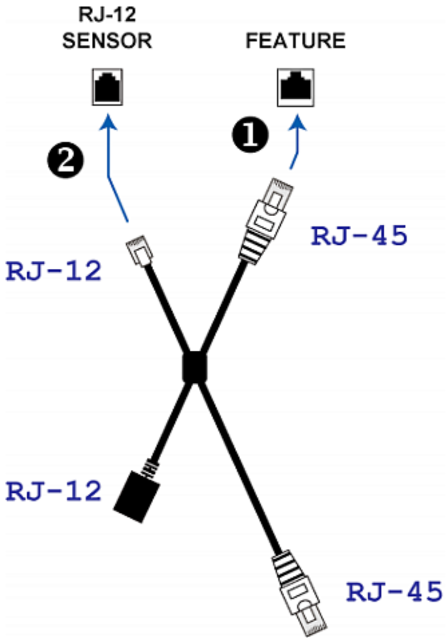
The X cable supplies 12V voltage from the SENSOR port of the EMX2-111 to the connected composite asset sensors.

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

To connect composite asset sensors via an X cable:

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

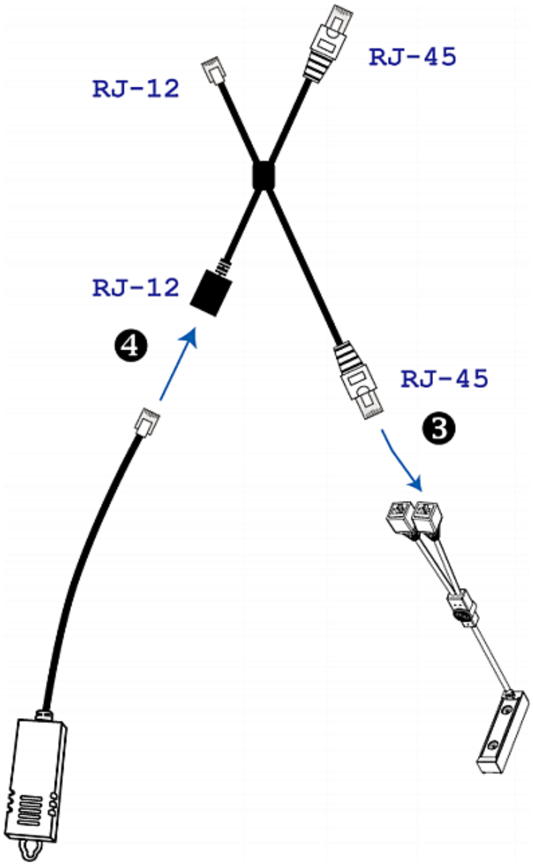
2. Plug the male phone connector of the X cable into the RJ-12 SENSOR port of the EMX device. **This step is required for enhancing the power supply to asset sensors.**



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 sensors.

   - A maximum of 5 additional composite asset sensors can be connected to the first composite asset sensor being attached to the X cable. See ***Connecting Composite Asset Sensors (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.

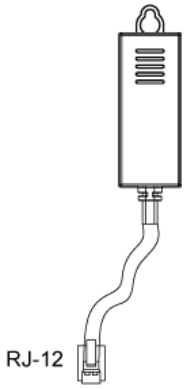
Model	Supported maximum number of sensors/actuators
EMX2-111	This model has only one SENSOR port so it can manage up to 32 sensors and/or actuators.
EMX2-888	This model has 8 SENSOR ports, which can manage up to 128 sensors and/or actuators in total. In addition, it has two built-in contact closure terminals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

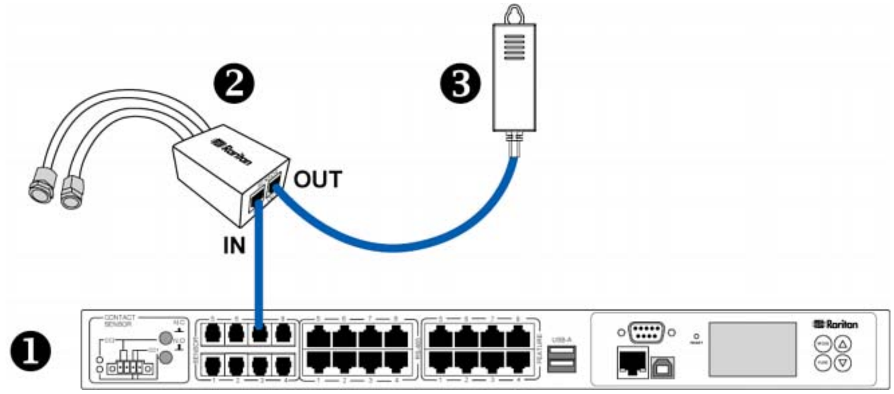
> Warning: For proper operation, wait for 15-30 seconds between each connection operation or each disconnection operation of environmental sensor packages.

▶ 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.

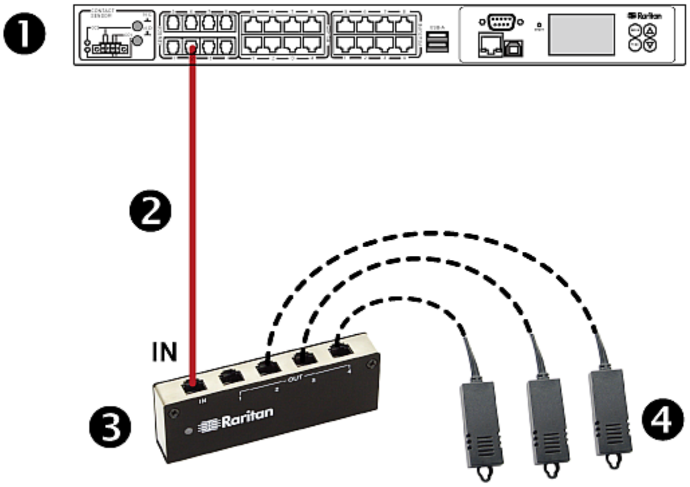
The DPX-ENVHUB4 sensor hub supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to this hub.

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

▶ 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

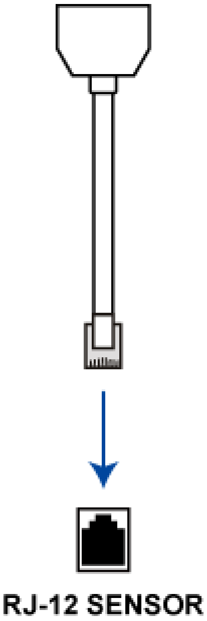
Using an Optional DPX-ENVHUB2 cable

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

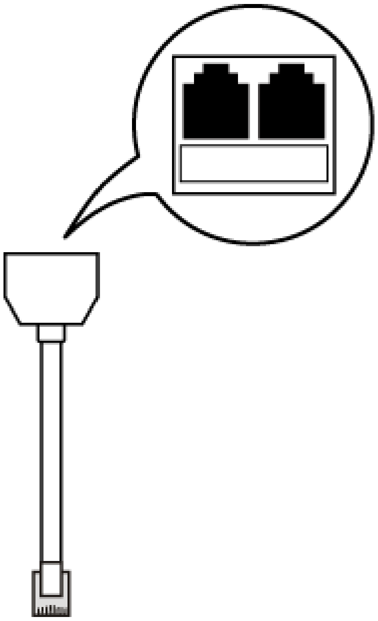
This cable supports DPX sensor packages only. Do NOT connect DPX2, DPX3 or DX sensor packages to it.

► **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.



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

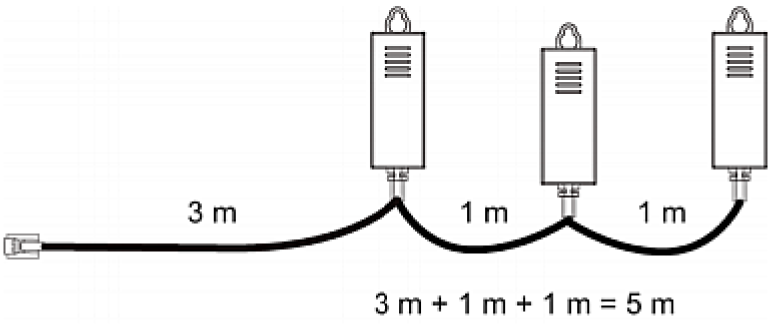
Sensor Connection Restrictions:

- 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.

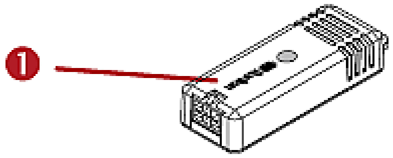
EMX2-888 → 33' (10 m) cable → Up to 8 hubs → 16' (5 m) cable → Up to 32 DPX-T3H1 sensor packages

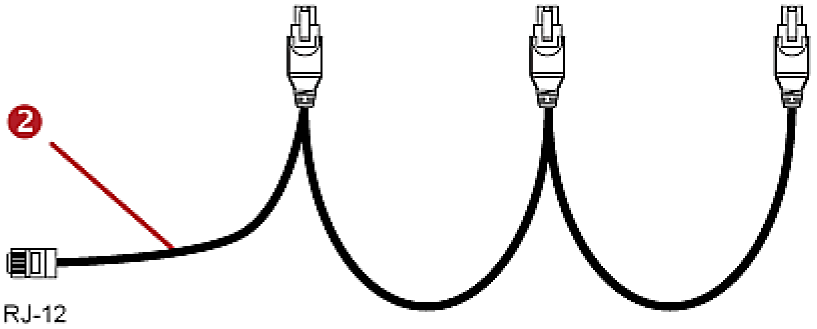
EMX2-111	→	33' (10 m) cable	→	Up to 1 hub	→	16' (5 m) cable	→	Up to 4 DPX-T3H1 sensor packages

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/***).





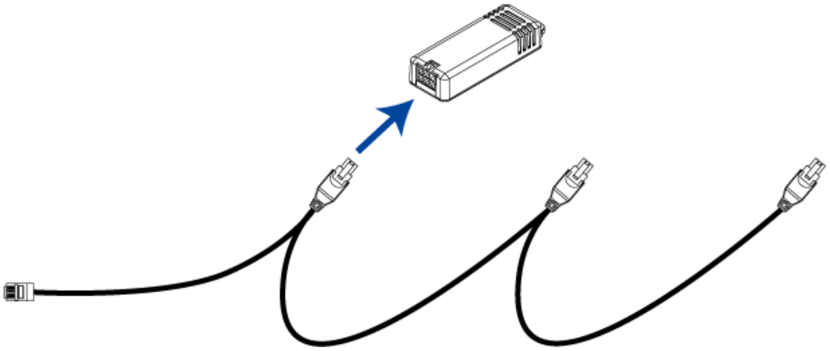
Item	
❶	DPX2 sensor package
❷	DPX2 sensor cable with one RJ-12 connector and three head connectors

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

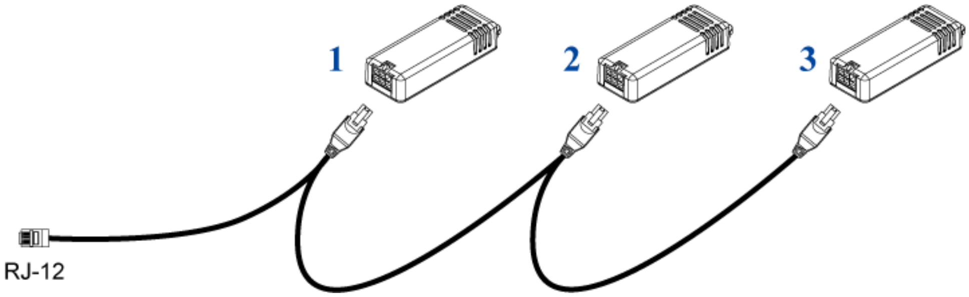
Warning: If there are free head connectors between a DPX2 sensor cable's RJ-12 connector and the final attached DPX2 sensor package, the sensor packages following the free head connector(s) on the same cable do NOT work properly. Therefore, always occupy all head connectors prior to the final sensor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

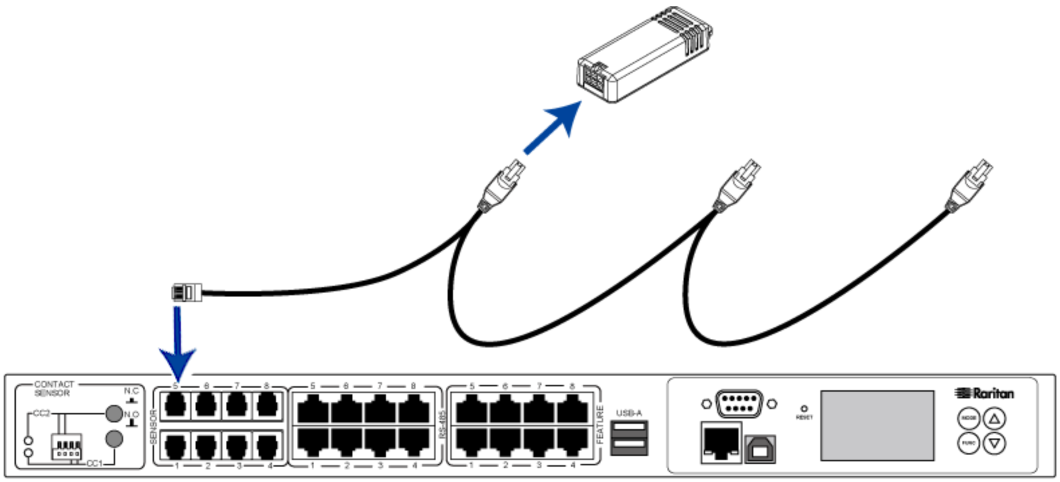


2. Connect remaining DPX2 sensor packages to the second and then the third head connector.



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.

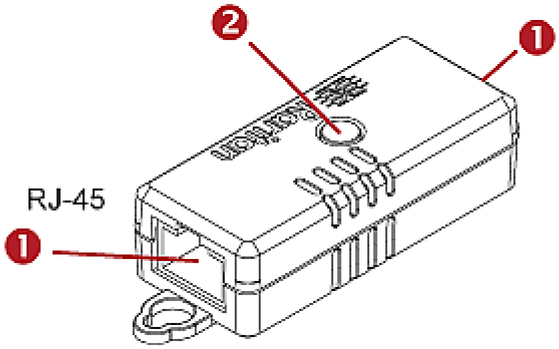


OR you can directly connect the DPX2 sensor package to a DX sensor chain without using any RJ-12 to RJ-45 adapter. See ***Connecting a DPX2 Sensor Package to DX*** (on page 52).

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.



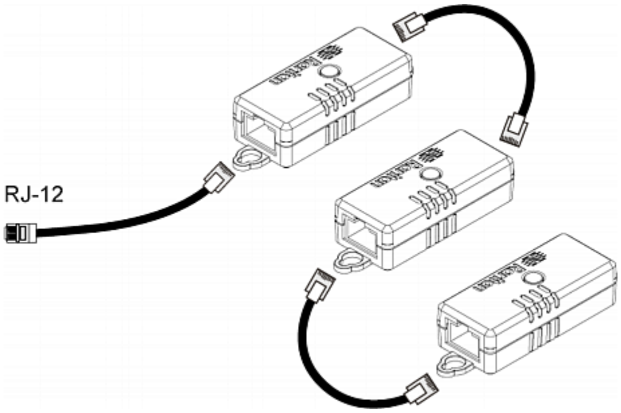
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DPX3 sensor package.
❷	LED for indicating the sensor status.

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.

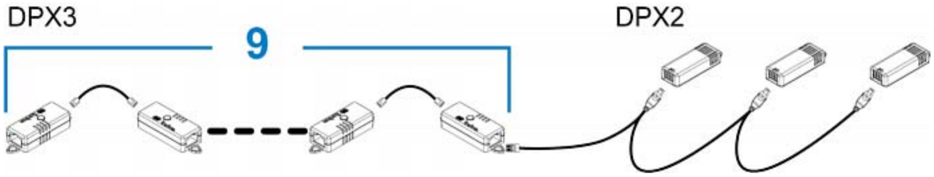
Connecting a DPX2 Sensor Package to DPX3

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.

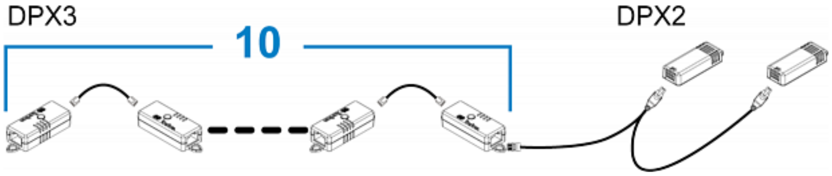
▶ When connecting a DPX2 sensor package containing three DPX2 sensors:

A maximum of nine DPX3 sensor packages can be cascaded because 12-3=9.



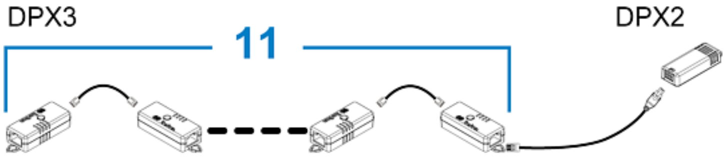
▶ When connecting a DPX2 sensor package containing two DPX2 sensors:

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/***).

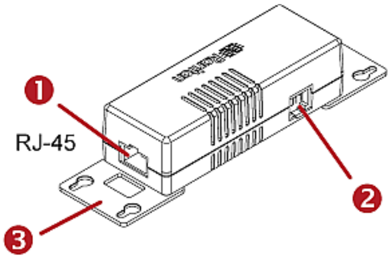
You can cascade up to 12 DX sensor packages.

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 sensors or actuators that have been under management, and then manually bring the last 4 functions into management. See **Unmanaging Environmental Sensors or Actuators** *(on page 256) and* **Managing Environmental Sensors or Actuators** *(on page 244).*



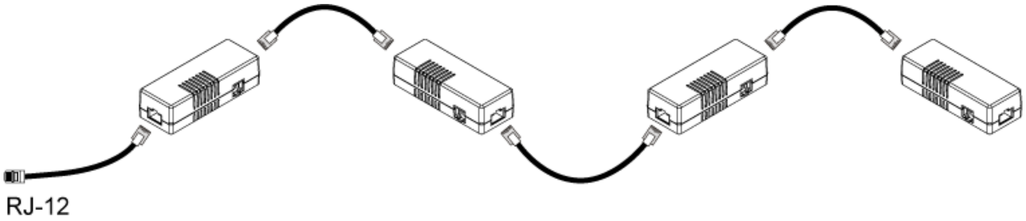
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DX sensor package.
❷	RJ-12 port, which is reserved for future use and now blocked.
❸	Removable rackmount brackets.

▶ **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.



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).

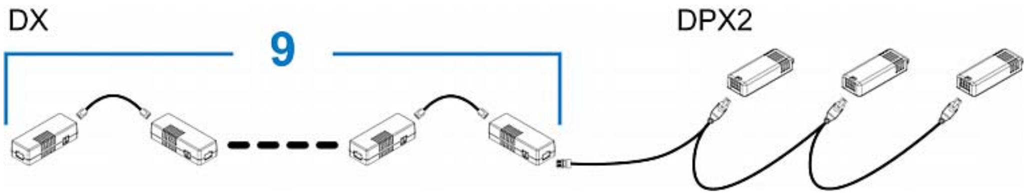
Connecting a DPX2 Sensor Package to DX

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.

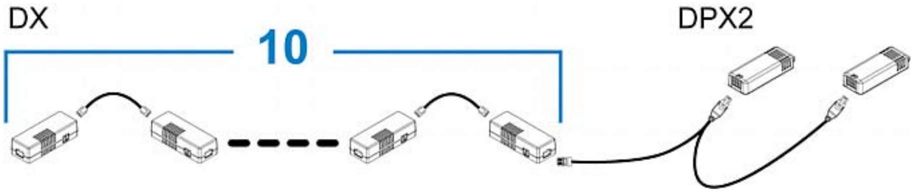
▶ When connecting a DPX2 sensor package containing three DPX2 sensors:

A maximum of nine DX sensor packages can be cascaded because 12-3=9.



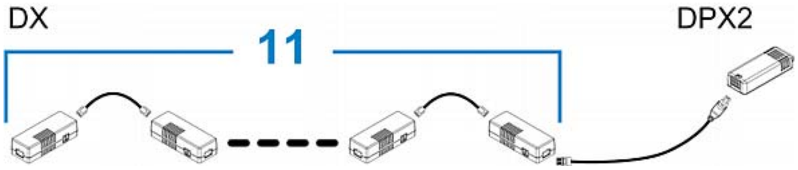
When connecting a DPX2 sensor package containing two DPX2 sensors:

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:

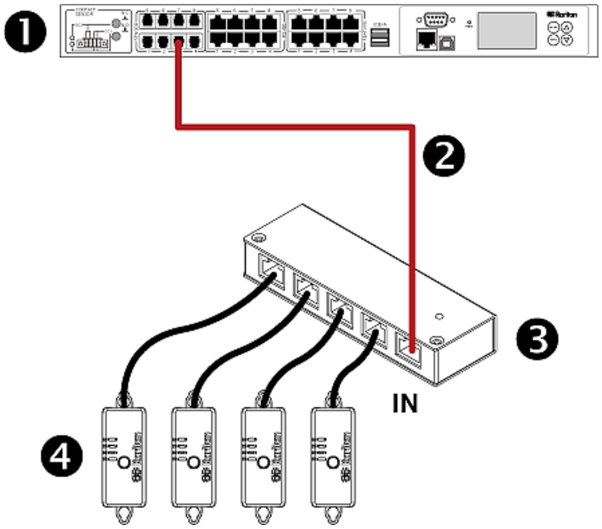
- All ports on the DPX3-ENVHUB4 sensor hub are RJ-45 instead of RJ-12 as the DPX-ENVHUB4 sensor hub.
- The DPX3-ENVHUB4 sensor hub supports all Raritan environmental sensor packages, including DPX, DPX2, DPX3 and DX sensor packages.
- To connect diverse types of sensor packages to this sensor hub, you 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

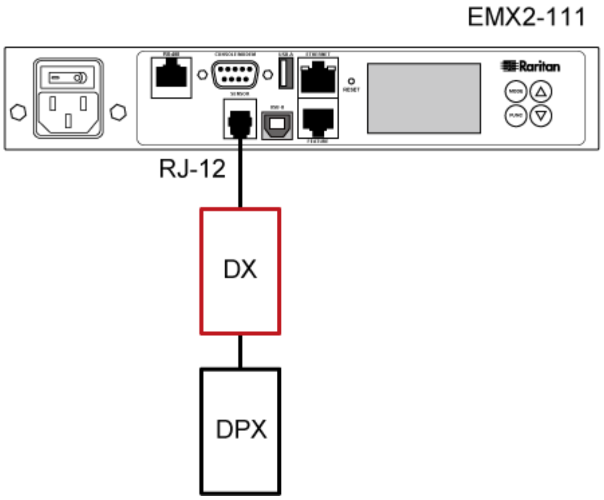
Mixing Diverse Sensor Types

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.

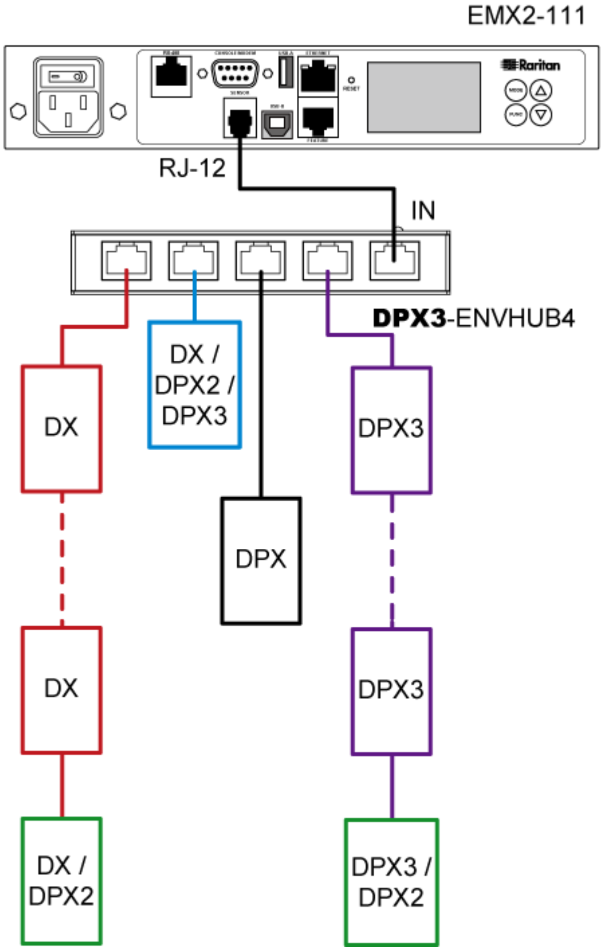


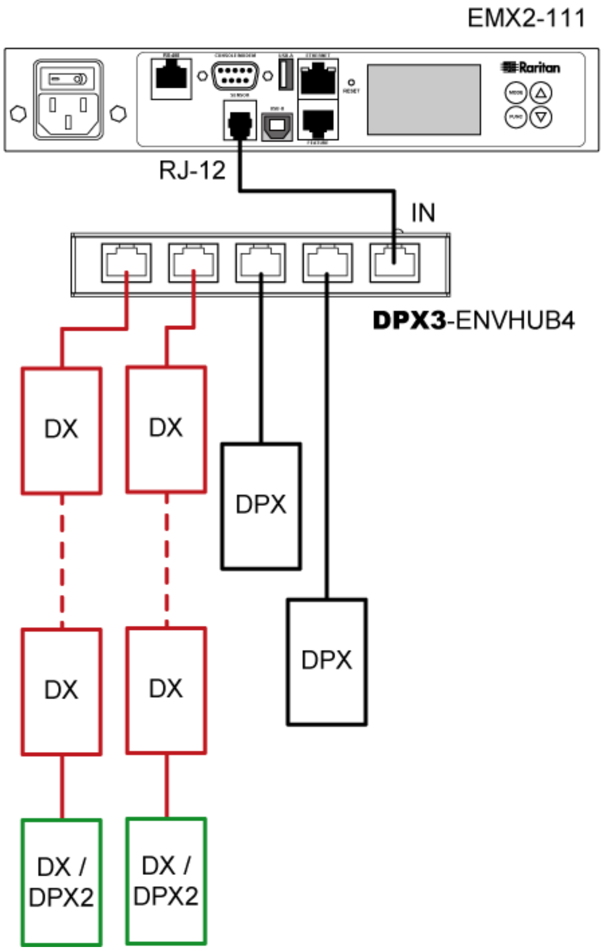
Diverse combinations via the DPX3-ENVHUB4 sensor hub:

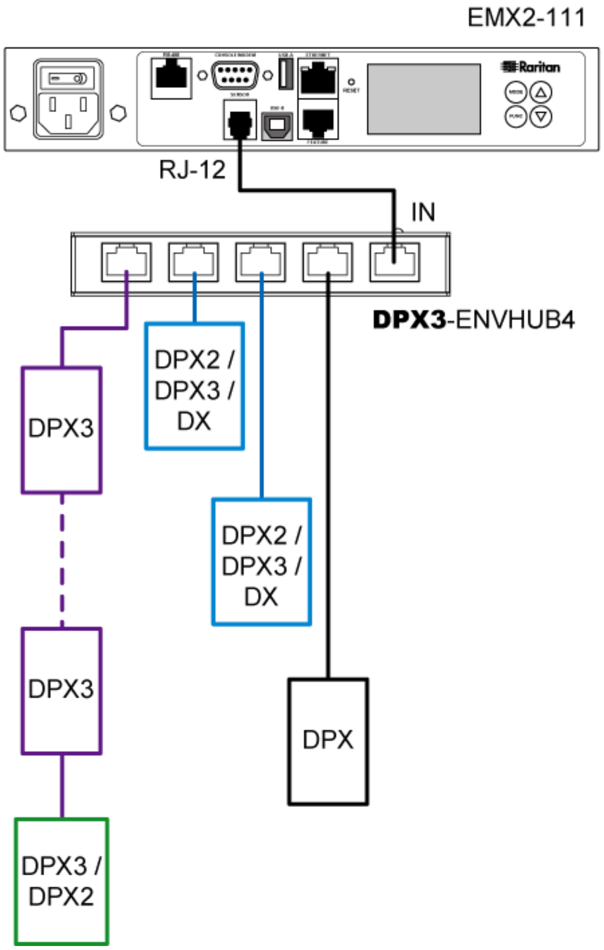
- You must use the **DPX3**-ENVHUB4 sensor hub instead of the old DPX-ENVHUB4 sensor hub. Each port on the hub supports any of the following:
  - A DX sensor package
  - A chain of DX sensor packages
  - A DPX3 sensor package
  - A chain of DPX3 sensor packages
  - A DPX2 sensor package
  - A DPX sensor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

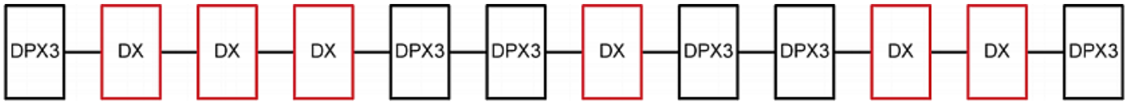



EMX2-111
RJ-12
IN
DPX3-ENVHUB4
DX
DX
DPX
DPX
DX
DX
DX / DPX2
DX / DPX2



Mix DPX3 and DX in a sensor chain:

Any DX sensor package in a chain can be replaced by a DPX3 sensor package. For example, the following diagram shows a sensor chain comprising both DX and DPX3 sensor packages. The total number of sensor packages in this chain cannot exceed 12.



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 UVC-compliant webcams are supported:

- Logitech® Webcam® Pro 9000, Model 960-000048
- Logitech QuickCam Deluxe for Notebooks, Model 960-000043
- Logitech QuickCam Communicate MP, Model 960-000240
- Logitech C200, C210, C270 and C920

Other UVC-compliant webcams may work. However, Raritan has neither tested them nor claimed that they will work properly. More information about the scores of UVC-compliant webcams can be found at ***http://www.ideasonboard.org/uvc*** (***http://www.ideasonboard.org/uvc***).

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 ***Viewing Webcam Snapshots or Videos*** (on page 267).

Connecting a GSM Modem

A Cinterion® MC52iT or MC55iT GSM modem can be connected to the EMX in order to send SMS messages containing event information. See ***Creating Actions*** (on page 188) 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 EMX.
   a. Click Device Settings > Serial Port Settings. The Serial Port Configuration dialog opens.
   b. If needed, enter the GSM modem SIM PIN.

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 135).

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 ***Creating an Event Rule*** (on page 188).

► **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 ***Configuring the LHX/SHX*** (on page 274) 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 EMX2-111 RS485 port. Once it is connected and the EMX detects it, the PM710 is viewed under the Auxiliary Port folder in the navigation tree.

Note: EMX2-888 does not support the PowerLogic PM710.

This device is only supported when plugged into the RS485 port using a PM710 supported cable (not provided by Raritan with the EMX). Refer to your Schneider Electric PowerLogic PM710 documentation for information on the pinouts for the meter.

Note: For information on the PM710 and any sensor-specific configuration required, see the PM710 user guide.

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 the PM710, such as emailing or sending an SMS message when thresholds are reached, and so on. See ***Creating an Event Rule*** (on page 188).

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).

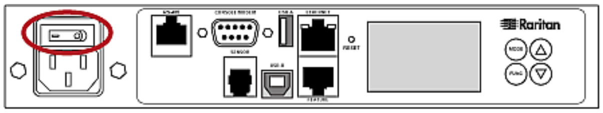
Chapter 5 Using the EMX

In This Chapter

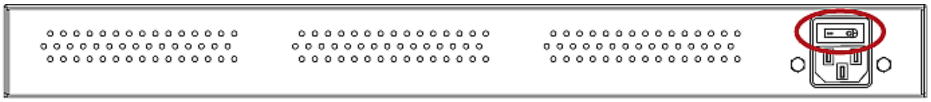
Power Switch

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.

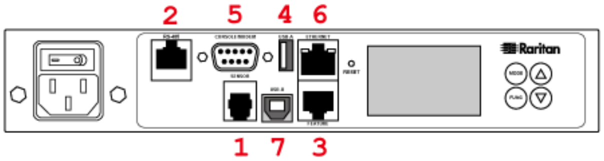
Note that a minimum of 10-second power-off period is required, or the device may not boot up properly.

Connection Ports

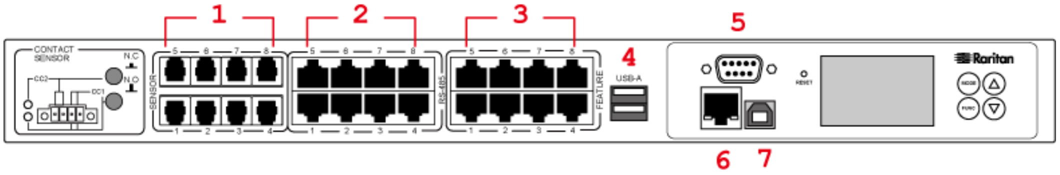
Depending on the model you purchased, the total number of ports available varies.

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

EMX2-111



EMX2-888

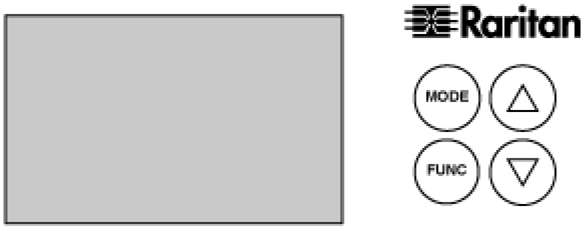


No.	Port	Used for...
1	SENSOR (RJ-12)	Connection to one of the following devices: ▪ Raritan's environmental sensor package(s). ▪ Raritan's sensor hub, which expands the number of a sensor port to four ports.
2	RS-485	Connection to an electrical device with the RS-485 interface. Currently the EMX supports 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 sensor, 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. Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the EMX device remotely using the web interface. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. *Note: Connection to this port is not required 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.

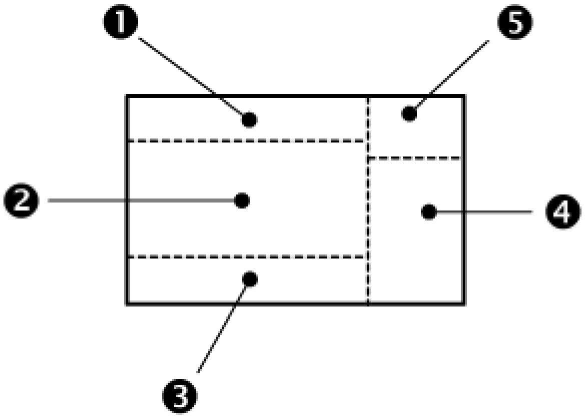


It consists of:

- A character LCD display
- Control buttons

Overview of the LCD Display

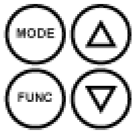
Different types of information are shown in different sections of the character LCD display. The diagram indicates the sections.



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 Sensor mode if an asset sensor 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 67).
- 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

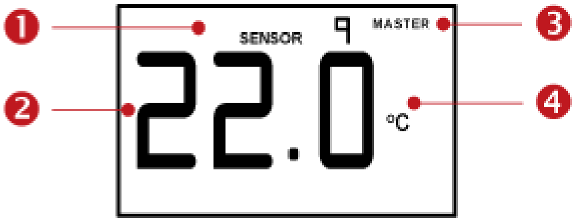
Operating the LCD Display

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).

Number	Example information
❷	The selected environmental sensor's reading is 22 °C.
❸	The word "MASTER" indicates the EMX is the master device in a USB-cascading configuration. See ***Cascading the EMX via USB*** (on page 22). *Note: For a standalone EMX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
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 discrete sensor:

States	Description
nor	The sensor is in the normal state.
ALA	The sensor enters the 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 discrete (on/off) 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:

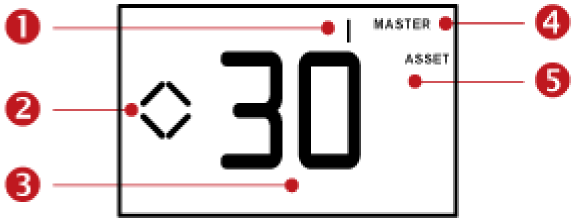
   s:AE --> s:17 --> s:A0 --> s:00 --> s:22

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 ☰. *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 sensor information.



Section	Example information
❶	"1" refers to the asset sensor 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.
❹	The word "MASTER" indicates the EMX is the master device in a USB-cascading configuration. See ***Cascading the EMX via USB*** (on page 22). *Note: For a standalone EMX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
❺	"ASSET" means that the LCD display enters the Asset Sensor mode.

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

1. Press the MODE button until the EMX enters the Asset Sensor 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 sensor. The rack unit number appears in the middle of the LCD display.

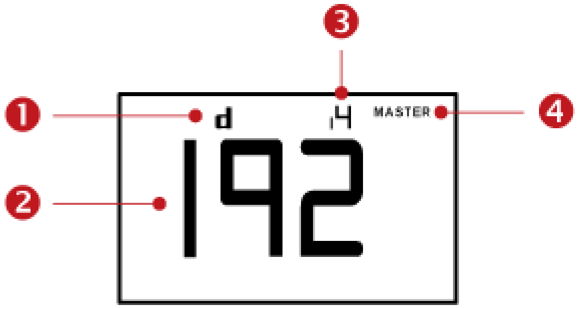
Note: Press and hold the Up or Down button for at least two (2) seconds to quickly move through several items at once.

- 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

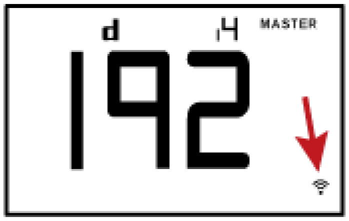
The IP address is available in the Device mode, which is indicated by the alphabet 'd' shown at the top of the LCD display. Note that the LCD display only shows the IPv4 address (if available).

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 USB-cascading configuration. See ***Cascading the EMX via USB*** (on page 22). *Note: For a standalone EMX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*

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.

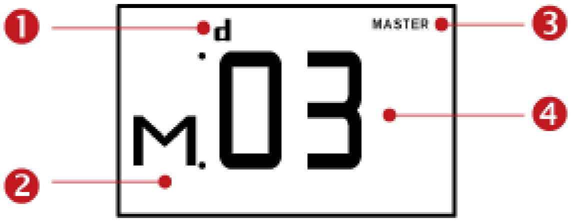
   For example, 192.168.84.4 cycles in this sequence:

   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.

Section	Example information
❸	The word "MASTER" indicates the EMX is the master device in a USB-cascading configuration. See ***Cascading the EMX via USB*** (on page 22). *Note: For a standalone EMX, this word is NOT displayed. For a slave device, it shows "SLAVE" instead.*
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:

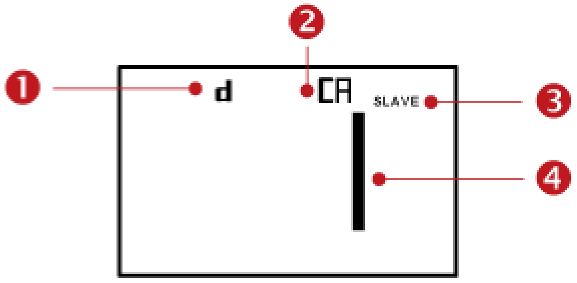
   M 00 --> M:0d --> M:5d --> M:03 --> M:5E --> M:1A

   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

A cascaded device's position is available by operating the LCD display. For information on the USB-cascading configuration, see ***Cascading the EMX via USB*** (on page 22).

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 USB-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

Note 1: For a standalone EMX, its position is the number 0, but the word "MASTER" is NOT shown on the LCD display.

Note 2: If reversing or disconnecting the USB cable from a slave device, causing the slave device to become a master or standalone device, you must plug an Ethernet cable to it to update its USB-cascading status.

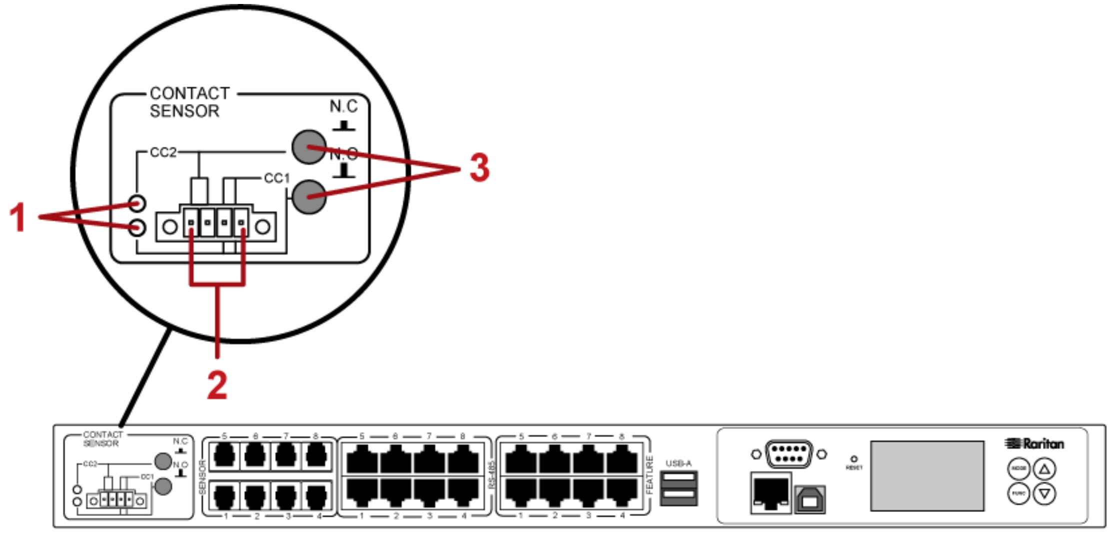
EMX2-888 Contact Closure Sensor Termination

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 541).*



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.

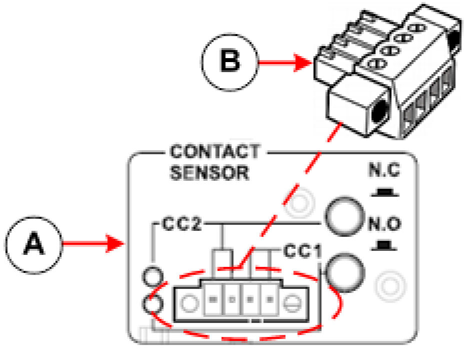
Tip: Alternatively, third-party CC switches can be connected to Raritan's DPX-CC2-TR or DX sensor package, which is then connected to a SENSOR port on the EMX. For sensor information, refer to the Environmental Sensors Guide or Online Help on the Raritan's website's **Support page** *(***http://www.raritan.com/support/***).*

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 541).*

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).

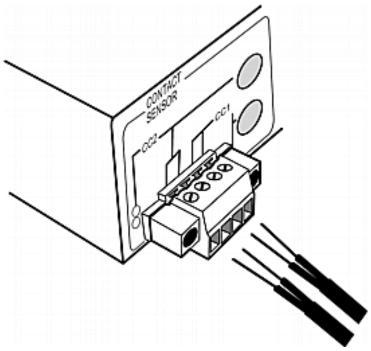
With this design, there are two ways to plug discrete detectors/switches:

- 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.

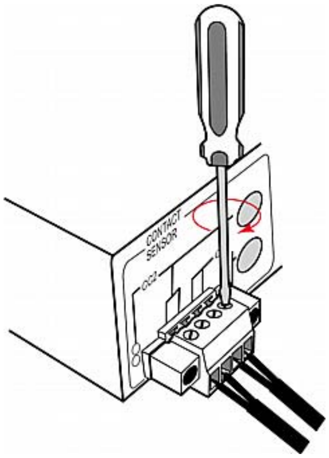
Important: It is not guaranteed that all third-party detectors/switches are compatible with the EMX. You need to test the compatibility after installing them.

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.



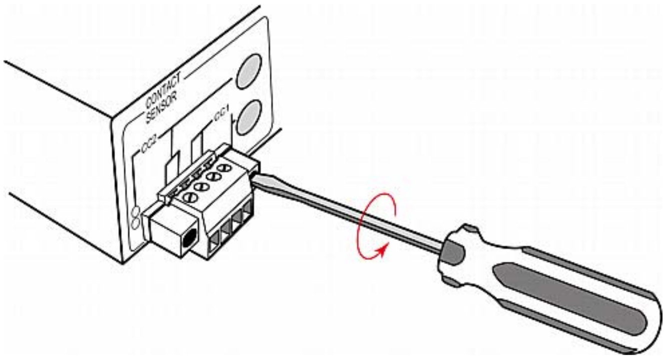
3. Use a screwdriver with a 2.5 mm wide shaft to tighten the screws above each termination point to secure the wires, using a torque of 0.196 N·m (2 kgf·cm).



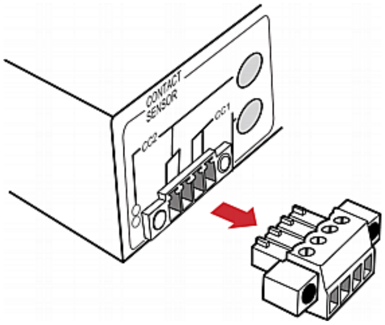
To make connections when the terminal module is separated from the EMX:

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

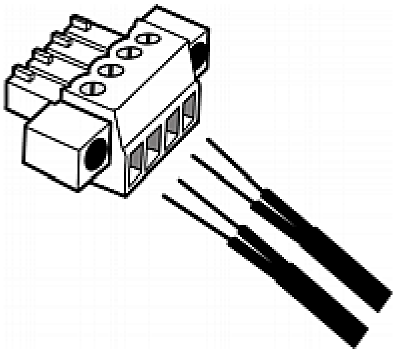
Note: The two screws are not removable, so just loosen them.



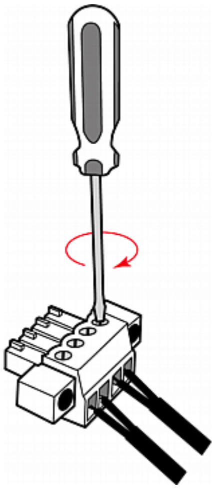
2. Remove the terminal module from the EMX.



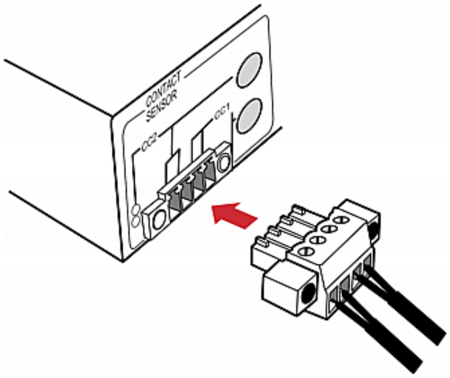
3. Strip the insulation and insert each wire of both detectors/switches into each termination point.



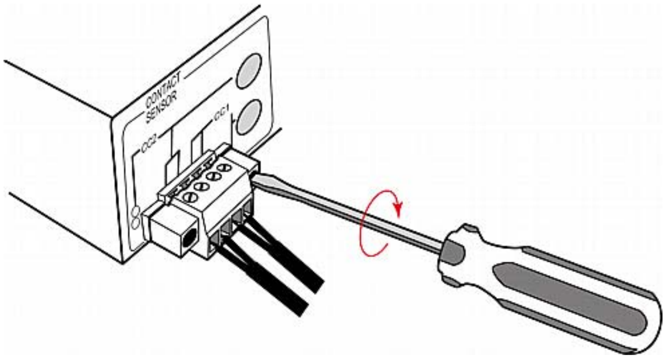
4. Use a screwdriver with a 2.5 mm wide shaft to tighten the screws above each termination point to secure the wires, using a torque of 0.196 N·m (2 kgf·cm).



5. Plug the terminal module back into the EMX.



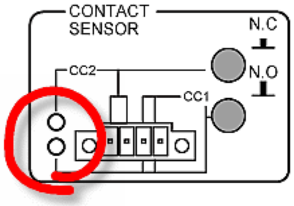
6. Tighten the two screws on two sides of the module to secure it.



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):**

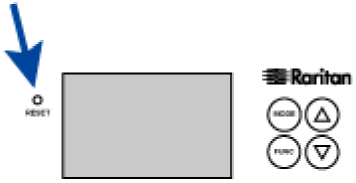
LED	Sensor state
Off	Open
Lit	Closed

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 477).

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 187).

Tip: You can remotely check this beeper's state via the web interface. See **Checking the Internal Beeper State** *(on page 148).*

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® 8, 9, 10 and 11
- Firefox® 25 and later
- Safari® 5.x (MacOS Lion)
- Google® Chrome® 32 and later
- Android 4.2 and later
- IOS 7.0
- Windows Edge

Note: Tablets such as iPad® are supported but not recommended for use with EMX2-888. Smartphones are not supported for use with EMX2-888.

Logging in to the Web Interface

To log in to the web interface, you must enter a user name and password.

The first time you log in to the EMX, use the default user name (admin) and password (raritan). For details, see the Quick Setup Guide accompanying the product.

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See ***Creating a User Profile*** (on page 149).

Login

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

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

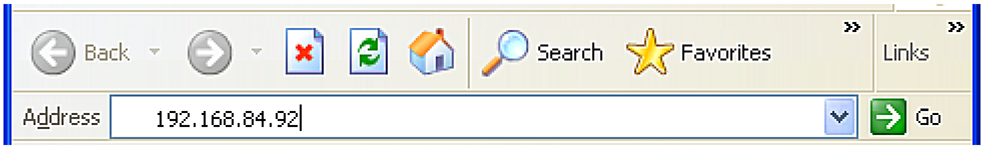
▶ **To log in to the web interface:**

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

   http(s)://<ip address>

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

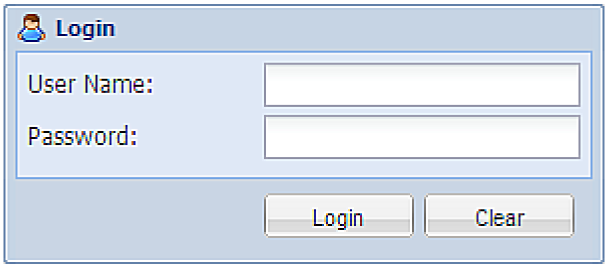
   Tip: If the link-local addressing has been enabled, you can type pdu.local *instead of an IP address. See* **APIPA and Link-Local Addressing** *(on page 4).*



192.168.84.92

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

3. Type your user name in the User Name field, and password in the Password field. Both the user name and password are case sensitive.



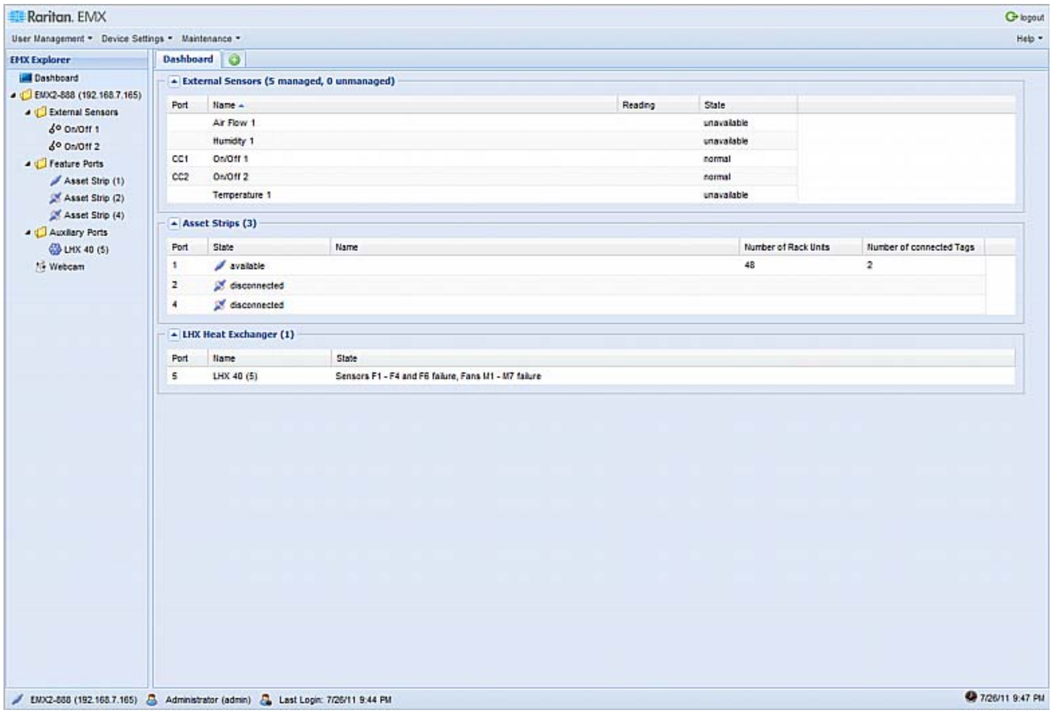
Note: If needed, click Clear to clear either the inputs or any error message that appears.

4. If a security agreement is displayed on the Login page, accept it. Otherwise, you cannot log in successfully.

   To select the agreement checkbox using the keyboard, press the Space bar.

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

   Depending on your hardware configuration, elements shown on the web interface may appear slightly different from this image.



External Sensors (5 managed, 0 unmanaged)

Port	Name	Reading	State
	Air Flow 1		unavailable
	Humidity 1		unavailable
CC1	On/Off 1		normal
CC2	On/Off 2		normal
	Temperature 1		unavailable

Asset Strips (3)

Port	State	Name	Number of Rack Units	Number of connected Tags
1	available		48	2
2	disconnected			
4	disconnected			

LHX Heat Exchanger (1)

Port	Name	State
5	LHX 40 (5)	Sensors F1 - F4 and F6 failure, Fans M1 - M7 failure

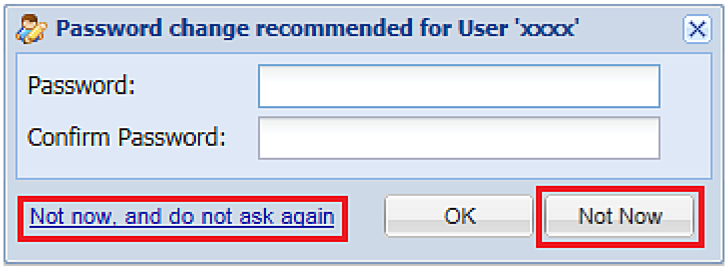
EMX2-888 (192.168.7.165) Administrator (admin) Last Login: 7/26/11 9:44 PM 7/26/11 9:47 PM

Note: The IP address to access a slave device in the USB-cascading configuration where the port forwarding mode is applied is a combination of the IP address and the port number. See **Port Forwarding Examples** *(on page 141).*

Password change request for 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 the password or ignore it.

- *Not Now* ignores the request for this time only.
- *Not now, and do not ask again* ignores the request permanently.
- Or enter the new password and click OK.


Password change recommended for User 'xxxx'
Password:
Confirm Password:
Not now, and do not ask again
OK
Not Now

Users without permissions listed must change password.

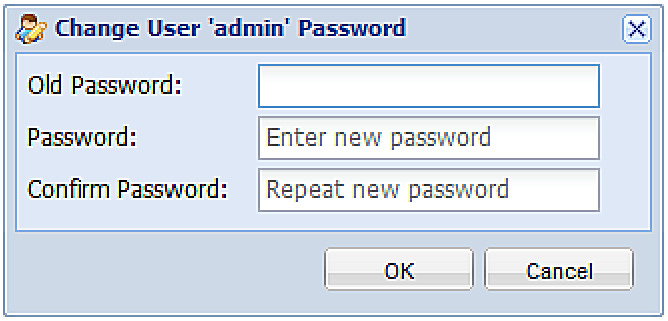
Changing Your Password

You must have the Change Own Password permission to change your own password. See ***Setting Up Roles*** (on page 154).

You must have Administrator Privileges to change other users' passwords. See ***Modifying a User Profile*** (on page 152).

To change your password:

- Choose User Management > Change Password. The Change User Password dialog appears.
- Passwords are case sensitive.
- Password length: 4 to 64 characters.



Change User 'admin' Password

Old Password:	
Password:	Enter new password
Confirm Password:	Repeat new password

Remembering User Names and Passwords

As of release 3.0.0, the EMX supports the password manager of Microsoft Internet Explorer® and Mozilla Firefox®.

You can choose to save the user name and password used to log in to the EMX when these two browsers ask whether you want to remember them. If yes, next time your user name and password can be automatically completed at login.

For information on how to activate a browser's password manager, see the user documentation accompanying Internet Explorer or Firefox.

The EMX does NOT support other browser password managers.

Logout

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

To log out of the web interface:

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

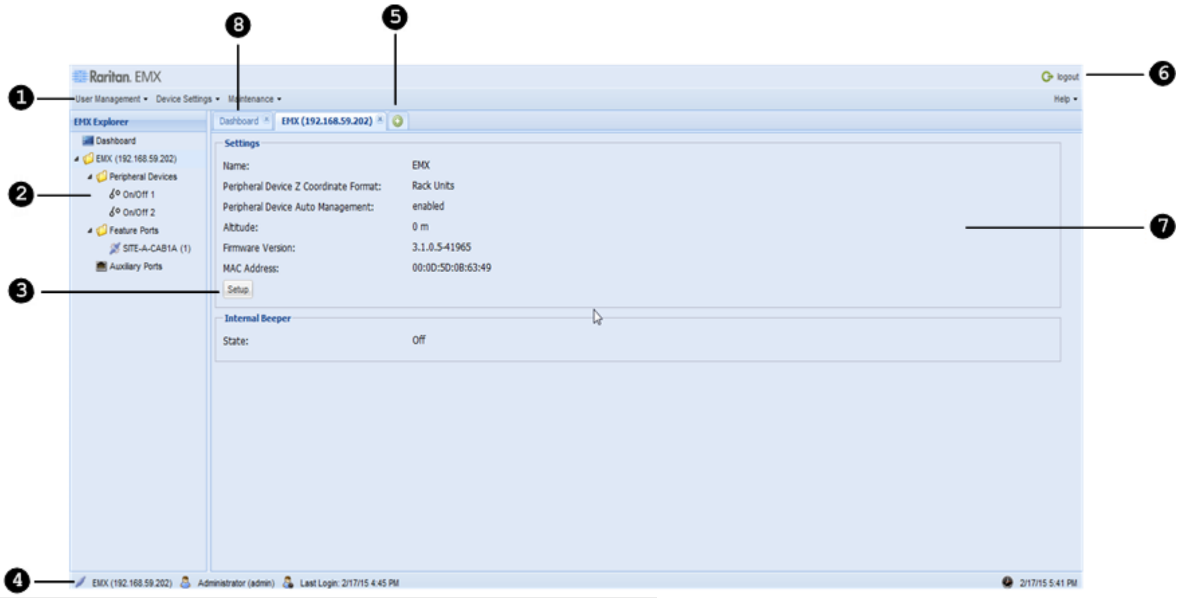
logout

- Close the web browser by clicking the Close button (☒) on the top-right corner of the browser.
- Close the web browser by choosing File > Close, or File > Exit. The command varies according to the version of the browser you use.
- Choose the Refresh command or click the Refresh button on the web browser.

2. Either the login page opens or the browser is closed, depending on your choice in the previous step.

Introduction to the Web Interface

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



Settings

Name: EMX

Peripheral Device Z Coordinate Format: Rack Units

Peripheral Device Auto Management: enabled

Altitude: 0 m

Firmware Version: 3.1.0.5-41965

MAC Address: 00:0D:5D:08:63:49

Internal Beeper

State: Off

EMX (192.168.59.202) Administrator (admin) Last Login: 2/17/15 4:45 PM 2/17/15 5:41 PM

❶	Menus
❷	EMX Explorer pane
❸	Setup button*
❹	Status bar
❺	Add Page icon
❻	Logout button

❼	Data pane
❽	Dashboard

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

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

Menus

- **User Management** contains user profiles, permissions, and password settings.
- **Device Settings** contains device name, network settings, security settings, and system time.
- **Maintenance** contains event log, hardware information, firmware upgrade and so on.
- **Help** displays firmware and open source information, and a link to the online help.

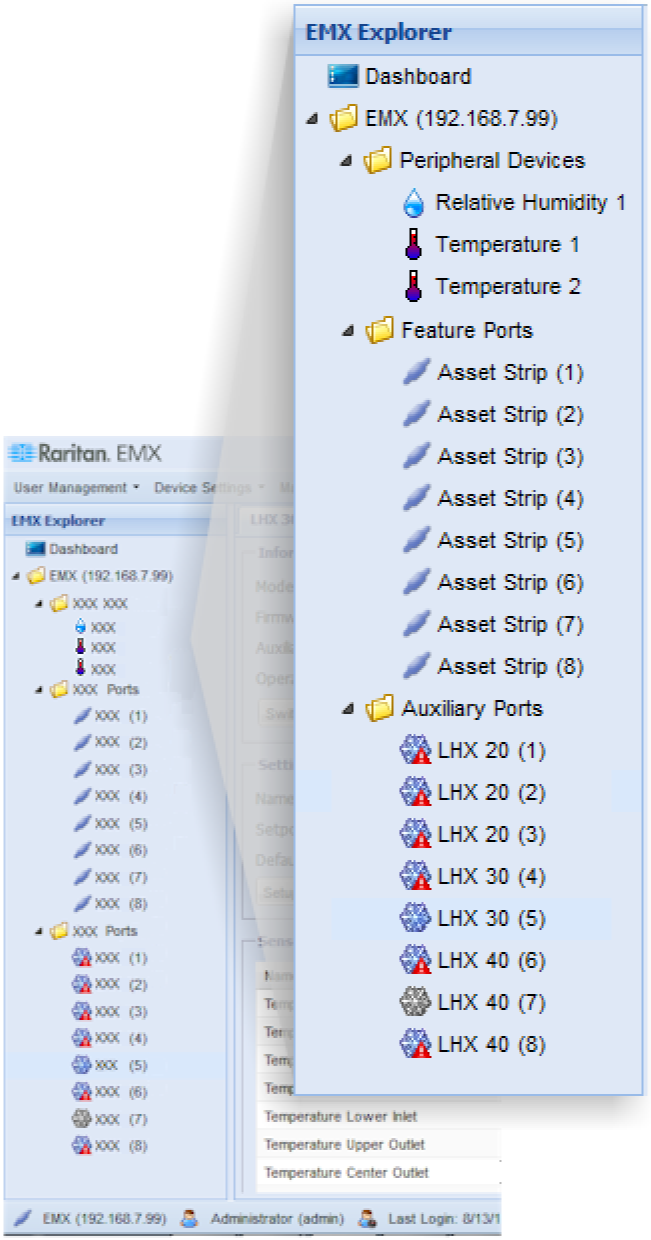
EMX Explorer Pane

The hierarchical tree to the left displays the EMX device you are accessing as well as all physical components embedded on or connected to this product, such as inlets, outlets, and environmental sensors. In addition, an icon named Dashboard is available for displaying the PDU summary information.

The tree structure comprises these hierarchical levels.

First level	Second level	Third level
Dashboard	None	None
EMX folder*	Peripheral Devices	A list of connected environmental sensors and actuators
	Feature Ports	One of the following is displayed, depending on your configuration: ▪ Auto ▪ Disabled ▪ Asset Strip ▪ External Beeper

First level	Second level	Third level
	Auxiliary Ports (RS-485)	If one of the following is connected: ▪ LHX-20 ▪ SHX-30 ▪ LHX-40 ▪ PowerLogic PM710
	**Webcam Snapashots	▪ Snapshots ▪ Webcam



*The EMX folder is named "EMX" by default. The name can be customized. See ***Naming the EMX*** (on page 110).

** A Webcam icon appears only when a supported Logitech® webcam is connected to the EMX. See ***Connecting a Logitech Webcam*** (on page 59).

Expanding the Tree

The icons representing all components implemented on or connected to the EMX device are expanded by default. If they are hidden, you may expand the tree manually to show all component icons.

▶ **To expand the tree:**

1. By default, the EMX folder has been expanded.

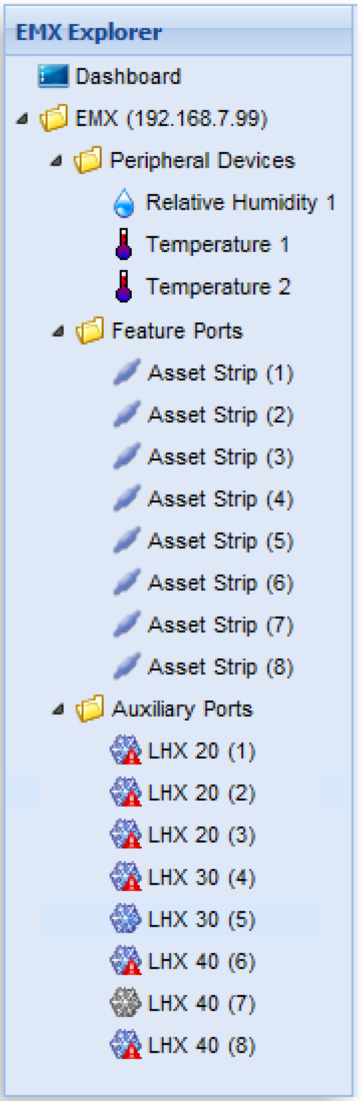
   Note: The EMX folder is named "EMX" by default. The name can be customized. See **Naming the EMX** *(on page 110).*

   If it is not expanded, click the white arrow ▷ prior to the folder icon, or double-click the folder. The arrow then turns into a black, gradient arrow ◢, and icons of components or component groups appear below the EMX folder.

2. To expand any component group at the second level, click the white arrow ▷ prior to the folder icon, or double-click the folder.

   The arrow then turns into a black, gradient arrow ◢, and icons representing individual components appear below the group folder.

3. Repeat Step 2 for other component groups you want to expand. The expanded tree looks similar to this image.



Collapsing the Tree

You can collapse the whole tree structure or a specific component group to hide all or partial tree items.

To collapse the whole tree:

- Click the black, gradient arrow ◢ prior to the EMX folder icon, or double-click the folder.

  Note: This folder's name changes after customizing the device name. See **Naming the EMX** *(on page 110).*

  The arrow then turns into a white arrow ▷, and all items below the EMX folder disappear.

To hide some tree items:

1. Click the black, gradient arrow ◢ prior to the component group folder that you want to collapse, or double-click the folder.

   The arrow then turns into a white arrow ▷, and all items below the folder disappear.

2. Repeat Step 1 for other component groups you want to collapse.

Determining How to Display Tree Items

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

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

How to Display Asset Sensors

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

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

To determine how to display connected asset sensors:

1. Click the Feature Ports folder. The Feature Ports page opens in the right pane, listing all FEATURE ports.

2. Select the number of the port that you want to configure, and click Setup. Or you can simply double-click that port number. The Feature Port Setup dialog for the selected port appears.
3. In the Detection Mode field, select the way to display connected asset sensors.
   - Disabled: When applied, disables to port and nothing connected to the port is detected.
   - Auto: An icon is displayed for this port only when the EMX device detects the physical connection of the asset sensor on this port. Otherwise, nothing is displayed. This is the default approach.
   - Pinned: An icon is displayed for this port all the time, but the icon image varies according to the connection status. If the connection of an asset sensor is detected on a specific Feature port, this icon is displayed on that port. If not detected, this icon appears instead. See ***Determining How to Display Tree Items*** (on page 94).

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

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

How to Display LHX/SHX Heat Exchangers

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

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

The EMX supports the LHX-20, LHX-40 and SHX-30 models.

Note: Schroff LHX/SHX Support must be enabled in order for the LHX/SHX to be displayed. See **Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support** *(on page 273).*

▸ To determine how to display connected LHX/SHX heat exchangers:

1. Click the Auxiliary Ports folder or the Feature Ports folder depending on which port you want to connect the sensor to.
2. Select the number of the port that you want to configure, and click Setup. Or you can simply double-click that port number. The Auxiliary Port Setup dialog for the selected port appears.

3. In the Detection Mode field, select the way to display connected LHX/SHX heat exchangers.
   - Disabled: When applied, disables to port and nothing connected to the port is detected.
   - Auto: An icon is displayed for this port only when the EMX device detects the physical connection of the LHX/SHX heat exchanger on this port. Otherwise, nothing is displayed. This is the default approach.
   - Pinned: An icon is displayed for this port all the time, but the icon image varies according to the connection status. See ***Device States and Icon Variations*** (on page 280).

   When the Pinned checkbox is selected, click the drop-down arrow to select the appropriate device type for this port: LHX-20, LHX-40 or SHX-30.
4. Click OK.

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

Setup Button

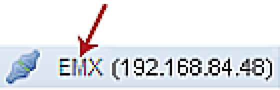
The Setup button is available for most tree items. It triggers a setup dialog where you can change settings for the selected tree item.

Status Bar

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

- **Device name:**

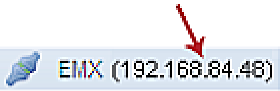
  This is the name assigned to the EMX device. The default is "EMX." See ***Naming the EMX*** (on page 110).



EMX (192.168.84.48)

- **IP address:**

  The numbers enclosed in parentheses is the IP address assigned to the EMX device. See ***Initial Network Configuration via CLI*** (on page 15) or ***Modifying Network Settings*** (on page 114).



EMX (192.168.84.48)

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

- **Login name:**

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

  Administrator (admin)

- **Last login time:**

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

  Last Login: 3/24/11 9:46 PM

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

  For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.

  There are different types of access clients:

  - Web GUI: Refers to the EMX web interface.
  - CLI: Refers to the command line interface (CLI).

    The information in parentheses following "CLI" indicates how this user is connected to the CLI.
    - *Serial*: Represents the local connection (serial RS-232 or USB).
    - *SSH*: Represents the SSH connection.
    - *Telnet*: Represents the Telnet connection.

- **System date and time:**

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

  3/24/11 10:18 PM

Add Page Icon

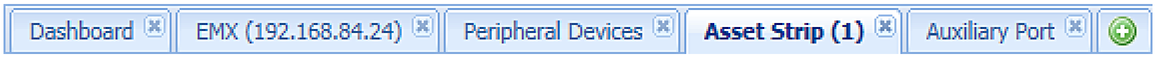
The Add Page icon ⊕, located on the top of the data pane, lets you open data pages of multiple tree items without overriding any opened page.

▶ To open new data pages:

1. Click the Add Page icon ⊕. A new tab along with a blank data page appears.

2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank page.
3. To open more data pages, repeat the above steps. All tabs representing opened pages are shown across the top of the page.

   The following diagram shows a multi-tab example.



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

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

Data Pane

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

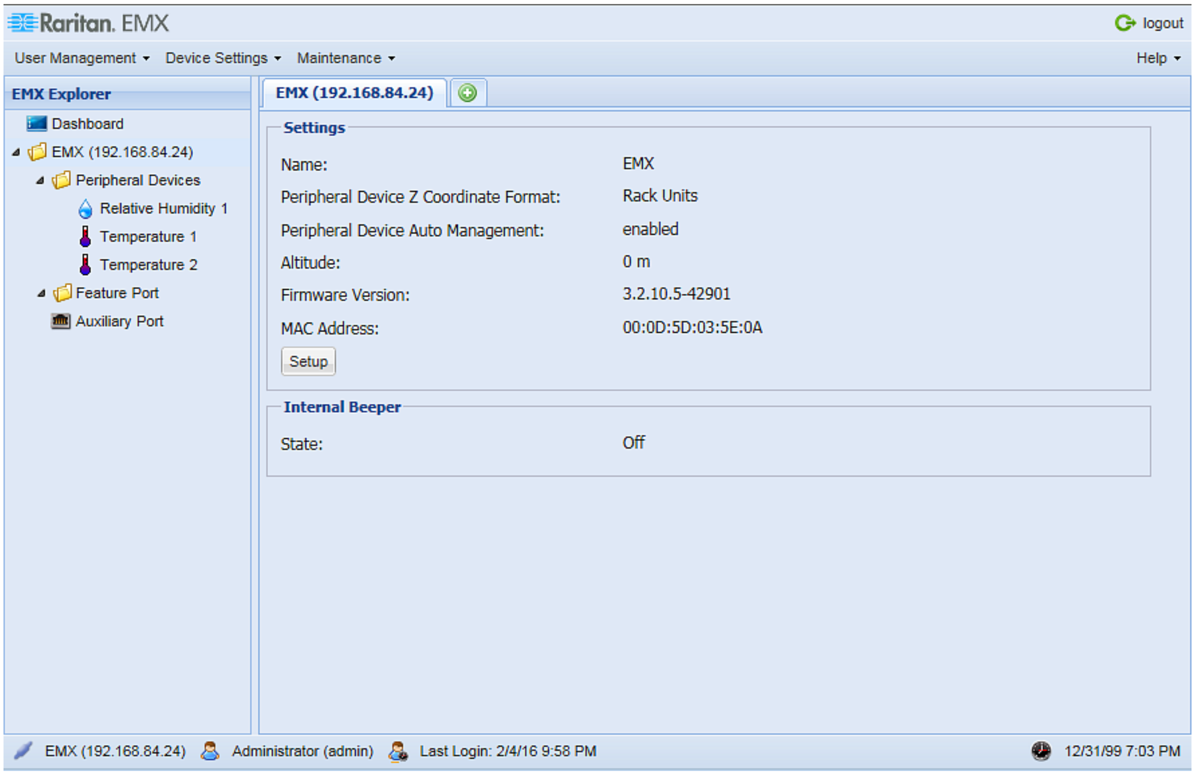
All tabs above the pane represent the opened data pages. The highlighted tab indicates the current selection.

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

▶ To adjust the pane's width:

1. Move the mouse pointer to the left border of the right pane.

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



Settings

Name:	EMX
Peripheral Device Z Coordinate Format:	Rack Units
Peripheral Device Auto Management:	enabled
Altitude:	0 m
Firmware Version:	3.2.10.5-42901
MAC Address:	00:0D:5D:03:5E:0A

Internal Beeper

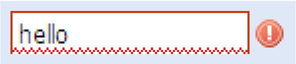
State: Off

More Information

This section explains additional web interface elements or operations that are useful.

Warning Icon

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



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

The Yellow- or Red-Highlighted Sensors

When a numeric sensor's reading enters the warning or critical range, the background color of the sensor row turns to yellow or red for alerting you.

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

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while discrete (on/off) sensors show sensor states only to indicate state changes.

See the table for the meaning of each color:

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

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

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

For information on threshold settings, see:

- ***Configuring Environmental Sensors or Actuators*** (on page 246)
- ***Configuring Temperature and Fan Thresholds*** (on page 276)

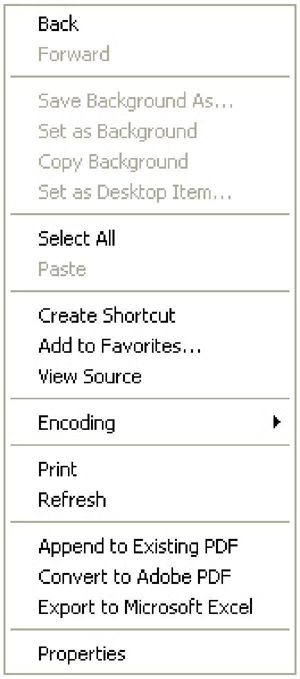
Browser-Defined Shortcut Menu

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

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

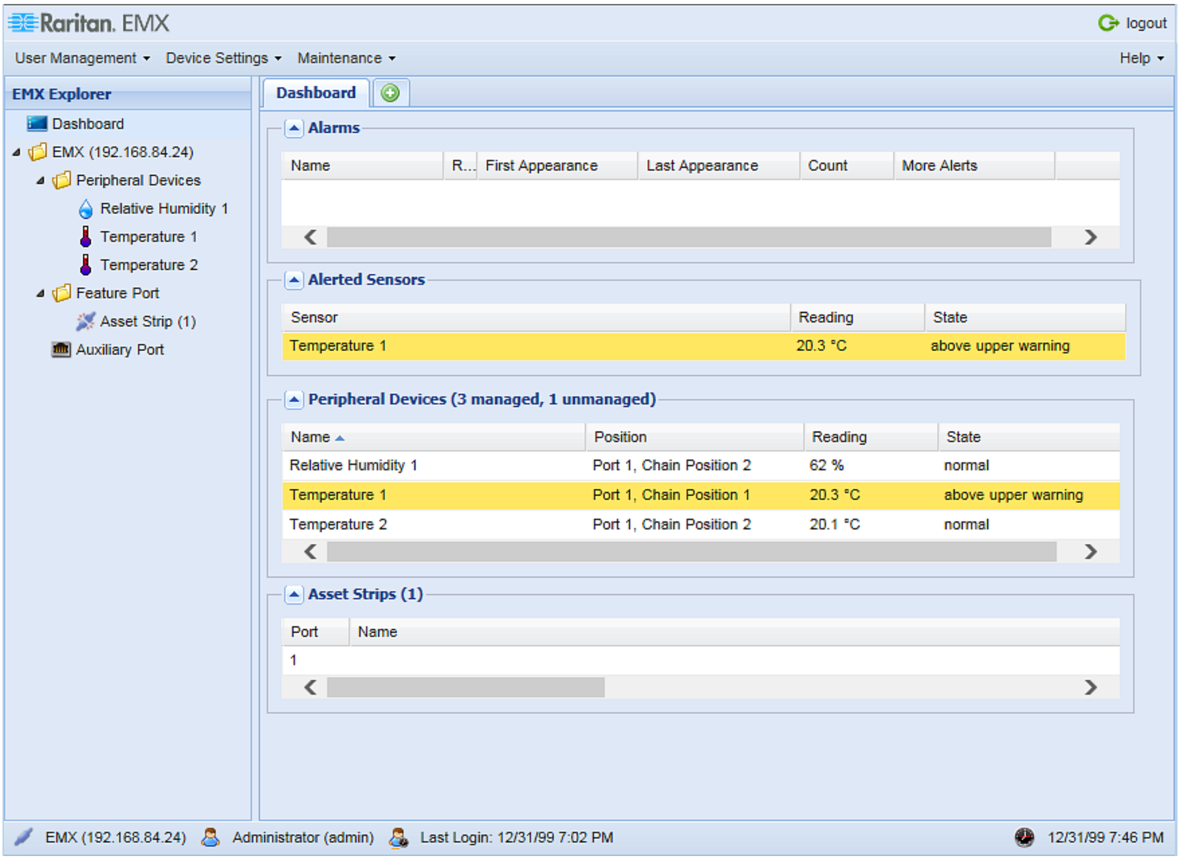
For information on each shortcut menu command or item, see the online help or documentation accompanying your web browser.

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



Dashboard

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



Alarms

Name	R...	First Appearance	Last Appearance	Count	More Alerts

Alerted Sensors

Sensor	Reading	State
Temperature 1	20.3 °C	above upper warning

Peripheral Devices (3 managed, 1 unmanaged)

Name	Position	Reading	State
Relative Humidity 1	Port 1, Chain Position 2	62 %	normal
Temperature 1	Port 1, Chain Position 1	20.3 °C	above upper warning
Temperature 2	Port 1, Chain Position 2	20.1 °C	normal

Asset Strips (1)

Port	Name
1	

EMX (192.168.84.24) Administrator (admin) Last Login: 12/31/99 7:02 PM 12/31/99 7:46 PM

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

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or at least one LHX built-in sensor fails on the heat exchanger. See **The Yellow- or Red-Highlighted Sensors** *(on page 100).*

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

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

▶ To collapse any section:

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

▶ To expand a collapsed section:

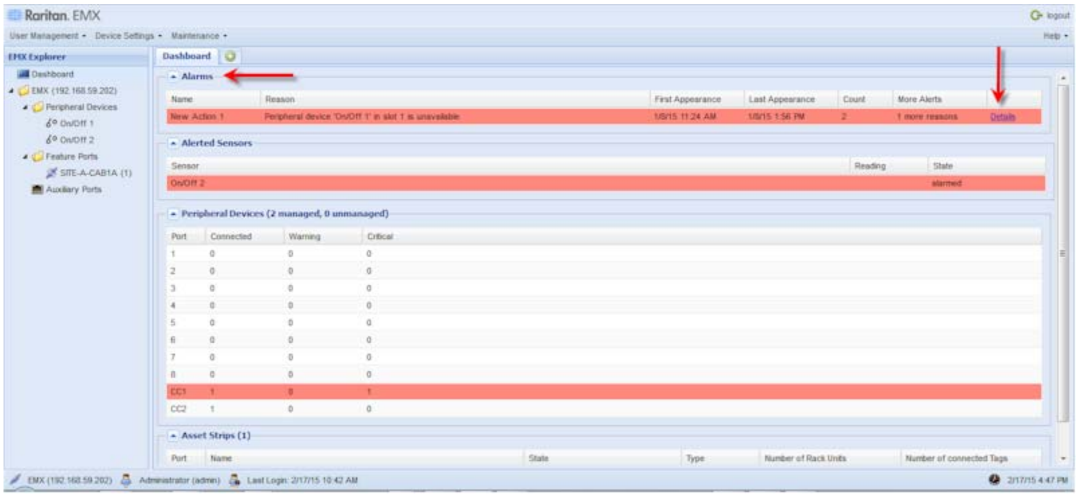
1. Locate the section you want to expand.
2. Click the downward arrow ▼ prior to the section title. The data specific to the section appears.

Alarms List

You can create event rules that request users to acknowledge certain alerts, and resend alert notifications if the acknowledgment action is not taken yet. See ***Creating Actions*** (on page 188).

If any of these alerts has not been acknowledged since its occurrence, the Alarms section on the dashboard shows this alert until it is acknowledged. All alerts on the Alarms section are highlighted in red.

Below is the illustration of the alarms list.



Alarms

Name	Reason	First Appearance	Last Appearance	Count	More Alerts	
New Action 1	Peripheral device 'On/Off 1' in slot 1 is unavailable	1/8/15 11:24 AM	1/8/15 1:56 PM	2	1 more reasons	Details

Alerted Sensors

Sensor	Reading	State
On/Off 2		alarmed

Peripheral Devices (2 managed, 0 unmanaged)

Port	Connected	Warning	Critical
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
CC1	1	0	1
CC2	1	0	0

Asset Strips (1)

Port	Name	State	Type	Number of Rack Units	Number of connected Tags

The following table explains each column of the alarms list.

Column	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.
More Alerts	▪ A dash is displayed when there is only one event triggering this alert. ▪ If there are other types of events triggering the same alert, the total number of these additional reasons is displayed. You can double click that alarm to view a list of all events that have occurred.

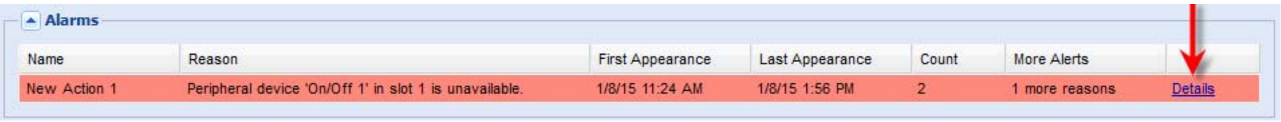
Column	Description
Details	Click "Details" to trigger a dialog showing both the alarm details and the acknowledgment button.

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

To acknowledge an alarm:

1. Double-click the alarm that you want to acknowledge, or click Details in the final column. A dialog appears.

Click Acknowledge Alarm to acknowledge it. That alarm then disappears from the Alarms section.



Alarms

Name	Reason	First Appearance	Last Appearance	Count	More Alerts	
New Action 1	Peripheral device 'On/Off 1' in slot 1 is unavailable.	1/8/15 11:24 AM	1/8/15 1:56 PM	2	1 more reasons	Details

Alerted Sensors

One of the sections on the Dashboard page only displays critical or warning conditions detected by internal or external sensors so that you are alerted to take actions. This section is labeled Alerted Sensors.

The Alerted Sensors section lists any or all of the following:

- Any sensor that enters the warning or critical range if the thresholds have been enabled
- Discrete (on/off) sensors that enter the alarmed state

Device Management

Displaying the Device Information

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

To display the device information:

1. Choose Maintenance > Device Information.

Tab	Information shown
Device Information	General device information, such as model name, serial number, firmware version, hardware revision, and so on.

Tab	Information shown
Asset Strips	Each asset sensor's ID, boot version, application version and protocol version.

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

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

Identifying Cascaded Devices

This section explains how to identify a cascaded EMX in the Device Information dialog.

For information on how to cascade devices using USB cables, see ***Cascading the EMX via USB*** (on page 22).

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

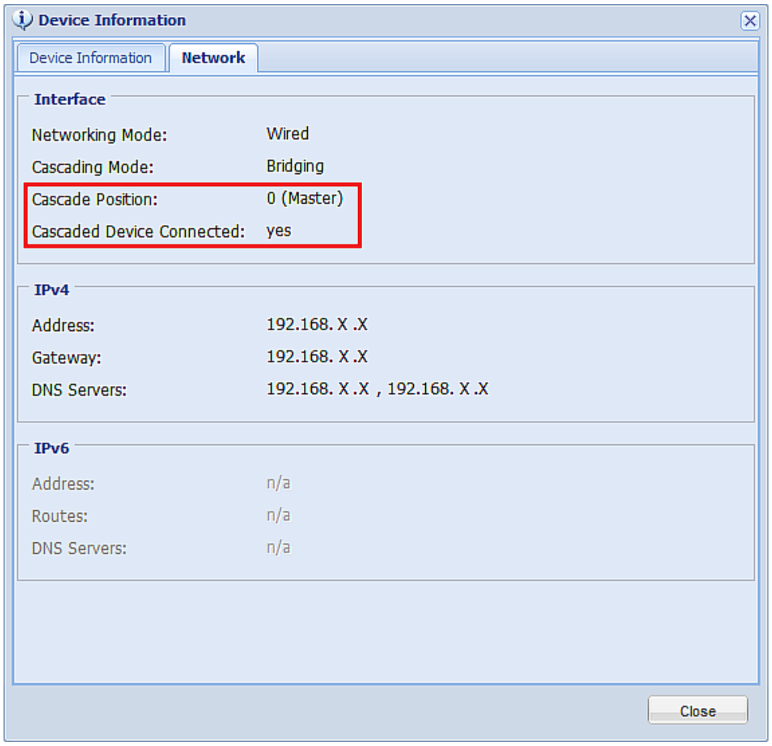
To identify the USB-cascading status of a EMX device:

1. Choose Maintenance > Device Information.
2. Select the Network tab and locate the Interface section. The Interface section contains four read-only fields as listed below.

Fields	Description
Networking Mode	Indicates how the EMX is connected to the LAN. ▪ Wired: The device is connected to the LAN through a standard network cable. ▪ Wireless: The device is connected to the LAN through a supported USB wireless LAN adapter. See ***USB Wireless LAN Adapters*** (on page 14). ▪ XXX (USB): XXX represents Wired or Wireless. The device is connected to the LAN through a USB-cascading configuration. That is, it is a slave device.
Cascading Mode	Shows the cascading mode applied. See ***Setting the Cascading Mode*** (on page 136).

Fields	Description
Cascade Position	Indicates the position of the EMX in the USB-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. This field is NOT available on a standalone EMX.
Cascaded Device Connected	Indicates whether the presence of a slave device is detected on the USB-A 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.



Interface

Networking Mode: Wired

Cascading Mode: Bridging

Cascade Position: 0 (Master)

Cascaded Device Connected: yes

IPv4

Address: 192.168. X .X

Gateway: 192.168. X .X

DNS Servers: 192.168. X .X , 192.168. X .X

IPv6

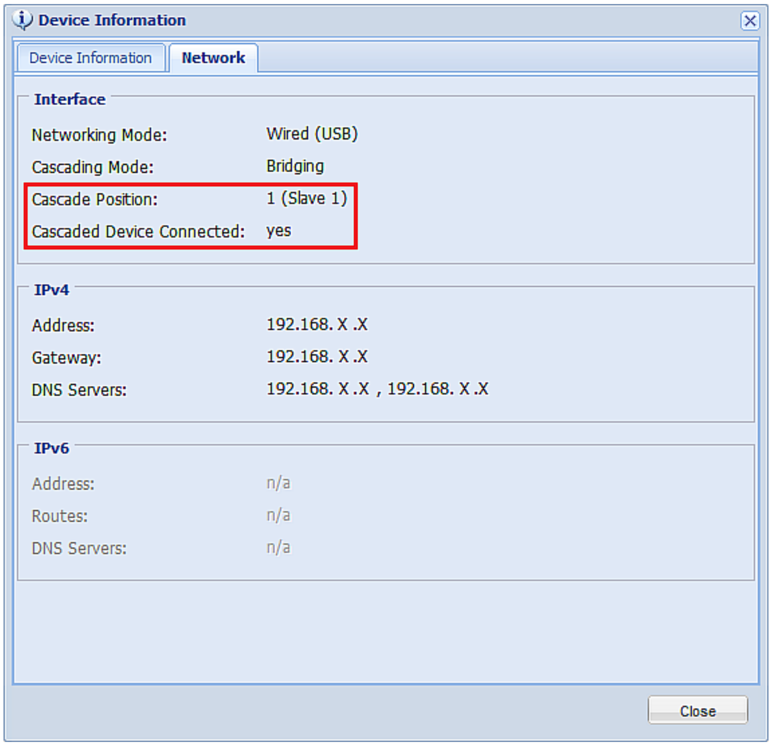
Address: n/a

Routes: n/a

DNS Servers: n/a

- 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.



Interface

Networking Mode: Wired (USB)

Cascading Mode: Bridging

Cascade Position: 1 (Slave 1)

Cascaded Device Connected: yes

IPv4

Address: 192.168. X .X

Gateway: 192.168. X .X

DNS Servers: 192.168. X .X , 192.168. X .X

IPv6

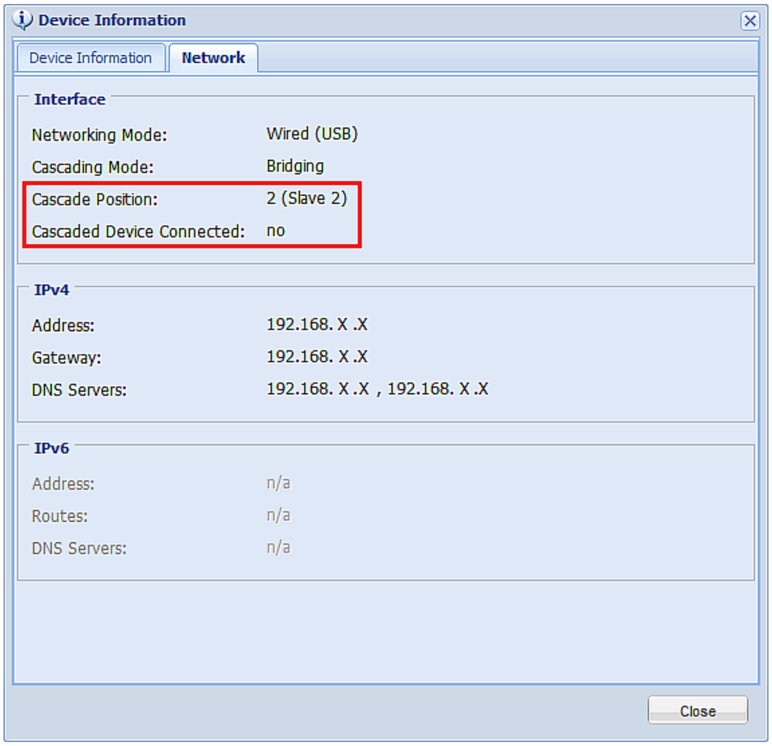
Address: n/a

Routes: n/a

DNS Servers: n/a

- 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.



Interface

Networking Mode: Wired (USB)

Cascading Mode: Bridging

Cascade Position: 2 (Slave 2)

Cascaded Device Connected: no

IPv4

Address: 192.168. X .X

Gateway: 192.168. X .X

DNS Servers: 192.168. X .X , 192.168. X .X

IPv6

Address: n/a

Routes: n/a

DNS Servers: n/a

Naming the EMX

To change the device name:

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

   Note: This folder's name changes after customizing the device name. See **Naming the EMX** *(on page 110).*

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

Modifying the Network Configuration

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

Modifying Network Interface Settings

The EMX supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See ***Connecting the EMX to Your Network*** (on page 14).

Wired Network Settings

The LAN interface speed and duplex mode were set during the initial configuration process.

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

▶ **To modify the network interface settings:**

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wired from the list.
4. To change the LAN speed, click the drop-down arrow in the Speed field and select an option from the list.
   - Auto: System determines the optimum LAN speed through auto-negotiation.
   - 10 Mbit/s: The LAN speed is always 10 Mbps.
   - 100 Mbit/s: The LAN speed is always 100 Mbps.
5. To change the duplex mode, click the drop-down arrow in the Duplex field and select an option from the list.
   - Auto: The EMX selects the optimum transmission mode through auto-negotiation.
   - Full: Data is transmitted in both directions simultaneously.
   - Half: Data is transmitted in one direction (to or from the EMX device) at a time.
6. Click OK.

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

Wireless Network Settings

Wireless SSID, PSK and BSSID parameters were set during the installation and configuration process. You can change them later.

Note for USB-cascading configuration: Port forwarding mode over wireless LAN is supported as of release 3.1.0. You must upgrade all devices in the chain to version 3.1.0 or higher if wireless networking is preferred. See **Cascading the EMX via USB** *(on page 22).*

▶ To modify the wireless interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the EMX device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See ***Connecting the EMX to Your Network*** (on page 14).
5. Type the name of the wireless access point (AP) in the SSID field.
6. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

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

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

Options	Description
No Authentication	Select this option when no authentication data is required.
PSK	A Pre-Shared Key is required for this option. ▪ In the Pre-Shared Key field, type the PSK string.

Options	Description
EAP - PEAP	PEAP stands for Protected Extensible Authentication Protocol. Enter the following authentication data: ▪ Inner Authentication: Only Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) is supported, allowing authentication to databases that support MSCHAPv2. ▪ Identity: Type your user name. ▪ Password: Type your password. ▪ CA Certificate: A third-party CA certificate may or may not be needed. If needed, follow the step below.

8. When the PEAP authentication requires a CA certificate, do the following:

   a. Select the "Enable Verification of TLS Certificate Chain" 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.

   b. Click Browse to select a TLS certificate file. Then you can:

      - Click Show to view the certificate's contents.

      - Click Remove to delete the installed certificate if it is inappropriate.

   c. Select the "Allow expired and not yet valid certificates" checkbox if intending to make the wireless network connection successful even though the installed TLS certificate chain contains any certificate that is outdated or not valid yet.

   d. Select the "Allow wireless connection if system clock is incorrect" checkbox to make the wireless network connection successful when the EMX system time is earlier than the firmware build before synchronizing with any NTP server. If the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail while this checkbox is not selected.

   The incorrect system time issue may occur when the EMX has once been powered off for a long time.

9. Click OK.

Modifying Network Settings

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

Selecting the Internet Protocol

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

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

▶ To select the appropriate Internet Protocol:

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

Modifying IPv4 Settings

You must enable the IPv4 protocol before you can modify the IPv4 network settings. See ***Selecting the Internet Protocol*** (on page 114).

▶ To modify IPv4 settings:

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

Option	Description
DHCP	To auto-configure the EMX, select DHCP. With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Netmask ▪ Default gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional) If your local network contains two subnets and IP forwarding has been enabled, you can click Append to add static routes so that your EMX can communicate with the other subnet. Each static route requires: ▪ Destination: IP address of the other subnet and subnet

Option	Description
	mask using the format "IP address/subnet mask." - Next Hop: IP address of the next hop router. See ***Static Route Examples*** (on page 118) for illustrations.

4. Click OK.

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

Modifying IPv6 Settings

You must enable the IPv6 protocol before you can modify the IPv6 network settings. See ***Selecting the Internet Protocol*** (on page 114).

To modify IPv6 settings:

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

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

Option	Description
	▪ IP address ▪ Default gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional) If your local network contains two subnets and IP forwarding has been enabled, you can click Append to add static routes so that your EMX can communicate with the other subnet. Each static route requires: ▪ Destination: IP address of the current subnet and prefix length using the format "IP address/prefix." ▪ Next Hop: IP address of the next hop router. See ***Static Route Examples*** (on page 118) for illustrations.

4. Click OK.

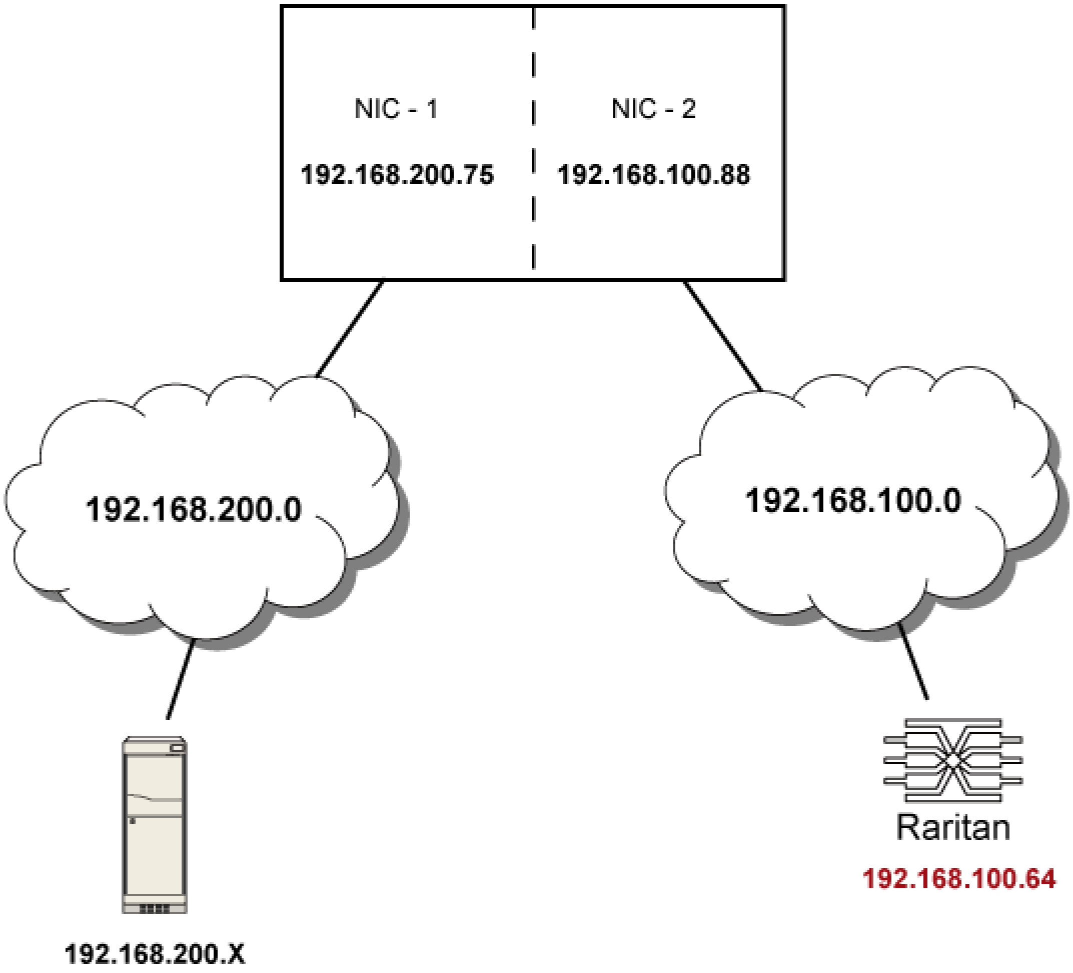
Note: The EMX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the EMX only uses the primary IPv4 and IPv6 DNS servers.

Static Route Examples

This section has 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.

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*

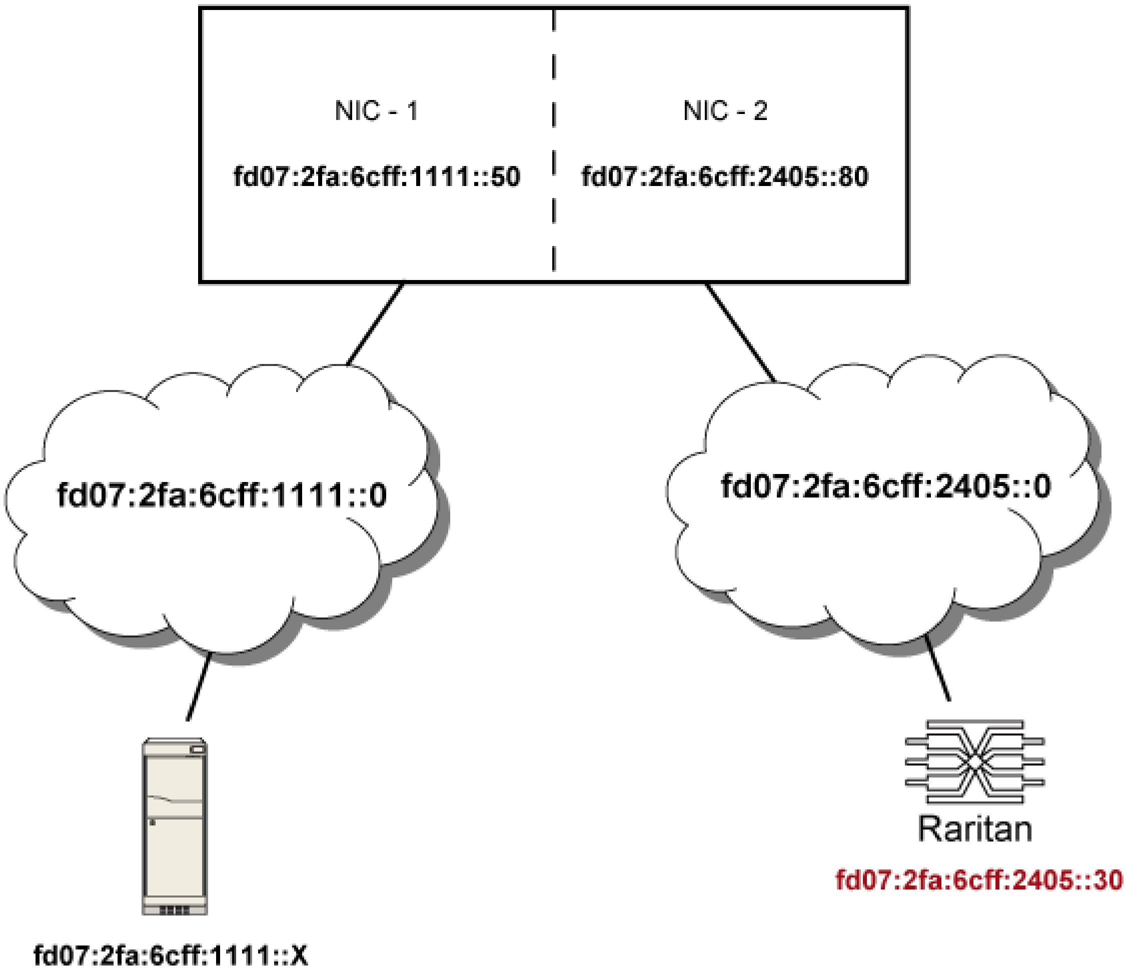


In this example, NIC-2 (192.168.100.88) is the next hop router for your EMX to communicate with any device in the other subnet 192.168.200.0. In the IPv4 "Append new Route" dialog, you should specify:

- Destination: `192.168.200.0/24`
- Next Hop: `192.168.100.88`

▶ 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*



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 "Append new Route" dialog, you should specify:

- Destination: `fd07:2fa:6cff:2405::0/64`
- Next Hop: `fd07:2fa:6cff:2405::80`

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 178).

Modifying Network Service Settings

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

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the command line interface. See ***Using the Command Line Interface*** (on page 309).

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

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

In addition, the EMX also supports the SNMP and Modbus/TCP protocols.

Changing HTTP(S) Settings

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.

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

By default, any access to the EMX device via HTTP is automatically redirected to HTTPS. You can disable this redirection if needed.

▶ To change HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP. The HTTP Settings dialog appears.
2. To use a different port for HTTP or HTTPS, type a new port number in the corresponding field. Valid range is 1 to 65535.

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

3. Enable or disable either or both ports.
   - To enable or disable the HTTP port, select or deselect the "HTTP access" checkbox.
   - To enable or disable the HTTPS port, select or deselect the "HTTPS access" checkbox.

▶ To enable or disable HTTPS redirection:

In the HTTP Settings dialog, the "Enforce use of HTTPS (redirect to HTTPS)" checkbox determines whether the HTTP access to the EMX is redirected to HTTPS.

- To enable the redirection, select the checkbox.
- To disable the redirection, deselect the checkbox.

Note: The redirection checkbox is configurable only when both HTTP and HTTPS ports have been enabled.

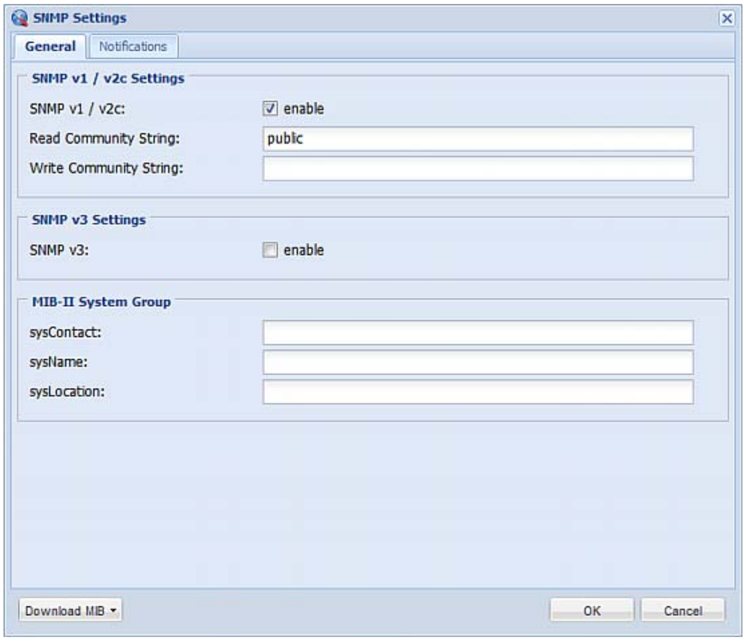
Configuring SNMP Settings

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

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 187).

▶ To configure SNMP communication:

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



SNMP Settings

General | Notifications

SNMP v1 / v2c Settings

SNMP v1 / v2c: ☑ enable

Read Community String: public

Write Community String:

SNMP v3 Settings

SNMP v3: □ enable

MIB-II System Group

sysContact:

sysName:

sysLocation:

2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding "enable" checkbox. For details, see ***Enabling SNMP*** (on page 298).
   - The SNMP v1/v2c read-only access is enabled by default.
3. Enter the MIB-II system group information, if applicable.

Important: You must download the SNMP MIB for your EMX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For details, see **Downloading SNMP MIB** *(on page 306).*

4. Click OK.

To configure SNMP notification destinations:

1. Click the Notifications tab in the same SNMP dialog.
2. Select the Enabled checkbox.
3. Select an SNMP notification type - SNMP v2c Trap, SNMP v2c Inform, SNMP v3 Trap, and SNMP v3 Inform.
4. Specify the SNMP notification destinations and enter necessary information. For details, refer to either of the following:
    - ***SNMPv2c Notifications*** (on page 301)
    - ***SNMPv3 Notifications*** (on page 303)
5. Click OK.

Tip: The SNMP notification destinations can be also set in the Event Rule Settings dialog. See **Modifying an Action** *(on page 231).*

Changing SSH Settings

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

To change SSH service settings:

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

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating a User Profile*** (on page 149).

Changing Telnet Settings

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

▶ **To change Telnet service settings:**

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

Changing Modbus/TCP Settings

You can enable or disable the Modbus/TCP access to the EMX or the read-only mode, or change the default TCP port for the Modbus service.

▶ **To change the Modbus service settings:**

1. Choose Device Settings > Network Services > Modbus. The Modbus Settings dialog appears.
2. To enable the Modbus/TCP access, select the Enable Modbus/TCP Access checkbox. To disable it, deselect the checkbox.
3. To use a different port, type a new port number in the port field. Valid range is 1 to 65535.
4. To enable the Modbus read-only mode, select the "Enable read-only mode" checkbox. To disable it, deselect the checkbox.

Enabling the Modbus Gateway

With the Modbus Gateway feature enabled, the EMX allows Modbus TCP clients on your network to communicate with the Modbus RTU devices connected 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 ***Modbus Gateway Settings*** (on page 125).

▶ 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.

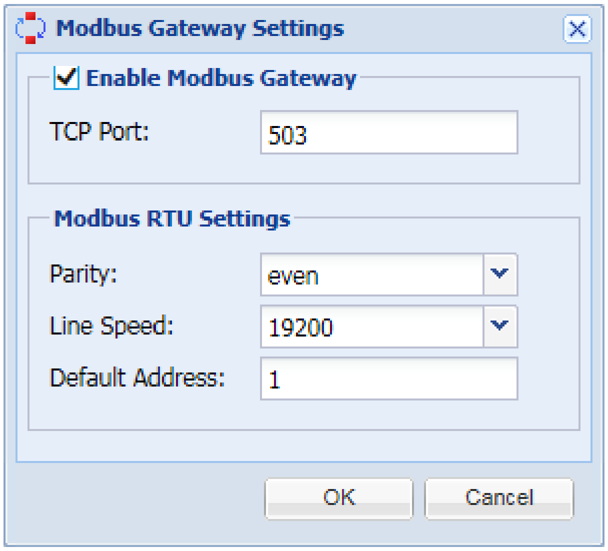
- The Modbus RTU devices on the bus are identified with their Modbus RTU addresses using the Modbus unit identifier addresses in the Modbus TCP protocol.

  If the Modbus TCP client does not support unit identifier addressing, refer to ***Modbus Gateway Settings*** (on page 125).

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

Modbus Gateway Settings

1. Choose Device Settings > Network Services > Modbus Gateway.
2. Select the Enable Modbus Gateway checkbox.



Modbus Gateway Settings

☑ Enable Modbus Gateway

TCP Port: 503

Modbus RTU Settings

Parity: even

Line Speed: 19200

Default Address: 1

Now configure the following:

- **TCP Port -** Required

Use the default port 503, or assign a different port. Valid range is 1 to 65535.

Port 502 is the default Modbus/TCP port for EMX, so you cannot use that port for the Modbus Gateway.

- **Parity and Line Speed -** Required

Use the default settings, or update if the Modbus RTU devices are using different communication parameters.

- **Default Address -** Optional

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.

Each Modbus RTU device unit identifier address is unique.

If the Modbus RTU address does not match the address entered in this dialog, communications between the Modbus TCP client and Modbus RTU device fail.

Enabling Service Advertisement

The EMX advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and mDNS (multicastDNS). 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 mDNS, which are required for resolving APIPA host names. See ***APIPA and Link-Local Addressing*** (on page 4).

► To enable Service Advertisement:

1. Click Device Settings > Network Services > Service Advertisement
2. Click "Yes" in the "Changing Service Advertisement" confirmation dialog box. The feature is enabled and the Service Advertisement checkbox is selected in the menu.

► To disable Service Advertisement:

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

Setting the Date and Time

Set the internal clock on the EMX device manually, or link to a Network Time Protocol (NTP) server.

► To set the date and time:

1. Choose Device Settings > Date/Time.
2. In the Time Zone field, select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.

If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.

4. Choose one of the methods to set the date and time:
   - To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
     - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on.
   - To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two ways to assign the NTP servers.
     - To use the DHCP-assigned NTP servers, make sure the "Always use the servers below and ignore DHCP-provided servers" checkbox is deselected. This method is usable only when either IPv4 or IPv6 DHCP is enabled.
     - To use the NTP servers that are manually specified, select the "Always use the servers below and ignore DHCP-provided servers" checkbox, and specify the primary NTP server in the First Time Server field. A secondary NTP server is optional.
       Click Check NTP Servers to verify the validity and accessibility of the specified NTP servers.

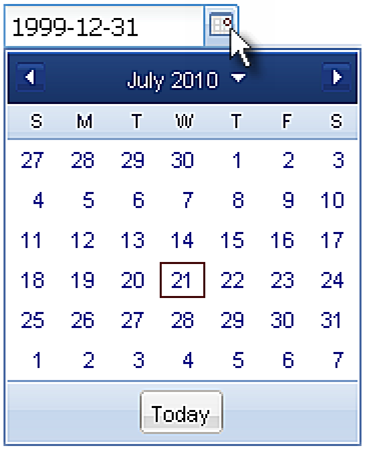
Note: If the EMX device's IP address is assigned through IPv4 or IPv6 DHCP, the NTP servers can be automatically discovered. When this occurs, the data you entered in the fields of First and Second Time Server will be overridden.

5. Click OK.

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 130).

How to Use the Calendar

The calendar icon 📅 next to the Date field is a convenient tool to quickly change the year, month and date.

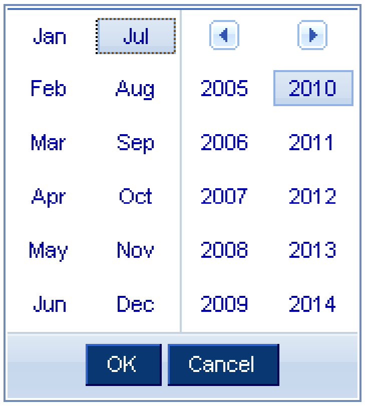


1999-12-31

S	M	T	W	T	F	S
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

▶ To select a date using the calendar:

1. To change the year shown in the calendar, do either of the following:
   - Press Ctrl+Up arrow or Ctrl+Down arrow to switch between years.
   - Click ▾, which is adjacent to the year, to show a list of years and months. Select the desired year from the list to the right and click OK. If the list does not show the desired year, click ◂ or ▸ to show additional years.



2. To change the month shown in the calendar, do one of the following:
   - Press Ctrl+Right arrow or Ctrl+Left arrow to switch between months.

- Click ◀ or ▶ on the top of the calendar to switch between months.
- Click ▼, which is adjacent to the year, to show a list of years and months. Select the desired month from the list to the left and click OK.

3. To select a date, click that date on the calendar.
   - Click Today if you want to select today.

Note: On the calendar, the date for today is marked with a red frame.

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 the 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.

Setting Default Measurement Units

Default measurement units are applied to the EMX web and CLI interfaces across all users, including users accessing the device via external authentication servers. Default units apply before users set their own preferred measurement units or the administrator changes preferred units for any user.

Note: To set preferred measurement units for your own, see **Setting Up Your Preferred Measurement Units** *(on page 153). If your preferences are different from the default measurement units, your preferences rather than the defaults apply to the EMX user interfaces after you log in.*

▶ To set up default user preferences:

1. Choose User Management > Default User Preferences.
2. Update any of the following as needed:
   - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
   - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
   - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.
3. Click OK.

Configuring the Feature Port

The EMX device supports connecting one of the following devices to its FEATURE port:

- Raritan asset management sensors (asset sensors). See ***Connecting Asset Management Sensors*** (on page 25).
- External beeper. See ***Connecting an External Beeper*** (on page 61).
- Schroff® LHX-20, SHX-30 or LHX-40 heat exchanger. See ***Connecting a Schroff LHX/SHX Heat Exchanger*** (on page 61).

By default, the FEATURE port can automatically detect and display the device connected to the FEATURE port. The only exception is the Schroff® LHX/SHX device, which requires enabling the LHX/SHX support before the EMX can detect or display it. See ***Managing the Schroff LHX/SHX Heat Exchanger*** (on page 272).

You can change the mode applied to the FEATURE port so that the EMX web interface only displays the device in the manner you wish.

▶ To configure the FEATURE port:

1. Click the Feature Port folder. The Feature Port page opens in the right pane.
2. Select the Port# 1 device on the Feature Port page, and click Setup. The Feature Port Setup dialog appears.
3. Select the desired mode in the Detection Mode field.
   - Auto: The EMX automatically detects and displays the device connected to the FEATURE port. This is the default.
   - Disabled: The FEATURE port is disabled so the EMX does not detect and display the connected device.
   - A specific device type: The EMX always displays the selected device type no matter which device is connected or whether the selected device is detected or not. After selecting a device type, the Mode column shows "Pinned." Available device types are listed below.

Device type	Description
Asset Strip	Raritan asset sensors.
External Beeper	An external beeper with the RJ-45 socket.

Device type	Description
LHX 20	Schroff® LHX-20 heat exchanger. All Schroff® SHX/LHX device types are available only after the LHX/SHX support is enabled. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 273).
SHX 30	Schroff® SHX-30 heat exchanger.
LHX 40	Schroff® LHX-40 heat exchanger.

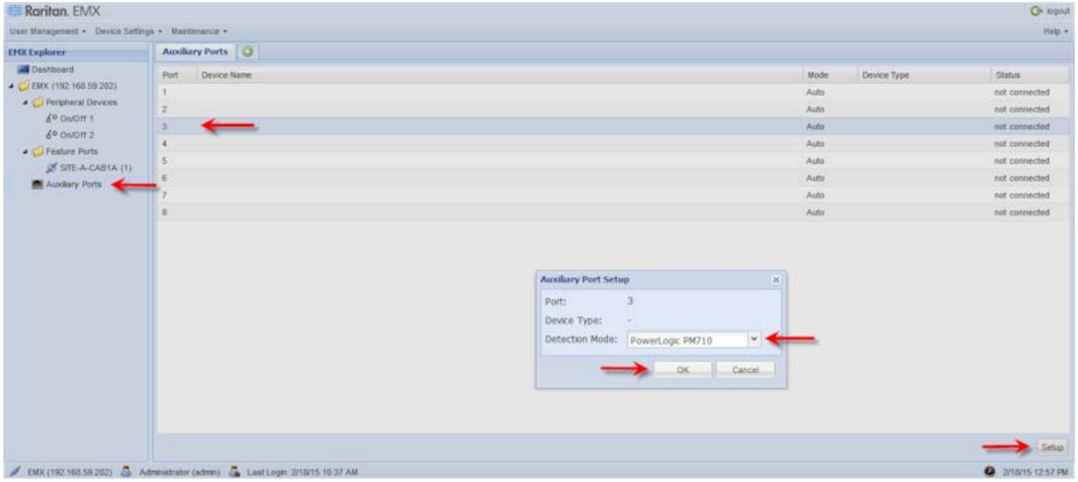
4. Click OK.

Configuring the Auxiliary Port

To configure the AUXILIARY port:

1. Click the Auxiliary Port folder in the EMX Explorer pane. The Auxiliary Port page opens in the right pane.
2. Select the Port# 1 device on the page, and click Setup at the bottom of the page. The Auxiliary Port Setup dialog appears.
3. Select the desired mode in the Detection Mode field.
   - Auto: The EMX automatically detects and displays the device connected to the AUXILIARY port. This is the default.
   - Disabled: The AUXILIARY port is disabled so the EMX does not detect and display the connected device.
   - A specific device type: The EMX always displays the selected device type no matter which device is connected or whether the selected device is detected or not. After selecting a device type, the Mode column shows "Pinned." Available device types are listed below.

- LHX-20
- SHX-30
- LHX-40
- PowerLogic PM710



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

Auxiliary Port Setup

Port: 3

Device Type: -

Detection Mode: PowerLogic PM710

Configuring the Serial Port

You can change the bit-rate of the serial port labeled CONSOLE / MODEM on the EMX device. The default bit-rate for both console and modem operation is 115200 bps.

The EMX supports the use of one of 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 needed when the EMX works in conjunction with Raritan's Dominion LX KVM switch. The 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.

▶ To change the serial port baud rate settings:

1. Choose Device Settings > Serial Port Settings. The Serial Port Configuration dialog appears.
2. In the "Connected device" field, select an appropriate option to force the serial port to enter the correct state.

Options	Description
Automatic detection	The EMX automatically detects the device type on the serial port. Select this option unless your EMX cannot correctly detect the connected device.
Force console	The port enters the local console state.
Force analog modem	The port enters the analog modem state.
Force GSM modem	The port enters the GSM modem state.

3. In the Console Baud Rate field, 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).

4. In the Modem Baud Rate field, select the baud rate used for the modem connected to the EMX.

▶ To configure the analog modem settings:

1. Click the Analog Modem tab.
2. Select the "Answer incoming calls" checkbox to enable the remote access via a modem. Otherwise, deselect this checkbox.
3. Specify the number of rings the EMX must wait before answering the call. You can either type a value or click the Up/Down arrow keys to adjust the value in the "Number of rings until answering" field.

▶ To configure the GSM modem settings:

1. Click the GSM Modem tab.
2. Enter the SIM PIN.
3. Select 'Use custom SMS center number' if a custom SMS will be used.
4. Enter the SMS center number in the SMS Center field.
5. Click Advanced Information to show information.
6. Enter the number of the recipient's phone in the Recipients Phone field, then click Send SMS Test to send a test SMS message.

Setting the Cascading Mode

A maximum of eight EMX devices can be cascaded using USB cables and therefore share only one Ethernet connection. See ***Cascading the EMX via USB*** (on page 22).

The Ethernet sharing mode applied to the USB-cascading configuration is either network bridging or port forwarding. This mode is determined by the master device. See ***Overview of the Cascading Modes*** (on page 138).

Only the Admin user or a user with the Administrator Privileges permission can configure the cascading mode.

To apply the "Port Forwarding" cascading mode, all cascaded EMX devices must be upgraded to version 2.5.20 or later, or those devices not supporting the "Port Forwarding" mode cannot be accessed over the network. See ***Updating the EMX Firmware*** (on page 291).

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:

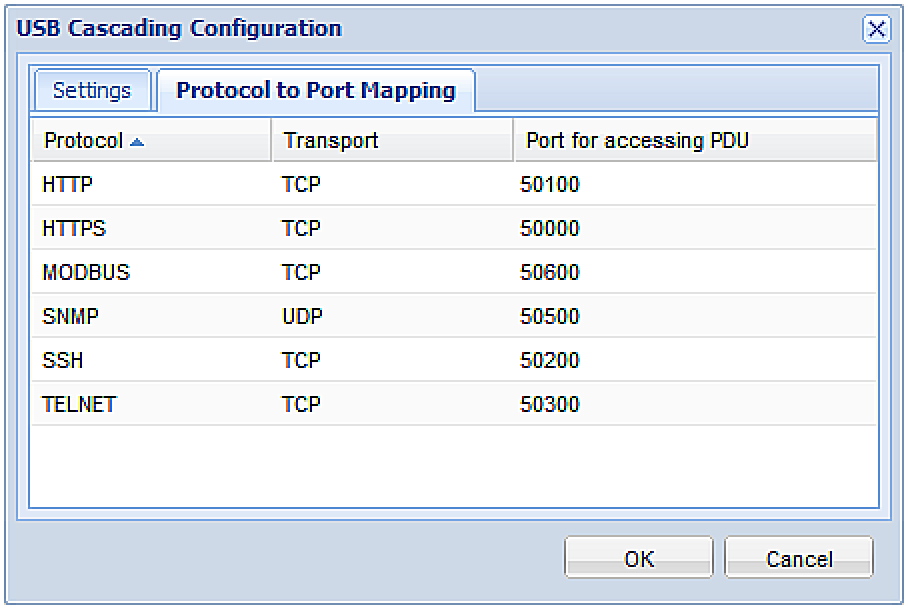
1. Log in to the master device's web interface.
2. Choose Device Settings > USB Cascading. The USB Cascading Configuration dialog appears.

3. Verify that the "Position in cascaded chain" field shows 0 (Master), indicating that this EMX is the master device.
4. Select the preferred cascading mode in the "Cascading mode" field.
   - Bridging: Each device in the USB-cascading configuration is accessed with a different IP address. This is the default.
   - Port Forwarding: Each device in the USB-cascading configuration is accessed with the same IP address but with a different port number assigned. For details the port numbers, see ***Port Number Syntax*** (on page 139).

Note: If reversing or disconnecting the USB cable from a slave device, causing the slave device to become a master or standalone device, you must plug an Ethernet cable to it to update its USB-cascading status.

5. Click OK.
6. If selecting Port Forwarding, a list of port numbers for diverse networking protocols will be available on the "Protocol to Port Mapping" tab of each cascaded device.

   Return to the same dialog and click the "Protocol to Port Mapping" tab to view the master device's port numbers.



Protocol ▲	Transport	Port for accessing PDU
HTTP	TCP	50100
HTTPS	TCP	50000
MODBUS	TCP	50600
SNMP	UDP	50500
SSH	TCP	50200
TELNET	TCP	50300

For information on accessing each cascaded device in the Port Forwarding mode, see ***Port Forwarding Examples*** (on page 141).

Overview of the Cascading Modes

You must apply a cascading mode to the USB-cascading configuration. See ***Setting the Cascading Mode*** (on page 136).

▶ Overview:

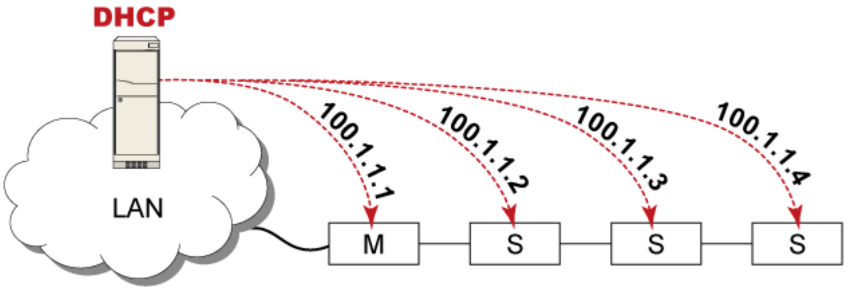
- The Bridging mode supports the wired network only while the Port Forwarding mode supports both wired and wireless networks.
- All cascading modes support both DHCP and static IP addressing.
- In the Bridging mode, each cascaded device has a unique IP address. In the Port Forwarding mode, all cascaded devices share the same IP address.
- Each cascaded device can be remotely accessed through the network regardless of the cascading mode applied.

▶ Illustration:

In the following diagrams, it is assumed that users enable the DHCP networking in the USB-cascading configuration comprising four devices. The first cascaded device is the master device (M) and the other are slave devices (S).

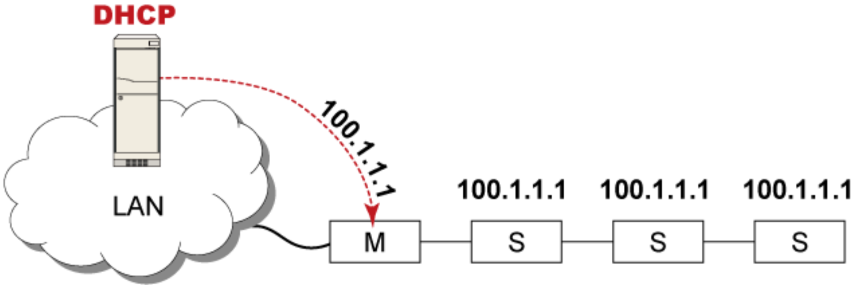
- **"Bridging" mode:**

  As illustrated in the following diagram, the DHCP server communicates with every cascaded device respectively and assigns four different IP addresses accordingly. Each device has one 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:**

  The DHCP server communicates with the master device only and assigns one IP address. All slave devices use 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 through the network. See ***Port Number Syntax*** (on page 139).



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:

Position	**XX**
Master device	00
Slave 1	01

Position	XX
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 141) for further illustrations.

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. See **Setting the Cascading Mode** *(on page 136).*

▶ 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, SNMP 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 139) for details.
- Slave device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a USB-cascading configuration comprising three Raritan products. 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 shown below.

Protocols	Port numbers
HTTPS	50000
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

Specifying the Device Altitude

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 539).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See ***Setting Default Measurement Units*** (on page 131).

► To specify the altitude of the EMX device:

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

   Note: This folder's name changes after customizing the device name. See **Naming the EMX** *(on page 110).*

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

Setting Data Logging

The EMX can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field.

Since the environmental sensors are measured per second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in log gets overwritten in the log.

Though the environmental sensors are measured per second, their readings may not be updated per second. See ***Information about Update Interval*** (on page 145). The update interval varies depending on how many environmental sensors are connected to the EMX device and the sensor type. The more the environmental sensors are connected, the larger the update interval is. Therefore, type a large number in the Measurements Per Log Entry field when there are a large number of environmental sensors connected.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: The EMX device's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** *(on page 298). In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is enabled. You must have "Administrator" or "" permissions to change the setting.

▶ To configure the data logging feature:

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Select the environmental sensors whose data logging you want to enable.

  - Select the checkboxes of the desired sensors in the Logging Enabled column, or use the Enable All and Disable All buttons to select or clear all.

5. Click OK.

Information about Update Interval

Raritan environmental sensors can be divided into two categories according to the update interval of the sensor's reading or state.

- Normal type: Sensor readings or states are updated in a longer interval, which varies between 3 to 40 seconds according to the total number of connected environmental sensors. Most Raritan environmental sensors belong to this type, such as the temperature or humidity sensor.
- High priority type: Sensor readings or states are updated in a shorter interval, which is less than or equal to 3 seconds. Raritan contact closure sensors belong to this type.

Configuring SMTP Settings

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

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See ***Viewing the Local Event Log*** (on page 232).

Note: See **Event Rules and Actions** *(on page 187) for information on creating event rules to send email notifications.*

▶ To set SMTP server settings:

1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the "Number of Sending Retries" field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.

7. If your SMTP server requires password authentication, do this:
   a. Select the Server Requires Authentication checkbox.
   b. Type a user name in the User Name field.
   c. Type a password in the Password field.
8. If your SMTP server supports the Transport Layer Security (TLS), select the "Enable SMTP over TLS (StartTLS)" checkbox. Then do the following:
   a. Click Browse to select the TLS CA certificate file. Then you may:
      - Click Show to view the installed certificate's contents.
      - Click Remove to delete the installed certificate if it is inappropriate.
   b. Select or deselect the "Allow expired and not yet valid certificates" checkbox.
      - To always send the email messages even though the installed certificate chain contains a certificate that is outdated or not valid yet, select this checkbox.
      - To prevent the email messages from being sent when any certificate in the installed certificate chain is outdated or not valid yet, deselect this checkbox.
9. Now that you have set the SMTP settings, you can test it to ensure it works properly. Do the following:
   a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
   b. Click Send Test Email.
   c. Check if the recipient(s) receives the email successfully.
10. Click OK.

Configuring Data Push Settings

If any Raritan asset sensors have been connected to EMX, you can push the asset sensor 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 sensors, see ***Connecting Asset Management Sensors*** (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. See ***Push Out Sensor Readings*** (on page 194).
- To push the data at a regular interval, schedule the data push action. See ***Scheduling an Action*** (on page 211).

▶ To configure data push settings:

1. Choose Device Settings > Data Push. The Data Push dialog appears.
2. Click New. The Add New Destination dialog appears.
3. In the URL field, determine the following information.
   - Click the arrow to select http or https.
   - Type the URL or host name in the accompanying text box.
4. If the destination server requires authentication, select the "Use authentication" checkbox, and provide the authentication information:
   - In the "User name" field, type the login name.
   - In the Password field, type the login password.
5. In the "Entry type" field, determine the data that will be transmitted.
   - Asset management information: Transmit the information of the specified asset sensor(s), including the general status of the specified sensor(s) and a list of asset tags on blade extension strips if any.
   - Asset management log: Transmit the log of all asset sensors, which is generated when there are changes made to asset tags and asset sensors, including asset tag connection or disconnection events.
6. If "Asset management information" is selected in the above step, specify the asset sensor(s) whose log to send. The EMX has only one FEATURE port so only one asset sensor is available.
   - To specify the asset sensor, select it in the Available list box and click ← (Add) or ⇤ (Add All).

- To remove the asset sensor, select it in the Selected list box and click ⇨ (Remove) or ⇥ (Remove All).

7. Click OK.

Checking the Internal Beeper State

The internal beeper of the EMX always turns OFF if there are no event rules that involve this beeper.

If intended, you can set an event rule to turn on the internal beeper when a specific event occurs. See ***Event Rules and Actions*** (on page 187).

You can remotely check this beeper's state.

▶ To check the internal beeper's state:

1. Click the EMX folder in the left pane.

   Note: This folder's name changes after customizing the device name. See **Naming the EMX** *(on page 110).*

2. Locate the "Internal Beeper" section in the right pane. Either of the following states is displayed.

   - Off: The beeper is turned off.
   - Active: The beeper is turned on. A field titled "Activation reason" appears below the beeper state, indicating why the beeper sounds an alarm.

     For example, if the internal beeper is turned on because of a specific event rule "BBB," the EMX shows the following "Activation reason:"

     ```
     Event Action triggered by rule: BBB
     ```

Tip: To check the internal beeper state via CLI, see **Device Configuration** *(on page 318).*

User and Role Management

The EMX is shipped with one built-in user profile: **admin**, which is used for initial login and configuration.

This profile has full system permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user.

Every user profile must have at least a role to determine the user's system permissions. See ***Setting Up Roles*** (on page 154).

To manage any settings, you must log in to the user account with appropriate permissions.

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

Creating a User Profile

To create a user profile:

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

Field	**Type this...**
User Name	The name the user enters to log in to the EMX. ▪ 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

Field	Type this...
	▪ Case sensitive

4. Select the Enabled checkbox. Enabled users can log in to the EMX device.

5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.

Note: Users with both the Change Local User Management and Change Security Settings permissions can choose to ignore the password change request. See **Login** *(on page 84).*

6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.

   a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring SNMP Settings** *(on page 122).*

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

Field	Description
Security Level	Click the drop-down arrow to select a preferred security level from the list: ▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This is the default.
Use Password as Authentication Pass Phrase	*This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.* When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase, disable the checkbox.
Authentication Pass Phrase	Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII

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

7. Click the SSH tab to enter the public key if the public key authentication for the SSH service is enabled. See ***Changing SSH Settings*** (on page 123).

   a. Open the SSH public key with a text editor.

   b. Copy and paste all contents in the text editor into the Public Key field on the SSH tab.

8. Click the Roles tab to determine the permissions of the user.

9. Select one or multiple roles by selecting corresponding checkboxes.

   - The Admin role provides full permissions.

   - The Operator role provides limited permissions for frequently-used functions. See ***Setting Up Roles*** (on page 154) for the scope of permissions. This role is selected by default.

- If no roles meet your needs, you can:
  - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 155).
  - *Create a new role by clicking the Manage Roles button:* See ***Creating a Role*** (on page 155).

Note: With multiple roles selected, a user has the union of all roles' permissions.

10. To change any measurement units displayed in the web interface and command line interface for this new user, click the Preferences tab, and do any of the following:

    - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
    - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
    - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

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

Note: The measurement unit change only applies to the web interface and command line interface. Users can change the measurement units at any time by setting up their own user preferences. See **Setting Up Your Preferred Measurement Units** *(on page 153).*

Modifying a User Profile

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

▶ To modify a user profile:

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

   To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.

5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 149).
6. To change the permissions, click the Roles tab and do one of these:
   - Select or deselect any role's checkbox.
   - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 155).
7. To change the measurement unit for temperature, length or pressure, click the Preferences tab, and select a different option from the drop-down list.

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

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

To delete user profiles:

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

Setting Up Your Preferred Measurement Units

The measurement units used in your EMX user interfaces can be changed according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users from the Preferences tab of the Manage Users dialog. See **Creating a User Profile** *(on page 149).*

Note: The measurement unit change only applies to the web interface and command line interface. Setting your preferences does not change the default measurement units, which apply to all users before any individual user or the administrator sets preferred measurement units on a per-user basis. See **Setting Default Measurement Units** *(on page 131) for information on changing default measurement units.*

▶ To change the measurement units applied to your EMX user interfaces:

1. Choose User Management > User Preferences. The Setup User Preferences dialog opens.
2. Update any of the following as needed:
   - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
   - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
   - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.
3. Click OK.

Setting Up Roles

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

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

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:
  - View Event Settings
  - View Local Event Log
  - Change Event Settings
  - Change Own Password
  - Change EMD Configuration
- The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 149).

Creating a Role

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

▶ To create a role:

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

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

2. Click New. The Create New Role dialog appears.
3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.
5. Click the Privileges tab to assign one or multiple permissions.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission you want from the Privileges list.
   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.
   d. Click Add to add the selected permission (and arguments if any).
   e. Repeat Steps *a* to *d* until you add all necessary permissions.
6. Click OK.

Now you can assign the new role to any users. See ***Creating a User Profile*** (on page 149) or ***Modifying a User Profile*** (on page 152).

Modifying a Role

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

▶ To modify a role:

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

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

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

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

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

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

6. To delete any permissions, do this:
   a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   b. Click Delete.
7. To add any permissions, do this:
   a. Click Add. The "Add Privileges to Role XXX" dialog appears, where XXX is the role name.
   b. Select the permission you want from the Privileges list.
   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right, such as the Switch Actuator permission. Then select one or multiple arguments.
   d. Click Add to add the selected permission (and arguments if any).
   e. Repeat Steps *a* to *d* until you add all necessary permissions.
8. To change a specific permission's arguments, do this:
   a. Select the permission by clicking it.
   b. Click Edit. The "Edit arguments of privilege XXX" dialog appears, where XXX is the privilege name.

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

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

Deleting a Role

You can delete any role other than the Admin role.

▶ To delete a role:

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

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

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

Access Security Control

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

Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up a TLS Certificate** *(on page 172) and* **Setting Up External Authentication** *(on page 178).*

Forcing HTTPS Encryption

You can force all accesses to the EMX via HTTP to be redirected to HTTPS. See ***Changing HTTP(S) Settings*** (on page 120).

Configuring the Firewall

The EMX has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the EMX device or to prevent them from receiving any data from the EMX.

The EMX allows you to configure the firewall rules for inbound and outbound traffic respectively. Inbound rules control the data sent to the EMX, and outbound rules control the data sent from the EMX.

By default the firewall is disabled.

► **To configure the firewall:**

1. Enable the firewall. See ***Enabling the Firewall*** (on page 158).
2. Set the default policy. See ***Changing the Default Policy*** (on page 158).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See ***Creating Firewall Rules*** (on page 159).

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

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

Enabling the Firewall

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

- **To enable the EMX firewall:**

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

Changing the Default Policy

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

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

Default policies for inbound and outbound traffic can be different.

- **To change the default policy for inbound traffic:**

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To determine the default policy for IPv4 addresses:
   a. Click the IPv4 tab if necessary.
   b. Ensure the Enable IPv4 Access Control checkbox is selected.
   c. Locate the Default Policy field in the Inbound Rules section.
   d. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
      - Accept: Accepts traffic from all IPv4 addresses.
      - Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
      - Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.
3. To determine the default policy for IPv6 addresses:
   a. Click the IPv6 tab.

b. Ensure the Enable IPv6 Access Control checkbox is selected.

c. Locate the Default Policy field in the Inbound Rules section.

d. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.

- Accept: Accepts traffic from all IPv6 addresses.
- Drop: Discards traffic from all IPv6 addresses, without sending any failure notification to the source host.
- Reject: Discards traffic from all IPv6 addresses, and an ICMP message is sent to the source host for failure notification.

4. Click OK. The new default policy is applied.

▶ To change the default policy for outbound traffic:

Locate the Outbound Rules section on the IPv4 or IPv6 tab and then follow the above procedure to set up its Default Policy field by selecting one of the following options.

- Accept: Permits traffic sent from the EMX to all IP addresses.
- Drop: Discards traffic sent from the EMX to all IP addresses, without sending any failure notification to the destination host.
- Reject: Discards traffic sent from the EMX to all IP addresses, and an ICMP message is sent to the destination host for failure notification.

Creating Firewall 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 firewall 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 by the EMX.

- **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. Make sure the IPv4 addresses entered are within the scope.

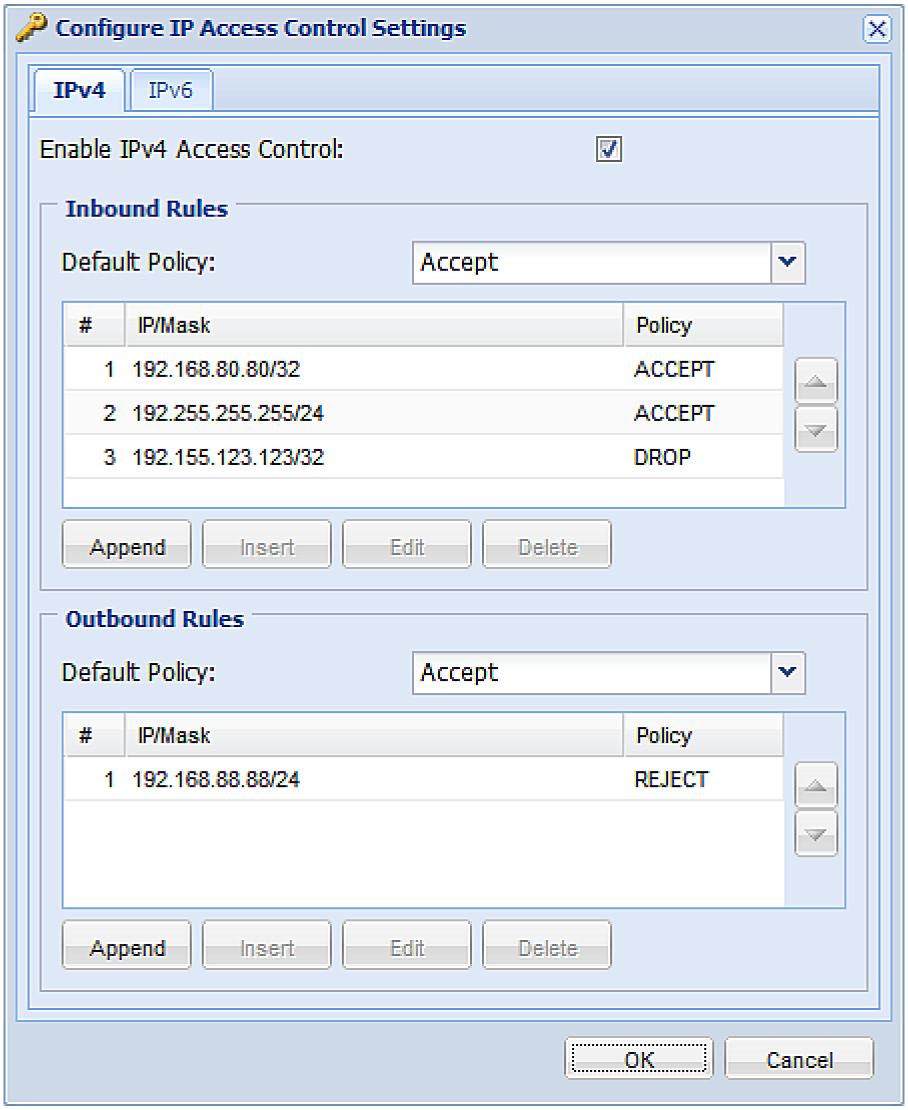
▶ To create firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Click the IPv4 tab for creating IPv4 firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. To set rules for inbound traffic, go to the Inbound Rules section. To set rules for outbound traffic, go to the Outbound Rules section.
5. Create specific rules. See the table for different operations.

Action	Procedure
Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject from the drop-down list in the Policy field. ▪ Accept: Accepts traffic from/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. ▪ Click OK. The system automatically numbers the rule.

Action	Procedure
Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type an IP address and subnet mask in the IP/Mask field. ▪ Select Accept, Drop or Reject from the drop-down list in the Policy field. ▪ Accept: Accepts traffic from/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. ▪ Click OK. The system inserts the rule and automatically renumbers the following rules.

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



Configure IP Access Control Settings

Enable IPv4 Access Control: ☑

Inbound Rules

Default Policy: Accept

#	IP/Mask	Policy
1	192.168.80.80/32	ACCEPT
2	192.255.255.255/24	ACCEPT
3	192.155.123.123/32	DROP

Outbound Rules

Default Policy: Accept

#	IP/Mask	Policy
1	192.168.88.88/24	REJECT

7. Click OK. The rules are applied.

Editing Firewall Rules

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

▶ To modify a firewall rule:

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

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

Sorting Firewall Rules

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

▶ To sort the firewall rules:

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

Deleting Firewall Rules

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

▶ To delete a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.

3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule that you want to delete. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to remove the selected rule(s) from the rules list.
7. Click OK.

Setting Up User Login Controls

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

Enabling User Blocking

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

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

Note: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command via a local connection. See **Unblocking a User** *(on page 434).*

▶ **To enable user blocking:**

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the User Blocking section.
3. To enable the user blocking feature, select the "Block user on login failure" checkbox.
4. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user is blocked from accessing the EMX device.
5. To determine how long the user's login is blocked, select the desired length of time from the drop-down list in the "Block timeout" field. The following describes available options.
   - Infinite: This option sets no time limit on blocking the login.

- X min: This type of option sets the time limit to X minutes, where X is a number.
- X h: This type of option sets the time limit to X hours, where X is a number.
- 1 d: This option sets the time limit to 1 day.

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

6. Click OK.

Enabling Login Limitations

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

To enable login limitations:

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

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

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

Enabling Strong Passwords

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

▶ To force users to create strong passwords:

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

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

Note: The maximum password length accepted by the EMX is 64 characters.

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

Enabling Password Aging

Password Aging determines whether users are required to change passwords at regular intervals. The default is to disable this feature.

▶ To force users to change passwords regularly:

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

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

4. Click OK.

Enabling and Editing the Security Banner

Use the EMX restricted service agreement (security banner) if you want to require users to read and accept a security agreement when they log in to the EMX.

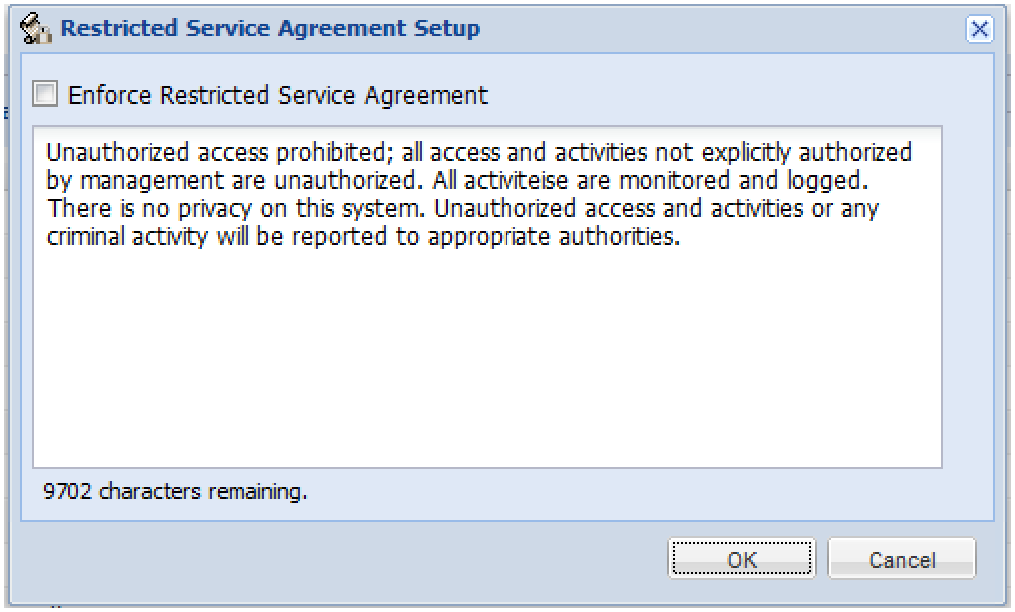
A default agreement is provided. You can edit or replace the default text as needed by typing directly in the security dialog or pasting text into it.

A maximum of 10,000 characters can be entered or pasted into the security banner.

If a user declines the agreement, they cannot log in. An event notifying you if a user has accepted or declined the agreement can be created. See ***Default Log Messages*** (on page 216)

▶ **To enable the service agreement:**

1. Click Device Services > Security > Restricted Service Agreement Banner. The Restricted Service Agreement Setup dialog opens.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit the text or replace it as needed.
4. Click OK.



□ Enforce Restricted Service Agreement

Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activiteise are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.

9702 characters remaining.

If the Restricted Service Agreement feature is enabled, the Restricted Service Agreement is displayed when any user logs in to the EMX. Do either of the following, or you cannot successfully log in to the EMX:

- 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, press the Space bar.

- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting Up Role-Based Access Control Rules

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

▶ **To set up role-based access control rules:**

1. Enable the feature. See ***Enabling the Feature*** (on page 168).
2. Set the default policy. See ***Changing the Default Policy*** (on page 169).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See ***Creating Role-Based Access Control Rules*** (on page 169).

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

Enabling the Feature

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

▶ **To enable role-based access control rules:**

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To enable the IPv4 firewall, click the IPv4 tab, and select the "Enable Role Based Access Control for IPv4" checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the "Enable Role Based Access Control for IPv6" checkbox.
4. Click OK.

Changing the Default Policy

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

To change the default policy:

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

Creating Role-Based Access Control Rules

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

To create role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Click the IPv4 tab for creating IPv4 firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.

3. Ensure the "Enable Role Based Access Control for IPv4" checkbox is selected on the IPv4 tab, or the "Enable Role Based Access Control for IPv6" checkbox is selected on the IPv6 tab.
4. Create specific rules:

Action	Do this...
Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role ▪ Click OK. The system automatically numbers the rule.
Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified

Action	Do this...
	role ▪ Click OK. The system inserts the rule and automatically renumbers the following rules.

5. Click OK.

Editing Role-Based Access Control Rules

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

▶ To modify a role-based access control rule:

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

Sorting Role-Based Access Control Rules

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

▶ To sort role-based access control rules:

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

6. Click OK.

Deleting Role-Based Access Control Rules

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

▶ **To delete a role-based access control rule:**

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

Setting Up a TLS Certificate

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.

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

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

Note 1: If you are using a TLS certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

Note 2: See **Forcing HTTPS Encryption** *(on page 157) for instructions on forcing users to employ TLS when connecting to the EMX.*

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

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

Certificate Signing Request

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

Creating a Certificate Signing Request

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

To create a CSR:

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

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

Field	Type this information
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.

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

- In the Key Creation Parameters section:

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

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.

5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.

   a. You are prompted to open or save the file. Click Save to save it onto your computer.

   b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.

   c. If intended, click Delete Certificate Signing Request to remove the CSR file permanently from the EMX device.

6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it onto your computer.

7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

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

▶ **To install the certificate:**

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

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

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

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

▶ **To create and install a self-signed certificate:**

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

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

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

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

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

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

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

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

Installing Existing Key and Certificate Files

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

Note: If you are using a TLS certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

To install existing key and certificate files:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Select the "Upload Key and Certificate" checkbox. The Key File and Certificate File fields appear.
4. In the Key File field, click Browse to select the private key file.
5. In the Certificate File field, click Browse to select the certificate file.
6. Click Upload. The selected files are installed on the EMX device.

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

7. Click Close to quit the dialog.

Downloading Key and Certificate Files

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

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

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

Setting Up External Authentication

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

- Local database of user profiles on the EMX device
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (RADIUS) protocol

By default, the EMX is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user.

If you prefer 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 profiles on the EMX in addition to providing the external AA server's 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.

Only users who have the "Change Authentication Settings" permission can set up or modify the authentication settings.

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.

Gathering the External Authentication Information

No matter which type of external authentication is preferred, the first step is to gather the data of all external AA servers that you want to use.

Gathering the LDAP Information

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

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over 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)

Gathering the RADIUS Information

To configure RADIUS authentication, you need to collect the RADIUS information. If you are not familiar with the remote RADIUS information, consult your RADIUS administrator for help.

Below is the RADIUS information to gather:

- 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 used by the RADIUS server
- UDP accounting port used by the RADIUS server

Adding Authentication Servers

Add all external AA servers that you want to use to the EMX. Later you can use the sequence of the server list to control the AA servers' access priority.

Adding LDAP Server Settings

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

If the external LDAP/LDAPS server authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See ***Viewing the Local Event Log*** (on page 232).

Note: An LDAPS server refers to a TLS-secured LDAP server.

▶ **To add new LDAP/LDAPS server settings:**

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

   Important: Without the TLS 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 TLS encryption is enabled.

5. 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.
6. Security - Determine whether you would like to use Transport Layer Security (TLS) encryption, which is a cryptographic protocol that allows the EMX to communicate securely with the LDAPS server.

   Three security options are available:
   - StartTLS
   - TLS

- None

7. Port (None/StartTLS) - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
8. Port (TLS) - The default is 636. Either use the default port or specify another port. This field is enabled only when "TLS" is selected in the Security field.
9. Enable verification of LDAP Server Certificate - Select this checkbox if you would like the EMX to verify the validity of the selected LDAP server certificate. For example, the EMX will check the certificate's validity period against the system time.
10. CA Certificate - Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click Browse to select the TLS CA certificate file.
    - Click Show to view the installed certificate's contents.
    - Click Remove to delete the installed certificate if it is inappropriate.
11. Allow expired and not yet valid certificates - If a certificate has been installed, use this checkbox to determine whether the validity period of the certificate affects the authentication.
    - To always make the authentication succeed regardless of the validity period, select this checkbox.
    - To make the authentication fail when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect the checkbox.
12. Anonymous Bind - For "OpenLDAP," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, select this checkbox.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
13. Use Bind Credentials - For "Microsoft Active Directory," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, deselect this checkbox. By default it is deselected.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, select this checkbox.
14. Bind DN - Specify the DN of the user who is permitted to search the LDAP directory in the defined search base. This information is required only when the Use Bind Credentials checkbox is selected.
15. Bind Password and Confirm Bind Password - Enter the Bind password in the Bind Password field first and then the Confirm Bind Password field. This information is required only when the Use Bind Credentials checkbox is selected.

16. Base DN for Search - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be: `cn=Users,dc=raritan,dc=com`. Consult your AA server administrator for the appropriate values to enter into these fields.
17. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
    - Login name attribute (also called AuthorizationString)
    - User entry object class
    - User search subfilter (also called BaseSearch)

    Note: The EMX will preoccupy the login name attribute and user entry object class with default values, which should not be changed unless required.
18. Active Directory Domain - Type the name of the Active Directory Domain. For example, testradius.com. Consult with your Active Directory Administrator for a specific domain name.
19. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the EMX can connect to the remote authentication server successfully.

    Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.
20. Click OK. The new LDAP server is listed in the Authentication Settings dialog.
21. To add additional LDAP/LDAPS servers, repeat Steps 3 to 20.
22. Click OK. The LDAP authentication is now in place.

▶ To duplicate LDAP/LDAPS server settings:

If you have added any LDAP/LDAPS server information to the EMX, and the server you are adding shares identical or similar settings with an existing server, the most convenient way is to duplicate that LDAP/LDAPS server's data.

1. Repeat Steps 1 to 4 in the above procedure to add the LDAP/LDAPS server you want.
2. Select the "Use settings from LDAP Server" checkbox.
3. Click the drop-down arrow below the checkbox to select the LDAP/LDAPS server whose settings you want to copy.
4. Make necessary changes to the information shown.
5. Click OK.

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).

More Information about AD or RADIUS Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see ***LDAP Configuration Illustration*** (on page 484).

For more information on RADIUS configuration, see ***RADIUS Configuration Illustration*** (on page 501).

Adding RADIUS Server Settings

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

To set up RADIUS authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Radius radio button to enable the RADIUS authentication.
3. Click New to add a RADIUS AA server. The "Create new RADIUS Server Configuration" dialog appears.
4. Type the IP address or host name of the RADIUS server in the IP Address / Hostname field.
5. Select an authentication protocol in the "Type of RADIUS Authentication" field. Your choices include:
   - 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.
6. By default, the EMX uses the standard RADIUS port 1812 (authentication) and 1813 (accounting). If you prefer to use non-standard ports, change the ports.
7. Type the timeout period in seconds in the Timeout field. This sets the maximum amount of time to establish contact with the RADIUS server before timing out. Default is 1 second.
8. Type the number of retries permitted in the Retries field. Default is 3.
9. Type the shared secret in the Shared Secret and Confirm Shared Secret fields. The shared secret is necessary to protect communication with the RADIUS server.

10. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the EMX can connect to the remote authentication server successfully.

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

11. Click OK. The new RADIUS server is listed in the Authentication Settings dialog.
12. To add additional RADIUS servers, repeat Steps 3 to 11.
13. Click OK. RADIUS authentication is now in place.

Sorting the Access Order

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

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

▶ To re-sort the authentication server access list:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server whose priority you want to change.
3. Click "Move up" or "Move down" until the selected server reaches the desired position in the list.
4. Click OK.

Testing the Server Connection

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

▶ To test the connection to an authentication server:

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

Editing Authentication Server Settings

If the configuration of any external authentication server has been changed, such as the port number, you must modify the authentication settings on the EMX device accordingly, or the authentication fails.

▶ To modify the external authentication configuration:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to edit.
3. Click Edit or double-click that server.
4. Make necessary changes to the information shown.
5. Click OK.

Deleting Authentication Server Settings

You can delete the settings of a specific authentication server when that server is no longer available or used for remote authentication.

▶ To remove one or multiple authentication servers:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click OK.

Disabling External Authentication

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

▶ To disable the external authentication service:

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

Enabling External and Local Authentication Services

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

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

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

▶ To enable both authentication services:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Make sure you have selected one external authentication radio button, such as the LDAP radio button.
3. Select the "Use Local Authentication if Remote Authentication service is not available" checkbox.
4. Click OK.

Event Rules and Actions

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

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

- System Event Log Rule: This causes ANY event occurred to the EMX to be recorded in the internal log. It is enabled by default.
- 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.
- System Tamper Detection Unavailable: This causes the EMX to sends alarm notifications if a DX tamper sensor has been connected and the EMX detects that the communication with the connected tamper sensor is lost.

If these do not satisfy your needs, you can create additional rules to respond to different events. You need the Administrator Privileges to configure event rules.

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

Components of an Event Rule

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

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

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

Creating an Event Rule

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

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

Creating Actions

The EMX comes with three 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.
- System Tamper Alarm: This action causes the EMX to show the alarm for the DX tamper sensor in the Alarms section of the Dashboard 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 ***Alarms List*** (on page 105).

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

The built-in actions cannot be deleted.

SNMP traps and informs can be created for an action. For information on traps and informs, see ***Configuring SNMP Settings*** (on page 122).

▶ **To create new actions:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action:

Action	Function
Execute an action group	Creates a group of actions comprising existing actions. See ***Action Group*** (on page 190).
Alarm	Requires the user to acknowledge the alert when it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See ***Alarm*** (on page 191).
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See ***External Beeper*** (on page 192).
Log event message	Records the selected events in the internal log. See ***Log an Event Message*** (on page 193).
Push out sensor readings	Sends asset management sensor data to a remote server using HTTP POST requests. See ***Push Out Sensor Readings*** (on page 194).
Request LHX/SHX maximum cooling	Applies the maximum cooling to the LHX/SHX device. See ***Request LHX/SHX Maximum Cooling*** (on page 195). This option is available only when the Schroff LHX/SHX support has been enabled.
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See ***Send a Snapshot via Email*** (on page 195).
Send email	Emails a textual message. See ***Send EMail*** (on page 196).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See ***Send an SNMP Notification*** (on page 197).
Syslog message	Makes the EMX automatically forward event messages to the specified syslog server. See ***Syslog Message*** (on page 200).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See ***Send Sensor Report*** (on page 201).
Send SMS message	Sends a message to a mobile phone. See ***Send SMS Message*** (on page 203).
Internal beeper	Turns on or off the internal beeper. See ***Internal Beeper*** (on page 204).

Action	Function
Switch LHX/SHX	Switches on or off the LHX/SHX device. See ***Switch LHX/SHX*** (on page 205). This option is available only when the Schroff LHX/SHX support has been enabled.
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See ***Record Snapshots to Webcam Storage*** (on page 206).
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See ***Switch Peripheral Actuator*** (on page 204).

6. Click OK to save the new action.

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

7. To create additional actions, repeat the above steps.
8. Click Close to quit the dialog.

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 an event rule rather than selecting all needed actions one by one per rule.

▶ To create an action group:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Execute an action group.
6. To mark an action as part of the action group, select it from the Available Actions list box, and click ← to move it to the Used Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all actions to the Used Actions list box, click ⇤. A maximum of 32 actions can be grouped.

7. To remove an action from the action group, select it from the Used Actions list box, and click ⇨ to move it to the Available Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all actions, click ⇥.

8. Click OK.
9. To create additional action groups, repeat Steps 3 to 8.

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 it reaches the maximum number of alert notifications.

For information on acknowledging an alarm, see ***Alarms List*** (on page 105).

▶ To create an Alarm action:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Alarm.
5. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications.
   a. In the Available Actions field, select the method to send 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, click Create New Notification Action to immediately create them.

   b. Click ⊕ to add the selected method to the Alarm Notifications list box.

   c. Repeat the above steps to add more methods if needed.

      - To remove any method from the Alarm Notifications list box, select that method and click ⊖.

6. In the Notification Options section, configure the notification-resending or -regenerating feature.

   a. To enable the notification-resending feature, select the "Enable re-scheduling of alarm notifications" checkbox. To disable this feature, deselect the checkbox.

   b. In the "Period in Minutes" field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly. You can either directly type a numeric value or click the Up/Down arrow keys to adjust the time.

   c. In the "Max. numbers" field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.

7. If needed, you can instruct the EMX to send the acknowledgment notification after the alarm is acknowledged in the Acknowledgment Notifications list box. **(Optional)**

   a. In the Available Actions field, select the method to send the acknowledge notification. Available methods are identical to those for generating alarm notifications.

   b. Click ⊕ to add the selected method to the Acknowledgment Notifications list box.

   c. Repeat the above steps to add more methods if needed.

      - To remove any method from the Acknowledgment Notifications list box, select that method and click ⊖.

8. Click OK.

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. Click the Actions tab.
2. Click New.

3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: External beeper.
5. From the Beeper Port drop-down list, select the port where the external beeper is connected. This port is the FEATURE port.
6. From the Beeper Action drop-down list, 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.
7. Click OK.

Note: 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.

Log an Event Message

This option records the selected events in the internal log.

To create a log event message:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Log event message.
6. Click OK.

Push Out Sensor Readings

If you have connected Raritan's asset sensors to the EMX, you can configure the EMX to push asset sensor data to a remote server after a certain event occurs.

Before creating this action, make sure that you have properly defined the destination servers and the sensor data type in the Data Push dialog. See ***Configuring Data Push Settings*** (on page 147).

Tip: To send the asset sensor data at a regular interval, schedule this action. See **Scheduling an Action** *(on page 211). Note that the "Asset management log" is generated only when there are changes made to any asset sensors or asset tags, such as connection or disconnection events.*

▶ To push out the sensor data:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Push out sensor readings.
6. Select a server or host which receives the asset sensor data in the Destination field.
   - If the desired destination is not available yet, go to the Data Push dialog to enter it. See ***Configuring Data Push Settings*** (on page 147).
7. Click OK.

Request LHX/SHX Maximum Cooling

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 273).

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%.

► **To request maximum cooling for SHX-30:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Request LHX/SHX maximum cooling.
6. Click OK.

Send a Snapshot via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

► **To create a send snapshot via email action:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send snapshots via email.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

If the SMTP server settings are not configured yet, click Configure. See ***Configuring SMTP Settings*** (on page 145) for the information of each field.

8. Select the webcam that is capturing the images you want sent in the email.
9. Use the slide bars to increase or decrease the following:
   - Number of Snapshots - the number of snapshots to be included in the sequence of images that are taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
   - Snapshots/Mail field - the number of snapshots from the sequence to be sent at one time in the email.
   - "Time before first Snapshot (s):" - the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.
   - "Time between Snapshots (s):" - the amount of time between when each snapshot is taken.
10. Click OK.

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
```

See ***Email and SMS Message Placeholders*** (on page 224) for a list and definition of available variables.

▶ To configure sending emails:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.

4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send email.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

   To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

   If the SMTP server settings are not configured yet, click Configure. See ***Configuring SMTP Settings*** (on page 145) for the information of each field. Default messages are sent based on the event. See ***Default Log Messages*** (on page 216) for a list of default log messages and events that trigger them.
8. If needed, select the Use Custom Log Message checkbox, and then create a custom message up to 1024 characters in the provided field.
   - To start a new line in the text box, press Enter.
   - Click the Information icon ⓘ to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See ***Email and SMS Message Placeholders*** (on page 224) for more details.
9. Click OK.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ To configure sending an SNMP notification:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.

5. In the Action field, click the drop-down arrow and select the desired action: Send SNMP notification.
6. Select the type of SNMP notification. See either procedure below according to your selection.

▶ To send SNMP v2c notifications:

1. From the Notification Type drop-down, select SNMPv2c Trap or SNMPv2c Inform.
2. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter 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, enter 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 only permits entering 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. From the Notification Type drop-down, 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:
   a. In the Timeout (sec) field, enter 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, enter 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 needed to access the host

   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

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 the Local Event Log*** (on page 232).

▶ **To configure a syslog message action:**

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Syslog message.
6. In the "Syslog server" field, specify the IP address to which the syslog is forwarded.
7. In the Transport Protocol field, select one of the syslog protocols: TCP or UDP. The default is UDP.

Transport protocol types	Next steps
UDP	▪ In the UDP Port field, specify an appropriate port number. Default is 514. ▪ Select the "Legacy BSD Syslog Protocol (UDP only)" checkbox if applicable.
TCP	If NO TLS certificate is required, type an appropriate port number in the TCP Port field.

Transport protocol types	Next steps
	If a TLS certificate is required, select the "Enable Secure Syslog over TLS" checkbox, and then do the following: a. Specify an appropriate port number in the "TCP Port (TLS)" 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 after a TLS certificate has been installed, 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.

8. Click OK.

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.

- Inlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor and active energy.
- Outlet sensors, including RMS current, RMS voltage, active power, apparent power, power factor, active energy and outlet state (for outlet-switching capable PDUs only).
- Overcurrent protector sensors, including RMS current and tripping state.
- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the EMX, such as temperature or humidity sensors.

To configure a sensor report action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.

4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send sensor report.
6. In the Destination Actions field, 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, click Create New Destination Action to immediately create them.

   b. To select any method, select it in the right list box, and click ⇦ to move it to the left list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

      To select all methods, simply click ⇤.

   c. To delete any method, select it in the left list box, and click ⇨ to move it back to the right list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

      To remove all methods, simply click ⇥.
7. In the Available Sensors field, select the desired sensor.

   a. Select the sensor type from the field to the left.

   b. Select the specific sensor from the field to the right.

   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.
8. 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.
9. To immediately send out the sensor report, click Send Report Now. A message appears, indicating whether the sensor report is sent successfully.

10. To save this action, click OK.

Note: 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 224).*

Send SMS Message

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 which is pulled from the EMX and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged in to the EMX in order to send SMS messages.

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
```

See ***Email and SMS Message Placeholders*** (on page 224) for a list and definition of available variables.

▶ To configure SMS message:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Send SMS message.
6. In the Recipient Phone Number field, specify the phone number of the recipient.
7. Select the Use Custom Log Message checkbox, then create a custom message in the provided field.

   Click the Information icon ⓘ to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See ***Email and SMS Message Placeholders*** (on page 224) for more details.

Note: Only the 7-bit ASCII charset is supported for SMS messages.

8. Click OK.

Internal Beeper

You can have the built-in beeper of the EMX turned on or off when a certain event occurs.

To switch the internal beeper:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Internal beeper.
5. 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.
6. Click OK.

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 this actuator when a specific event occurs.

Note: For information on connecting actuators to the EMX, see **DX Sensor Packages** *(on page 51).*

To switch on or off the system connected to an actuator:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
4. In the Action field, click the drop-down arrow and select the desired action: Switch peripheral actuator.
5. From the Operation drop-down list, select an operation for the selected actuator.

- Turn On: Turns on the selected actuator.
- Turn Off: Turns off the selected actuator.

6. To select the actuator where this action will be applied, select it from the Available Actuators list and click ← to add it to the Switched Actuators list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To add all actuators to the Switched Actuators list box, click ⇤.

7. To remove any actuator from the Switched Actuators list, select it and click → to move it back to the Available Actuators list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all actuators, click ⇥.

8. Click OK.

Switch LHX/SHX

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 273).

Use this action to switch the LHX/SHX on or off when, for example, temperature thresholds are reached.

▸ To create a switch LHX/SHX action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Switch LHX/SHX.
6. From the Operation drop-down, select Turn LHX/SHX On or Turn LHX/SHX Off.
7. From the Available LHX/SHXs list box, click on the LHX/SHX to be turned on or off, then click ← or ⇤ to add to the Switched LHX/SHXs list box. Use → or ⇥ to remove the LHX/SHX from the Switched LHXs list box, thereby removing the action.
8. Click OK.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

▶ To configure a record snapshot to webcam storage action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting at 1.
5. In the Action field, click the drop-down arrow and select the desired action: Record snapshots to webcam storage.
6. Select a webcam from the Webcam drop-down.
7. Selecting the action to perform - Start recording or Stop recording. If "Start recording" is selected, do the following:
    a. Use the slide bar to specify the total number of snapshots to be taken when the event occurs. The maximum amount of snapshots that can be stored on the EMX is ten (10). If you set it for a number greater than ten and the storage location is on the EMX, after the tenth snapshot is taken and stored, the oldest snapshots are overwritten.

    Tip: By default, the storage location is on the EMX. You can specify a remote server to store the snapshots. See **Configuring Webcam Storage** *(on page 265).*

    b. In the "Time before first Snapshot (s):" field, use the slide bar to specify the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.

    c. In the "Time between Snapshots (s):" field, use the slide bar to specify the amount of time between each snapshot being taken.
8. Click OK.

Creating Rules

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

By default, the EMX provides the following built-in event rules:

- System Event Log Rule
- System SNMP Notification Rule
- System Tamper Detection Alarmed
- System Tamper Detection Unavailable

If the built-in rules do not satisfy your needs, create new ones.

▶ To create event rules:

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

   Note: To select all items or events listed on the same submenu, select the option enclosed in brackets, such as <Any sub-event>, <Any Server> and <Any user>.

6. According to the event you selected in the previous step, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or 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 event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The EMX takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The EMX takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts). ▪ For connection state for USB cascading and auxiliary/RS-485 devices, assertion is displayed as "connected" and deassertion as "disconnected"
Discrete (on/off) sensor state change	Available radio buttons include "Alarmed," "No longer alarmed" and "Both." ▪ Alarmed: The EMX takes the action only when the chosen sensor enters the alarmed state, that is, the abnormal state. ▪ No longer alarmed: The EMX takes the action only when the chosen sensor returns to normal. ▪ Both: The EMX takes the action both when the chosen sensor enters or quits the alarmed state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The EMX takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The EMX takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The EMX takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	Available radio buttons include "Link state is up," "Link state is down" and "Both." ▪ Link state is up: The EMX takes the action only when the network link state changes from down to up. ▪ Link state is down: The EMX takes the action only when the network link state changes from up to down. ▪ Both: The EMX takes the action whenever the network link state changes.
Function enabled or disabled	Available radio buttons include "Enabled," "Disabled" and "Both." ▪ Enabled: The EMX takes the action only when the chosen function is enabled. ▪ Disabled: The EMX takes the action only when the chosen function is disabled. ▪ Both: The EMX takes the action when the chosen function is either enabled or disabled.
User logon state	Available radio buttons include "Logged in," "Logged out," and "Both." ▪ Logged in: The EMX takes the action only when the selected user logs in. ▪ Logged out: The EMX takes the action only when the selected user logs out. ▪ Both: The EMX takes the action both when the selected user logs in and logs out.
Restricted service agreement	Available radio buttons include "Accepted," "Declined," and "Both." ▪ 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

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

7. In the Actions field, select the desired action from the "Available actions" list box, and click ⇦ to move it to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   - To add all actions, simply click ⇤.
   - If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box.

8. To remove any action, select it from the "Selected actions" list box, and click ⇨ to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   - To remove all actions, click ⇥.

9. Click OK to save the new event rule.

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

10. Repeat Steps 2 to 10 to create additional event rules.

11. Click Close to quit the dialog.

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

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 environmental sensor regularly by scheduling the "Send Sensor Report" action.

When scheduling an action, make sure you have a minimum of 1-minute buffer time between this action's execution time and creation time. Otherwise, the scheduled action will NOT be performed at the specified time if the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling this action at 10:59 am or earlier.

▶ To schedule any action(s):

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Scheduled Actions tab.
3. Click New.
4. In the "Timer name" field, type a name for this scheduled action. The default name is New Timer <n>, where <n> is the sequential number starting at 1.
5. Make sure the Enabled checkbox is selected, or the EMX will not carry out this scheduled action.
6. Select the desired time frequency from the Execution Time field and then specify the time interval or a specific date and time in the Time field.

Time options	Frequency settings
Minutes	The frequency in minutes ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	The hourly option sets the timing 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	You need to specify the time for this daily option. For example, if you specify 13:30 in the Time field, 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 Monday.
Monthly	Both the date and time must be specified for the monthly option. The dates range from 1 to 31, and the time is specified in 24-hour format. 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.
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Date - 1 to 31. ▪ Time - the value is specified in 24-hour format.

7. In the Actions field, select the desired action from the "Available actions" list box, and click ← to move it to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   - To add all actions, simply click ⇤.
   - If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box. See ***Creating Actions*** (on page 188).

     When creating new actions from the Scheduled Actions tab, 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.

8. To remove any action, select it from the "Selected actions" list box, and click → to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

- To remove all actions, click ➡|.

9. Click OK.

Send Sensor Report Example

Below is an example of a scheduled action set to send a temperature sensor report via email hourly.

In this example,

a. Define a 'Send email' destination action that is name *Send Sensor Temp Report Email*.

- This destination action sends an email to the specified recipient(s).

b. Define a 'Send sensor report' action that is named *Send Hourly Temperature Sensor Readings*.

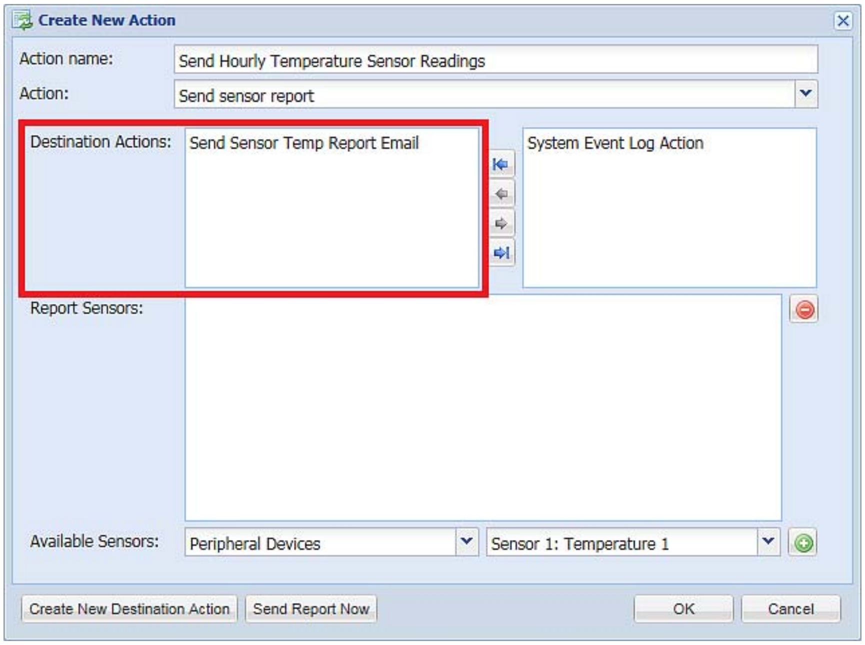
- This action reports temperature sensor readings via the selected destination action -- Send Sensor Temp Report Email.

c. Define a timer that is named *Hourly Sensor Temperature Readings*.

- This timer determines that the 'Send Hourly Temperature Sensor Readings' action shall take place on an hourly basis.

▶ Detailed steps:

1. If you have not already done so, create the destination action 'Send Sensor Temp Report Email', which is performed when the 'Send Hourly Temperature Sensor Readings' action occurs.



Create New Action

Action name: Send Hourly Temperature Sensor Readings

Action: Send sensor report

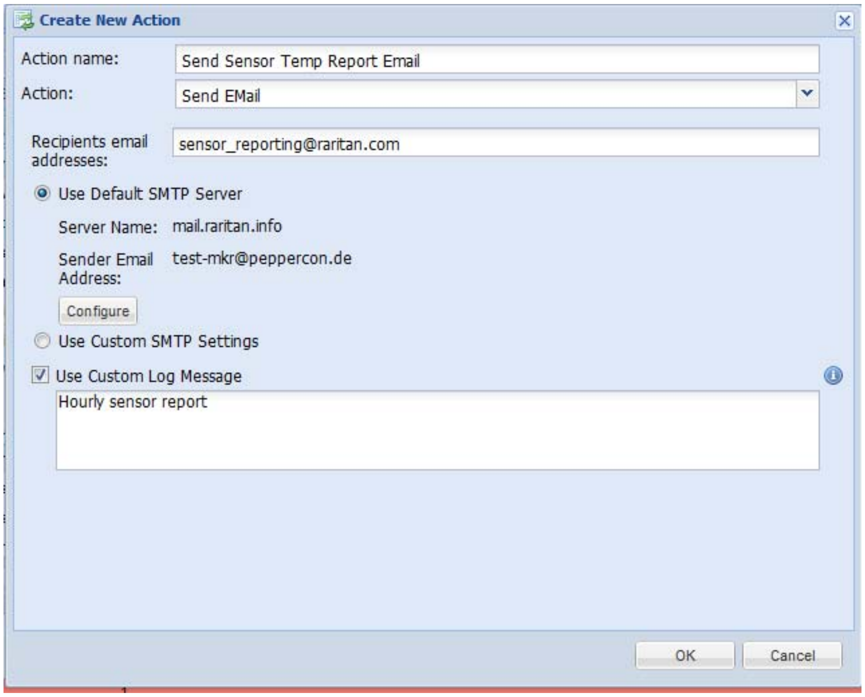
Destination Actions: Send Sensor Temp Report Email

System Event Log Action

Report Sensors:

Available Sensors: Peripheral Devices | Sensor 1: Temperature 1

- You must create the destination action as illustrated below prior to creating the 'Send Hourly Temperature Sensor Readings' action. For details, see ***Send EMail*** (on page 196).



Create New Action

Action name: Send Sensor Temp Report Email

Action: Send EMail

Recipients email addresses: sensor_reporting@raritan.com

● Use Default SMTP Server

Server Name: mail.raritan.info

Sender Email Address: test-mkr@peppercon.de

○ Use Custom SMTP Settings

☑ Use Custom Log Message

Hourly sensor report

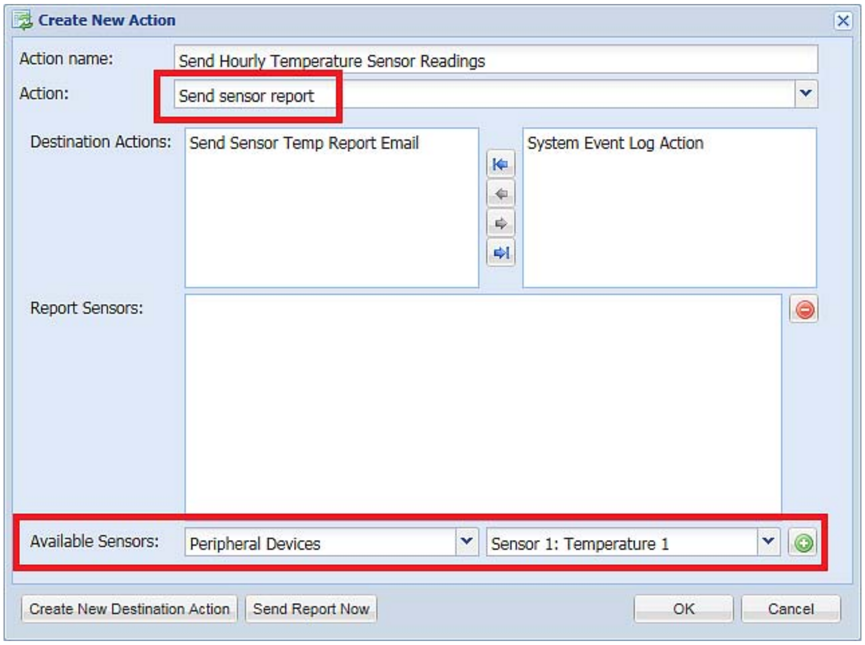
2. Create the 'Send sensor report' action -- *Send Hourly Temperature Sensor Readings*.

   a. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.

   b. Click the Actions tab > New.

   c. Enter the following information.

- Type the action's name -- *Send Hourly Temperature Sensor Readings*.
- Select the 'Send sensor report' action.
- Select the destination action 'Send Sensor Temp Report Email'.
- Add the desired temperature sensor(s) from the Available Sensors list to the Report Sensors box.



Create New Action

Action name: Send Hourly Temperature Sensor Readings

Action: Send sensor report

Destination Actions: Send Sensor Temp Report Email

System Event Log Action

Report Sensors:

Available Sensors: Peripheral Devices | Sensor 1: Temperature 1

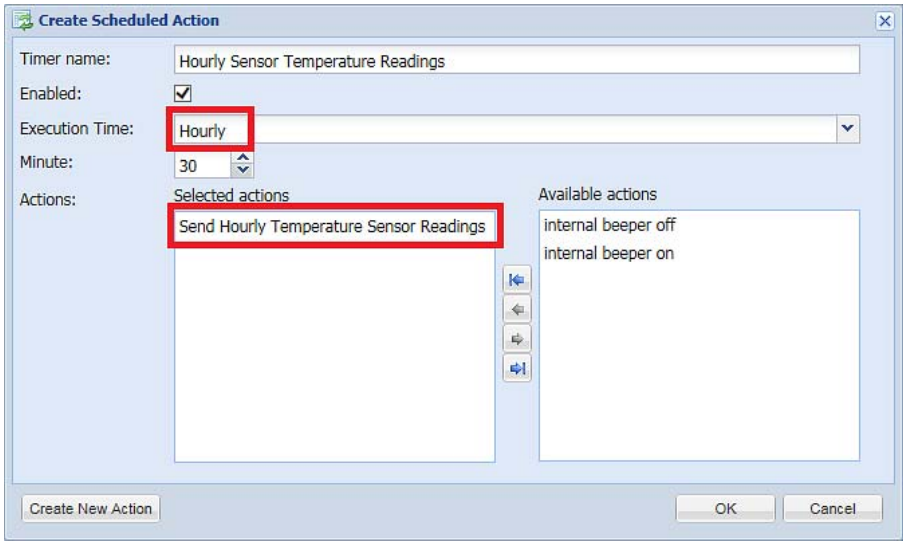
d. Click OK. For details, see ***Send Sensor Report*** (on page 201).

3. Create a timer for this newly-created action in the same Event Rule Settings dialog.

a. Click the Scheduled Actions tab > New.

b. Enter the following information.

- Type the timer name -- *Hourly Sensor Temperature Readings.*
- Select the Enabled checkbox.
- Select Hourly, and set the Minute to 30.
- Select the 'Send Hourly Temperature Sensor Readings' action.


Create Scheduled Action

Timer name: Hourly Sensor Temperature Readings

Enabled: ☑

Execution Time: Hourly

Minute: 30

Actions:

Selected actions: Send Hourly Temperature Sensor Readings

Available actions: internal beeper off, internal beeper on

c. Click OK. For details, see ***Scheduling an Action*** (on page 211).

Then the EMX will regularly send out an email containing the specified temperature sensor readings at 0:30 am, 1:30 am, 2:30 am, 3:30 am, 4:30 am, and so on until 23:30 pm every day.

Default Log Messages

Following are default log messages triggered and emailed to specified recipients when EMX events occur (are TRUE) or, in some cases, do not occur (are FALSE). See ***Send EMail*** (on page 196) for information configuring email messages to be sent when specified events occur.

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Firmware Update	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'.	
Asset Management > Device Config Changed	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]'	
Asset Management > Blade Extension Overflow	Blade extension overflow 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]'.	

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

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion 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.	
Device > Features > Schroff LHX / SHX Support	Schroff LHX / SHX support enabled.	Schroff LHX / SHX support disabled.
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	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	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 Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Peripheral Device Slot > * > Numeric Sensor > Below lower warning	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	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 > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor > 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] [SENSORREADINGUNIT].	Sensor '[PLSENSORNAME]' on Power Logic Device at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
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 '[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.
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.
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.

Email and SMS Message Placeholders

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

Note: Click the Information icon ℹ *to open the Event Context Information dialog, which contains a list of placeholders and their definitions. Then select the desired placeholder, and either double-click it or click the "Paste into Message" button to insert it into the customized message.*

Placeholder	Description
[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

Placeholder	Description
[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
[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

Placeholder	Description
[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
[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

Sample Event Rules

Sample Asset-Management-Level Event Rule

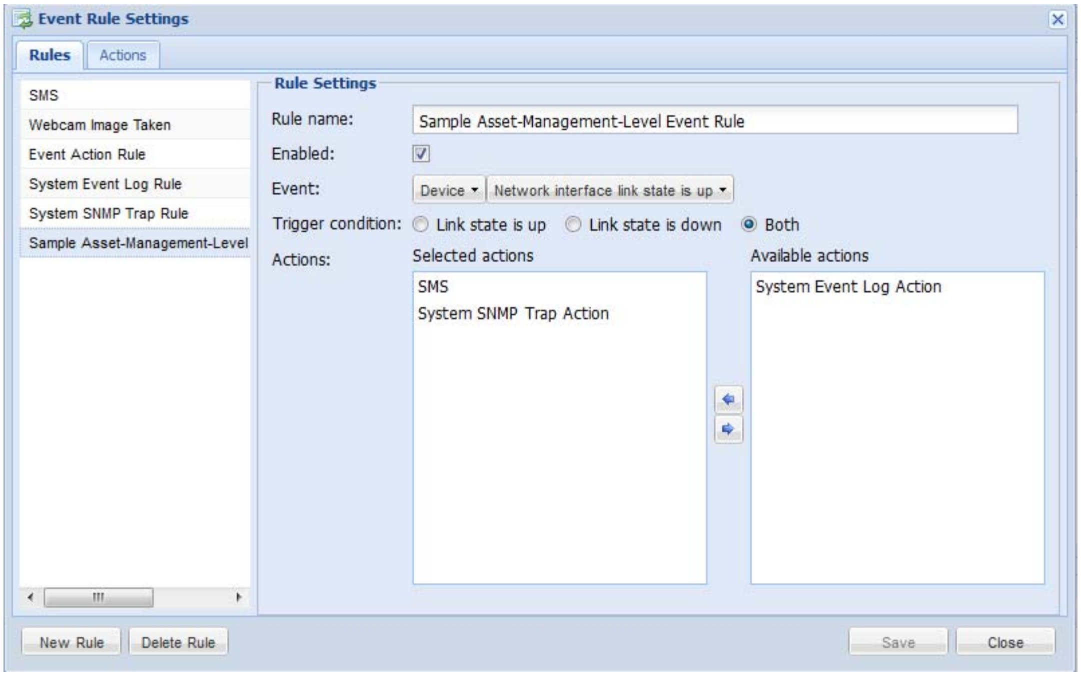
In this example, we want the EMX to record in the internal log when an asset sensor network link goes up or down. The sample event rule looks like this:

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

To create the above event rule:

1. Enter a name for the rule.
2. Select the Enabled checkbox to enable the rule.

3. From the Event drop-down, select Device > "Network interface link state is up". These selections indicate we are specifying an event regarding asset sensor management, and we want the EMX to respond to the event related to physical connections and/or disconnections.
4. Select the Both radio button since we want both connection and disconnection actions to be recorded when either action is taken.
5. Select "System Event Log Action" as we intend to record this event in the internal log when the specified events occur.



SMS
Webcam Image Taken
Event Action Rule
System Event Log Rule
System SNMP Trap Rule
Sample Asset-Management-Level

Rule Settings

Rule name: Sample Asset-Management-Level Event Rule

Enabled: ☑

Event: Device ▾ Network interface link state is up ▾

Trigger condition: ○ Link state is up ○ Link state is down ● Both

Actions: Selected actions: SMS, System SNMP Trap Action

Available actions: System Event Log Action

Sample Sensor-Level Event Rule

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

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

▶ To create the above event rule:

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

3. Select "Numeric Sensor" to indicate the sensor is a numeric sensor.

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

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

Sample User-Activity-Level Event Rule

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

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

▶ To create the above event rule:

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

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 event again.

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

Modifying an Event Rule

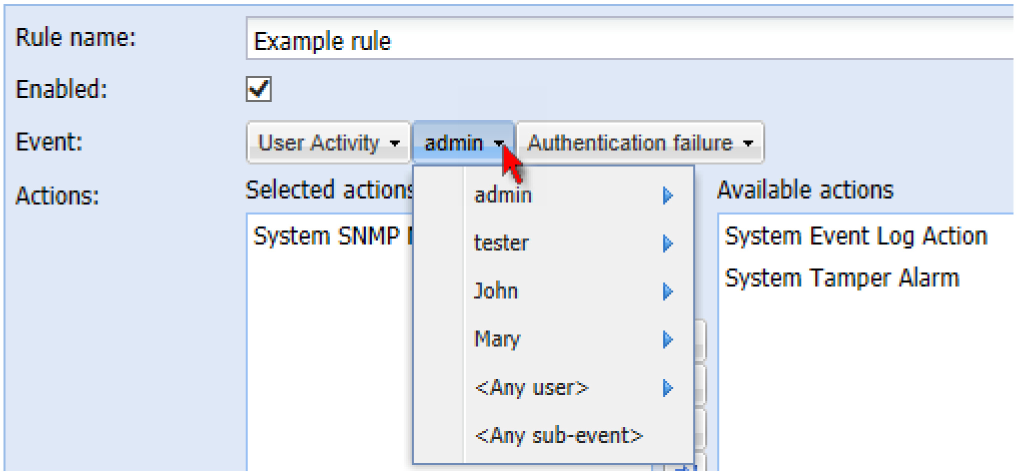
You can change an event rule's event, action, trigger condition and other settings, if any.

Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule, System SNMP Notification Rule, System Tamper Detection Alarmed, and System Tamper Detection Unavailable.

▶ **To modify an event rule:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify and click Edit, or simply double-click that rule.
3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

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



Rule name: Example rule

Enabled: ☑

Event: User Activity ▾ admin ▾ Authentication failure ▾

Actions:

Selected actions: System SNMP

Available actions: System Event Log Action, System Tamper Alarm

5. If the "Trigger condition" field is available, you may select a radio button other than the current selection to change the rule triggering condition.

6. To change the action(s), do any of the following in the Actions field:

   ▪ To add any action, select it from the "Available actions" list box, and click ←. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   ▪ To add all actions, click ⇤.

   ▪ To remove any action, select it from the "Selected actions" list box, and click → to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   ▪ To remove all actions, click ⇥.

   ▪ To create a new action, click Create New Action. The newly created action will be moved to the "Selected actions" list box once it is created. See ***Creating Actions*** (on page 188) for information on creating an action.

7. Click OK to save the changes.

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

8. Click Close to quit the dialog.

Modifying an Action

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

Exception: The built-in actions "System Event Log Action" and "System Tamper Alarm" are not user-configurable.

▶ **To modify an action:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify and click Edit, or simply double-click that action.
4. Make necessary changes to the information shown.
5. Click OK to save the changes.

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

6. Click Close to quit the dialog.

Deleting an Event Rule or Action

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

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

▶ **To delete an event rule or action:**

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
   a. Ensure the Rules tab is selected. If not, click the Rules tab.
   b. Select the desired rule from the list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   c. Click Delete.
   d. Click Yes on the confirmation message.
3. To delete an action:
   a. Click the Actions tab.
   b. Select the desired action from the list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   c. Click Delete.

   d. Click Yes on the confirmation message.

4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the EMX to generate an alert. The measurement then returns to a value within the threshold, but the EMX does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the EMX uses. See ***"To De-assert" and Deassertion Hysteresis*** (on page 534).

Managing Event Logging

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

Viewing the Local Event Log

You can view over 2000 historical events that occurred to the EMX device in the local event log.

When the log size exceeds 256KB, each new entry overwrites the oldest entry.

▶ **To display the local log:**

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

   Each event entry in the local log consists of:

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

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

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

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

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

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

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

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

- Click ⏭ to view the latest events.
- View a specific type of events only by selecting an event type in the Filter Event Class field.

Viewing the 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 engineers.

▶ To display the wireless LAN diagnostic log:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click Show WLAN Diagnostic Log. The WLAN Diagnostic Log dialog appears.

   Each entry in the log consists of the event's:

   - ID number
   - Date and time
   - Description

   Note: The Show WLAN Diagnostic Log button is available only when the Network Interface is set to Wireless.

3. The dialog shows the final page by default. You can:
   - Switch between different pages by doing one of the following:

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

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

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

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

   - Click ⏭ to view the latest events.

▶ To clear the diagnostic log:

1. Click Clear WLAN Diagnostic Log.

2. Click Yes on the confirmation message.

Clearing Event Entries

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

▶ **To delete all event entries:**

1. Choose Maintenance > View Event Log. The Event Log dialog appears.
2. Click Clear Event Log.
3. Click Yes on the confirmation message.

Viewing Connected Users

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

▶ **To view connected users:**

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

Column	Description
User Name	The login name used by each connected user.
IP Address	The IP address of each user's host. For the login via a 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 EMX 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*: Represents the local connection (serial RS-232 or USB). - *SSH*: Represents the SSH connection. - *Telnet*: Represents the Telnet connection.

Column	Description
Idle Time	The length of time for which a user remains idle. The unit "min" represents minutes.

2. To disconnect any user, click the corresponding Disconnect button.
   a. A dialog appears, prompting you to confirm the operation.
   b. Click Yes to disconnect the user or No to abort the operation. If clicking Yes, the connected user is forced to log out..
3. Click Close to quit the dialog.

Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** *(on page 269).*

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.

Adding IT Devices for Ping Monitoring

EMX can monitor the accessibility of any type of IT equipment, such as database servers, remote authentication servers, power distribution units (PDUs), and so on.

EMX 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 to meet your own needs.

Tip: To make the EMX automatically log, send notifications or perform other actions for any server accessibility or inaccessibility events, you can create event rules associated with server monitoring. See **Event Rules and Actions** *(on page 187).*

► **To add IT equipment for ping monitoring:**

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.

2. Click New. The Add New Server dialog appears.
3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.
4. Provide the information required.

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 (in seconds) after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time (in seconds) after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time (in seconds) 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 OK.
6. To add more IT devices, repeat Steps 2 to 5.
7. Click Close to quit the dialog.

In the beginning, the status of the monitored 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.

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 source for your EMX is different from the power source for that PDU.

This requires two steps: set up the PDU monitoring and create an event rule.

▶ Step 1: Set up the ping monitoring for the target PDU

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New.
3. Type 192.168.84.95 in the "IP address/hostname" field.
4. Ensure the "Enable ping monitoring for this server" checkbox is selected.
5. To make the EMX declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, do the following:
    a. In the "Number of successful pings to enable feature" field, type 3.
    b. In the "Wait time (in seconds) after successful ping" field, type 5.
6. To make the EMX declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 pings * 3 seconds), do the following:
    a. In the "Number of consecutive unsuccessful pings for failure" field, type 4.
    b. In the "Wait time (in seconds) after unsuccessful ping" field, type 3.
7. In the "Wait time (in seconds) before resuming pinging" field, type 60 to make the EMX stops 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.

▶ Step 2: Create an event rule to send SNMP notifications for this PDU

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click New.

3. In the "Rule name" field, type "Send SNMP notifications for PDU (192.168.84.95) inaccessibility."
4. Select the Enabled checkbox to enable this new rule.
5. In the Event field, choose Server Monitoring > 192.168.84.95 > Unreachable.
6. In the "Trigger condition" field, select the Unreachable radio button. This makes the EMX react only when the target PDU becomes inaccessible.
7. Select the System SNMP Notification Action from the "Available actions" list box, and click ← to add it to the "Selected actions" list box.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Configuring SNMP Notifications** *(on page 300).*

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever needed.

▶ To modify the ping monitoring settings for an IT device:

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

Deleting Ping Monitoring Settings

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

▶ To delete ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.

4. Click Yes on the confirmation message.
5. Click Close to quit the dialog.

Checking Server Monitoring States

Server monitoring results are available in the Server Reachability dialog after specifying IT devices for the EMX device to monitor their network accessibility.

▶ To check the server monitoring states and results:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
   - ✓ : This icon denotes that the monitoring for the corresponding device is enabled.
   - ✗ : This icon denotes that the monitoring for the corresponding device is disabled.
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.

4. Click Close to quit the dialog.

Environmental Sensors and Actuators

The EMX can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed. If an actuator is connected to the EMX, you can use it to control a system or mechanism.

▶ To add environmental sensors and actuators:

1. Physically connect environmental sensor packages to the EMX device. See ***Connecting Environmental Sensor Packages*** (on page 39).
2. Log in to the EMX web interface. The EMX should have detected the connected sensors and actuators, and display them in the web interface.

3. Identify each sensor and actuator. See ***Identifying Environmental Sensors and Actuators*** (on page 240).
4. The EMX should automatically manage the detected sensors and actuators. Verify whether detected sensors and actuators are managed. If not, have them managed. See ***Managing Environmental Sensors or Actuators*** (on page 244).
5. Configure the sensors and actuators. See ***Configuring Environmental Sensors or Actuators*** (on page 246). The steps include:
   a. Name the sensor or actuator.
   b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
   c. Mark the sensor or actuator's physical location on the rack or in the room.
   d. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while discrete (on/off) sensors show sensor states only to indicate state changes. Only numeric sensors have threshold settings. As for actuators, they are used to control a device or system so they show state changes only.

Identifying Environmental Sensors and Actuators

Raritan has developed four types of environmental sensor packages - DPX, DPX2, DPX3 and DX series. The ways to identify each type of environmental sensor packages in the web interface are different.

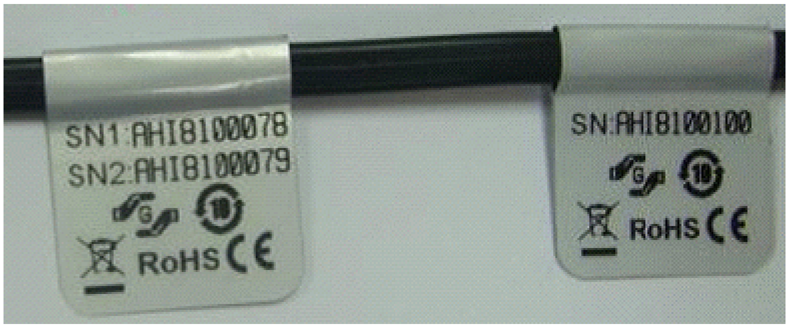
- DPX series: This type of environmental sensor package can be identified through its serial number.
- DPX2, DPX3 and DX series: This type of environmental sensor package can be identified either through its serial number or through its chain position, which consists of the sensor port and its location in the daisy chain.

See ***Matching the Serial Number*** (on page 241) and ***Matching the Position*** (on page 242) in the EMX User Guide.

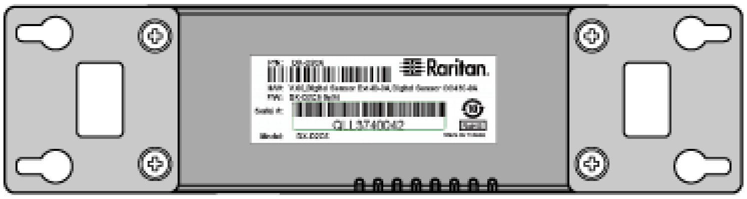
Note: For detailed information on each sensor package, refer to the Environmental Sensors Guide or Online Help on the Raritan website's **Support page** *(***http://www.raritan.com/support/***).*

Matching the Serial Number

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



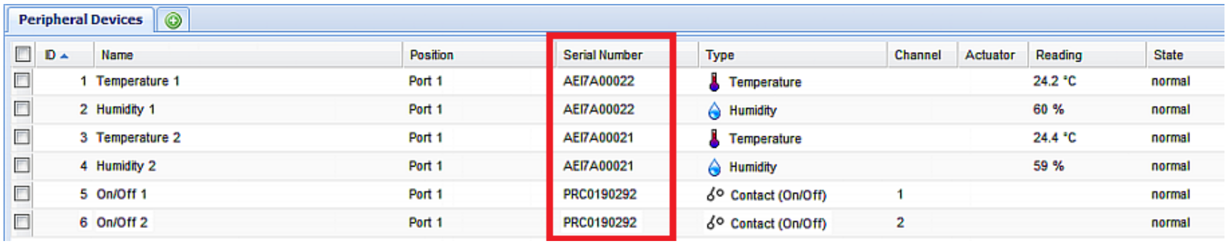
A DPX2, DPX3 or DX sensor has a serial number tag attached to its rear side.



The serial number for each sensor or actuator appears listed in the web interface after each sensor or actuator is detected by the EMX.

▶ To identify each detected environmental sensor or actuator via serial numbers:

1. Click Peripheral Devices in the left pane.
2. Match the serial number from the tag to those listed in the sensor table.



Peripheral Devices

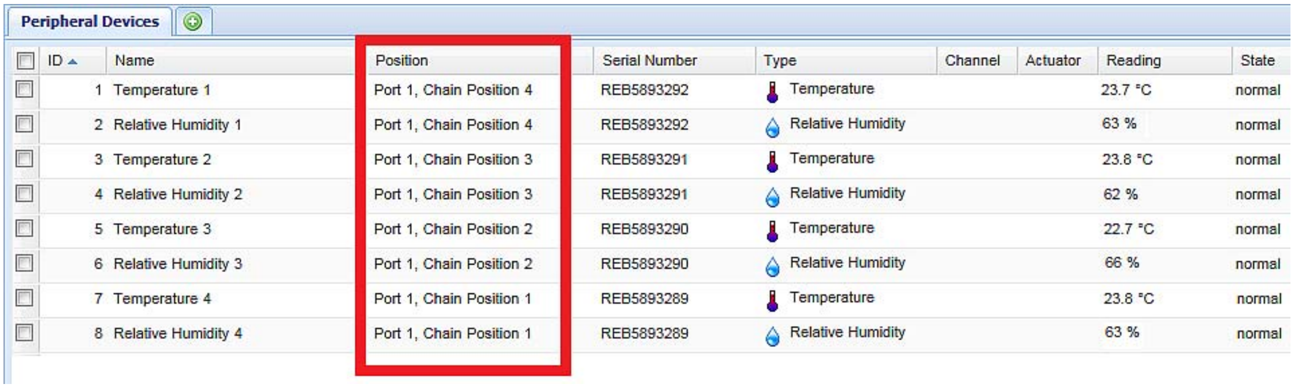
□	ID ▲	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
□	1	Temperature 1	Port 1	AEI7A00022	Temperature			24.2 °C	normal
□	2	Humidity 1	Port 1	AEI7A00022	Humidity			60 %	normal
□	3	Temperature 2	Port 1	AEI7A00021	Temperature			24.4 °C	normal
□	4	Humidity 2	Port 1	AEI7A00021	Humidity			59 %	normal
□	5	On/Off 1	Port 1	PRC0190292	Contact (On/Off)	1			normal
□	6	On/Off 2	Port 1	PRC0190292	Contact (On/Off)	2			normal

Matching the Position

DPX2, DPX3 and DX sensor packages can be daisy chained. The EMX can indicate each sensor or actuator's position by showing the sensor port where the environmental sensor package is connected as well as its sequence in a sensor daisy chain.

▶ To identify an environmental sensor or actuator through its position:

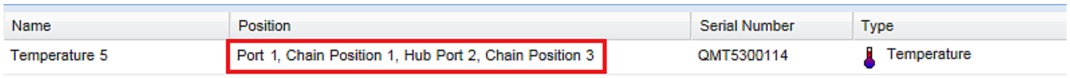
1. Click Peripheral Devices in the left pane.
2. Locate the Position column, which shows one, two or four pieces of position information.
   - The sensor port number, such as Port 1, Port 2, Port 3 and so on.
   - The sensor or actuator's location in the sensor chain, such as Chain Position 1, Chain Position 2, and so on.



□	ID ▲	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
□	1	Temperature 1	Port 1, Chain Position 4	REB5893292	Temperature			23.7 °C	normal
□	2	Relative Humidity 1	Port 1, Chain Position 4	REB5893292	Relative Humidity			63 %	normal
□	3	Temperature 2	Port 1, Chain Position 3	REB5893291	Temperature			23.8 °C	normal
□	4	Relative Humidity 2	Port 1, Chain Position 3	REB5893291	Relative Humidity			62 %	normal
□	5	Temperature 3	Port 1, Chain Position 2	REB5893290	Temperature			22.7 °C	normal
□	6	Relative Humidity 3	Port 1, Chain Position 2	REB5893290	Relative Humidity			66 %	normal
□	7	Temperature 4	Port 1, Chain Position 1	REB5893289	Temperature			23.8 °C	normal
□	8	Relative Humidity 4	Port 1, Chain Position 1	REB5893289	Relative Humidity			63 %	normal

   - If a DPX3-ENVHUB4 sensor hub is used, the port number on the hub is also indicated, such as Hub Port 1, Hub Port 2, and so on.

     In addition, two pieces of chain position information are displayed -- the first one indicates the sensor hub's chain position, which is always *Chain Position 1*, and the second one indicates the sensor's or actuator's chain position.



Name	Position	Serial Number	Type
Temperature 5	Port 1, Chain Position 1, Hub Port 2, Chain Position 3	QMT5300114	Temperature

▶ DPX sensor position information:

The EMX only displays the sensor port where the DPX sensor package is physically connected. No chain position information is displayed.

For example, if a DPX sensor package is connected to the SENSOR port numbered 1, its Position column only shows "Port 1" no matter a DPX3-ENVHUB4 sensor hub is used or not.

Note: For the EMX devices with only one SENSOR port, it always shows "Port 1."

DPX2, DPX3 and DX sensor position information:

The EMX displays the sensor package's position in the chain in addition to the sensor port number for DPX2, DPX3 and DX sensor packages.

For example:

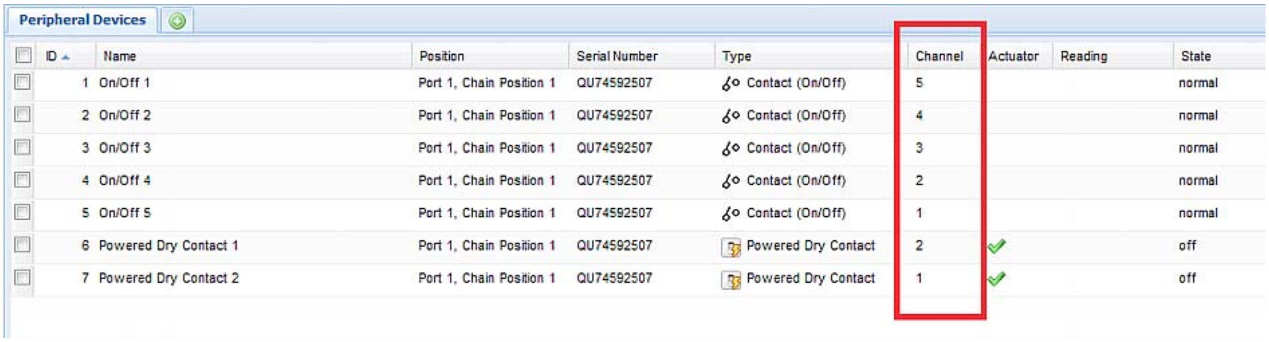
- If a DPX2, DPX3 or DX sensor or actuator is located on the second sensor package in the sensor chain directly connected to the SENSOR port 1, its Position column shows "Port 1, Chain Position 2."
- If this sensor chain is connected to the SENSOR port 1 via the DPX3-ENVHUB4 sensor hub, this sensor's or actuator's Position column becomes "Port 1, Chain Position 1, Hub Port x, Chain Position 2," where x is the hub's port to which this sensor or actuator is physically connected.

Identifying Sensor or Actuator Channels

A sensor package may have multiple contact closure (CC) or dry contact (DC) channels, such as DX-D2C6 or DX-PD2C5.

When the EMX initially detects and automatically manages a sensor package with multiple channels, all channels are assigned with ID numbers in sequence.

If you manually manage these channels by selecting "Automatically assign a sensor number," the EMX assigns ID numbers randomly because this option assumes that users do not care about the sequence. In this case, see the Channel column to identify each channel correctly. For example, CC1 or DC1 is Channel 1, CC2 or DC2 is Channel 2, and so on.



Peripheral Devices

□	ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
□	1	On/Off 1	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	5			normal
□	2	On/Off 2	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	4			normal
□	3	On/Off 3	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	3			normal
□	4	On/Off 4	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	2			normal
□	5	On/Off 5	Port 1, Chain Position 1	QU74592507	Contact (On/Off)	1			normal
□	6	Powered Dry Contact 1	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	2	✓		off
□	7	Powered Dry Contact 2	Port 1, Chain Position 1	QU74592507	Powered Dry Contact	1	✓		off

Managing Environmental Sensors or Actuators

The EMX starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed. To control an actuator, you also need to have it managed.

The EMX device can manage a maximum of 32 environmental sensors or actuators.

When there are less than 32 managed sensors or actuators, the EMX automatically brings detected environmental sensors or actuators under management by default. You have to manually manage a sensor or actuator only when it is not under management.

Tip: You can disable the automatic management feature so that newly connected environmental sensors or actuators are NOT brought under management automatically. See **Disabling the Automatic Management Function** *(on page 257).*

▶ To manually manage an environmental sensor or actuator:

1. Click Peripheral Devices in the left pane.
2. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To manage multiple ones, select multiple checkboxes.

   Note: To identify all detected sensors or actuators, see **Identifying Environmental Sensors and Actuators** *(on page 240).*

3. Click Manage. If you selected only one sensor or actuator, the "Manage peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor or actuator's serial number and <sensor type> is its type.

   Note: For a sensor package with contact closure (CC) or dry contact (DC) channels, a channel number is added to the end of the <sensor type>.

4. There are two ways to manage a sensor or actuator:
   - To manage it by letting the EMX assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors or actuators.
   - To manage it by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

     If the number you selected was already assigned to a sensor or actuator, that sensor or actuator becomes released after losing this ID number.

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

The manual assignment method is unavailable if you selected multiple sensors or actuators in Step 2.

5. Click OK. The EMX starts to display the managed sensor or actuator's reading and state.
6. To manage additional ones, repeat Steps 2 to 5.

Note: When the total number of managed sensors and actuators reaches the maximum, you CANNOT manage additional sensors or actuators unless you remove or replace any managed ones. To remove a sensor or actuator, see **Unmanaging Environmental Sensors or Actuators** *(on page 256).*

▶ Special note for a Raritan humidity sensor:

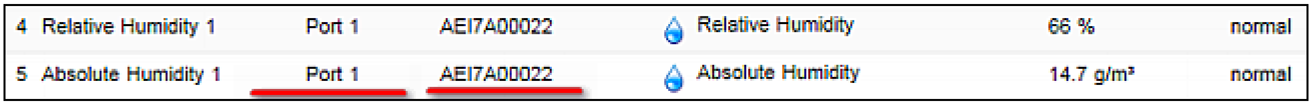
As of release 3.1.0, a Raritan humidity sensor is able to provide two measurements in the user interface - relative and absolute humidity values.

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

Note: Prior to release 3.1.0, only relative humidity values are available.

Relative humidity sensors can be "automatically" managed but absolute humidity sensors CANNOT. You must "manually" manage absolute humidity sensors if absolute humidity measurements are required.

Relative and absolute humidity values of the same humidity sensor share the same serial number and port position as illustrated below.



4	Relative Humidity 1	Port 1	AEI7A00022	Relative Humidity	66 %	normal
5	Absolute Humidity 1	Port 1	AEI7A00022	Absolute Humidity	14.7 g/m^3	normal

However, relative and absolute values of the same humidity sensor DO NOT share the same ID number. The above diagram shows that the two values have different ID numbers -- one is 4 and the other is 5.

Configuring Environmental Sensors or Actuators

You can change the default name to easily identify the managed sensor or actuator, and describe its location with X, Y and Z coordinates.

▶ **To configure environmental sensors or actuators:**

1. Click Peripheral Devices in the left pane.
2. Select the sensor or actuator that you want to configure.
3. Click Setup in the right pane. The "Setup of peripheral device <serial number> (<sensor type>)" dialog appears, where <serial number> is its serial number and <sensor type> is its type.

   For example, *Setup of peripheral device AEI7A00022 (Temperature)*.

4. Configure available fields properly.

Fields	Description
Name	Assign a name for identification.
Description	Type any descriptive text as needed.
Location (X, Y and Z)	Describe the sensor's or actuator's location by assigning alphanumeric values to the X, Y and Z coordinates. See ***Describing the Sensor's or Actuator's Location*** (on page 248). When the term "Rack Units" appears inside the parentheses in the Z location field, indicating that the Z coordinate format is set to Rack Units, you must type an integer number. See ***Setting the Z Coordinate Format*** (on page 247).
Binary Sensor Subtype	This field is available only when the selected sensor is a contact closure sensor. Select one of the following sensor types: ▪ Contact: The detector/switch is designed to detect the door lock or door open/closed status. ▪ Smoke Detection: The detector/switch is designed to detect the appearance of smoke. ▪ Water Detection: The detector/switch is designed to detect the appearance of water on the floor. ▪ Vibration: The detector/switch is designed to detect the vibration in the floor.
Alarmed to Normal Delay	This field is available only when the selected sensor is the DX-PIR presence detector. It determines the wait time before the EMX announces that the presence detector returns to the normal state after it is back to normal. Type both the time and measurement units in this field. For example, type '30 s' for 30 seconds, or '2 min' for 2 minutes.

5. If the selected sensor is a numeric sensor, its threshold settings are displayed in the dialog. See ***Sensor Threshold Settings*** (on page 529) for detailed information.

   There are two types of thresholds: sensor-specific thresholds and default thresholds.

   To use the sensor-specific threshold settings, select the Use Sensor Specific Thresholds radio button.

   - Click Edit or double-click the threshold setting row to open the threshold setup dialog.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 534).
   - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 532).

   To use the default threshold settings, select the Use Default Thresholds radio button. To modify the default threshold settings, see ***Changing Default Thresholds*** (on page 249).

   Note: The Upper Critical and Lower Critical values are points at which the EMX considers the operating environment critical and outside the range of the acceptable threshold.

6. Click OK.
7. Repeat the same steps to configure additional ones.

Tip: You can configure thresholds of multiple sensors at a time as long as these sensors belong to the same type. See **Setting Thresholds for Multiple Sensors** *(on page 250).*

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors and actuators.

▶ To determine the Z coordinate format:

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

   Note: This folder's name changes after customizing the device name. See **Naming the EMX** *(on page 110).*

2. Click Setup on the Settings page. The Setup dialog appears.
3. In the Peripheral Device Z Coordinate Format field, click the drop-down arrow and select an option from the list.
   - Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors or actuators.
   - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.
4. Click OK.

Describing the Sensor's or Actuator's Location

Use the X, Y and Z coordinates to describe each sensor or actuator's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = *Brown Cabinet Row*

Y = *Third Rack*

Z = *Top of Cabinet*

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 24 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 24 characters.

Tip: To configure and retrieve these coordinate values over SNMP, see the EMX MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** *(on page 309).*

Changing Default Thresholds

The default thresholds are the initial threshold values that automatically apply to numeric environmental sensors. These values are configured on a sensor type basis, which include:

- Temperature sensors
- Humidity sensors (both relative and absolute humidity)
- Air pressure sensors
- Air flow sensors
- Vibration sensors

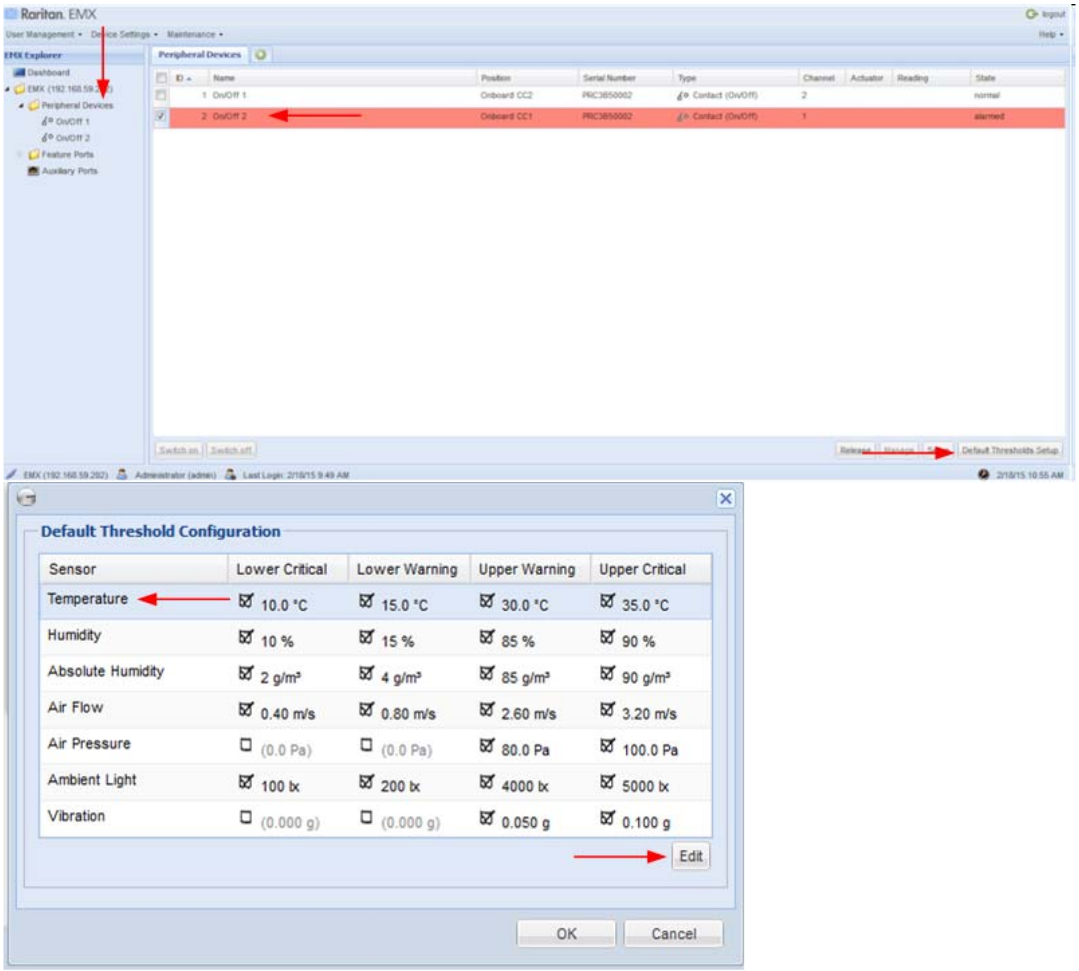
Note that changing the default thresholds re-determine the initial thresholds applying to the environmental sensors that are added or detected later on.

In addition, changing the default thresholds also change the thresholds of those environmental sensors where the default thresholds have been selected as their threshold option. See ***Configuring Environmental Sensors or Actuators*** (on page 246).

▶ To change the default threshold settings:

1. Click Peripheral Devices in the EMX Explorer pane, and the Peripheral Devices page opens in the right pane.
2. Click Default Thresholds Setup on the Peripheral Devices page. A dialog appears, showing a list of all numeric environmental sensor types.
3. Select the desired sensor type.
4. Click Edit or double-click that sensor type to adjust its threshold settings, deassertion hysteresis or assertion timeout.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 534).
   - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 532).
5. Repeat the above step to modify the threshold settings of other numeric sensor types.

6. Click OK.



	ID	Name	Position	Serial Number	Type	Channel	Actuator	Reading	State
□	1	On/Off 1	Onboard CC2	PRC3850002	Contact (On/Off)	2			normal
☑	2	On/Off 2	Onboard CC1	PRC3850002	Contact (On/Off)	1			alarmed

Sensor	Lower Critical	Lower Warning	Upper Warning	Upper Critical
Temperature	☑ 10.0 °C	☑ 15.0 °C	☑ 30.0 °C	☑ 35.0 °C
Humidity	☑ 10 %	☑ 15 %	☑ 85 %	☑ 90 %
Absolute Humidity	☑ 2 g/m³	☑ 4 g/m³	☑ 85 g/m³	☑ 90 g/m³
Air Flow	☑ 0.40 m/s	☑ 0.80 m/s	☑ 2.60 m/s	☑ 3.20 m/s
Air Pressure	□ (0.0 Pa)	□ (0.0 Pa)	☑ 80.0 Pa	☑ 100.0 Pa
Ambient Light	☑ 100 lx	☑ 200 lx	☑ 4000 lx	☑ 5000 lx
Vibration	□ (0.000 g)	□ (0.000 g)	☑ 0.050 g	☑ 0.100 g

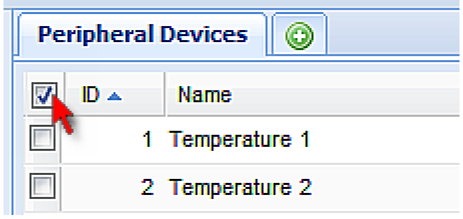
Setting Thresholds for Multiple Sensors

You can configure thresholds for multiple environmental sensors of *the same type* at a time. For example, if you want all temperature sensors to have identical upper and lower thresholds, follow the procedure below to set up all temperature sensors together.

► To configure thresholds of multiple environmental sensors:

1. Click the Peripheral Devices folder in the EMX Explorer pane, and the Peripheral Devices page opens in the right pane.
2. Select the checkboxes of those environmental sensors whose threshold settings should be the same. Make sure the selected sensors belong to the same type.

- To select all of those listed on the Peripheral Devices page, simply select the checkbox in the header row.



Peripheral Devices

☑	ID ▲	Name
□	1	Temperature 1
□	2	Temperature 2

3. Click Setup. Note that the Setup button is disabled if any of the selected sensors belongs to a different type.
4. Configure the thresholds as described in ***Configuring Environmental Sensors or Actuators*** (on page 246).
5. Click OK.

Viewing Sensor and Actuator Data

Readings and states of the environmental sensors or actuators will display in the web interface after the sensors and actuators are properly connected and managed.

The Dashboard page shows the information of managed environmental sensors and actuators only, while the Peripheral Devices page shows the information of both managed and unmanaged ones.

Both pages indicate an environmental sensor or actuator's position in either of the following manners:

- **Port <n>**, where <n> is the number of the SENSOR port on the EMX where a specific environmental sensor package is connected. DPX sensor packages show this information only.
- **Port <n>, Chain Position <pos_num>**, where <pos_num> is the sensor package's sequential position in a sensor daisy chain. DPX2, DPX3 and DX sensor packages show this information.

If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or at least one LHX built-in sensor fails on the heat exchanger. See ***The Yellow- or Red-Highlighted Sensors*** (on page 100).

▶ To view managed environmental sensors and actuators only:

1. Click the Dashboard icon in the EMX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Peripheral Devices section on the Dashboard page. The section shows:
   - Total number of managed sensors and actuators
   - Total number of unmanaged sensors and actuators

- Information of each managed sensor and actuator, including:

  - Name

  - Position

  - Reading (for numeric sensors)

  - State

To view both managed and unmanaged ones:

Click Peripheral Devices in the left pane.

Detailed information for each connected sensor or actuator is displayed, including:

- ID number
- Name
- Position
- Serial number
- Type
- Channel (for a sensor package with contact closure or dry contact channels)
- Whether the sensor is an 'Actuator' or not (if yes, this icon ✓ appears in the Actuator column)
- Reading
- State

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete sensors. For example, a contact closure sensor is a discrete (on/off) sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors show both numeric readings and sensor states to indicate environmental or internal conditions while discrete (on/off) sensors show sensor states only to indicate state changes.

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors

Sensor state	Applicable to
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity or communications with the sensor is lost.

The EMX pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor package show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The EMX continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

For DPX2, DPX3 or DX sensor packages, all of the connected sensor packages also enter the *unavailable* states if any of them is upgrading its sensor firmware.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, usually this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

For a Raritan's DPX floor water sensor, the normal state must be set to Normally Open, which means no water is detected.

Note: See the Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch. This guide is available on Raritan's **Support page** *(***http://www.raritan.com/support/***).*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

> *Lower Warning threshold <= Reading < Upper Warning threshold*

Note: The symbol <= means smaller than (<) or equal to (=).

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

Usually for a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

For Raritan's floor water sensor, the normal state must be set to Normally Closed, which means no water is detected. The *alarmed* state indicates that the presence of water is detected.

Note: See the Environmental Sensors Guide or Online Help for information on setting the normal state or dip switch. This guide is available on Raritan's **Support page** *(***http://www.raritan.com/support/***).*

Tip: A contact closure sensor's LED is lit after entering the alarmed *state. Determine which contact closure switch is in the "abnormal" status according to the corresponding LED.*

"below lower critical" State

This state means a numeric sensor's reading is below the lower critical threshold as indicated below:

Reading < Lower Critical Threshold

"below lower warning" State

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

Lower Critical Threshold <= Reading < Lower Warning Threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper warning" State

This state means a numeric sensor's reading is above the upper warning threshold as indicated below:

Upper Warning Threshold <= Reading < Upper Critical Threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

Upper Critical Threshold <= Reading

Note: The symbol <= means smaller than (<) or equal to (=).

States of Managed Actuators

DX sensor packages with dry contact channels allow you to connect actuators. An actuator has only three states described below. Note that an actuator is never highlighted in red or yellow regardless of the actuator states.

- unavailable: The communication with the actuator is lost.
- On: The actuator has been turned on.
- Off: The actuator has been turned off.

States of Unmanaged Sensors or Actuators

All sensors or actuators that are physically connected to the EMX while NOT under management always show the following state:

- unmanaged

Note: For firmware versions prior to 3.2.1, unmanaged sensors or actuators show the state "unavailable."

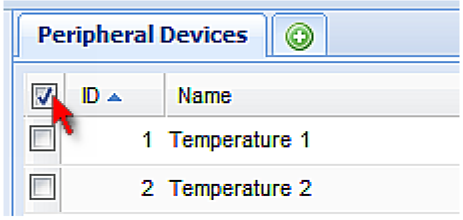
Unmanaging Environmental Sensors or Actuators

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the EMX device stops retrieving the sensor's reading and/or state. This procedure also applies if you want to unmanage an actuator.

To release a managed sensor or actuator:

1. Click Peripheral Devices in the left pane.
2. Select the checkbox of the desired sensor or actuator on the Peripheral Devices page. To release multiple ones, select multiple checkboxes.
   - To select all of those listed on the Peripheral Devices page, simply select the checkbox in the header row.

Note: If the desired action cannot be performed on any of the selected sensors or actuators, that action becomes unavailable. Deselect the inapplicable ones to perform the action.



☑	ID ▲	Name
□	1	Temperature 1
□	2	Temperature 2

3. Click Release.

After a sensor or actuator is removed from management:

- The ID number assigned to it is released, and can be automatically assigned to any newly-detected sensor or actuator if the Auto Management feature has been enabled. See ***Disabling the Automatic Management Function*** (on page 257).
- If it is no longer connected to the EMX, it disappears from the sensor list on the Peripheral Devices page.
- If it remains connected, it continues to be listed on the Peripheral Devices page but its state is changed to *unmanaged*. See ***States of Unmanaged Sensors or Actuators*** (on page 255).

Disabling the Automatic Management Function

The factory default is to enable the automatic management feature for environmental sensors and actuators. Therefore, when the total number of managed sensors and actuators has not reached 32 yet, the EMX automatically brings newly-connected environmental sensors and actuators under management after detecting them.

When this feature is disabled, the EMX no longer automatically manages any newly-detected environmental sensors and actuators, and therefore neither ID numbers are assigned nor sensor readings or states are available for newly-added ones.

▶ To disable the automatic management feature:

1. Click the EMX folder in the left pane.

   Note: The EMX folder's name can be customized. See **Naming the EMX** *(on page 110).*

2. Click Setup in the Settings section. The setup dialog appears.
3. Deselect the Peripheral Device Auto Management checkbox.
4. Click OK.

Controlling Actuators

If you have any DX sensor packages with actuators connected, which can move or control a mechanism or system, you can remotely turn on or off the actuators to control the connected mechanism or system.

▶ To turn on or off an individual actuator:

1. Expand the Peripheral Devices folder in the left pane to show a list of environmental sensors and/or actuators.
2. Click the desired actuator from the navigation tree. That actuator's page opens in the right pane.
3. Click "Switch on" to turn on the actuator, or "Switch off" to turn it off.

▶ To turn on or off multiple actuators:

1. Click Peripheral Devices in the left pane.
2. Select the checkboxes of the desired actuators on the Peripheral Devices page.

   Tip: An actuator is indicated with the icon ✓ displayed in the 'Actuator' column.

3. Click "Switch on" or "Switch off" to turn on or off the selected actuators. Confirm you want to switch when prompted.

Asset Management

Configure the asset management settings only when an asset sensor is physically connected to the EMX device.

Note: To set up an asset management system, see **Connecting Asset Management Sensors** *(on page 25).*

Configuring the Asset Sensor

The EMX cannot detect how many rack units (tag ports) a connected asset management sensor supports, so you must provide this information manually.

When you add an asset management sensor, you name it. Additionally, you can provide a description to identify each asset sensor.

The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the port number where the asset sensor is connected. In EMX, a Feature port is identified with a combination of the name "Asset Strip" and the port number.

To configure an asset sensor:

1. Connect the asset sensor to the EMX if it is not already.
2. Expand the Feature Ports folder in the navigation tree.
3. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

4. Click Setup in the Settings section. The Setup of Asset Strip dialog appears.
5. Enter a name of the asset sensor.
6. In the "Number of Rack Units" field, type the total number of rack units supported by the AMS. Default is 48.
7. Here, rack units are the number of asset management tag ports on the asset management strip. For example, if the AMS has 48 asset management tag ports, it supports up to 48 rack units on a cabinet.
8. Determine how to number all rack units on the asset sensor by selecting an option in the Numbering Mode.
   - Top-Down: The rack units are numbered in the ascending order from the highest to the lowest rack unit.

- Bottom-Up: The rack units are numbered in the descending order from the highest to the lowest rack unit.

9. In the Numbering Offset field, select the starting number. For example, if you select 3, the first rack unit is numbered 3, the second is numbered 4, the third is numbered 5, and so on until the final number.

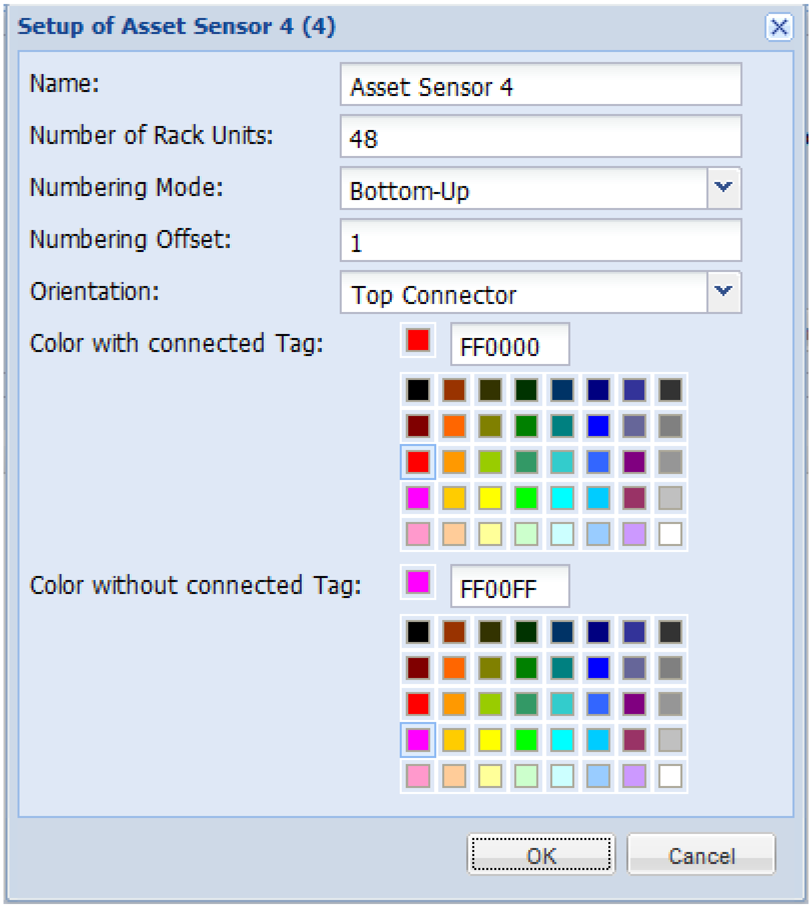
10. Indicate how the asset sensor is mounted on the rack in the Orientation field. The rack unit that is most close to the RJ-45 connector of the asset sensor will be marked with the index number 1 in the web interface.

    For the latest version of asset sensors with a built-in tilt sensor, it is NOT necessary to configure the orientation setting manually. The EMX device can detect the orientation of the asset sensors and automatically configure it.

    - Top Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
    - Bottom Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

11. Change the LED color settings as needed. See ***Setting Asset Sensor LED Colors*** (on page 260).

12. Click OK.



Setup of Asset Sensor 4 (4)

Name: Asset Sensor 4

Number of Rack Units: 48

Numbering Mode: Bottom-Up

Numbering Offset: 1

Orientation: Top Connector

Color with connected Tag: FF0000

Color without connected Tag: FF00FF

Setting Asset Sensor LED Colors

Each LED on the asset sensor indicates the presence and absence of a connected asset tag by changing its color.

By default the LED color of the tag ports with tags connected is green, and the color of the tag ports without tags connected is red. You can change the default LED color settings for all tag ports on an asset sensor assembly.

This feature is accessible only by users with Administrative Privileges.

▶ To configure all LED colors:

1. Expand the Feature Ports folder in the navigation tree.
2. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

3. Click Setup on the asset sensor page. The setup dialog for that asset sensor appears.
4. To change the LED color denoting the presence of a tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color with connected Tag" field.
5. To change the LED color denoting the absence of a tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color without connected Tag" field.
6. Click OK.

Tip: To make a specific LED's color settings different from other LEDs, see **Configuring a Specific Rack Unit** *(on page 261).*

Configuring a Specific Rack Unit

In the EMX web interface, a rack unit refers to a tag port on the asset sensor. You can name a specific rack unit, or change its LED color settings so that this LED behaves differently from others on the same asset sensor.

To change an LED's settings:

1. Connect the asset sensor to the EMX if it is not already.
2. Expand the Feature Ports folder in the navigation tree.
3. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

4. Select the rack unit whose LED settings you want to change.
5. Click Configure Rack Unit or double-click the selected rack unit. The setup dialog for the selected rack unit appears.
6. In the Name field, type a name for identifying this rack unit.
7. Select either Auto or Manual Override as this rack unit's LED mode.
   - Auto (based on Tag): This is the default setting. With this option selected, the LED follows the global LED color settings.
   - Manual Override: This option differentiates this LED's behavior. After selecting this option, you must select an LED mode and/or an LED color for the selected rack unit.

- LED Mode: Select On to have the LED stay lit, Off to have it stay off, "Slow blinking" to have it blink slowly, or "Fast blinking" to have it blink quickly.
- LED Color: If you select On, "Slow blinking" or "Fast blinking" in the LED Mode field, select an LED color by either clicking a color in the color palette or typing the hexadecimal RGB value of a color in the accompanying text box.

8. Click OK.

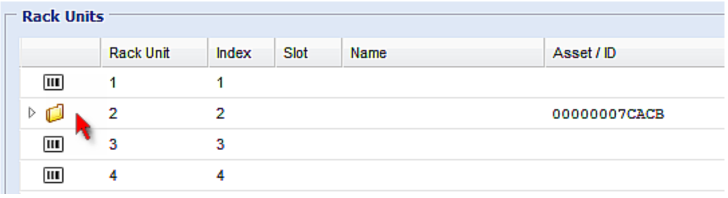
Expanding a Blade Extension Strip

A blade extension strip, like an asset sensor, has multiple tag ports. After connecting it to a specific asset sensor, it is displayed as a folder on that asset sensor's page.

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

▶ To expand a blade extension strip folder:

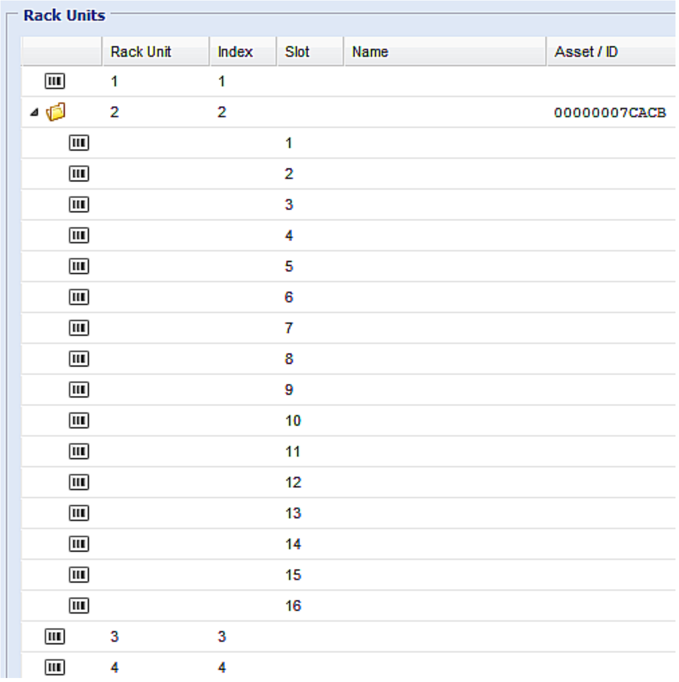
1. Click the desired asset sensor in the left pane. The selected asset sensor's page opens in the right pane.
2. Locate the rack unit (tag port) where the blade extension strip is connected.



Rack Units

	Rack Unit	Index	Slot	Name	Asset / ID
	1	1			
▷	2	2			00000007CACB
	3	3			
	4	4			

3. Double-click that rack unit or click the white arrow ▷ prior to the folder icon. The arrow then turns into a black, gradient arrow ◢, and all tag ports of the blade extension strip appear below the folder.



Rack Units

	Rack Unit	Index	Slot	Name	Asset / ID
	1	1			
◢	2	2			00000007CACB
			1		
			2		
			3		
			4		
			5		
			6		
			7		
			8		
			9		
			10		
			11		
			12		
			13		
			14		
			15		
			16		
	3	3			
	4	4			

▶ To collapse a blade extension strip:

- Double-click the blade extension strip folder, or click the black, gradient arrow ◢ prior to the folder icon. All tag ports under the folder are hidden.

Displaying the Asset Sensor Information

The hardware and software information of the connected asset sensor is available through the web interface.

▶ To display the asset sensor information:

1. Expand the Feature Ports folder in the navigation tree.
2. Click the desired asset sensor in the left pane. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

3. Click Extended Device Info, where the asset sensor data is displayed.
4. Click Close to quit the dialog.

Webcam Management

With a Logitech® webcam connected to the EMX device, 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 Sanpshots and Configuration."
- To configure webcam settings, you need the "Change Webcam Configuration" permission.

For more information on the Logitech webcam, see the user documentation accompanying it. For information on connecting a webcam to the EMX, see ***Connecting a Logitech Webcam*** (on page 59).

You can manually store snapshots taken from the webcam onto the EMX or a remote server. See ***Saving Snapshots*** (on page 268) or ***Configuring Webcam Storage*** (on page 265).

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 269).

Events that trigger emails containing snapshots from a webcam can be created. See ***Creating Actions*** (on page 188).

Configuring Webcams

Before you can configure a webcam, it must be connected to the EMX. See ***Connecting a Logitech Webcam*** (on page 59).

► To configure a webcam:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Click on the webcam you want to configure and then click Setup at the bottom right of page. The Webcam Setup dialog opens.
3. Enter a name for the webcam. Up to 64 characters are supported.
4. Type the location information in each location field if needed. Up to 63 characters are supported.
5. 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.
6. Select the webcam mode. This can be changed as needed once the webcam is configured.

a. Video - the webcam is in video mode. Set the Framerate (frames per second) rate.

b. Snapshot - the webcam displays images from the webcam. Set the "Time between Snapshots" rate as measured in seconds.

7. Click OK. The image or video from the webcam is now available in the EMX once you click on the webcam in the navigation tree.

▶ To edit a webcam configuration:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Double-click on the webcam you want to edit. The webcam image or video opens in a new tab.
3. Click Setup ⚙.
4. Edit the information as needed. Changes to the resolution do not apply to existing, stored images - it applies only to images and videos taken after the resolution is changed.
5. Click OK.

Configuring Webcam Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the EMX by default. Up to ten (10) images can be stored on the EMX at once.

To save more than 10 snapshots, save the images on a Common Internet File System/Samba.

Note: NFS and FTP are not supported for this release and are disabled on the dialog.

Snapshot files are saved as JPG files. The snapshot file is named based on the number of the snapshot starting from 1. So the first snapshot that is taken is named 1.jpg, the second is 2.jpg and so on.

Unless snapshots are deleted manually, the oldest snapshot is automatically deleted from the device when the number of snapshots exceeds ten. Rebooting the EMX deletes all webcam snapshots that are saved on the device.

▶ To configure another storage location for images:

1. In the navigation tree, click Snapshots under the Webcam Management folder. The Snapshots page opens.
2. Click on the Setup Storage icon ⚙. The Storage Setup dialog opens.

3. By default, Local, meaning the EMX, is the designated default storage.
4. Select CIFS/Samba as the storage location.
5. Enter the server where to store the images.
6. If needed, enter the share drive/folder to store the images in.
7. Enter the username and password needed to access the server where the images are stored.
8. Enter or use the slide bar to set the number of images that can be saved to the storage location.
9. Click OK.

Adjusting Image Properties

If any snapshot or video properties, such as the brightness, contrast, saturation, and gain settings, do not satisfy your needs, adjust them.

▶ To adjust the image or video properties:

1. Select the webcam shown on the Webcam Management page or in the navigation tree. See ***Configuring Webcams*** (on page 264).
2. Click Setup or ⚙.
3. Click the Controls tab.
4. Adjust the desired property by adjusting the corresponding slide bar.

   Or click "Set to webcam defaults" to restore all settings to this webcam's factory defaults.
5. Click OK.

Viewing Webcam Snapshots or Videos

You can switch between snapshots or live videos being captured by a webcam.

The snapshot or video is displayed either in the EMX web interface or in a Primary Standalone Live Preview window that you open.

You can open a maximum of five Primary Standalone Live Preview windows.

Note: For remote Live Preview sessions, such as those accessed via a link in an email or instant message, a total of up to three (3) simultaneous Live Preview sessions are supported at a time. One (1) from the originator in the EMX interface, and up to two (2) remote sessions. See **Sending Snapshots or Videos in an Email or Instant Message** *(on page 269).*

► To switch between snapshot and video modes:

1. Click the desired webcam's icon in the navigation tree.

   Snapshots or videos captured by the webcam are displayed in the right pane of the EMX web interface once a webcam is selected in the navigation tree.

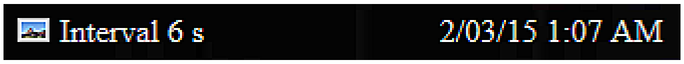
   Snapshots and videos can also be displayed in Live Preview mode in the Primary Standalone Live Preview window by clicking on the Live Preview icon .

   Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Viewing Connected Users** *(on page 234).*

2. By default the EMX enters the snapshot mode. Wait around one minute for the snapshot to appear.

   In the snapshot mode, three pieces of information are displayed on the top of the image:

   - A snapshot mode icon .
   - The interval time between snapshots (in seconds).
   - A time stamp.



Interval 6 s 2/03/15 1:07 AM

The webcam's location information, if available, is displayed in the Location pane of the EMX web interface.

- To change any image settings, click Setup ⚙. See ***Configuring Webcams*** (on page 264) or ***Adjusting Image Properties*** (on page 266).
- To save the snapshot being displayed, click the "Store Snapshot to Webcam Storage" icon 💾. See ***Saving Snapshots*** (on page 268).

3. To switch to the video mode, click Setup ⚙ and select Video in the Webcam Mode field.

   In the video mode, two pieces of information are displayed on the top of the image:

   - A video mode icon ▶.
   - The number of frames to take per second (fps).

1 fps

   To change any video settings, click Setup ⚙.

4. To return to the snapshot mode, repeat the above step and select Snapshot.

Saving Snapshots

If it is intended to keep the snapshot being displayed on the webcam, you can manually save it onto the EMX. A snapshot is saved as a JPEG file and stored on the Snapshots page.

> Warning: The snapshots stored on the EMX are cleared when rebooting the EMX. Check the importance of the snapshots before performing the reset.

▶ To save the snapshot being displayed:

1. In the navigation tree, click on the webcam you want to take a snapshot with. The webcam image is displayed in the right pane.

   The webcam must be in snapshot mode in order to take snapshots. If the webcam is in video mode, click Setup in the right pane above the video image to open the Webcam Setup dialog, then select the Snapshot radio button.

2. Once the snapshot image being taken by the selected webcam is displayed in the right pane, click the Store Snapshot to Webcam Storage 💾 icon above the image to take a snapshot. Up to ten (10) snapshots can be stored at once on the device.

3. Click on the Snapshots icon in the navigation tree to verify that those snapshots are successfully saved and listed on the Snapshots page.

Tip: To store snapshots on a remote server rather than the EMX, see **Configuring Webcam Storage** *(on page 265).*

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, which permits a link to the snapshot or video being captured.

You are able to email or instant message up to two (2) recipients a link to webcams attached to the EMX. Users can then click on the links and view snapshots or videos.

A total of three sessions based on the same URL are supported, including a Primary Standalone Live Preview window of the sender and two remote sessions of the recipients.

Note: All Live Preview sessions sharing the same URL, including one Primary Standalone Live Preview window and two associated remote sessions, are identified as one single "<webcam>" user in the Connected Users dialog. You can disconnect a "<webcam>" user from this dialog to terminate a specific Primary Standalone Live Preview window and all of its remote sessions. See **Viewing Connected Users** *(on page 234).*

For explanation of this topic, the message sender is User A and the recipient is User B.

The recipient is able to access the snapshot or video image via the link in any of the following scenarios:

- The snapshot or video remains open in the Primary Standalone Live Preview window in User A's side. If so, even though User A logs out of the EMX interface or the login session times out, the link is available.

  Or

- At least a remote session based on the same URL remains open. If so, even though User A has closed the Primary Standalone Live Preview window, the link is available.

  Or

- Neither the Primary Standalone Live Preview window nor any remote 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 ***Enabling Login Limitations*** (on page 165).

Tip: If the idle timeout has not expired, the <webcam> user for that Live Preview URL remains shown in the Connected Users dialog.

Best Practice

As a best practice, User A should open the snapshot or video using a Primary Standalone Live Preview window and leave that window open at least until User B opens the snapshot or video via the link.

Once User B opens the snapshot or video via the link, User A can close the Primary Standalone Live Preview window.

User B should let User A know that the link has been opened.

▶ To send a snapshot or video link via email or instant message:

1. In the navigation tree, click on the webcam that is capturing the snapshot or video you want to provide a link to other people. The snapshot or video is displayed in Live Preview mode in the right pane.
2. Click on the Live Preview icon located above the snapshot or video. The snapshot or video opens in a standalone Live Preview window.
3. Copy the URL from the Live Preview window, paste it into the email or instant message application. Leave the Live Preview window open at least until the recipient opens the snapshot or video via the link.

Managing the Snapshots Saved to EMX

A maximum of 10 saved snapshots can be stored and displayed on the Snapshots page of the EMX.

See ***Saving Snapshots*** (on page 268) for instructions on storing snapshots on the EMX.

The Snapshots page is categorized into three sections: Storage, Snapshot and Details.

- Storage: shows a list of all saved snapshots.

  On the top of the Storage section, the number following "Used" indicates the total of saved snapshots and the number following "Size" indicates maximum number of snapshots allowed in storage.

- Snapshot: displays the image of the snapshot being selected.
- Details: shows the information which had been entered when the snapshot was saved, including resolution and location settings.

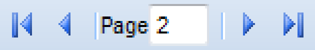
Tip: To save more than 10 snapshots, save snapshots onto a remote server. See **Configuring Webcam Storage** *(on page 265).*

To view the saved snapshots:

1. In the navigation tree, click Snapshots under the Webcam Management folder. The snapshots are displayed in the right pane in the Storage section of the page.
2. View an individual snapshot by clicking on a snapshot file in the Storage section of the page.

   The size of each snapshot file, the date and time each snapshot was taken, and the webcam that took each snapshot, is displayed when viewing snapshots.

   Details, such as the webcam location and/or labels, if any, are displayed in the Details section below the snapshot in the right pane. This information is defined when the webcam is initially configured. See ***Configuring Webcams*** (on page 264).
3. Use the navigation icons to move through each snapshot, or enter a specific page number to jump to that snapshot page.

   Page 2
4. Click the Refresh icon ⟳ to refresh the page. New snapshots are displayed if they are available.

To delete any snapshot from the storage:

- Delete snapshots by selecting the checkbox next to the snapshot you want to delete, then clicking the Delete icon ✖ at the top of the section. To select and delete all snapshots at once, click the checkbox in the checkbox column header, then click the Delete icon.

Managing the Schroff LHX/SHX Heat Exchanger

The EMX supports monitoring and administering the Schroff® LHX-20, LHX-40 and SHX-30 heat exchanger if this device is connected to the EMX.

From the EMX, you can do the following remotely:

- Name a connected LHX heat exchanger
- Monitor LHX sensors and operational states
- Configure the air outlet temperature setpoint
- Configure the default fan speed
- Configure sensor thresholds (for alert generation)
- Request maximum cooling using the fan speed and opening the cold water valve
- Acknowledge alerts remotely (for example, return to normal operation after maximum cooling is requested)

The exact information is dependent on your Schroff model. See your Schroff LHX/SHX manual for details on each device's settings and features.

▶ To monitor one LHX/SHX heat exchanger using the EMX:

1. Connect an LHX-20, LHX-40 or SHX-30 heat exchanger to the EMX if it is not connected yet. See ***Connecting a Schroff LHX/SHX Heat Exchanger*** (on page 61).
2. Enable the support of LHX/SHX heat exchanger on the EMX. See ***Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support*** (on page 273).
3. Configure the connected heat exchanger. See ***Configuring the LHX/SHX*** (on page 274).
4. Now you can remotely monitor or control the connected LHX/SHX heat exchanger via the EMX.
   - To monitor the heat exchanger, see ***Monitoring the LHX/SHX*** (on page 277).
   - To control the heat exchanger, see ***Turning the LHX/SHX On or Off*** (on page 282).

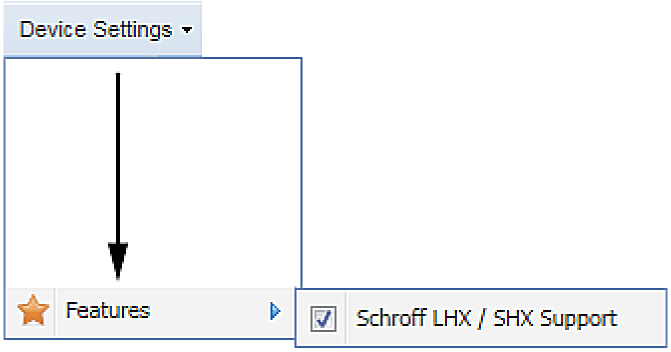
Enabling and Disabling Schroff LHX/SHX Heat Exchanger Support

By default, Schroff LHX/SHX Heat Exchanger support is disabled. As such, support needs to be enabled before the device appears in the navigation tree or on the dashboard.

Additionally, Schroff LHX/SHX Heat Exchanger support must be enabled in order for the LHX-MIB to be accessible through SNMP.

▶ To enable the Schroff LHX/SHX Heat Exchanger:

1. Select Device Settings > Features, and then select the Schroff LHX/SHX Support checkbox.



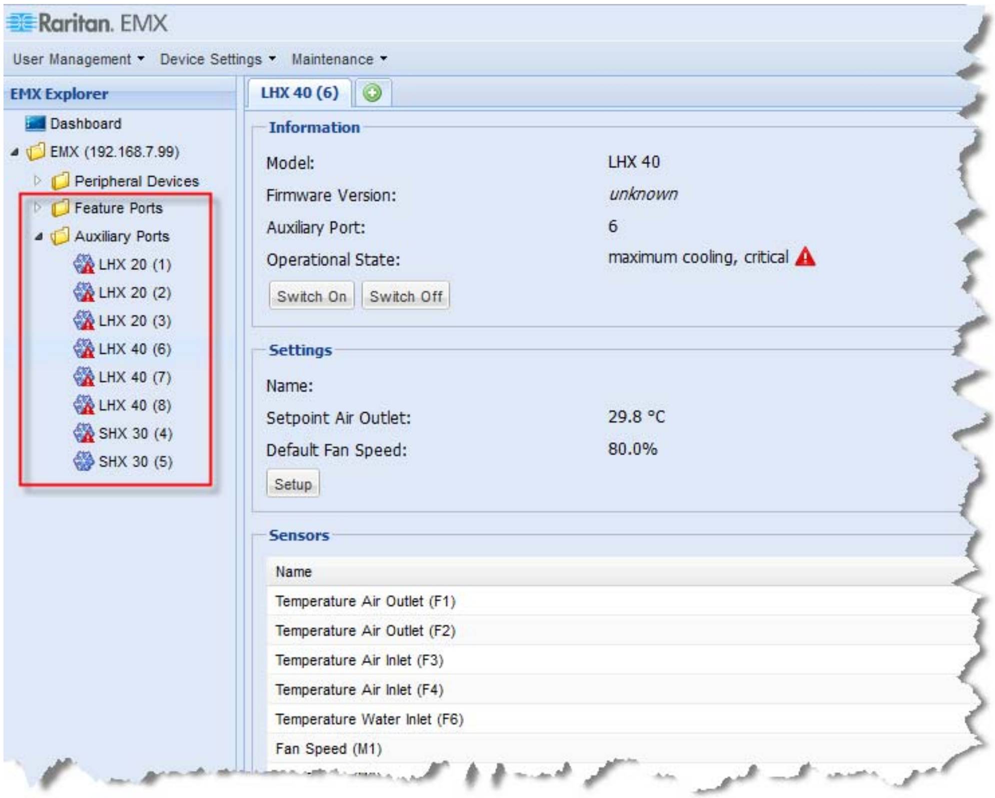
2. Click Yes to confirm.
3. Reboot the EMX.

Configuring the LHX/SHX

After enabling the LHX/SHX support on the EMX, the EMX should automatically detect the connected LHX/SHX device and display it under the Auxiliary Ports or the Feature Ports folder, depending on the port it is connected to.

After this device is displayed, you can set LHX/SHX temperature or fan speed thresholds for alerts or to customize the name of the LHX/SHX device for easy identification. See ***Configuring the Auxiliary Port*** (on page 133) or ***Configuring the Feature Port*** (on page 132).

After this device is displayed, you can set LHX/SHX temperature or fan speed thresholds for alerts or to customize the name of the LHX/SHX device for easy identification.



Model: LHX 40
Firmware Version: *unknown*
Auxiliary Port: 6
Operational State: maximum cooling, critical

Name:
Setpoint Air Outlet: 29.8 °C
Default Fan Speed: 80.0%

Name
Temperature Air Outlet (F1)
Temperature Air Outlet (F2)
Temperature Air Inlet (F3)
Temperature Air Inlet (F4)
Temperature Water Inlet (F6)
Fan Speed (M1)

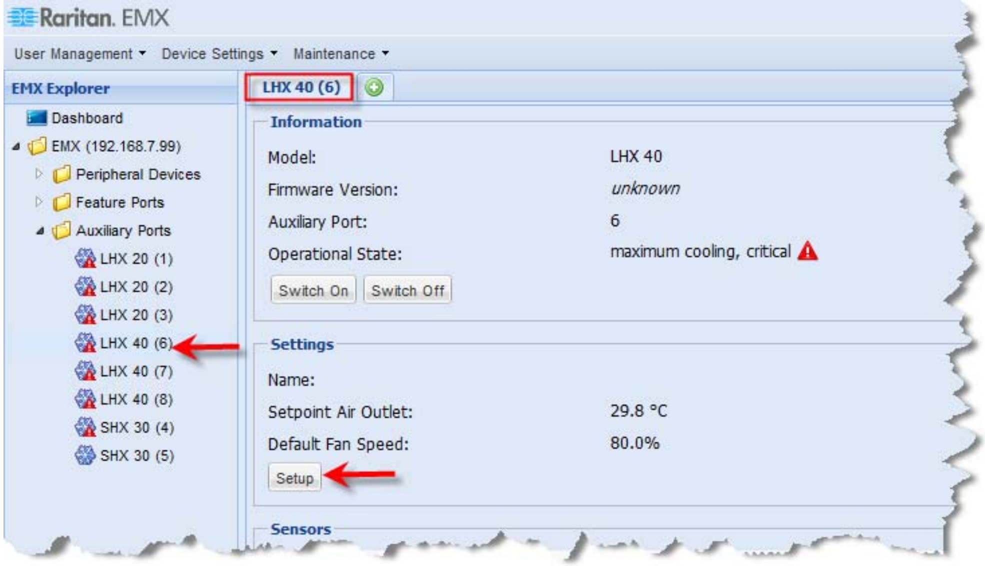
Note: The LHX/SHX settings are stored on the EMX port where the LHX/SHX device is connected, and are lost if that device is moved to a different port.

Setting Up an LHX/SHX

Once a Schroff LHX/SHX heat exchanger is connected, you can set up the device by giving it a name, and configure its setpoint air outlet and default fan speed.

▶ To set up the LHX/SHX:

1. Expand the Auxiliary Ports or Feature Ports folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.



Information

Model: LHX 40

Firmware Version: *unknown*

Auxiliary Port: 6

Operational State: maximum cooling, critical ⚠

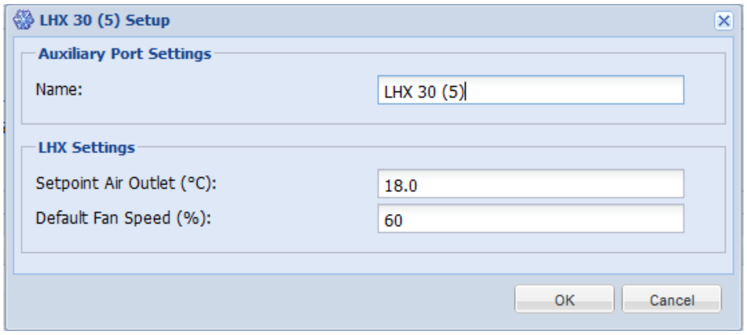
Settings

Name:

Setpoint Air Outlet: 29.8 °C

Default Fan Speed: 80.0%

3. Click Setup in the Settings section of the page. The Setup dialog opens.
4. Type a name for the heat exchanger in the Name field. The customized LHX/SHX heat exchanger's name is followed by the device type and port number in parentheses.
5. Enter the air outlet's temperature set point in the Setpoint Air Outlet (°C) field.
6. Enter the default fan speed in the Default Fan Speed (%) field.



LHX 30 (5) Setup

Auxiliary Port Settings

Name: LHX 30 (5)

LHX Settings

Setpoint Air Outlet (°C): 18.0

Default Fan Speed (%): 60

7. Click OK.

Configuring Temperature and Fan Thresholds

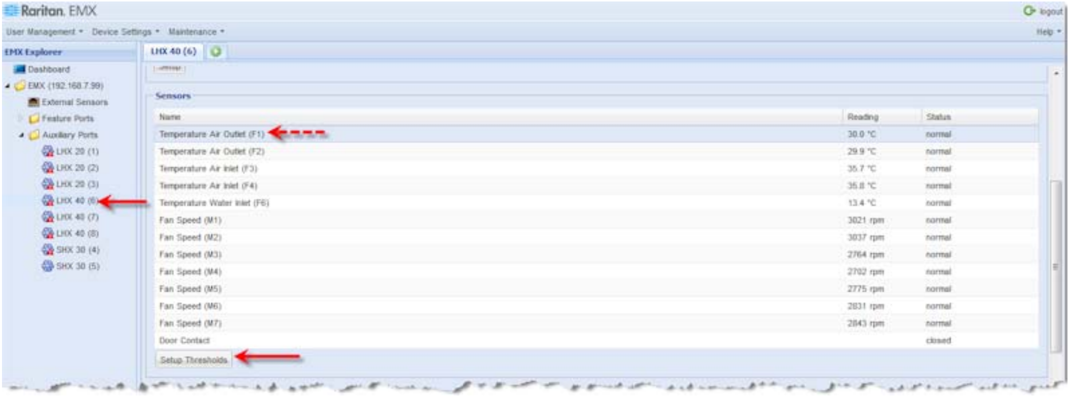
An LHX/SHX heat exchanger is implemented with various sensors for detecting the air temperature, water temperature, and fan speed.

You can set thresholds for these sensors so that the EMX alerts you when any sensor readings are getting close to a critical condition.

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

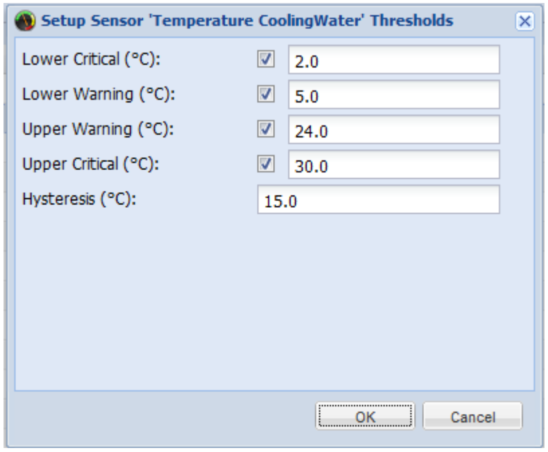
▶ To configure the thresholds for a sensor:

1. Expand the Auxiliary Ports or Feature Ports folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.
3. Select the desired sensor in the Sensors table and click Setup Thresholds, or double-click that sensor.



Name	Reading	Status
Temperature Air Outlet (F1)	30.0 °C	normal
Temperature Air Outlet (F2)	29.9 °C	normal
Temperature Air Inlet (F3)	35.7 °C	normal
Temperature Air Inlet (F4)	35.8 °C	normal
Temperature Water Inlet (F6)	13.4 °C	normal
Fan Speed (M1)	3021 rpm	normal
Fan Speed (M2)	3037 rpm	normal
Fan Speed (M3)	2764 rpm	normal
Fan Speed (M4)	2702 rpm	normal
Fan Speed (M5)	2775 rpm	normal
Fan Speed (M6)	2831 rpm	normal
Fan Speed (M7)	2843 rpm	normal
Door Contact		closed

The setup dialog for the selected sensor appears.



Lower Critical (°C): ☑ 2.0
Lower Warning (°C): ☑ 5.0
Upper Warning (°C): ☑ 24.0
Upper Critical (°C): ☑ 30.0
Hysteresis (°C): 15.0

4. Adjust the threshold and deassertion hysteresis settings. The Upper Critical and Lower Critical values are points at which the EMX considers the operating environment critical and outside the range of the acceptable threshold.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To set the deassertion hysteresis, type a numeric value in the Deassertion Hysteresis field. See ***"To De-assert" and Deassertion Hysteresis*** (on page 534).
   - To set the assertion timeout, type a numeric value in the Assertion Timeout (samples) field. See ***"To Assert" and Assertion Timeout*** (on page 532).
5. Click OK.

Monitoring the LHX/SHX

The EMX web interface lets you monitor the status of the connected LHX/SHX heat exchanger as well as the status of LHX/SHX built-in sensors.

Viewing the Summary

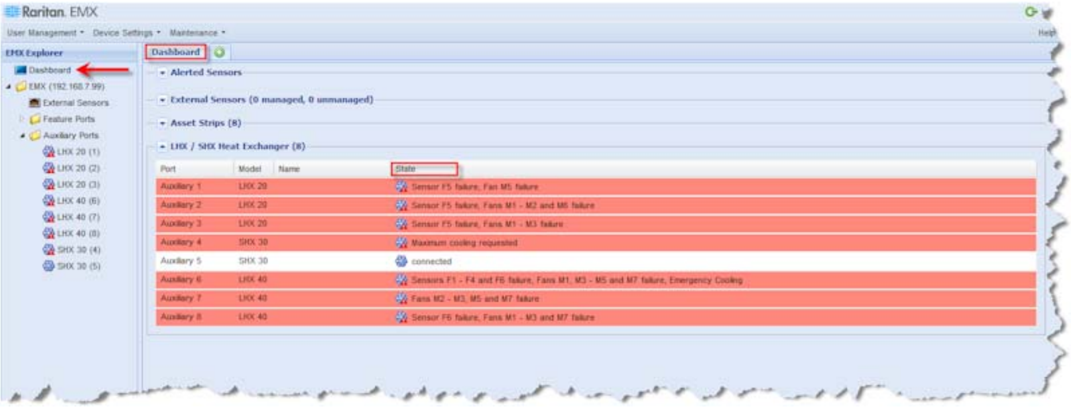
The Dashboard, Auxiliary Port and Feature Port pages display the summary of all connected LHX/SHX heat exchangers, including the port number where each heat exchanger is connected, and each heat exchanger's status.

If an LHX/SHX is highlighted in red in the summary, it indicates that there is LHX/SHX sensor failure on that heat exchanger. View the State column to identify failed sensors.

▶ LHX/SHX summary on the Dashboard page:

1. Click the Dashboard icon in the EMX Explorer pane. The Dashboard page opens in the right pane.

2. Locate the LHX/SHX Heat Exchanger section where the LHX/SHX summary is shown.



Port	Model	Name	State
Auxiliary 1	LHX 20		Sensor F5 failure, Fan M5 failure
Auxiliary 2	LHX 20		Sensor F5 failure, Fans M1 - M2 and M6 failure
Auxiliary 3	LHX 20		Sensor F5 failure, Fans M1 - M3 failure
Auxiliary 4	SHX 30		Maximum cooling requested
Auxiliary 5	SHX 30		connected
Auxiliary 6	LHX 40		Sensors F1 - F4 and F6 failure, Fans M1, M3 - M5 and M7 failure, Emergency Cooling
Auxiliary 7	LHX 40		Fans M2 - M3, M5 and M7 failure
Auxiliary 8	LHX 40		Sensor F6 failure, Fans M1 - M3 and M7 failure

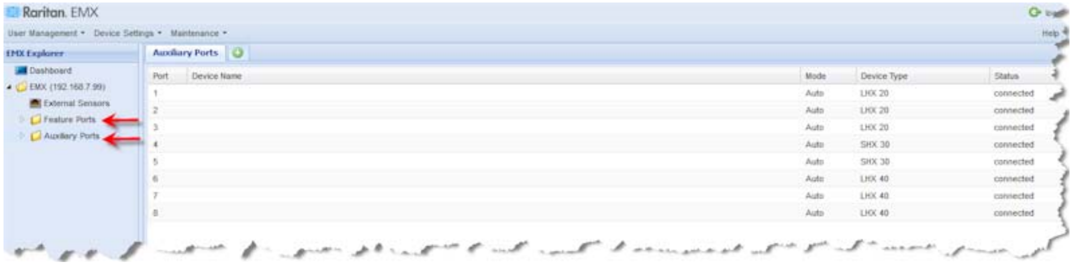
LHX/SHX summary on the Ports page:

- Click the Auxiliary Ports folder in the EMX Explorer pane.

  - OR -

- Click the Feature Ports folder.

  The port page opens in the right pane, showing the LHX/SHX summary.



Port	Device Name	Mode	Device Type	Status
1		Auto	LHX 20	connected
2		Auto	LHX 20	connected
3		Auto	LHX 20	connected
4		Auto	SHX 30	connected
5		Auto	SHX 30	connected
6		Auto	LHX 40	connected
7		Auto	LHX 40	connected
8		Auto	LHX 40	connected

Viewing Details

An LHX/SHX heat exchanger page shows detailed information, including:

- Device information and settings, such as the LHX/SHX device name
- The air outlet temperature
- The default fan speed
- Readings and states of all LHX/SHX built-in sensors
- Alerts and errors, such as failed LHX/SHX sensors or emergency cooling activation
- Accumulative operating hours

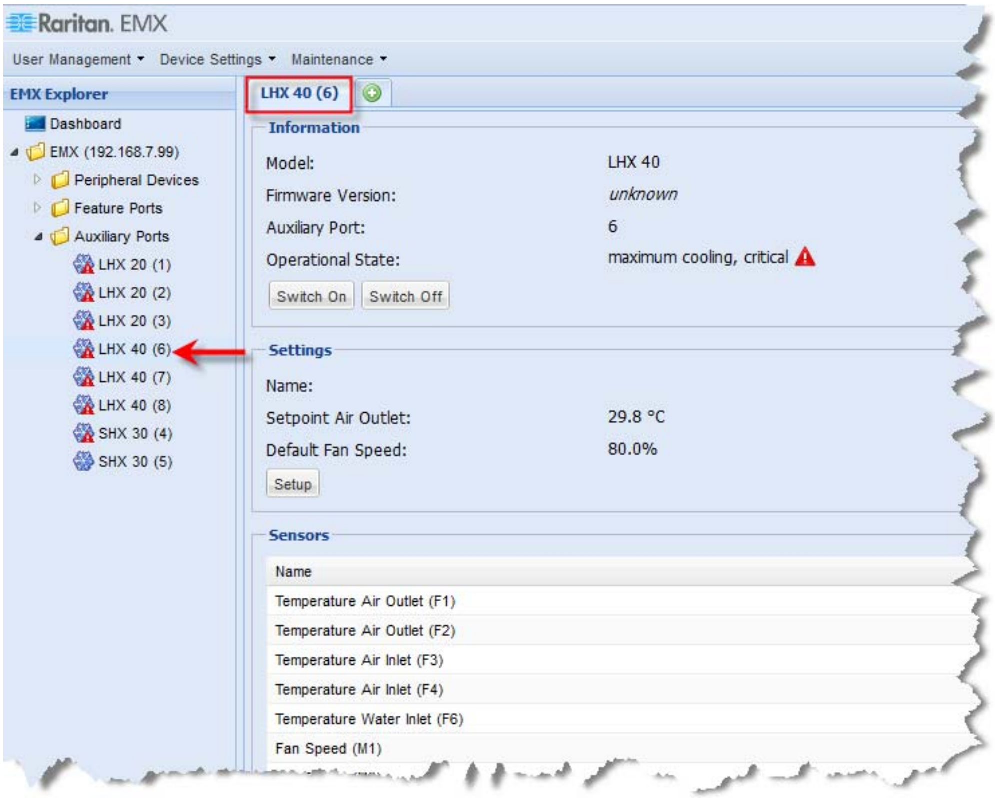
If any LHX/SHX sensor enters the critical or warning level, that sensor row is highlighted in red or yellow. See ***The Yellow- or Red-Highlighted Sensors*** (on page 100).

In addition, SHX-30 models indicate the number of power supplies present and if a condenser pump is present, since those options are supported by the SHX-30.

► **To view details of a specific LHX/SHX heat exchanger:**

1. Expand the Auxiliary Ports or Feature Ports folder as needed.

2. Click the desired LHX/SHX device. Its page opens in the right pane.



Information

Model: LHX 40

Firmware Version: *unknown*

Auxiliary Port: 6

Operational State: maximum cooling, critical ⚠

Settings

Name:

Setpoint Air Outlet: 29.8 °C

Default Fan Speed: 80.0%

Sensors

Name
Temperature Air Outlet (F1)
Temperature Air Outlet (F2)
Temperature Air Inlet (F3)
Temperature Air Inlet (F4)
Temperature Water Inlet (F6)
Fan Speed (M1)

Device States and Icon Variations

The EMX web interface changes icons to represent different statuses of the connected LHX/SHX heat exchanger.

Icons	Device status
❄	The heat exchanger is turned ON and operating normally.
❄	The heat exchanger is turned OFF.
❄⚠	The heat exchanger is turned ON but enters the critical state because of any LHX/SHX sensor failure.
❄⚠	At least one of the LHX/SHX sensor readings has entered the warning range.
❄✖	NO LHX/SHX device is detected on the specific port.

To identify the cause of a critical state, refer to:

- ***Viewing the Summary*** (on page 277)
- ***Alert States and LHX Event Log*** (on page 281)

Alert States and LHX Event Log

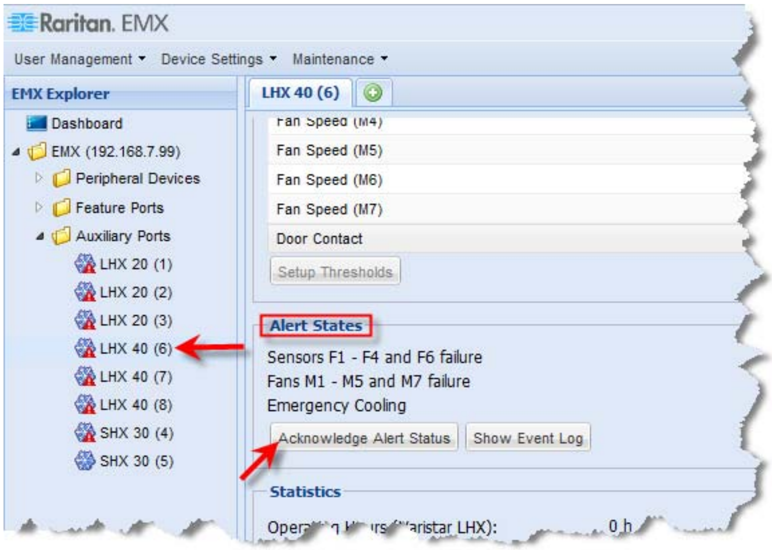
Remote Alert Acknowledgment is supported by the LHX-20 and LHX-40. The SHX-30 does not support Remote Alert Acknowledgment.

When an LHX heat exchanger is physically connected to the EMX device, a section labeled Alert States appears on its device page.

The Alert States section contains information identifying the LHX sensors that currently fail.

A button labeled Show Event Log is located in the Alert States section. To view LHX events associated with the EMX, click this button.

Note: To view the event log for an SHX-30, click Maintenance > View Event Log.



Sensors F1 - F4 and F6 failure
Fans M1 - M5 and M7 failure
Emergency Cooling

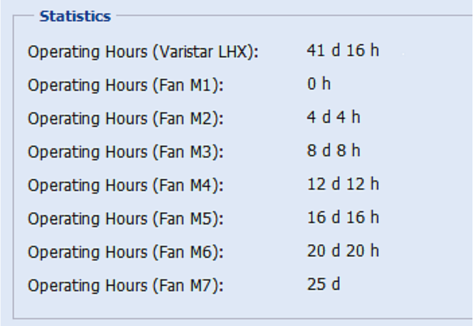
Opera‧‧‧n H‧‧‧rs (Varistar LHX): 0 h

Tip: The Dashboard, Auxiliary Ports and Feature Ports pages also point out failed sensors. See **Viewing the Summary** *(on page 277).*

Operating Hours

Operating hours are the accumulative time since the LHX/SHX heat exchanger is first connected to the EMX device and turned ON.

The EMX web interface displays the operating hours both for the heat exchanger and its fans. Operating hour information is located in the Statistics section of each heat exchanger page.



Statistics

Operating Hours (Varistar LHX):	41 d 16 h
Operating Hours (Fan M1):	0 h
Operating Hours (Fan M2):	4 d 4 h
Operating Hours (Fan M3):	8 d 8 h
Operating Hours (Fan M4):	12 d 12 h
Operating Hours (Fan M5):	16 d 16 h
Operating Hours (Fan M6):	20 d 20 h
Operating Hours (Fan M7):	25 d

Below are the time units used for operating hours:

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

For example, "3d 5h" means the total operating time is 3 days and 5 hours.

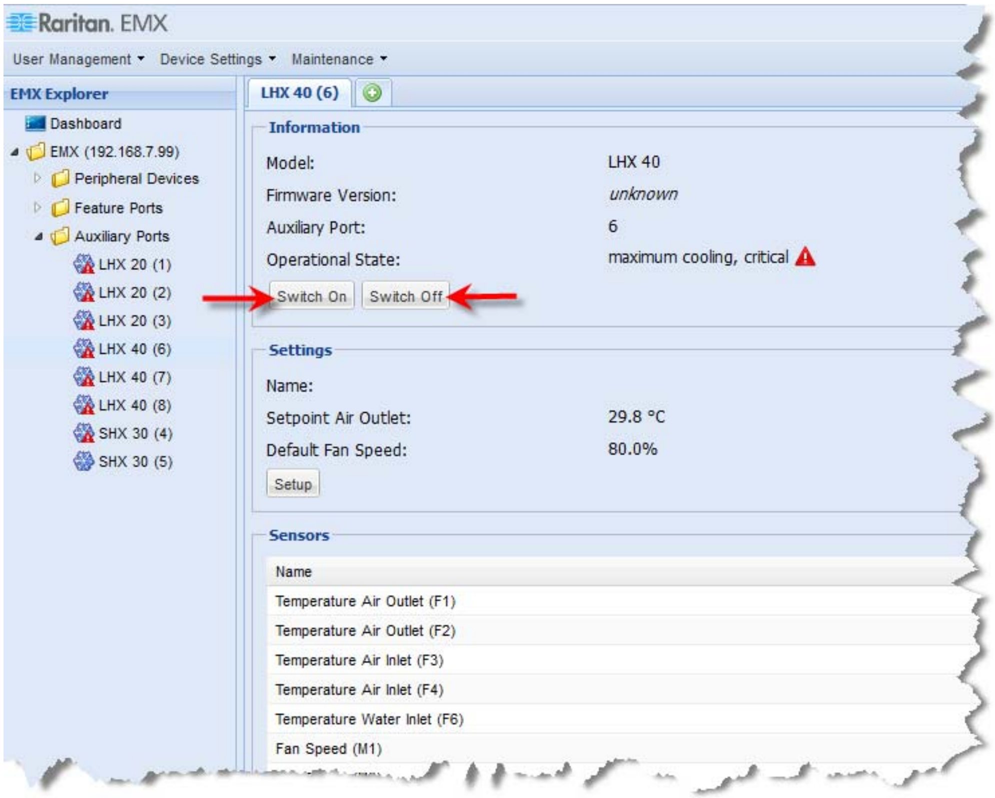
Turning the LHX/SHX On or Off

The EMX allows you to remotely turn on or off a connected heat exchanger.

▶ To control the LHX/SHX heat exchanger:

1. Expand the Auxiliary Ports or Feature Ports folder as needed.
2. Click the desired LHX/SHX device. Its page opens in the right pane.

In the Information section, click either Switch Off or Switch On.



Information

Model:	LHX 40
Firmware Version:	*unknown*
Auxiliary Port:	6
Operational State:	maximum cooling, critical ⚠

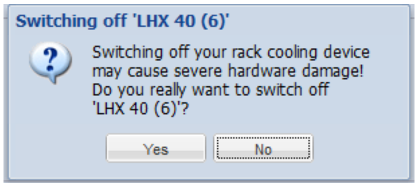
Settings

Name:	
Setpoint Air Outlet:	29.8 °C
Default Fan Speed:	80.0%

Sensors

Name
Temperature Air Outlet (F1)
Temperature Air Outlet (F2)
Temperature Air Inlet (F3)
Temperature Air Inlet (F4)
Temperature Water Inlet (F6)
Fan Speed (M1)

3. If you clicked Switch Off, a dialog appears, prompting you to confirm the operation. Click Yes to turn it off or No to abort the operation.



Switching off 'LHX 40 (6)'

Switching off your rack cooling device may cause severe hardware damage! Do you really want to switch off 'LHX 40 (6)'?

The heat exchanger's icon changes after being turned on or off. See ***Device States and Icon Variations*** (on page 280).

Requesting Maximum Cooling for an SHX-30

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

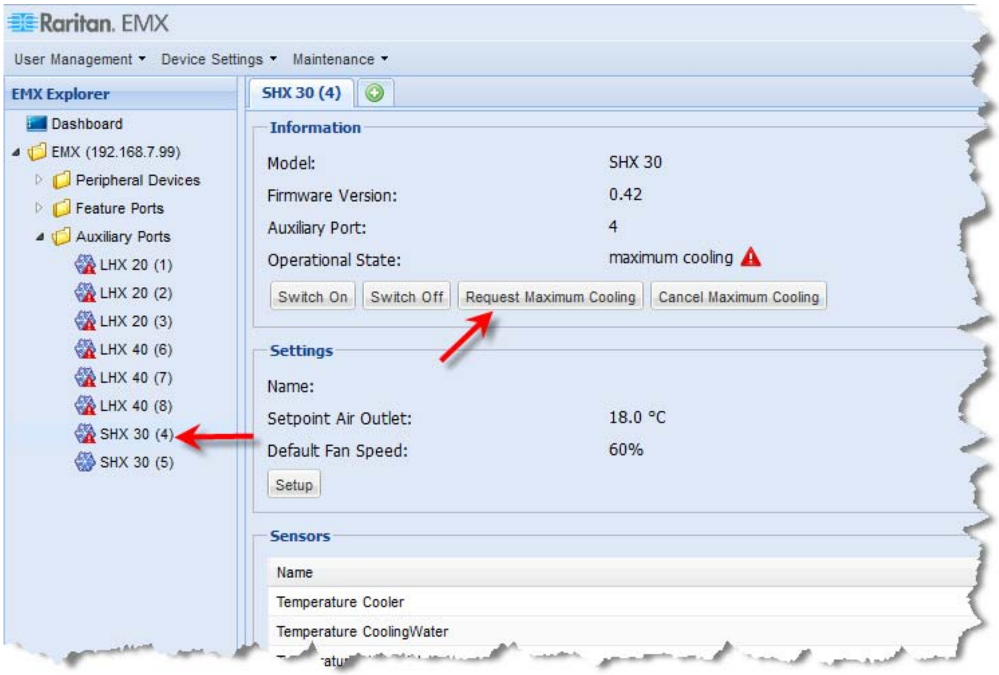
When you click Request Maximum Cooling on the EMX web interface, the SHX-30 enters into emergency cooling mode and runs at its maximum cooling level of 100% in order to cool the device.

When maximum cooling is requested for an SHX-30, the message "Maximum cooling requested" is displayed in the Alerts section of the page.

For additional information on the SHX-30 maximum cooling feature, see the SHX-30 documentation.

To request maximum cooling for an SHX-30:

1. Depending on the port your SHX-30 is connected to, expand the corresponding Auxiliary Ports or Feature Ports folder. A list of all ports is displayed under the folder.
2. Click the desired SHX-30 device. Its page opens in the right pane.
3. In the Information section of the page, click Request Maximum Cooling to cool the device. The maximum cooling process begins.
4. Click Cancel Maximum Cooling to stop the process (if needed).



Model: SHX 30

Firmware Version: 0.42

Auxiliary Port: 4

Operational State: maximum cooling ⚠

Name:

Setpoint Air Outlet: 18.0 °C

Default Fan Speed: 60%

Name
Temperature Cooler
Temperature CoolingWater

Managing Schneider Electric PowerLogic PM710

Configuring the PM710 and Configuring Threshold Settings

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: EMX2-888 does not support the PowerLogic PM710.

▶ To configure the PM710:

1. Connect the PM710 sensor to EMX2-111 if it is not already connected. See ***Connecting the Schneider Electric PowerLogic PM710*** (on page 63).
2. Pin the auxiliary port to the PM710.
3. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.
4. Click the desired sensor in the EMX Explorer pane. The page specific to that sensor opens in the right pane.
5. Click Setup in the Settings section. The Setup dialog opens.
6. Enter a name for the sensor in the Name field.
7. Leave the device address, line speed and parity as is so it matches the PM710 settings.
8. Click OK.
9. Configure the threshold settings if needed. Click on Thresholds at the bottom right of the Sensors section or Power Quality section of the page. The Thresholds dialog opens and displays the sensor readings gathered by EMX.
10. Select a reading and then click Edit, or double click on a reading to open its corresponding Threshold dialog.
11. Check the checkboxes next to the readings you want to set thresholds for, then edit the thresholds as needed. Click OK to save the changes.

Resetting the PM710 Minimum and Maximum Values

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. Review your PM710 documentation for additional information.

▶ To reset the PM710 minimum and maximum values:

1. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.
2. Click the desired sensor in the EMX Explorer pane. The page specific to that sensor opens in the right pane.
3. Click on Reset All Min / Max Values at the bottom left of the Sensors section of the page.
4. Click OK to confirm. All values are reset.

Clearing the PM710 Energy Accumulators

The PM710 saves energy accumulator values, which can be reset as needed. Review your PM710 documentation for additional information.

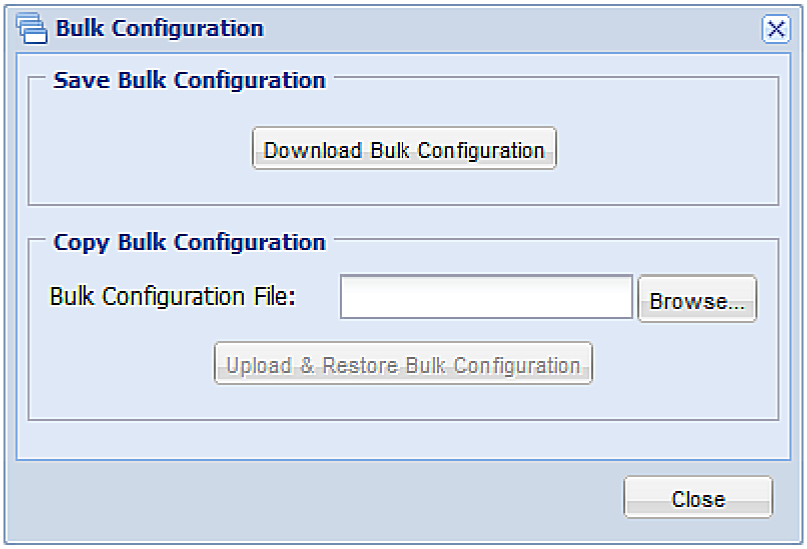
▶ To clear the PM710 energy accumulator values:

1. If the Auxiliary Ports folder is not expanded, expand it to show all devices connected to the RS-485 ports.
2. Click the desired sensor in the EMX Explorer pane. The page specific to that sensor opens in the right pane.
3. Click "Clear all Energy Accumulators" at the bottom left of the Sensors section of the page.
4. Click OK to confirm. All values are clear.

Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured EMX device to your PC. You can use this configuration file to copy that configuration to other EMX devices of the same model and firmware version.

You must have the Administrator Privileges or "Unrestricted View Privileges" to save and copy the EMX configurations.



Note: No device-specific data is saved to the Bulk Configuration file, such as environmental sensor or certain network settings. To back up or restore a specific EMX device's all settings, use the Backup/Restore feature instead. See **Backup and Restore of EMX Device Settings** *(on page 290).*

Tip: For the alternative to configure multiple EMX devices, see **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 454). For the other alternative, see* **Configuration or Firmware Upgrade with a USB Drive** *(on page 443).*

Saving the EMX Configuration

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

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

- Device name
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Environmental sensor and actuator names
- States and values of environmental sensors and actuators
- TLS Certificate
- Asset management sensor names and rack unit names
- SNMP name, location, and contact
- Server monitor entries

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

To save a configuration file:

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

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

Tip: You can also save a configuration file using a Secure Copy (SCP) command. See **Bulk Configuration via SCP** *(on page 481).*

Copying the EMX Configuration

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

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

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

▶ To copy a EMX configuration:

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See ***Firmware Upgrade*** (on page 291).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse to select the configuration file stored on your PC.
5. Click Upload & Restore Bulk Configuration to copy the file.

   A message appears, prompting you to confirm the operation and enter the admin password.
6. Enter the admin password, then click Yes to confirm the operation.
7. Wait until the EMX device resets and the Login page re-appears, indicating that the configuration copy is complete.

Note: On startup, the EMX performs all of its functions, including event rules and logs, based on the new configuration file you have selected instead of the previous configuration prior to the device reset. For example, "Bulk configuration copied" is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

Tip: You can also copy a configuration file using a Secure Copy (SCP) command. See **Bulk Configuration via SCP** *(on page 481).*

Backup and Restore of EMX Device Settings

Different from the Bulk Configuration file, the backup file contains device-specific data like network settings. To back up or restore EMX device 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 the bulk configuration among multiple EMX devices, perform the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 287).*

▶ To download a backup EMX XML file:

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Save Device Settings section, 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:

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Copy Device Settings section, click Browse to locate the 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 Yes to confirm the operation.
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 file you have selected instead of the previous configuration prior to the device reset. For example, "Bulk configuration copied" is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

Tip: You can also back up and restore a configuration file using a Secure Copy (SCP) command. See **Backup and Restore via SCP** *(on page 482).*

Firmware Upgrade

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

Firmware files are available on Raritan website's ***Support page*** (***http://www.raritan.com/support/***).

Updating the EMX Firmware

You must be the system administrator or log in to the user profile 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.

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

To update the firmware:

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

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

   During the firmware update:

   - A progress bar appears in the web interface, indicating the update status.
   - The front panel display on the EMX shows three digits: 'FuP' or 'FUP.'
   - No users can successfully log in to the EMX.
   - The user management operation, if any, is forced to suspend.

7. When the update is complete, a message appears, indicating the update is successful.
8. The EMX resets, and the Login page re-appears. You can now log in and resume your operation.

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

Note 2: If you are using the EMX with an SNMP manager, 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 298) in the User Guide.*

Tip: There are other alternatives to update the firmware. See **Firmware Update via SCP** *(on page 480), and* **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** *(on page 454). Or see* **Firmware Upgrade via USB** *(on page 453).*

Viewing Firmware Update History

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

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

To view the firmware update history:

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

Full Disaster Recovery

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

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

Updating the Asset Sensor Firmware

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

During the firmware upgrade, the following events take place:

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

Network Diagnostics

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

- Ping
- Trace Route
- List TCP Connections

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 435).*

Pinging a Host

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

To ping a host:

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.

3. In the Number of Requests field, type a number up to 20 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

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

▶ To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > Trace Route. The "Trace Route to Host" dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. In the Timeout (s) field, type a timeout value in seconds to end the trace route operation. Note that if the timeout value is too small, the trace route results may be incomplete.
4. To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select the Use ICMP Packets checkbox.
5. Click Run. A dialog appears, displaying the Trace Route results.

Listing TCP Connections

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

▶ To list TCP connections:

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

Downloading Diagnostic Information

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

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

This feature is accessible only by users with Administrative Privileges or "Unrestricted View Privileges."

▶ To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic Information. You are then prompted to save or open the file.
2. Click Save to save the file.
3. E-mail this file as instructed by Raritan Technical Support.

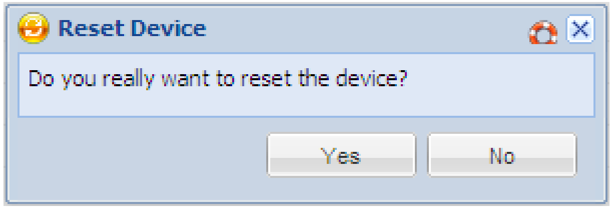
Rebooting the EMX

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

Note: Rebooting the EMX deletes all webcam snapshots that are saved on the device.

▶ To reboot the device:

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



Do you really want to reset the device?

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

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

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the EMX help

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 Help > About EMX. The About EMX dialog appears, with a list of open source packages displayed.
2. You can click any link in the dialog to access related information or download any software package.

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. Choose Help > User Guide. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. 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 ⌂.
4. 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.

5. 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.

6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon ✉ in the toolbar.
9. To email your comments or suggestions regarding the online help to Raritan, click the "Send feedback" icon 💬.
10. To print the currently selected topic, click the "Print this page" icon 🖨.

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

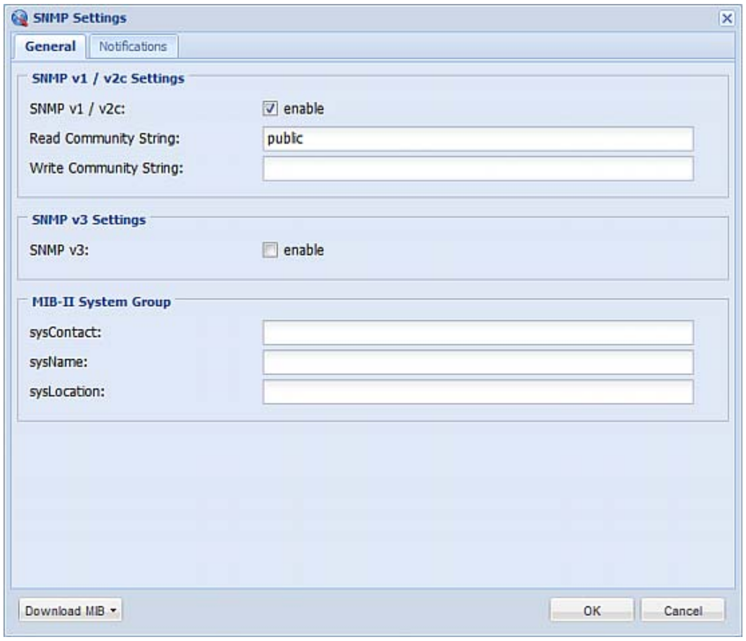
Enabling SNMP

By default, SNMP v1/v2c is enabled on the EMX so the EMX can communicate with an SNMP manager. If you have disabled the SNMP, it must be enabled to communicate with an SNMP manager.

Note that read-only access is enabled and the community string is public.

To enable SNMP:

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



SNMP v1 / v2c Settings

SNMP v1 / v2c: ☑ enable

Read Community String: public

Write Community String:

SNMP v3 Settings

SNMP v3: □ enable

MIB-II System Group

sysContact:

sysName:

sysLocation:

2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
   - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

   Tip: You can permit or disallow a user to access the EMX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 299).*

4. Enter the MIB-II system group information, if applicable:
   a. sysContact - the contact person in charge of the system
   b. sysName - the name assigned to the system
   c. sysLocation - the location of the system
5. Select the MIB to be downloaded. The SNMP MIB for your EMX is used by the SNMP manager.

   Important: You must download the SNMP MIB for your EMX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For details, see **Downloading SNMP MIB** *(on page 306).*

6. Click OK.

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and the EMX.

▶ **To configure users for SNMP v3 encrypted communication:**

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 149).

5. Click OK. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Notifications

The EMX automatically keeps an internal log of events that occur. See ***Event Rules and Actions*** (on page 187). These events can also be used to send SNMP v2c or v3 notifications to a third-party destination.

The EMX provides you with the ability to create SNMPv2c and SNMPv3 TRAP communications, or SNMPv2c and SNMPv3 INFORM communications.

SNMP TRAP communications capture and send information via SNMP, but no confirmation that the communication between the devices has succeeded is provided by the receiving device.

SNMP INFORM communications capture and send information via SNMP, and an acknowledgment that the communication was received by the receiving device is provided. If the inform communication fails, it is resent. You can define the number of times and the intervals to resend the inform communication, or leave the defaults of five resends in three second intervals.

Note: SNMP INFORM communications may take up slightly more network resources than SNMP TRAP communications since there are additional communications between the devices, and due to additional network traffic created should the initial communication fail and another is sent.

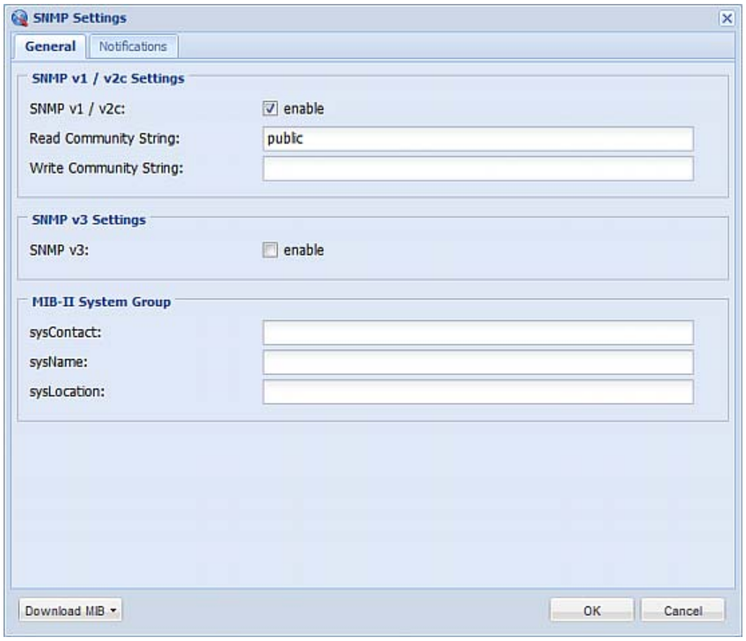
Use SNMP TRAP rules if you do not need confirmation that the communication has succeeded, and if you need to conserve network resources. Use SNMP INFORM communications to ensure more reliable communications, and if network resources can be managed with the potential additional network traffic.

Note: You should update the MIB used by your SNMP manager when updating to a new EMX release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** *(on page 306).*

SNMPv2c Notifications

To configure the EMX to send SNMP notifications:

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



SNMP Settings

General | Notifications

SNMP v1 / v2c Settings

SNMP v1 / v2c: ☑ enable

Read Community String: public

Write Community String:

SNMP v3 Settings

SNMP v3: □ enable

MIB-II System Group

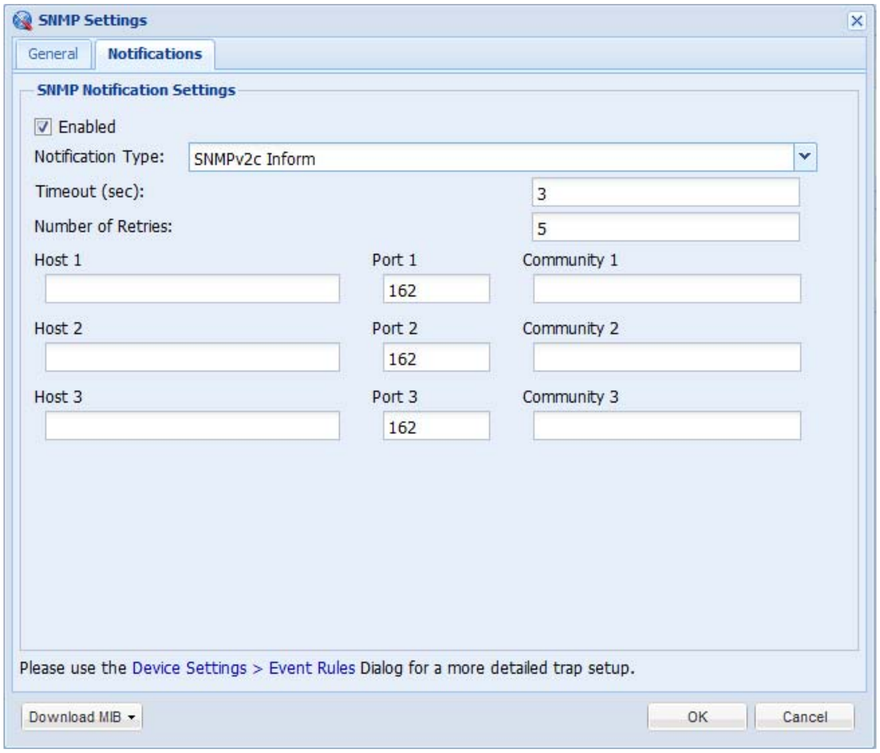
sysContact:

sysName:

sysLocation:

2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.



SNMP Notification Settings

☑ Enabled

Notification Type: SNMPv2c Inform

Timeout (sec): 3

Number of Retries: 5

Host 1	Port 1	Community 1
	162	

Host 2	Port 2	Community 2
	162	

Host 3	Port 3	Community 3
	162	

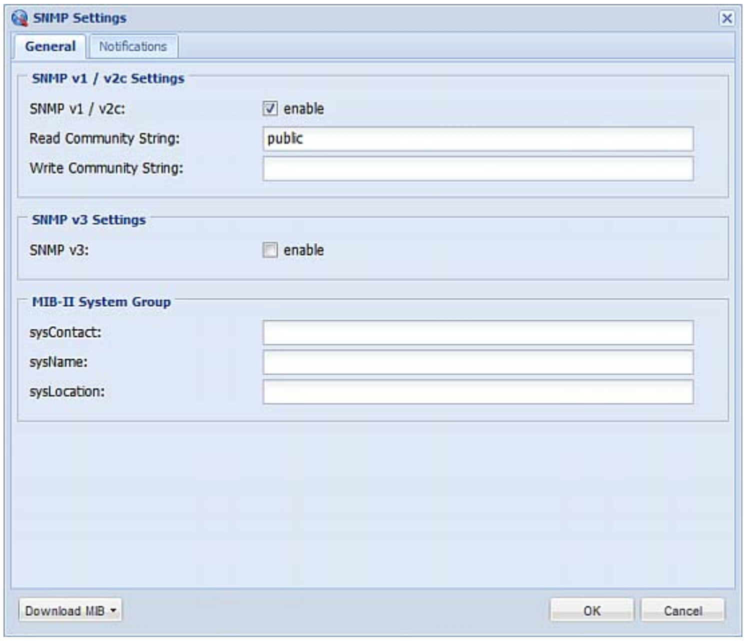
Please use the Device Settings > Event Rules Dialog for a more detailed trap setup.

4. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter 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, enter 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.
5. 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. You can specify up to 3 SNMP destinations.
6. In the Port fields, enter the port number used to access the device(s).
7. 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.
8. Click OK.

SNMPv3 Notifications

▶ To configure the EMX to send SNMPv3 notifications:

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



SNMP v1 / v2c Settings

SNMP v1 / v2c: ☑ enable

Read Community String: public

Write Community String:

SNMP v3 Settings

SNMP v3: □ enable

MIB-II System Group

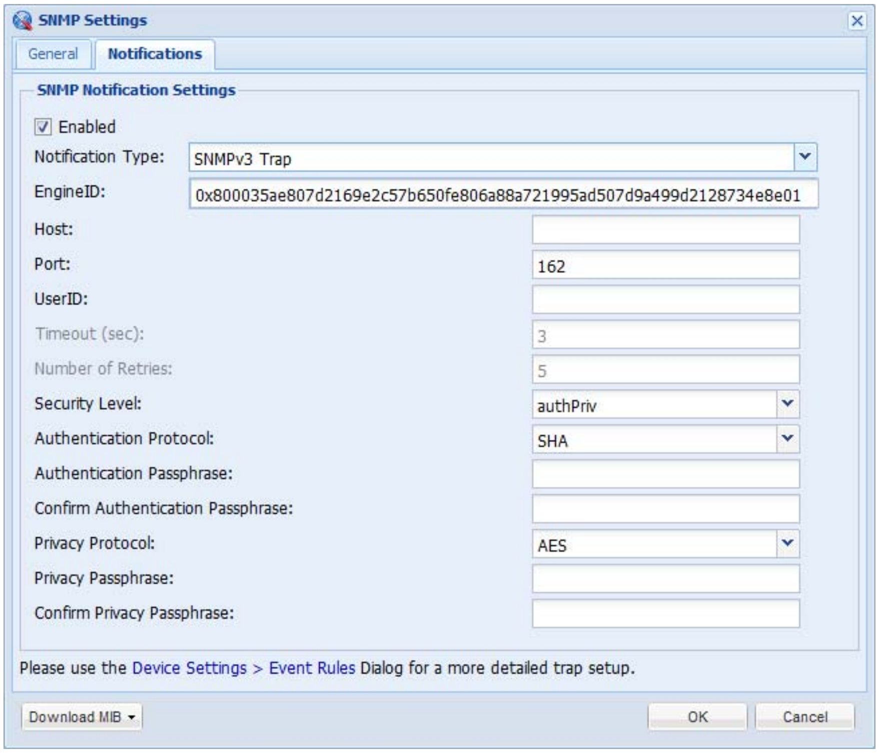
sysContact:

sysName:

sysLocation:

2. On the Notifications tab, select the Enabled checkbox to enable the SNMP notification feature.

3. From the Notification Type drop-down, select the type of SNMP notification.



SNMP Notification Settings

☑ Enabled

Notification Type: SNMPv3 Trap

EngineID: 0x800035ae807d2169e2c57b650fe806a88a721995ad507d9a499d2128734e8e01

Host:

Port: 162

UserID:

Timeout (sec): 3

Number of Retries: 5

Security Level: authPriv

Authentication Protocol: SHA

Authentication Passphrase:

Confirm Authentication Passphrase:

Privacy Protocol: AES

Privacy Passphrase:

Confirm Privacy Passphrase:

Please use the Device Settings > Event Rules Dialog for a more detailed trap setup.

4. For SNMP TRAPs, the engine ID is prepopulated.
5. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter 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, enter 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.
6. 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 needed to access the host
   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

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.

Downloading SNMP MIB

The SNMP MIB file for the EMX can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

▶ **File download via the SNMP Settings dialog:**

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB. A submenu of MIB files appears.
3. Select the desired MIB file to download.
   - EMD-MIB: The SNMP MIB file for managing the EMX device.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
   - LHX-MIB: The SNMP MIB file for managing the LHX/SHX heat exchanger(s).
4. Click Save to save the file onto your computer.

▶ **File download via the Device Information dialog:**

1. Choose Maintenance > Device Information.
2. Click the "download" link in the EMD-MIB, ASSETMANAGEMENT-MIB or LHX-MIB field to download the desired SNMP MIB.

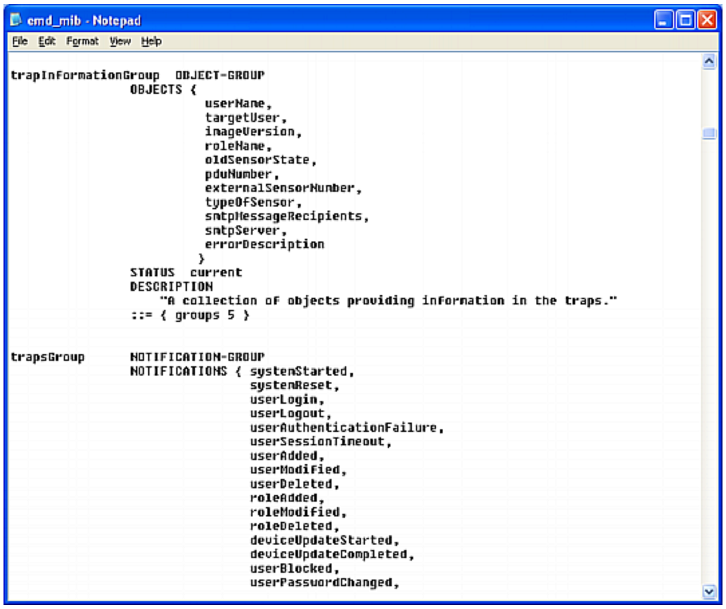
   The "USB Console INF file" link lets you download the USB-to-serial driver that may be required only when the EMX is connected to a computer via a USB cable. See ***Installing the USB-to-Serial Driver (Optional)*** (on page 12) for details.
3. Click Save to save the file onto your computer.

Note: If the LHX/SHX support has been enabled, LHX-MIB is available for download in either dialog.

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.



```
trapInformationGroup  OBJECT-GROUP
                OBJECTS {
                          userName,
                          targetUser,
                          imageVersion,
                          roleName,
                          oldSensorState,
                          pduNumber,
                          externalSensorNumber,
                          typeOfSensor,
                          smtpMessageRecipients,
                          smtpServer,
                          errorDescription
                         }
                STATUS  current
                DESCRIPTION
                    "A collection of objects providing information in the traps."
                ::= { groups 5 }


trapsGroup      NOTIFICATION-GROUP
                NOTIFICATIONS { systemStarted,
                                systemReset,
                                userLogin,
                                userLogout,
                                userAuthenticationFailure,
                                userSessionTimeout,
                                userAdded,
                                userModified,
                                userDeleted,
                                roleAdded,
                                roleModified,
                                roleDeleted,
                                deviceUpdateStarted,
                                deviceUpdateCompleted,
                                userBlocked,
                                userPasswordChanged,
```

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 Setting Power Thresholds 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.

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.

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 **Modifying Network Service Settings** *(on page 120).*

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:

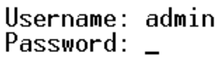
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   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 313) 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.

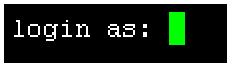
With SSH or Telnet

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 ***Modifying Network Service Settings*** (on page 120) in the User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

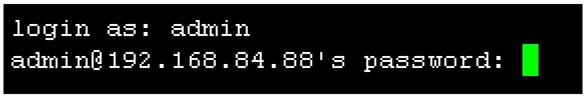


```
login as:
```

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 313) 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 135).
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 338).
- 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 436).

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 315).*

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 313).*

Network Configuration

This command shows all network configuration, such as the IP address, networking mode, and MAC address.

```
#        show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

```
#        show network ip <option>
```

Variables:

- <option> is one of the options: *all*, *v4* or *v6*.

Option	Description
all	This options shows both IPv4 and IPv6 settings. *Tip: You can also type the command without adding this option "all" to get the same data.*
v4	This option shows the IPv4 settings only.
v6	This option shows the IPv6 settings only.

LAN Interface Settings

This command shows the LAN interface information only, including LAN interface speed, duplex mode, current LAN interface status and LAN interface MAC address.

```
#        show network interface
```

Networking Mode

This command shows whether the current networking mode is wired or wireless.

```
#        show network mode
```

Note: If the EMX is a slave device connected to the LAN via the master EMX device, the `show network mode` command displays wired(USB) *instead of* wired*.*

Wireless Configuration

This command only shows the wireless configuration of the EMX device, such as the SSID parameter.

```
#        show network wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show network wireless details
```

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, 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.

Option	Description
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 327) 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 Peripheral Devices page of the EMX web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A discrete (on/off) sensor displays the sensor state instead of the numeric 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 Peripheral Devices 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 discrete (on/off) 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
```

USB-Cascading Configuration Information

This command shows the USB-cascading configuration, such as the cascading mode and device position.

```
#        show cascading
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show cascading details
```

Asset Sensor Settings

This command shows the asset sensor settings, such as the total number of rack units (tag ports), asset sensor state, numbering mode, orientation, available tags and LED color settings.

```
#        show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset sensor information. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific asset sensor number	Displays the settings of the asset sensor connected to the specified FEATURE port number. For the EMX device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Sensor

For the Raritan asset sensor, a rack unit refers to a tag port. This command shows the settings of a specific rack unit or all rack units on an asset sensor, such as a rack unit's LED color and LED mode.

```
#        show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset sensor. *Tip: You can also type the command without adding this option "all" to get the same data.*

Option	Description
A specific number	Displays the settings of the specified rack unit on the specified asset sensor. Use the index number to specify the rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.

Blade Extension Strip Settings

This command shows the information of a blade extension strip, including the total number of tag ports, and if available, the ID (barcode) number of any connected tag.

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit (tag port) on the selected asset sensor. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <blade_slot> is one of the options: *all* or a specific number of a tag port on the blade extension strip.

Option	Description
all	Displays the information of all tag ports on the specified blade extension strip connected to a particular rack unit. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the information of the specified tag port on the blade extension strip connected to a particular rack unit. The number of each tag port on the blade extension strip is available on the Asset Strip page.

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.
serverMonitor	Server-monitoring records, such as a server being declared reachable or unreachable.

Event type	Description
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>
```

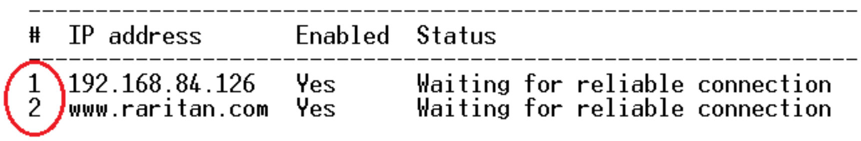
To show detailed information, add the parameter "details" to the end of the command.

```
#       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.*

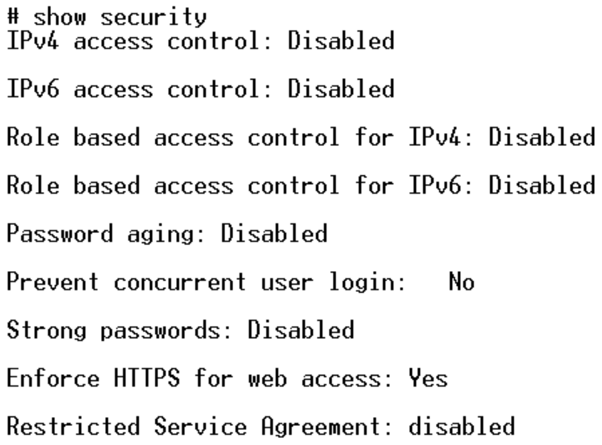
Option	Description
A specific integer number	Displays the specified number of last entries in the reliability error log.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

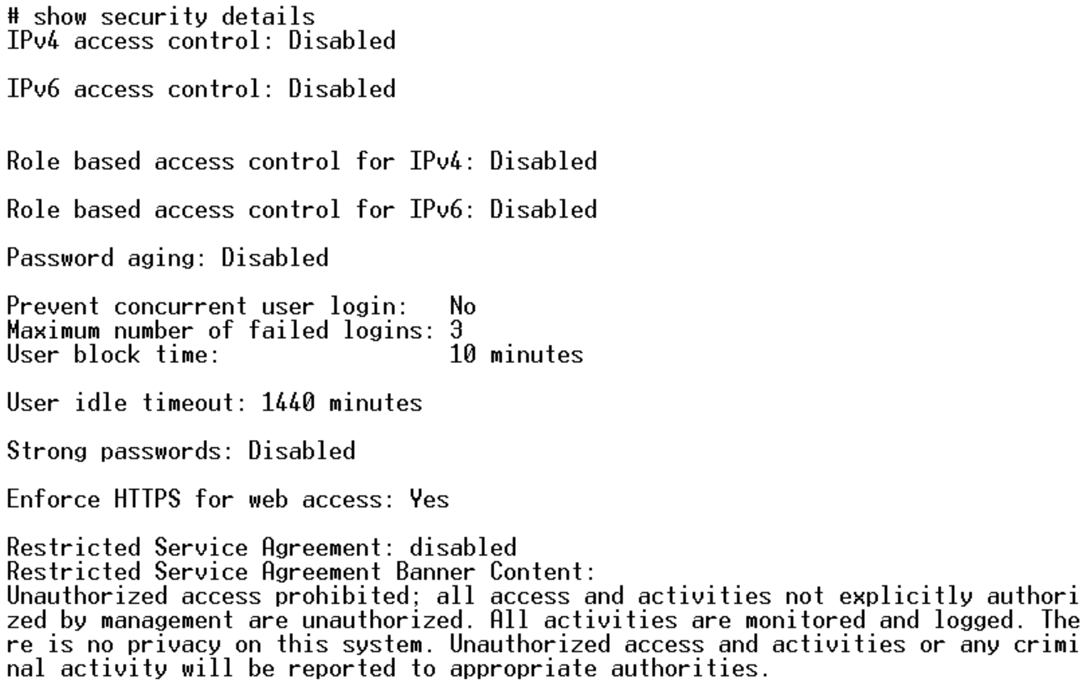
The diagram shows the output of the *show security* command.



```
# 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 313).*

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 313).*

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 338).

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 313).

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 144).

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 144).

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 539).

```
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 410).*

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 ***Disabling the Automatic Management Function*** (on page 257).

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.

Setting the Networking Mode

If your EMX device is implemented with both wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command enables the wired or wireless networking mode.

```
config:#   network mode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and the EMX does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Configuring IP Protocol Settings

By default, only the IPv4 protocol is enabled. You can enable both the IPv4 and IPv6 protocols, or only the IPv6 protocol for your EMX device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command determines which IP protocol is enabled on the EMX.

```
config:#   network ip proto <protocol>
```

Variables:

- <protocol> is one of the options: *v4Only*, *v6Only* or *both*.

Mode	Description
v4Only	Enables IPv4 only on all interfaces. This is the default.

Mode	Description
v6Only	Enables IPv6 only on all interfaces.
both	Enables both IPv4 and IPv6 on all interfaces.

Selecting IPv4 or IPv6 Addresses

This command determines which IP address is used when the DNS server returns both of IPv4 and IPv6 addresses. You need to configure this setting only after both IPv4 and IPv6 protocols are enabled on the EMX.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variables:

- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

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 347).

- **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.
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

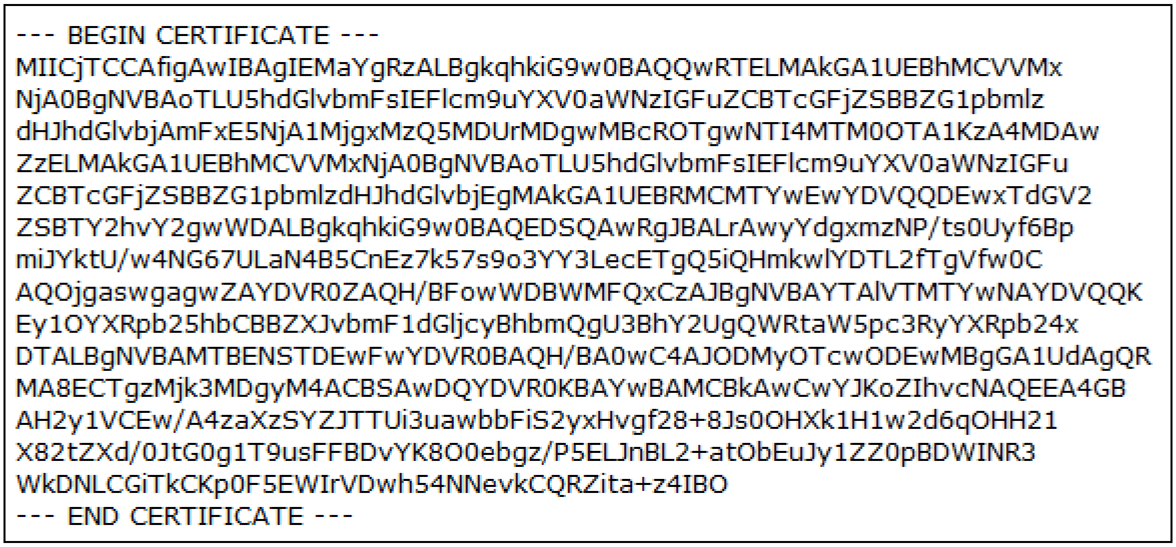
This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

To provide a CA certificate:

1. Make sure you have entered the configuration mode. See ***Entering Configuration Mode*** (on page 338).
2. Type the following command and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.



```
--- BEGIN CERTIFICATE ---
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAkGA1UEBhMCVVMx
NjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFuZCBTcGFjZSBBZG1pbmlz
dHJhdGlvbjAmFxE5NjA1MjgxMzQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAw
ZzELMAkGA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGFu
ZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEwYDVQQDEwxTdGV2
ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwRgJBALrAwyYdgxmzNP/ts0Uyf6Bp
miJYktU/w4NG67ULaN4B5CnEz7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0C
AQOjgaswgagwZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQQK
Ey1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRtaW5pc3RyYXRpb24x
DTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0wC4AJODMyOTcwODEwMBgGA1UdAgQR
MA8ECTgzMjk3MDgyM4ACBSAwDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GB
AH2y1VCEw/A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOHH21
X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atObEuJy1ZZ0pBDWINR3
WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZita+z4IBO
--- END CERTIFICATE ---
```

5. Select and copy the contents 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
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

   ```
   config:#
   ```

Setting the BSSID

This command 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 IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

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 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

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 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your EMX device. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Subnet Mask

After selecting the static IP configuration mode, you can use this command to define the subnet mask.

```
config:#   network ipv4 subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

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 the IPv4 Primary DNS Server

After selecting the static IP configuration mode, use this command to specify the primary DNS server. If you have selected the DHCP configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv4 DHCP-Assigned DNS Server*** (on page 351).

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting the IPv4 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command to specify the secondary DNS server. If you have selected the DHCP configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv4 DHCP-Assigned DNS Server*** (on page 351).

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

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

Overriding the IPv4 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

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*.

► **Add a static route:**

```
config:#   network ipv4 staticRoutes add <dest-1> <hop>
```

► **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>
```

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.
- <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*.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

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 preferredHostName <name>
```

Variables:

- <name> is a host name which:
    - Consists of alphanumeric characters and/or hyphens
    - Cannot begin or end with a hyphen
    - Cannot contain more than 63 characters
    - Cannot contain punctuation marks, spaces, and other symbols

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 ipAddress <ip address>
```

Variables:

- <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 the IPv6 Primary DNS Server

After selecting the static IP configuration mode, use this command to specify the primary DNS server. If you have selected the automatic configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 355).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. This value uses the IPv6 address format.

Setting the IPv6 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command to specify the secondary DNS server. If you have selected the automatic configuration mode, you still can manually specify DNS servers with this command and then override the DHCP-assigned DNS servers. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 355).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. This value uses the IPv6 address format.

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

Overriding the IPv6 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

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*.

▶ **Add a static route:**

```
config:#   network ipv6 staticRoutes add <dest-1> <hop>
```

▶ **Delete a static route**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> <dest-2> <hop>
```

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.
- <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.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network interface*.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The EMX selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the EMX device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

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.
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 type a valid SSH public key for each user profile to log in over the SSH connection. See ***Specifying the SSH Public Key*** (on page 397).

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 the Service Advertisement

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See ***Enabling Service Advertisement*** (on page 127) 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.

Mode	Description
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.

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 365).*

- **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 366).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See ***Setting NTP Parameters*** (on page 366).
- Make the customized NTP servers override the DHCP-assigned ones. See ***Overriding DHCP-Assigned NTP Servers*** (on page 367).

This command is available either in the administrator/user mode or in the configuration mode. See ***Different CLI Modes and Prompts*** (on page 313).

► **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.
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 431).*

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.

Option	Description
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.

If the Restricted Service Agreement feature is enabled, the Restricted Service Agreement is displayed when any user logs in to the EMX. Do either of the following, or you cannot successfully log in to the EMX:

- 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, press the Space bar.

- 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 338).*

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 431).

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.

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 431).

▶ 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 431).

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.
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 431).*

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 431).*

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 338).
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 431).

▶ 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 431).

► 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.

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 403).

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 431).

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 399).*

- **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 338).
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 338).

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 431).

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 396).*

▶ 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 403).
- <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

Privilege	Description
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 403).
- <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 403).
- <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 417).*

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 417).*

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 340).*

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 431).

- **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
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℃ and Upper Critical threshold to 24℃ 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 431).

▶ **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.
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 534).
- <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 532).

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 431).

▶ 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.

Note: To specify the Z coordinate using the rack units, see **Setting the Z Coordinate Format for Environmental Sensors** *(on page 340).*

- <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

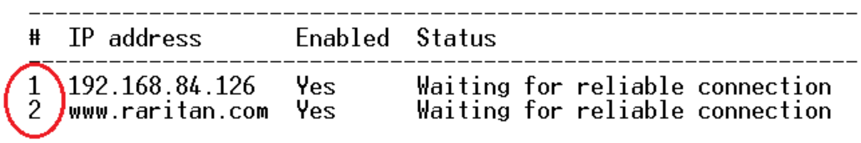
This command removes a monitored IT device from the server reachability list.

```
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 431).

▶ 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
```

USB-Cascading Configuration Commands

A USB-cascading configuration command begins with *cascading*. You can set the cascading mode on the master device.

Note: You CANNOT change the cascading mode on slave devices.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#   cascading mode <mode>
```

Variables:

- <mode> is one of the following cascading modes:

Mode	Description
bridging	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.

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset sensor (if any) or the settings of LEDs on the asset sensor.

Asset Sensor Management

An asset sensor management configuration command begins with `assetStrip`.

Naming an Asset Sensor

This command syntax names or changes the name of an asset sensor connected to the EMX device.

```
config:#   assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset sensor connected to the EMX device.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Note: For the Raritan asset sensor, a rack unit refers to a tag port.

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <number> is the total number of rack units available on the connected asset sensor. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset sensors connected to the EMX device. The numbering mode changes the rack unit numbers.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset sensors connected to the EMX device.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <number> is a starting number for numbering rack units on the connected asset sensor. This value is an integer number.

Specifying the Asset Sensor Orientation

This command syntax specifies the orientation of the asset sensors connected to the EMX device. Usually you do not need to perform this command unless your asset sensors do NOT come with the tilt sensor, causing the EMX unable to detect the asset sensors' orientation.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset sensor #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 sensor(s) to indicate the absence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Rack Unit Configuration

For the Raritan asset sensor, a rack unit refers to a tag port. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset sensor.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset sensor follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See ***Setting LED Colors for Connected Tags*** (on page 425) and ***Setting LED Colors for Disconnected Tags*** (on page 426). 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 428) and ***Setting an LED Mode for a Rack Unit*** (on page 428) 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 sensor. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it. See **Setting LED Colors for Connected Tags** *(on page 425) and* **Setting LED Colors for Disconnected Tags** *(on page 426).*

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the EMX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.
blinkSlow	This mode has the LED blink slowly.

Mode	Description
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Sensor 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 needed when the EMX works in conjunction with Raritan's Dominion LX KVM switch. The 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 device type on the serial port. Select this option unless your EMX cannot correctly detect the connected device.
forceConsole	The port enters the local console state.
forceAnalogModem	The port enters the analog modem state.

Option	Description
forceGsmModem	The port enters the GSM modem state.

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 313).

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.

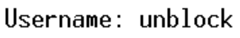
```
#     control actuator 8 on
```

Unblocking a User

If any user is blocked from accessing the EMX, you can unblock them at the local console.

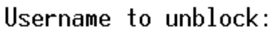
To unblock a user:

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 310).
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 478) 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 313).

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.

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.

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
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	—	—	—
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		1-wire signal for external environmental sensor packages

Serial RS-232 Port Pinouts

RS-232 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

RS-485 Port Pinouts

RS-485 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	—	—	—
2	—	—	—
3	D+	bi-directional	Data +
4	—	—	—
5	—	—	—
6	D-	bi-directional	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 454).*

▶ To use a USB drive to configure the EMX or upgrade firmware:

1. Verify that both the USB drive and your EMX meet the requirements. See ***System and USB Requirements*** (on page 444).
2. Prepare required configuration files. See ***Configuration Files*** (on page 444).
3. Copy required configuration files to the root directory of the USB drive.
   - For firmware upgrade, an appropriate firmware binary file is also required.
4. Plug the USB drive into the USB-A port of the EMX.
5. The initial message shown on the front panel display depends on the first task performed by the EMX.
   - If no firmware upgrade task will be performed, a happy smiley as shown below is displayed after around 30 seconds.

     =-]
   - If the USB drive contains the firmware upgrade data, the EMX first performs the firmware upgrade, showing the upgrade message on the front panel display, and then shows the happy smiley when the firmware upgrade completes successfully. See ***Firmware Upgrade via USB*** (on page 453).
6. After the happy smiley appears, press and hold one of the control buttons next to the front panel display for one second until the display turns blank.
7. Wait for several seconds until the EMX resumes normal operation, indicated by the normal message of the front panel display.

Tip: You can remove the USB drive and plug it into another EMX for performing the same task(s) once the happy smiley or the firmware upgrade message displays.

If nothing is shown on the display and no task is performed after plugging the USB drive, check the log file in the USB drive.

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 contents using the firmware which was running when plugging the USB drive into the EMX, not the new firmware after firmware upgrade.

▶ **USB drive requirements:**

- The drive must contain a single partition formatted as a Windows FAT32 filesystem.
- The drive must contain a configuration file called *fwupdate.cfg* in its root directory. See ***fwupdate.cfg*** (on page 446).

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 446).

- **config.txt:**

  This file is used for configuring device settings. See ***config.txt*** (on page 449).

- **devices.csv:**

  This file is required only when there are device-specific settings to configure for multiple EMX devices. See ***devices.csv*** (on page 451).

Raritan provides a Mass Deployment Utility, which helps you to quickly generate all configuration files for your EMX. See ***Creating Configuration Files via Mass Deployment Utility*** (on page 452).

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 a single = character, without any surrounding spaces. Keys are not case sensitive.

This section only explains common options of 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 449).

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 451).

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 **Saving the EMX Configuration** *(on page 288) 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 EMX Device Settings** *(on page 290) 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.

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 446).

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.

You can use Raritan's Mass Deployment Utility to create this file by yourself, or contact Raritan to get a device configuration file specific to your EMX model and firmware version.

▶ 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 a single = character, 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 451)
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}
   ```

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 of the USB drive.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See ***fwupdate.cfg*** (on page 446).

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
  ```

Creating Configuration Files via Mass Deployment Utility

The Mass Deployment Utility is an Excel file that lets you fill in basic information required for the three configuration files, such as the admin account and password.

After entering required information, you can generate all configuration files with only one click, including *fwupdate.cfg*, *config.txt* and *devices.csv*.

▶ To use the Mass Deployment Utility:

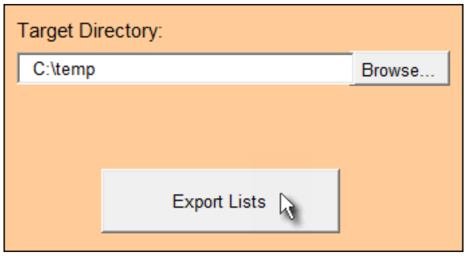
1. Download the Mass Deployment Utility from the Raritan website.
   - The utility is named *mass_deployment-xxx* (where xxx is the version number).
   - It is available on the EMX section of the ***Support page*** (***http://www.raritan.com/support/***).
2. Make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility. See the user documentation accompanying your Excel.
3. Launch Excel to open this utility.

   Note: Other office suites, such as OpenOffice and LibreOffice, are not supported.

4. Read the instructions in the 1st spreadsheet of the utility.
5. Enter information in the 2nd and 3rd spreadsheets.
   - The 2nd spreadsheet contains information required for *fwupdate.cfg* and *config.txt*.
   - The 3rd spreadsheet contains device-specific information for *devices.csv*.
6. Return to the 2nd spreadsheet to execute the export macro.

   a. In the Target Directory field, specify the folder where to generate the configuration files. For example, you can specify the connected USB drive.

   b. Click Export Lists to generate configuration files.



Target Directory:

C:\temp

7. Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade any EMX with these files. See ***Configuration or Firmware Upgrade with a USB Drive*** (on page 443).

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 446).

▶ 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.
   - **=-[** (sad smiley): Failed. Check the log file in the USB drive or contact Raritan Technical Support to look into the failure cause.

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 443).

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 444) or contact Raritan Technical Support to properly prepare some or all of the following files:
   - *fwupdate.cfg (always required)*

- *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 455).
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 456)
   - ***DHCP IPv6 Configuration in Windows*** (on page 466)
   - ***DHCP IPv4 Configuration in Linux*** (on page 473)
   - ***DHCP IPv6 Configuration in Linux*** (on page 475)
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 454).

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

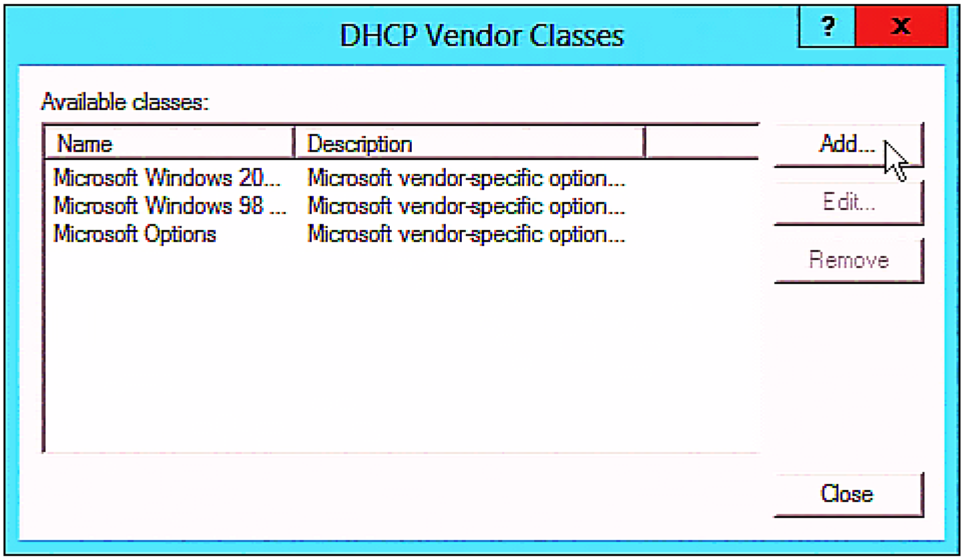
For those EMX devices using IPv4 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

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.

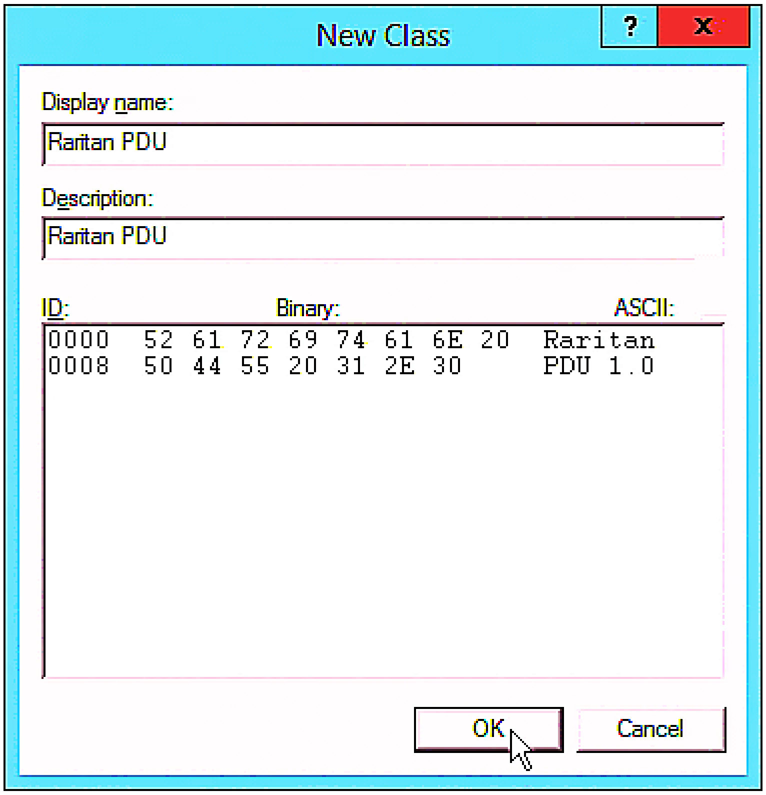
   b. Click Add to add a new vendor class.



Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

   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.



Display name: Raritan PDU

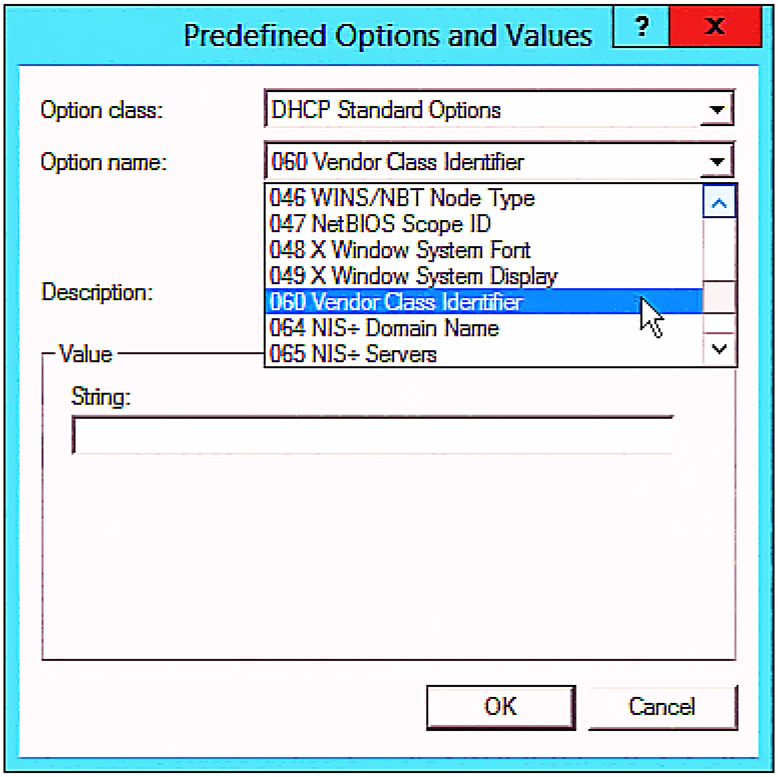
Description: Raritan PDU

```
ID:         Binary:                       ASCII:
0000    52 61 72 69 74 61 6E 20   Raritan
0008    50 44 55 20 31 2E 30      PDU 1.0
```

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.



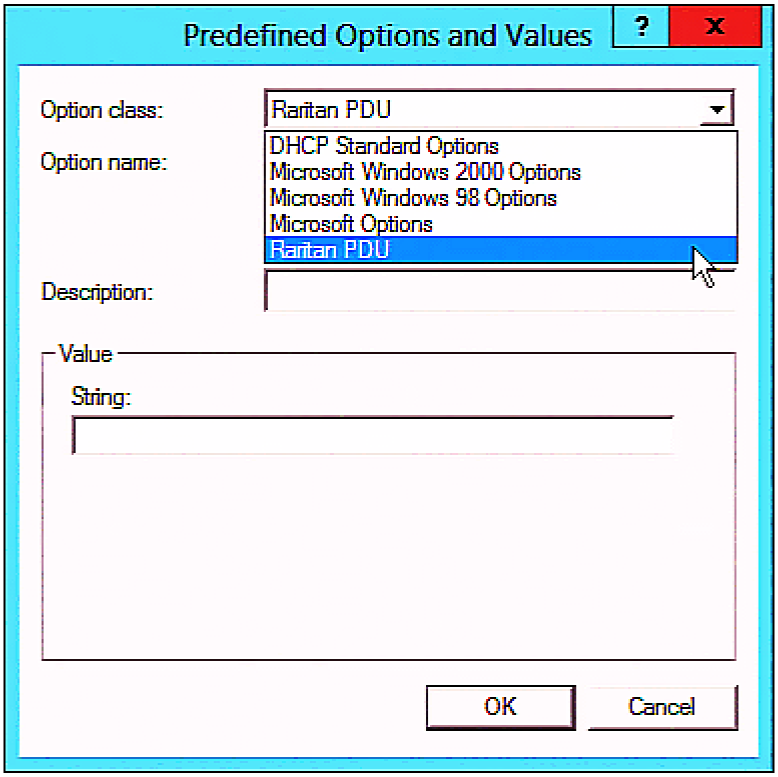
Predefined Options and Values

Option class: DHCP Standard Options

Option name: 060 Vendor Class Identifier

3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

a. Select Raritan PDU in the "Option class" field.


Predefined Options and Values
?
X
DHCP Standard Options
Microsoft Windows 2000 Options
Microsoft Windows 98 Options
Microsoft Options
Raritan PDU
Value
OK
Cancel

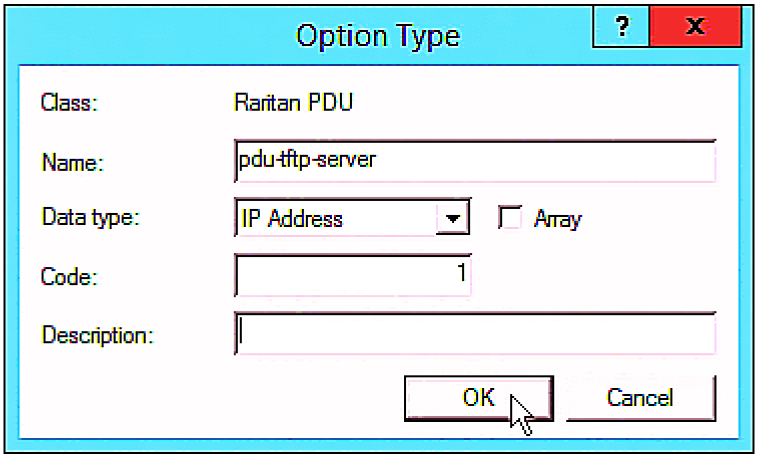
Option class: Raritan PDU

Option name:

Description:

String:

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.



Class: Raritan PDU

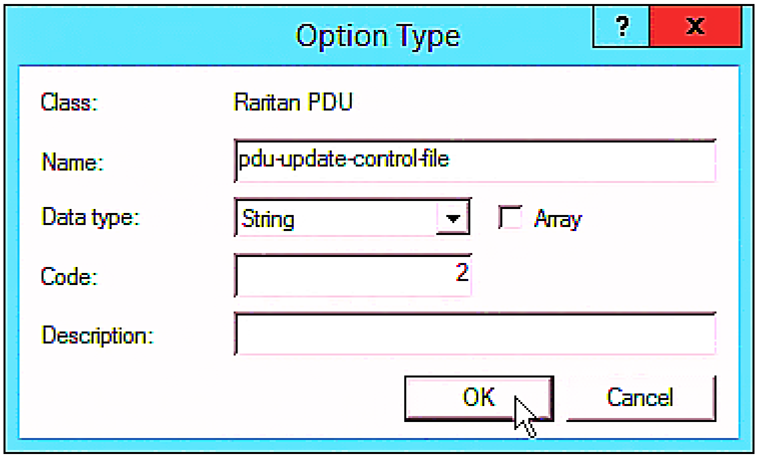
Name: pdu-tftp-server

Data type: IP Address □ Array

Code: 1

Description:

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.



Class: Raritan PDU

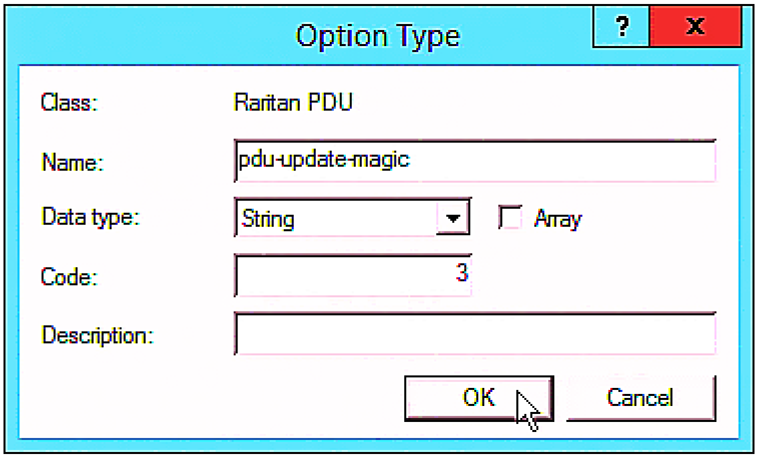
Name: pdu-update-control-file

Data type: String ☐ Array

Code: 2

Description:

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.



Class: Raritan PDU

Name: pdu-update-magic

Data type: String ☐ Array

Code: 3

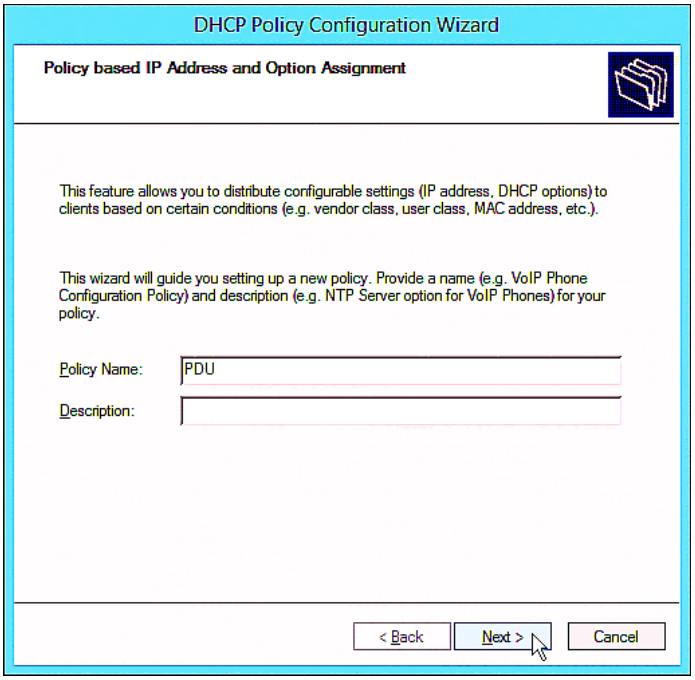
Description:

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.



DHCP Policy Configuration Wizard

Policy based IP Address and Option Assignment

This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

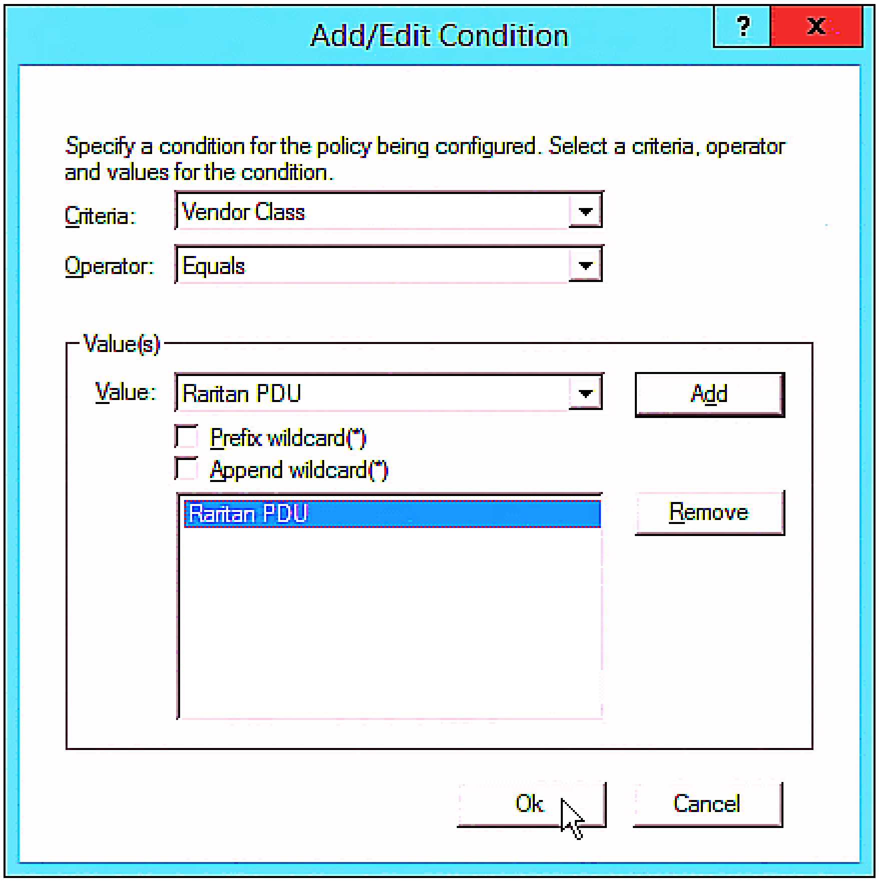
This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name: PDU

Description:

c. Click Add to add a new condition.

d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.



Add/Edit Condition

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria: Vendor Class

Operator: Equals

Value(s)

Value: Raritan PDU

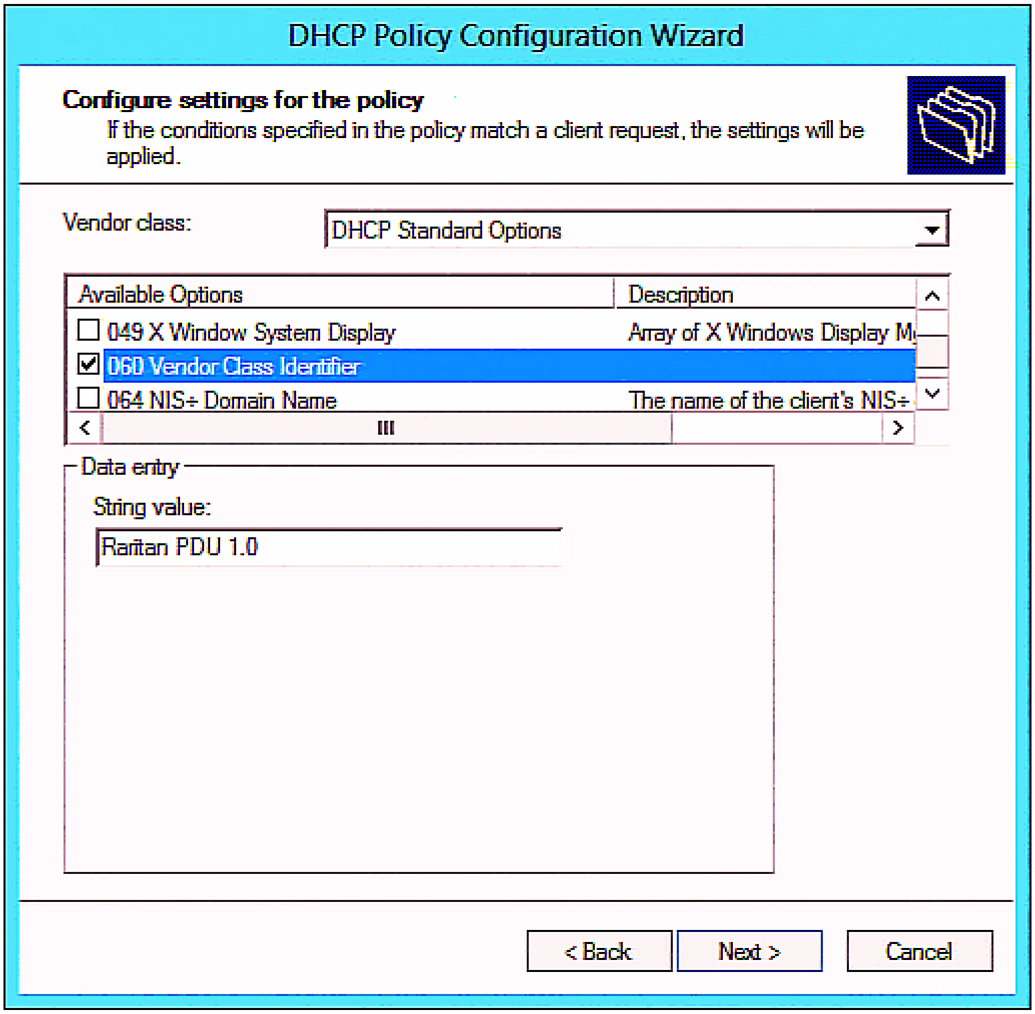
□ Prefix wildcard(*)

□ Append wildcard(*)

Raritan PDU

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.



DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.

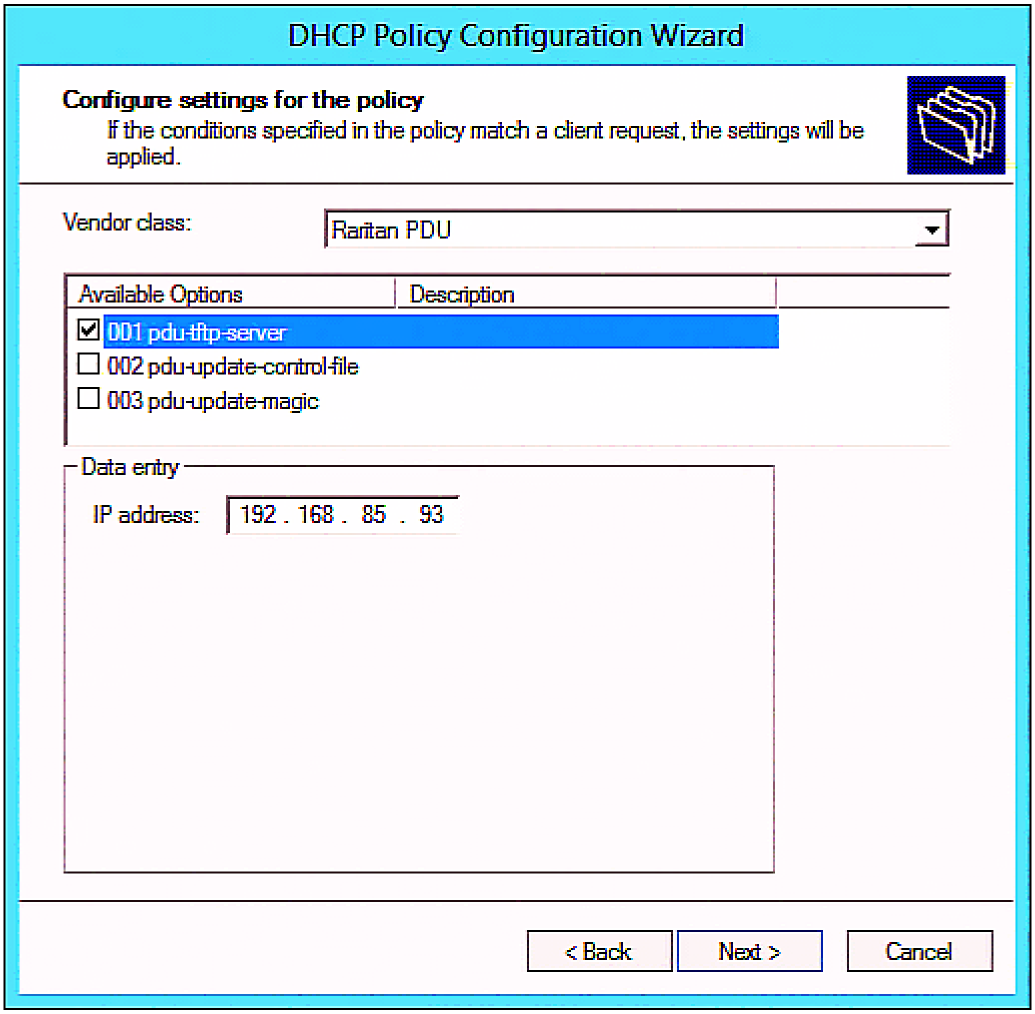
Vendor class: DHCP Standard Options

Available Options	Description
☐ 049 X Window System Display	Array of X Windows Display M
☑ 060 Vendor Class Identifier	
☐ 064 NIS+ Domain Name	The name of the client's NIS+

Data entry

String value: Raritan PDU 1.0

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.



DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.

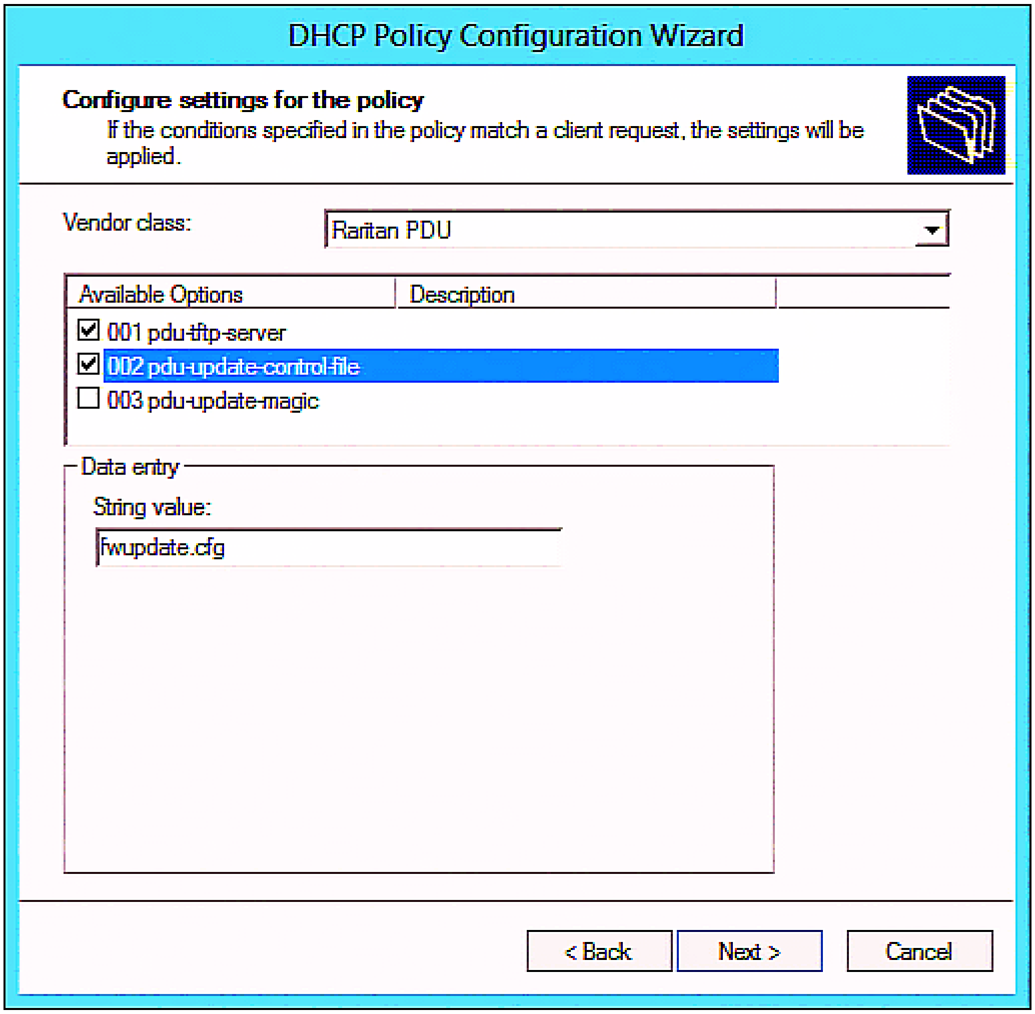
Vendor class: Raritan PDU

Available Options	Description
☑ 001 pdu-tftp-server	
□ 002 pdu-update-control-file	
□ 003 pdu-update-magic	

Data entry

IP address: 192 . 168 . 85 . 93

h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: Raritan PDU

Available Options	Description
☑ 001 pdu-tftp-server	
☑ 002 pdu-update-control-file	
□ 003 pdu-update-magic	

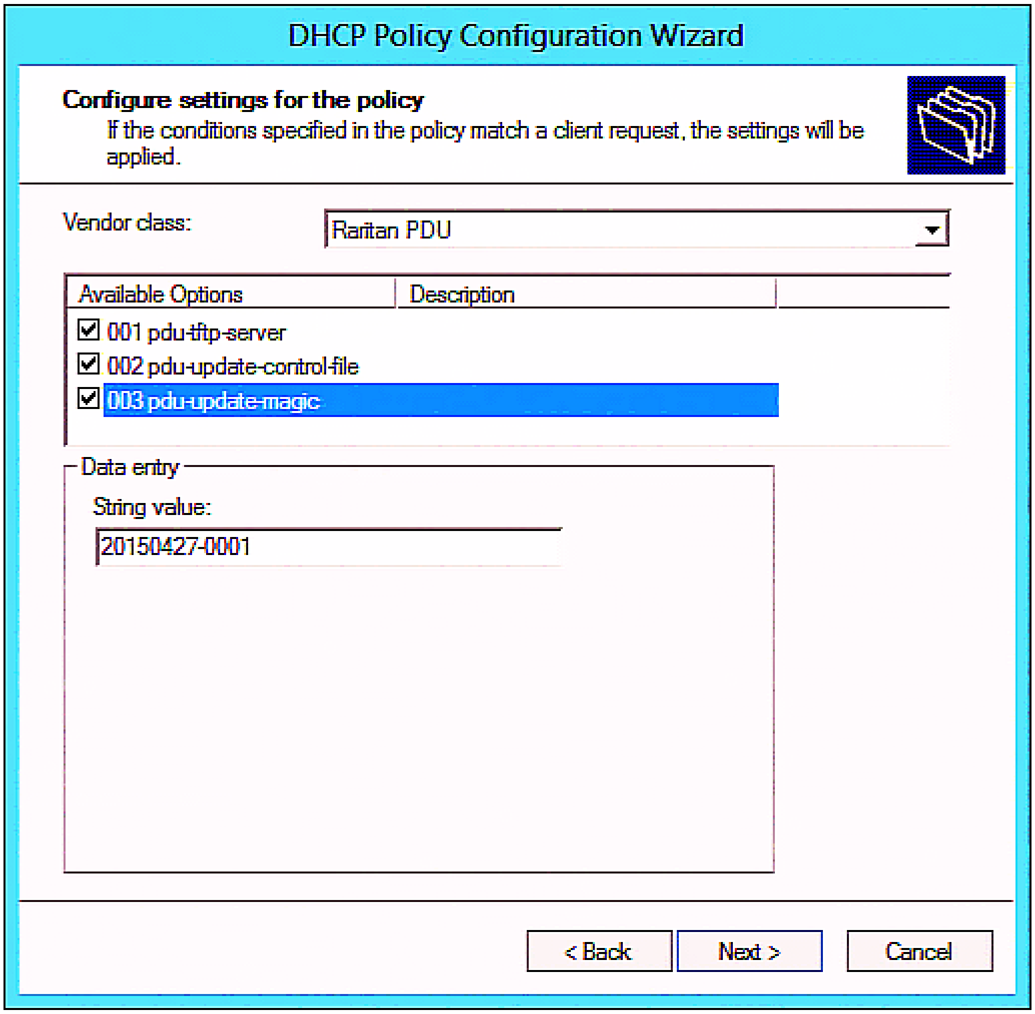
Data entry

String value: fwupdate.cfg

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.

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 Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.

Vendor class: Raritan PDU

Available Options	Description
☑ 001 pdu-tftp-server	
☑ 002 pdu-update-control-file	
☑ 003 pdu-update-magic	

Data entry

String value: 20150427-0001

DHCP IPv6 Configuration in Windows

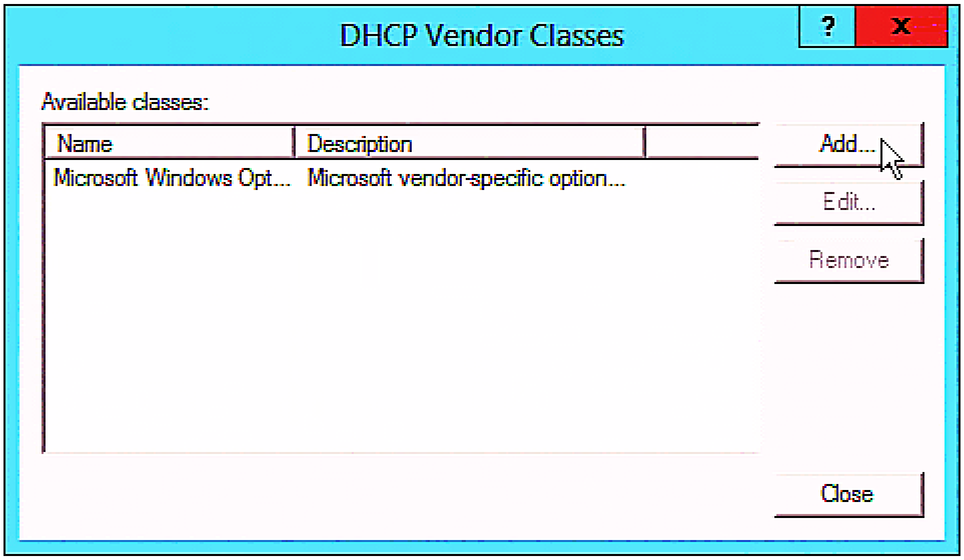
For those EMX devices using IPv6 addresses, follow this procedure to configure your DHCP server. The following illustration is based on Microsoft® Windows Server 2012 system.

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.

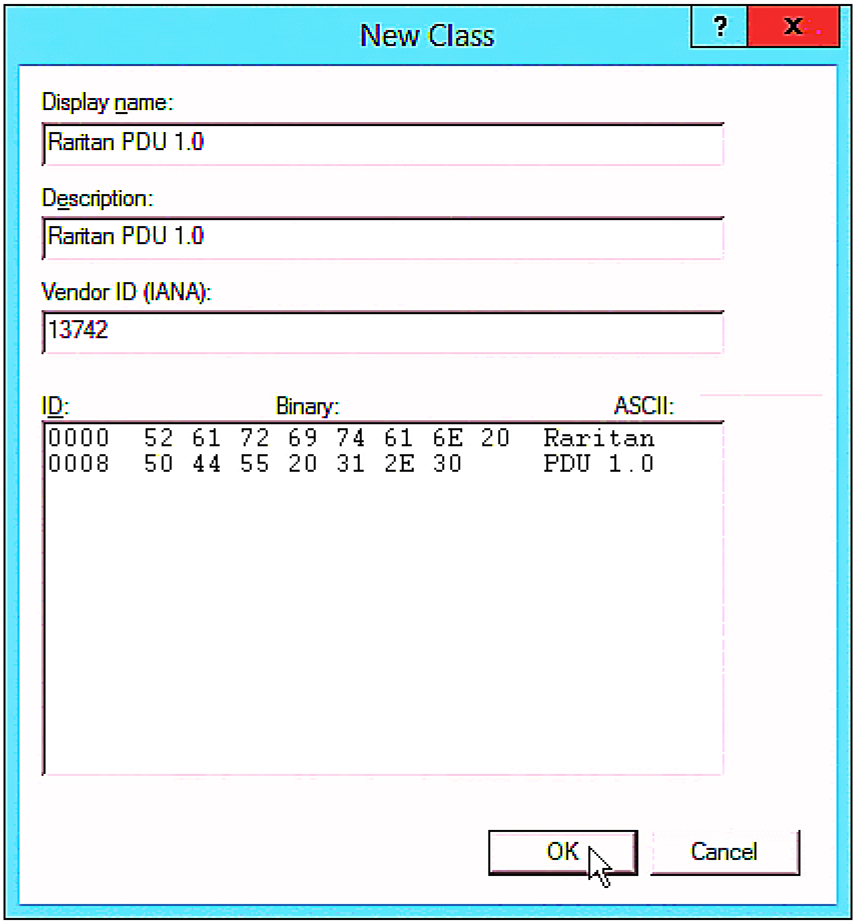
b. Click Add to add a new vendor class.



Name	Description
Microsoft Windows Opt...	Microsoft vendor-specific option...

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.



Display name:
Raritan PDU 1.0

Description:
Raritan PDU 1.0

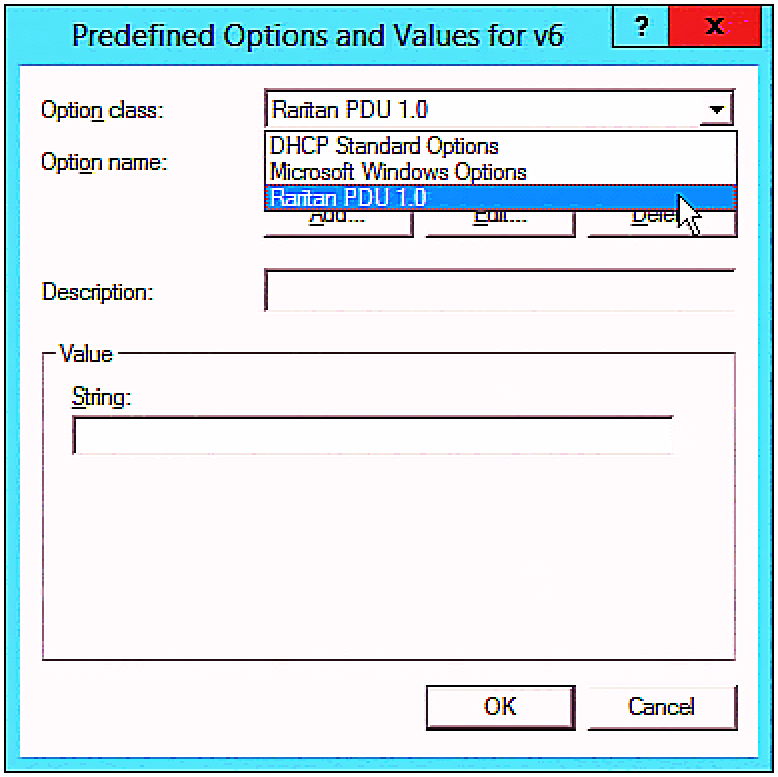
Vendor ID (IANA):
13742

```
ID:                 Binary:                        ASCII:
0000   52 61 72 69 74 61 6E 20    Raritan
0008   50 44 55 20 31 2E 30       PDU 1.0
```

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.



Predefined Options and Values for v6

Option class: Raritan PDU 1.0

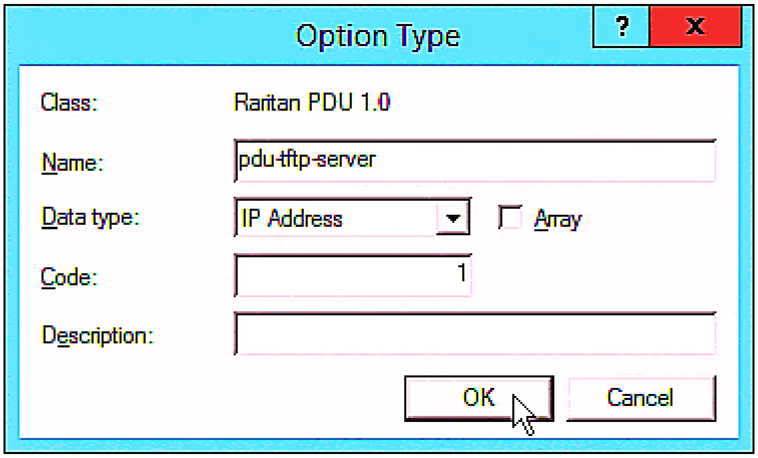
Option name:

Description:

Value

String:

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.



Option Type

Class: Raritan PDU 1.0

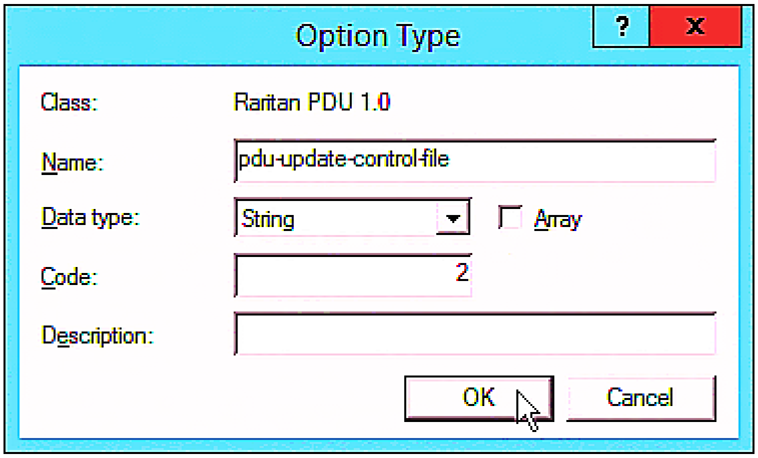
Name: pdu-tftp-server

Data type: IP Address ☐ Array

Code: 1

Description:

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.



Class: Raritan PDU 1.0

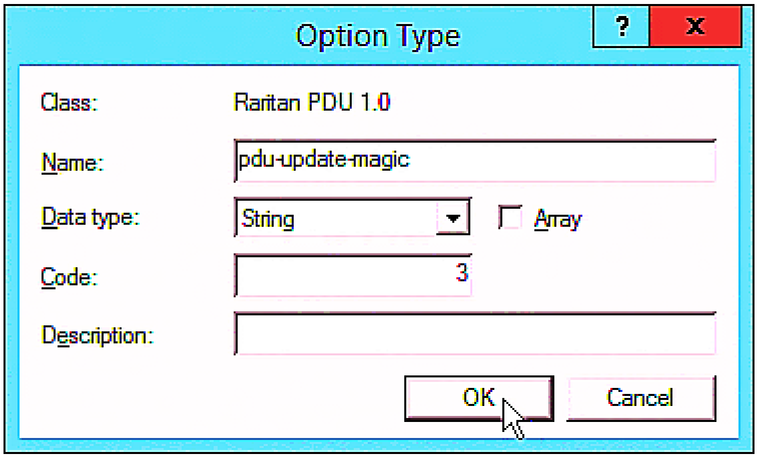
Name: pdu-update-control-file

Data type: String □ Array

Code: 2

Description:

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.



Class: Raritan PDU 1.0

Name: pdu-update-magic

Data type: String □ Array

Code: 3

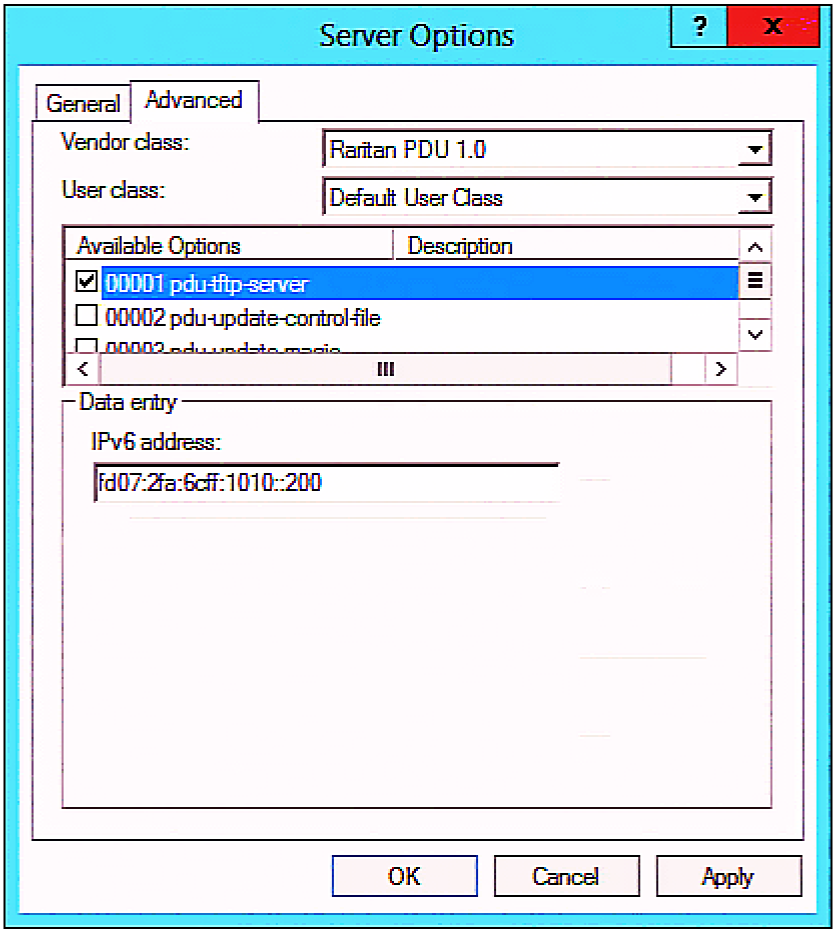
Description:

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.



Server Options

General | Advanced

Vendor class: Raritan PDU 1.0

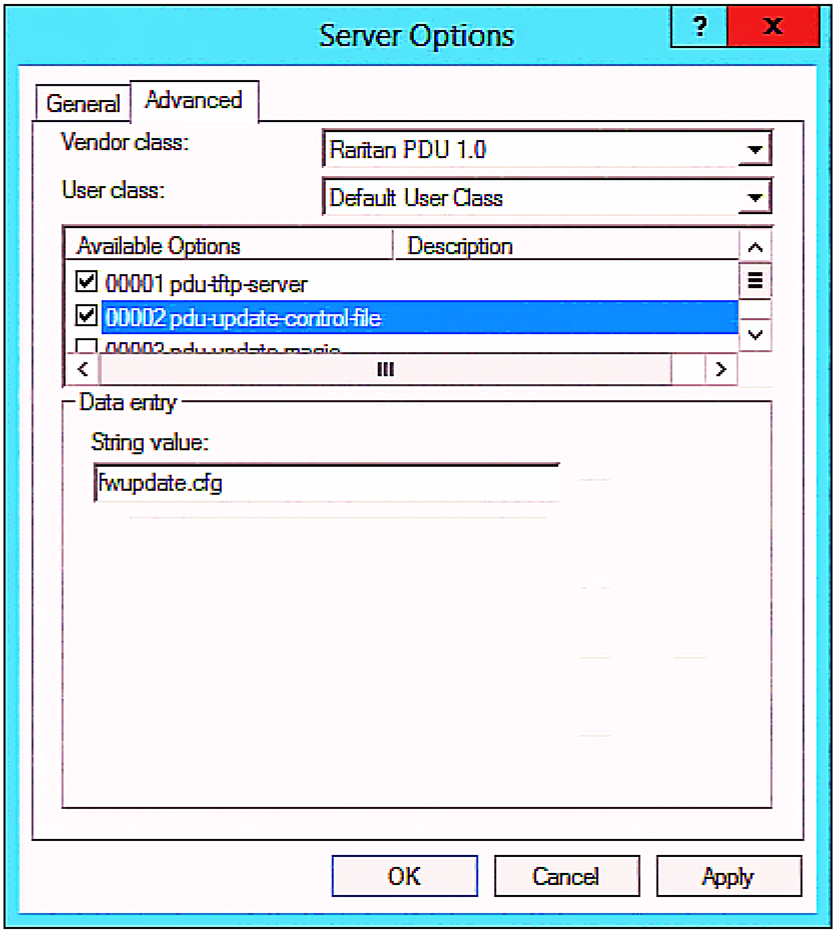
User class: Default User Class

Available Options	Description
☑ 00001 pdu-tftp-server	
□ 00002 pdu-update-control-file	
□ 00003 pdu-update-magic	

Data entry

IPv6 address: fd07:2fa:6cff:1010::200

d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.



Vendor class: Raritan PDU 1.0

User class: Default User Class

☑ 00001 pdu-tftp-server

☑ 00002 pdu-update-control-file

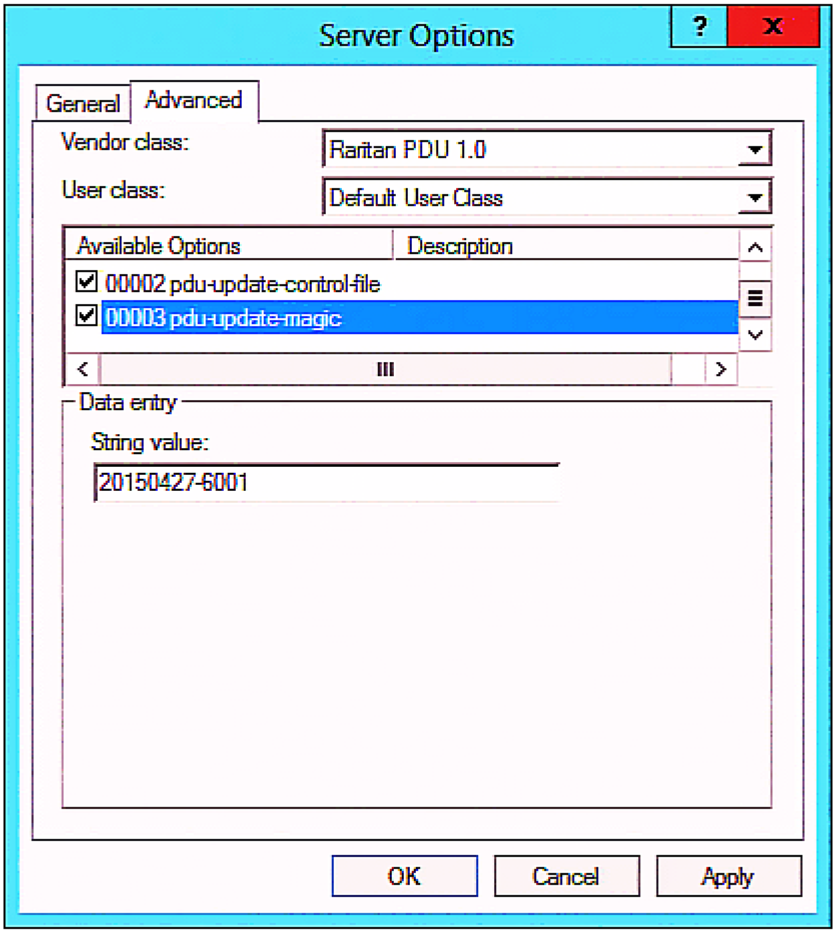
☐ 00003 pdu-update-magic

String value: fwupdate.cfg

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.



Vendor class: Raritan PDU 1.0

User class: Default User Class

☑ 00002 pdu-update-control-file

☑ 00003 pdu-update-magic

String value: 20150427-6001

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.

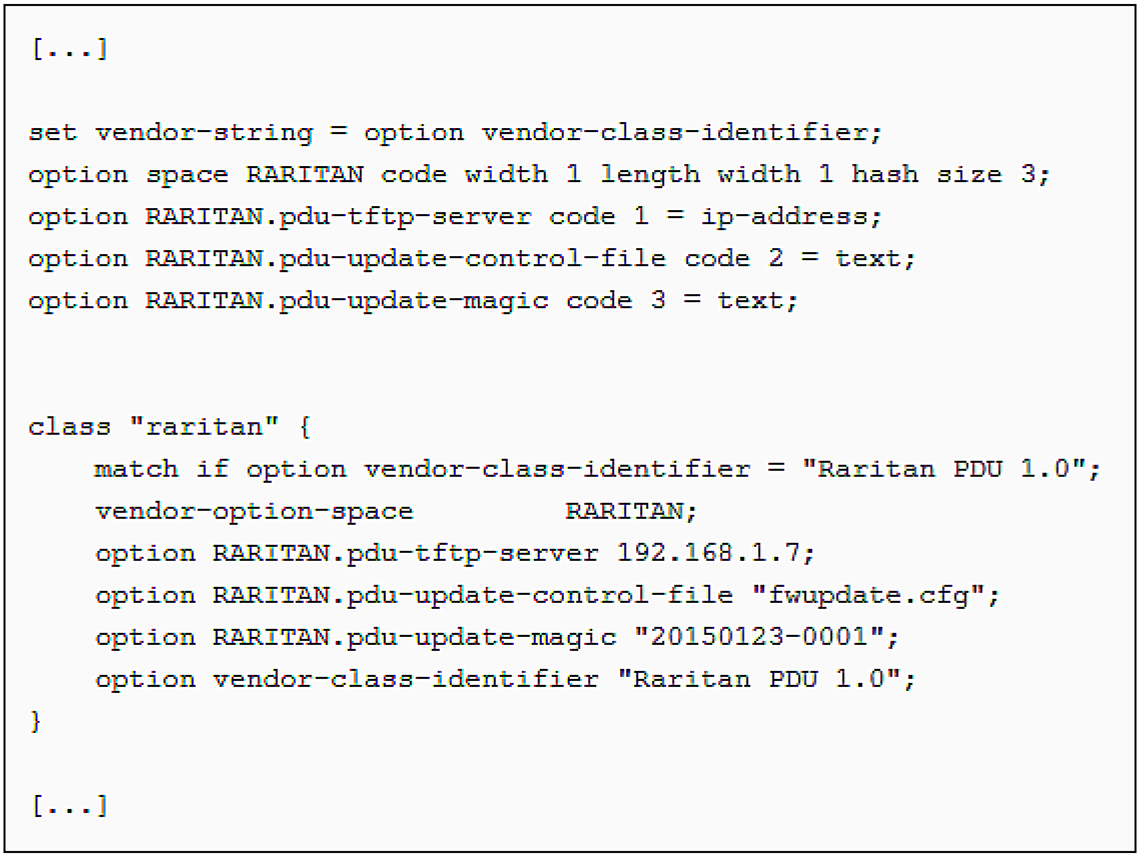
3. Set the following three sub-options in the "vendor-encapsulated-options" (option 43).
   - code 1 (pdu-tftp-server) = the TFTP server's IPv4 address
   - code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
   - code 3 (pdu-update-magic) = any string

     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

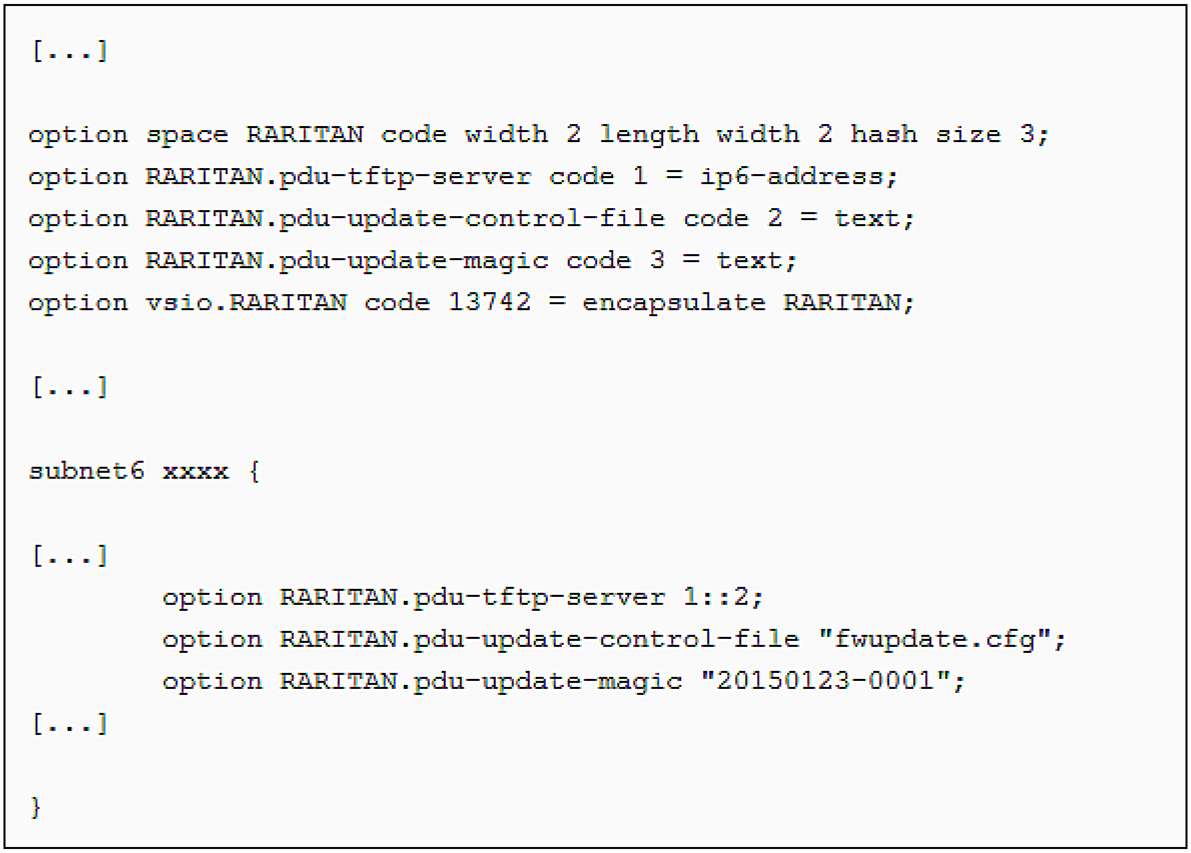
- code 2 (pdu-update-control-file) = the name of the control file "fwupdate.cfg"
- code 3 (pdu-update-magic) = any string

  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.

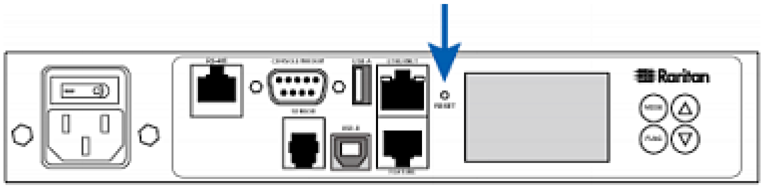
In This Chapter

Using the Reset Button

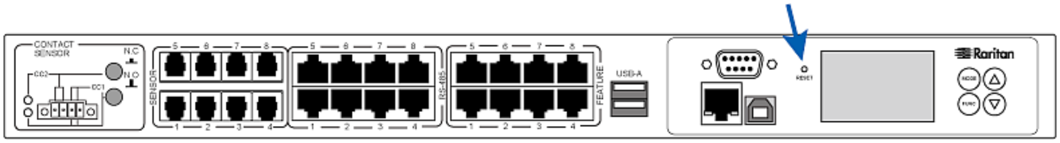
An RS-232 serial connection to a computer is required for using the reset button.

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 11).
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 309).

▶ **To reset to factory defaults after logging in to the CLI:**

1. Connect to the EMX device. See ***Logging in to CLI*** (on page 310) or ***Connecting the EMX to a Computer*** (on page 11).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the EMX. 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 Available 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 ***Firmware Update via Web Interface*** (see "***Updating the EMX Firmware***" on page 291).

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

► To update the firmware using the SCP command:

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 so the PSCP syntax is similar.
`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 287).

To save the configuration using the SCP command:

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 that you want to update.

2. Type the password when the system prompts you to type it.
3. The system saves the configuration from the EMX to a file named "bulk_config.xml."

To copy the configuration using the SCP command:

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 that you want to update.

2. Type the password when the system prompts you to type it.

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 command examples:

- Save operation's example:

```
scp  admin@192.168.87.50:/bulk_config.xml
```

- Copy operation's example:

```
scp  bulk_config.xml
admin@192.168.87.47:/bulk_restore
```

Tip: The PSCP works in a similar way to the SCP so its syntax is similar.
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 using the SCP command:

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 that you want to update.

2. Type the password when the system prompts you to type it.
3. The system saves the settings from the EMX to a file named "backup_settings.xml."

To restore the settings using the SCP command:

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 that you want to update.

2. Type the password when the system prompts you to type it.
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 command examples:

- Backup example:

```
scp  admin@192.168.87.50:/backup_settings.xml
```

- Settings restoration example:

```
scp  backup_settings.xml
admin@192.168.87.50:/settings_restore
```

Tip: The PSCP works in a similar way to the SCP so its syntax is similar.
Backup operation -- `pscp <user name>@<device ip>:/backup_settings.xml`
Restoration operation -- `pscp backup_settings.xml <user name>@<device ip>:/settings_restore`

Appendix F 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:

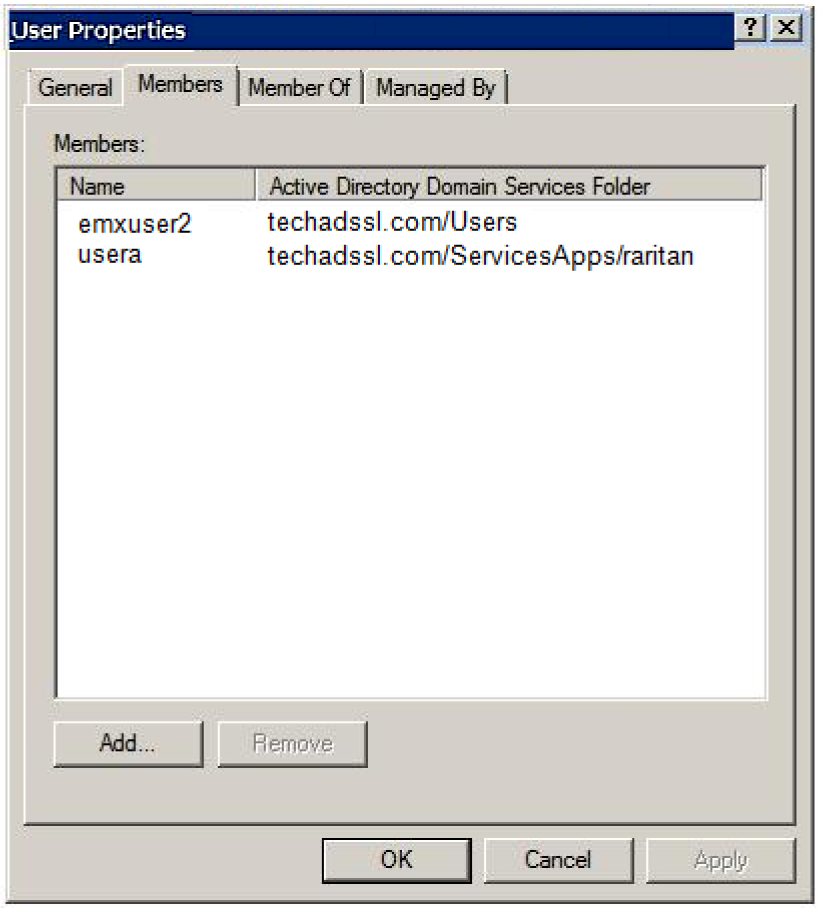
- The groups (roles) for the EMX are named *EMX_Admin* and *EMX_User*.
- User accounts *emxuser*, *emxuser2*, *usera* and *userb* already exist on the AD server.

▶ 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.

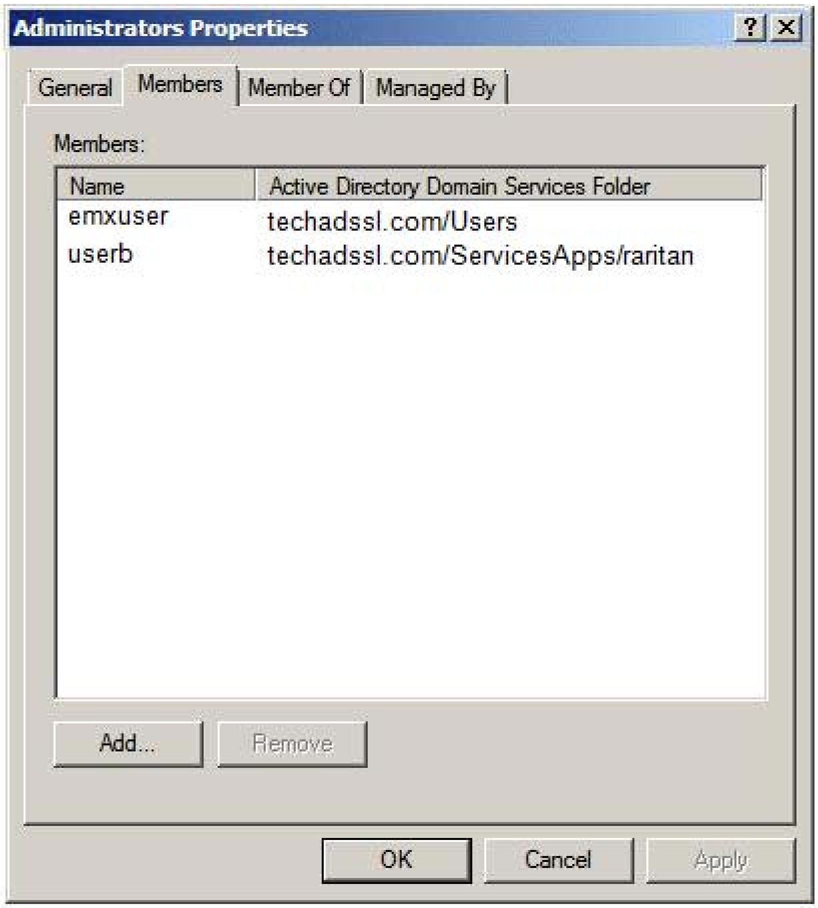
2. Add the *emxuser2* and *usera* accounts to the EMX_User group.



Members:

Name	Active Directory Domain Services Folder
emxuser2	techadssl.com/Users
usera	techadssl.com/ServicesApps/raritan

3. Add the *emxuser* and *userb* accounts to the EMX_Admin group.



Name	Active Directory Domain Services Folder
emxuser	techadssl.com/Users
userb	techadssl.com/ServicesApps/raritan

4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the EMX Device

You must enable and set up LDAP authentication properly on the EMX device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Modifying Network Settings*** (on page 114) and ***Role of a DNS Server*** (on page 120).
- 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.

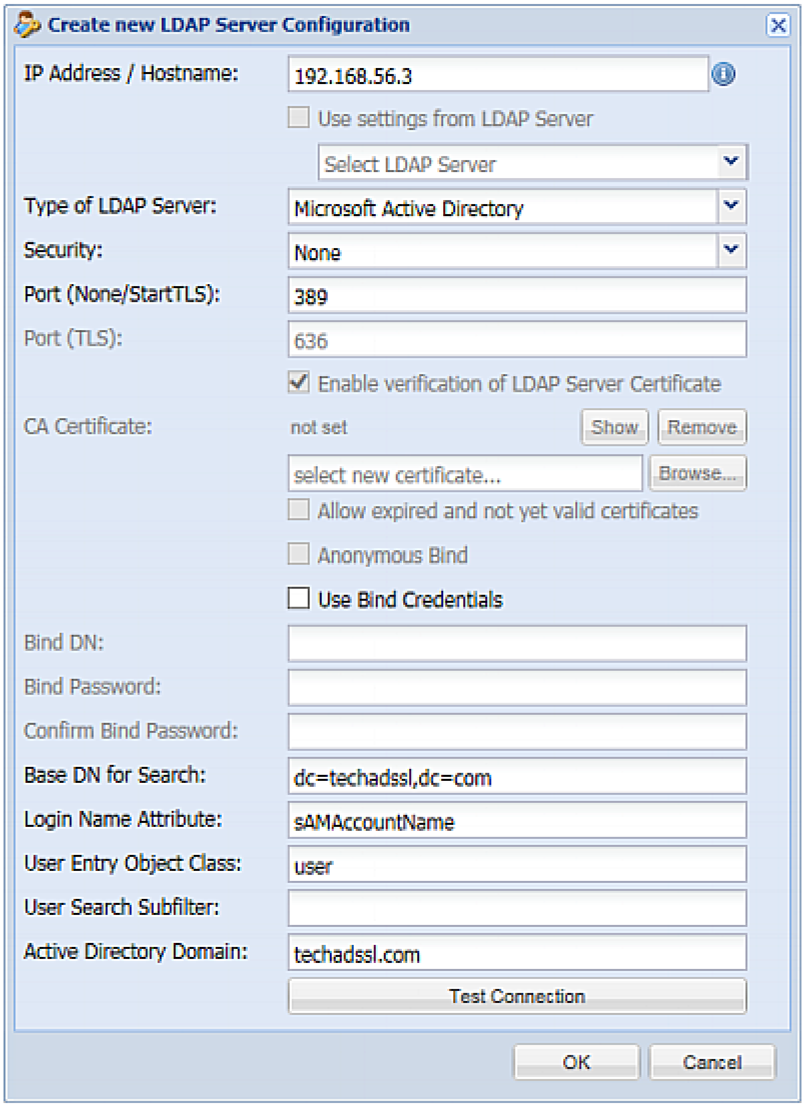
To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate the LDAP/LDAPS authentication.
3. Click New to add an LDAP/LDAPS AA server. The "Create new LDAP Server Configuration" dialog appears.
4. Provide the EMX with the information about the AD server.
   - IP Address / Hostname - Type the domain name `techadssl.com` or IP address `192.168.56.3`.

   Important: Without the TLS 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 TLS encryption is enabled.

   - Use settings from LDAP server - Leave the checkbox deselected.
   - Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
   - 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) and CA Certificate - Skip the two fields since the TLS encryption is not enabled.
   - Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.
   - Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.

- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.



Create new LDAP Server Configuration

IP Address / Hostname: 192.168.56.3

□ Use settings from LDAP Server

Select LDAP Server

Type of LDAP Server: Microsoft Active Directory

Security: None

Port (None/StartTLS): 389

Port (TLS): 636

☑ Enable verification of LDAP Server Certificate

CA Certificate: not set

select new certificate...

□ Allow expired and not yet valid certificates

□ Anonymous Bind

□ Use Bind Credentials

Bind DN:

Bind Password:

Confirm Bind Password:

Base DN for Search: dc=techadssl,dc=com

Login Name Attribute: sAMAccountName

User Entry Object Class: user

User Search Subfilter:

Active Directory Domain: techadssl.com

5. Click OK. The LDAP server is saved.
6. Click OK. 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.

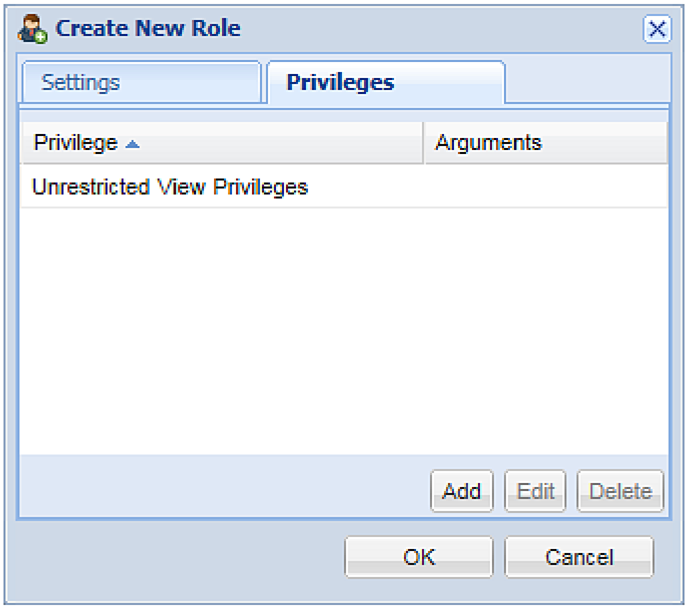
▶ To create the EMX_User role with appropriate permissions assigned:

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

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

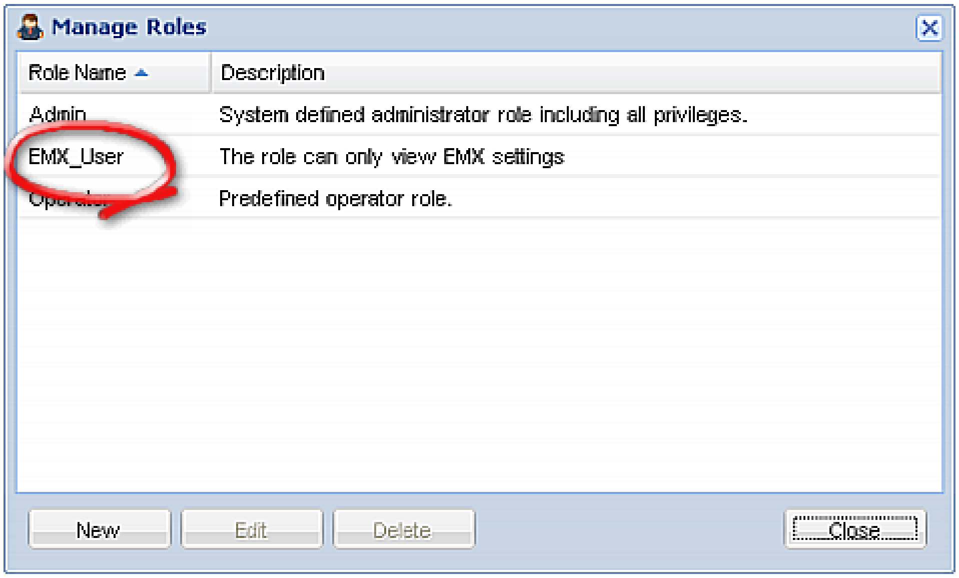
2. Click New. The Create New Role dialog appears.
3. Type `EMX_User` in the Role Name field.
4. Type a description for the EMX_User role in the Description field. In this example, we type "The role can only view EMX settings" to describe the role.
5. Click the Privileges tab to select "Unrestricted View Privileges," which includes all View permissions. The "Unrestricted View Privileges" permission lets users view all settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission "Unrestricted View Privileges" from the Privileges list.

c. Click Add.



Privilege ▲	Arguments
Unrestricted View Privileges	

6. Click OK. The EMX_User role is created.



Role Name ▲	Description
Admin	System defined administrator role including all privileges.
EMX_User	The role can only view EMX settings
Operator	Predefined operator role.

7. Keep the Manage Roles dialog opened to create the EMX_Admin role.

▶ **To create the EMX_Admin role with full permissions assigned:**

1. Click New. The Create New Role dialog appears.
2. Type `EMX_Admin` in the Role Name field.

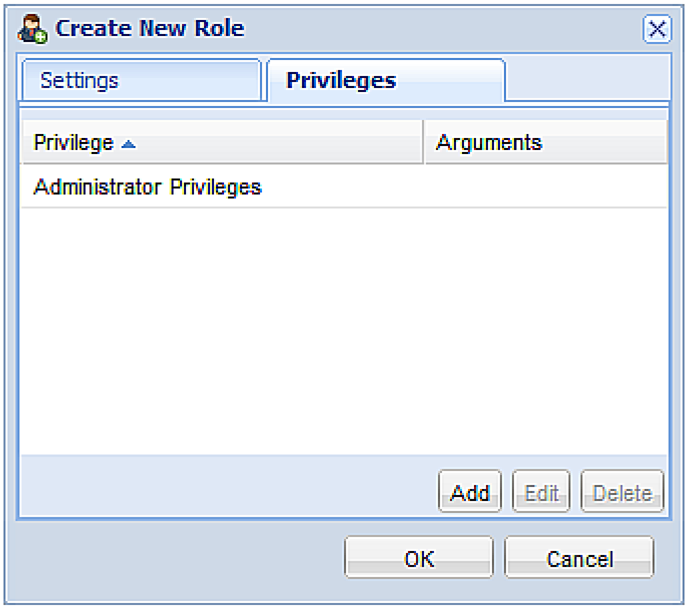
3. Type a description for the EMX_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.

4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all EMX settings.

    a. Click Add. The "Add Privileges to new Role" dialog appears.

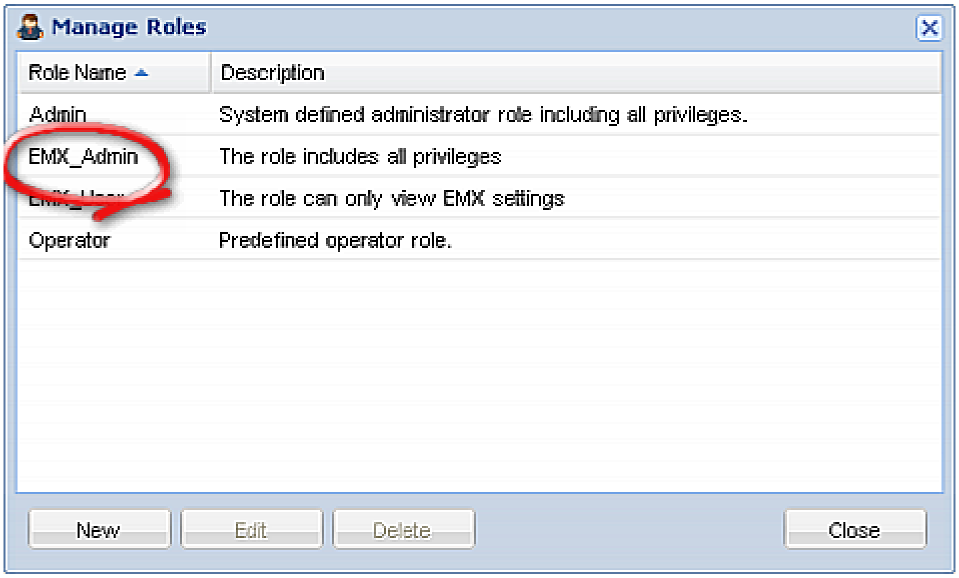
    b. Select the permission named Administrator Privileges from the Privileges list.

    c. Click Add.



Privilege ▲	Arguments
Administrator Privileges	

5. Click OK. The EMX_Admin role is created.



Role Name ▲	Description
Admin	System defined administrator role including all privileges.
EMX_Admin	The role includes all privileges
EMX_User	The role can only view EMX settings
Operator	Predefined operator role.

6. Click Close to quit the dialog.

Appendix G 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.

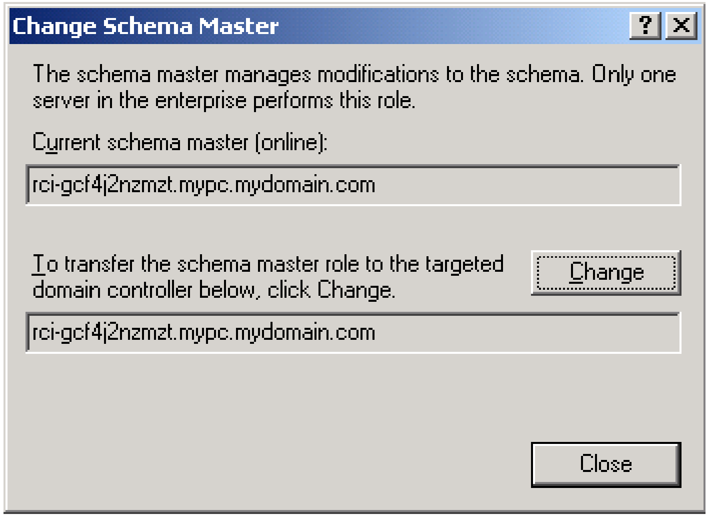
1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.
2. Run Active Directory Console and select Active Directory Schema.

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.



Change Schema Master

The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

Current schema master (online):

rci-gcf4j2nzmzt.mypc.mydomain.com

To transfer the schema master role to the targeted domain controller below, click Change.

rci-gcf4j2nzmzt.mypc.mydomain.com

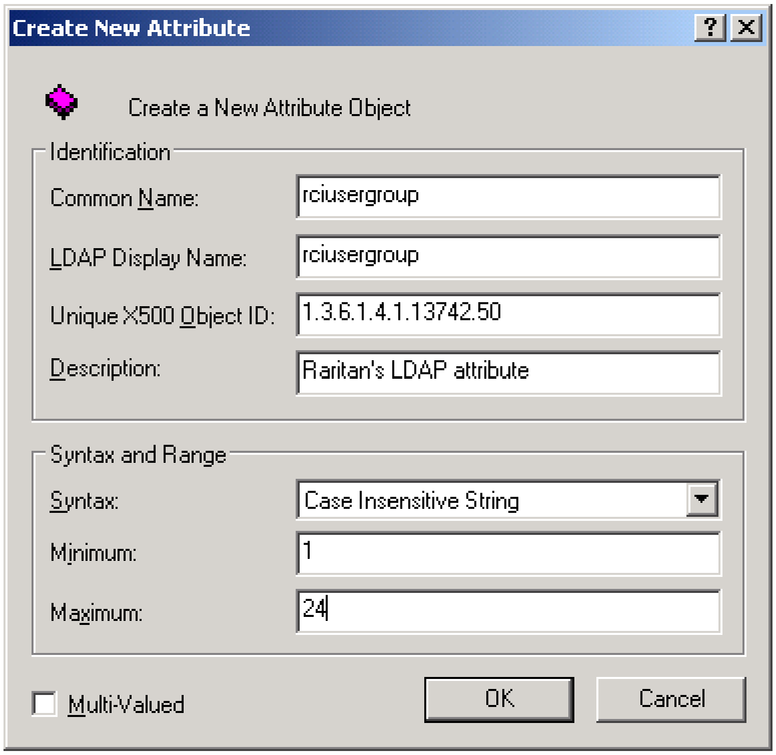
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**
3. Click OK.

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.


Create New Attribute

Create a New Attribute Object

Identification

Common Name: rciusergroup

LDAP Display Name: rciusergroup

Unique X500 Object ID: 1.3.6.1.4.1.13742.50

Description: Raritan's LDAP attribute

Syntax and Range

Syntax: Case Insensitive String

Minimum: 1

Maximum: 24

□ Multi-Valued

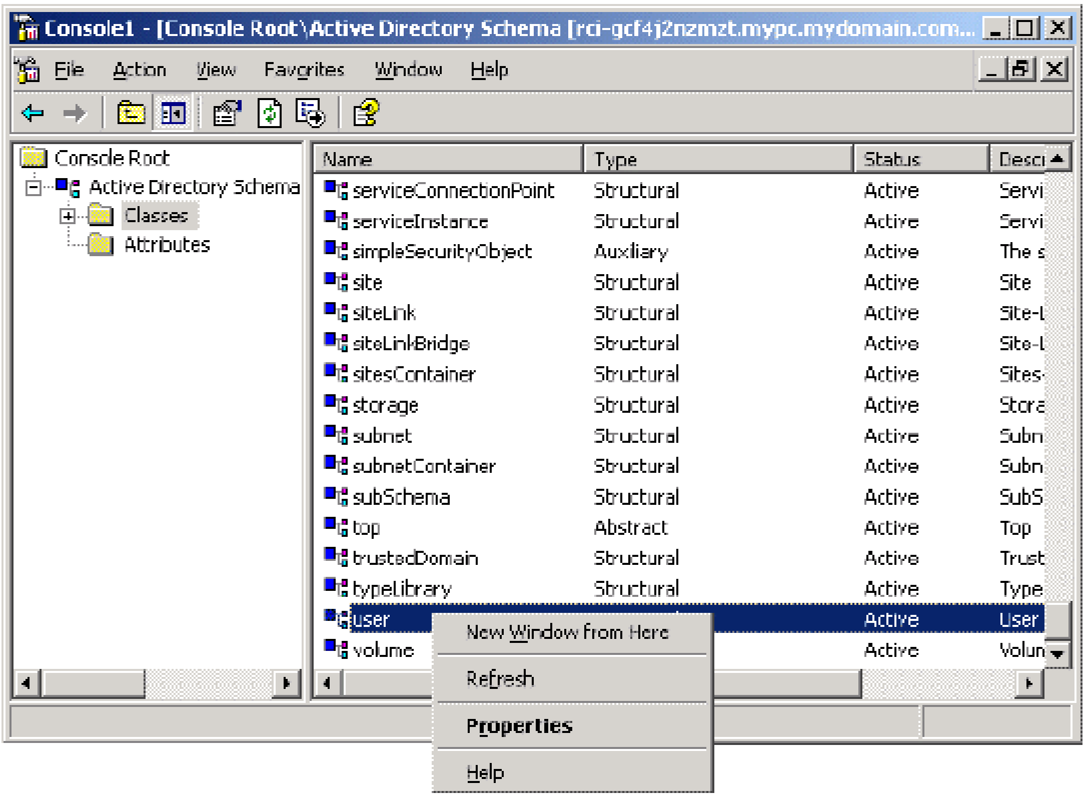
4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String 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.



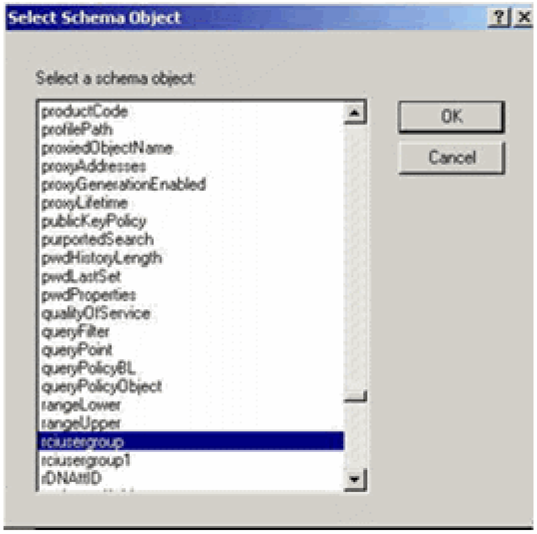
Name	Type	Status	Desci
serviceConnectionPoint	Structural	Active	Servi
serviceInstance	Structural	Active	Servi
simpleSecurityObject	Auxiliary	Active	The s
site	Structural	Active	Site
siteLink	Structural	Active	Site-l
siteLinkBridge	Structural	Active	Site-l
sitesContainer	Structural	Active	Sites-
storage	Structural	Active	Stora
subnet	Structural	Active	Subn
subnetContainer	Structural	Active	Subn
subSchema	Structural	Active	SubS
top	Abstract	Active	Top
trustedDomain	Structural	Active	Trust
typeLibrary	Structural	Active	Type
user		Active	User
volume		Active	Volun

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

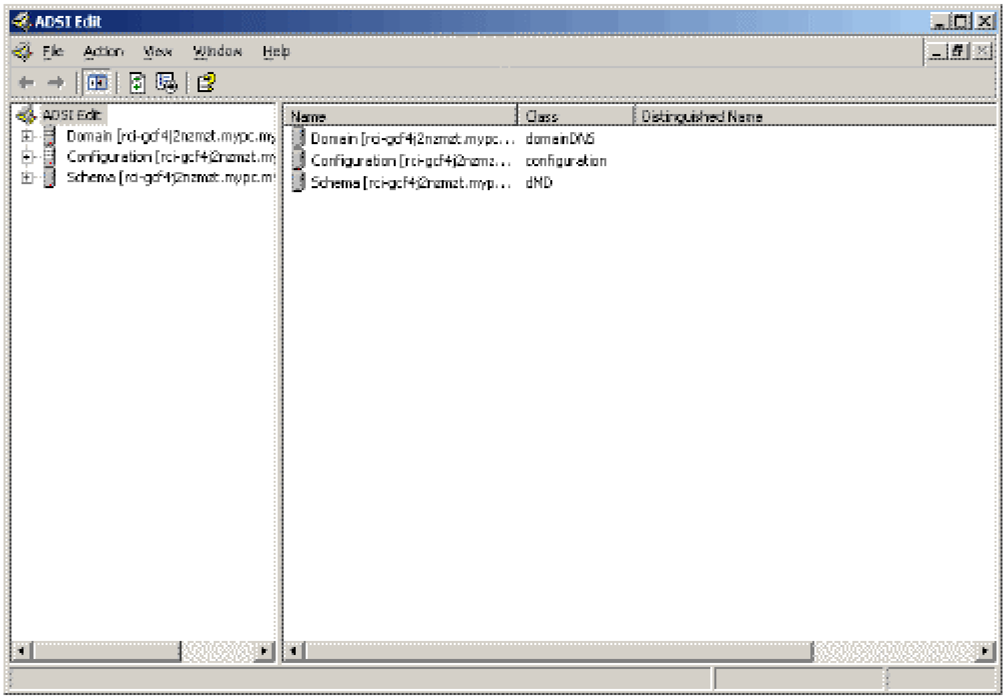
To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level 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.

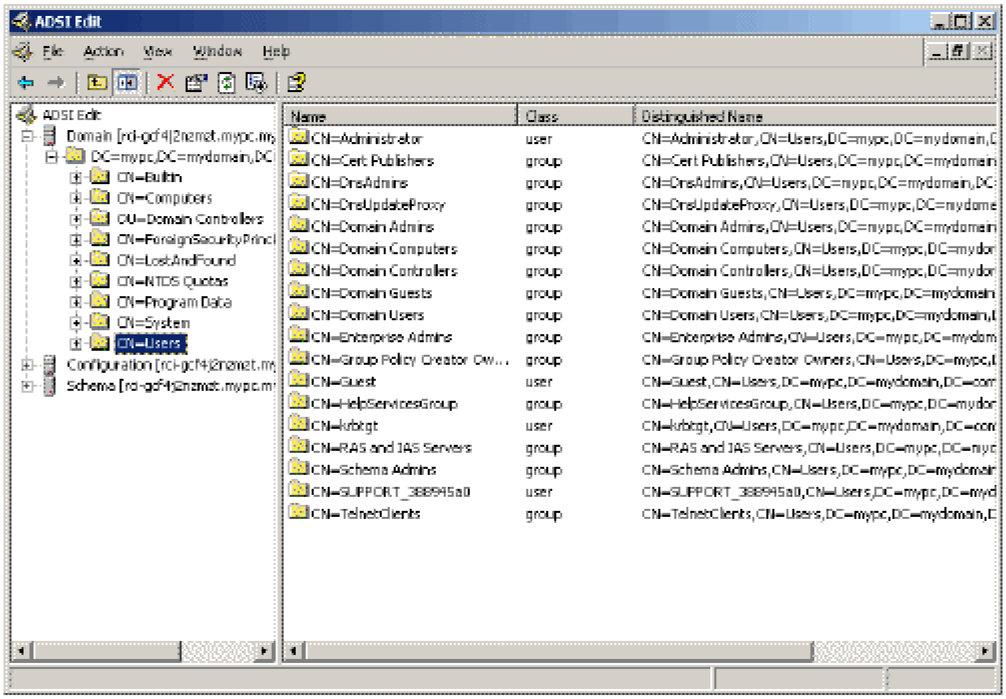
3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.


ADSI Edit
File
Action
View
Window
Help
ADSI Edit
Domain [rci-gcf4j2nzmzt.mypc.my
Configuration [rci-gcf4j2nzmzt.my
Schema [rci-gcf4j2nzmzt.mypc.m

Name	Class	Distinguished Name
Domain [rci-gcf4j2nzmzt.mypc...	domainDNS	
Configuration [rci-gcf4j2nzmz...	configuration	
Schema [rci-gcf4j2nzmzt.myp...	dMD	

4. Open the Domain.

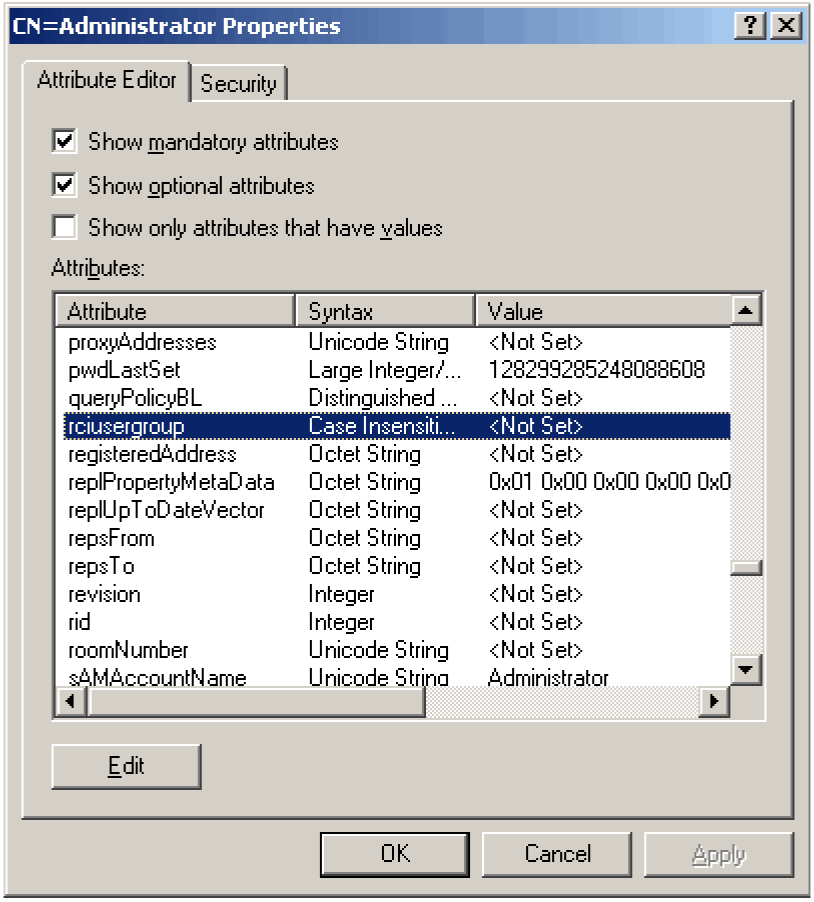
5. In the left pane of the window, select the CN=Users folder.



Name	Class	Distinguished Name
CN=Administrator	user	CN=Administrator,CN=Users,DC=mypc,DC=mydomain,D
CN=Cert Publishers	group	CN=Cert Publishers,CN=Users,DC=mypc,DC=mydomain
CN=DnsAdmins	group	CN=DnsAdmins,CN=Users,DC=mypc,DC=mydomain,DC:
CN=DnsUpdateProxy	group	CN=DnsUpdateProxy,CN=Users,DC=mypc,DC=mydome
CN=Domain Admins	group	CN=Domain Admins,CN=Users,DC=mypc,DC=mydomain
CN=Domain Computers	group	CN=Domain Computers,CN=Users,DC=mypc,DC=mydor
CN=Domain Controllers	group	CN=Domain Controllers,CN=Users,DC=mypc,DC=mydor
CN=Domain Guests	group	CN=Domain Guests,CN=Users,DC=mypc,DC=mydomain
CN=Domain Users	group	CN=Domain Users,CN=Users,DC=mypc,DC=mydomain,I
CN=Enterprise Admins	group	CN=Enterprise Admins,CN=Users,DC=mypc,DC=mydom
CN=Group Policy Creator Ow...	group	CN=Group Policy Creator Owners,CN=Users,DC=mypc,I
CN=Guest	user	CN=Guest,CN=Users,DC=mypc,DC=mydomain,DC=com
CN=HelpServicesGroup	group	CN=HelpServicesGroup,CN=Users,DC=mypc,DC=mydor
CN=krbtgt	user	CN=krbtgt,CN=Users,DC=mypc,DC=mydomain,DC=con
CN=RAS and IAS Servers	group	CN=RAS and IAS Servers,CN=Users,DC=mypc,DC=myc
CN=Schema Admins	group	CN=Schema Admins,CN=Users,DC=mypc,DC=mydomair
CN=SUPPORT_388945a0	user	CN=SUPPORT_388945a0,CN=Users,DC=mypc,DC=myd
CN=TelnetClients	group	CN=TelnetClients,CN=Users,DC=mypc,DC=mydomain,D

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.



☑ Show mandatory attributes

☑ Show optional attributes

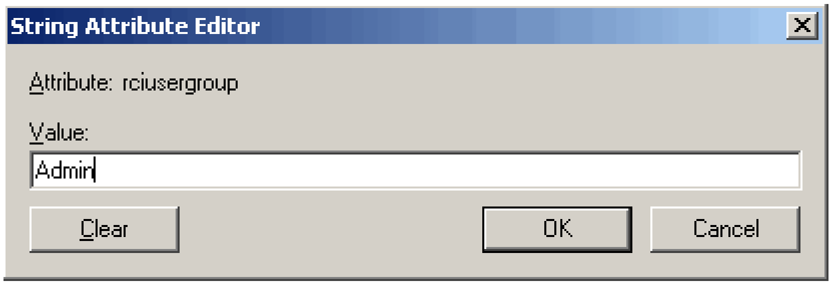
☐ Show only attributes that have values

Attributes:

Attribute	Syntax	Value
proxyAddresses	Unicode String	<Not Set>
pwdLastSet	Large Integer/...	128299285248088608
queryPolicyBL	Distinguished ...	<Not Set>
rciusergroup	Case Insensiti...	<Not Set>
registeredAddress	Octet String	<Not Set>
replPropertyMetaData	Octet String	0x01 0x00 0x00 0x00 0x0
replUpToDateVector	Octet String	<Not Set>
repsFrom	Octet String	<Not Set>
repsTo	Octet String	<Not Set>
revision	Integer	<Not Set>
rid	Integer	<Not Set>
roomNumber	Unicode String	<Not Set>
sAMAccountName	Unicode String	Administrator

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.



Attribute: rciusergroup

Value:

Admin

Appendix H 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 non-Windows RADIUS server, such as FreeRADIUS.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the EMX device. See ***Adding RADIUS Server Settings*** (on page 183).
2. Configure roles on the EMX device. See ***Creating a Role*** (on page 155).
3. Configure your RADIUS server. See ***Microsoft Network Policy Server*** (on page 501) or ***Non-Windows RADIUS Server*** (on page 525).

In This Chapter

Microsoft Network Policy Server

In this Microsoft NPS illustration, we assume that the NPS is running on the Windows 2008 system.

Three major steps are required for configuring Windows 2008 NPS:

a. Add your EMX device to NPS as a RADIUS client

b. Configure connection request policies on NPS

c. Configure a vendor-specific attribute on NPS

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See ***AD-Related Configuration*** (on page 522).

Step A: Add Your EMX as a RADIUS Client

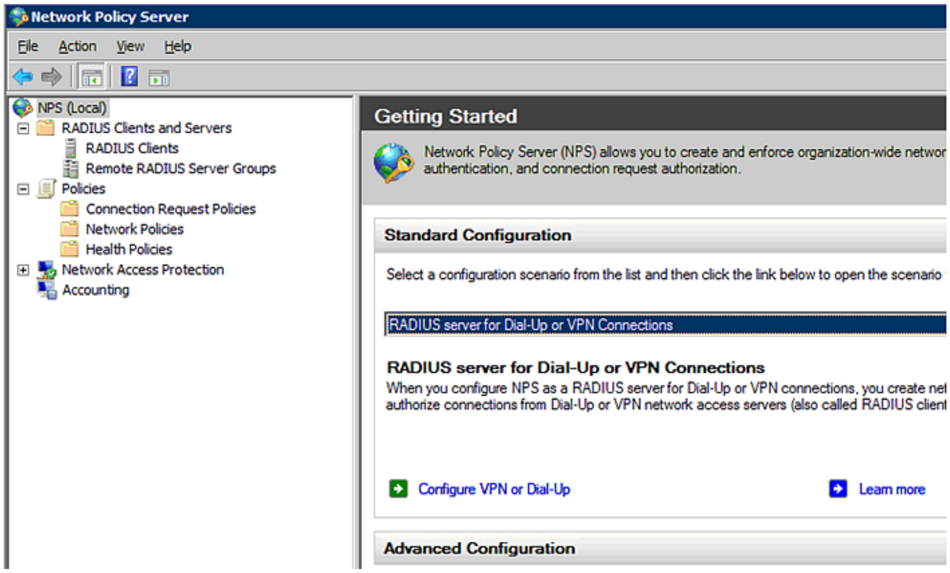
The RADIUS implementation on a EMX follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

In this illustratrion, we assume:

- 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.



Network Policy Server (NPS) allows you to create and enforce organization-wide networ authentication, and connection request authorization.

Standard Configuration

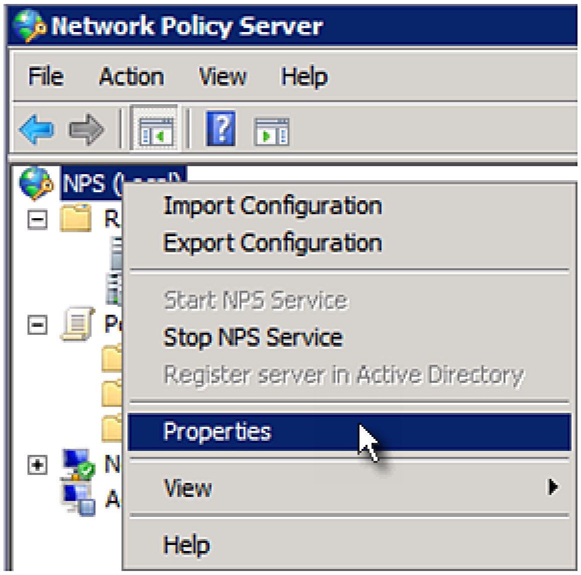
Select a configuration scenario from the list and then click the link below to open the scenario

RADIUS server for Dial-Up or VPN Connections

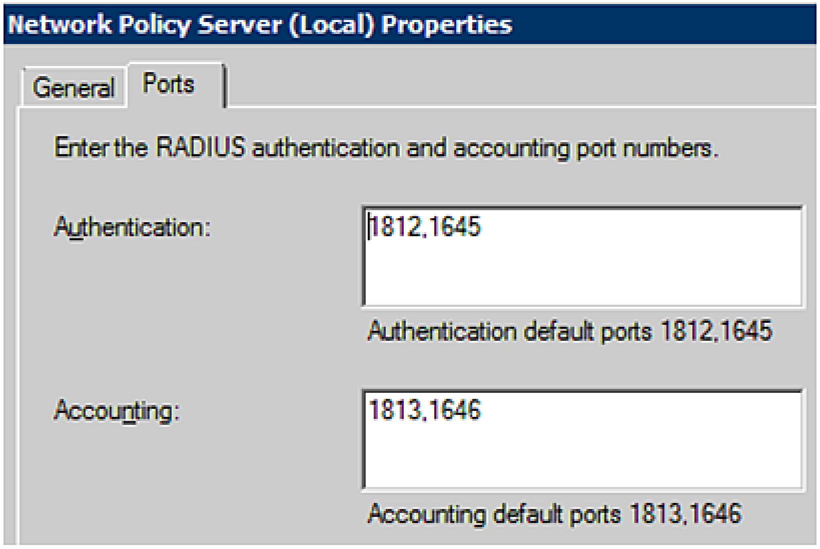
RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create net authorize connections from Dial-Up or VPN network access servers (also called RADIUS client

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.



Enter the RADIUS authentication and accounting port numbers.

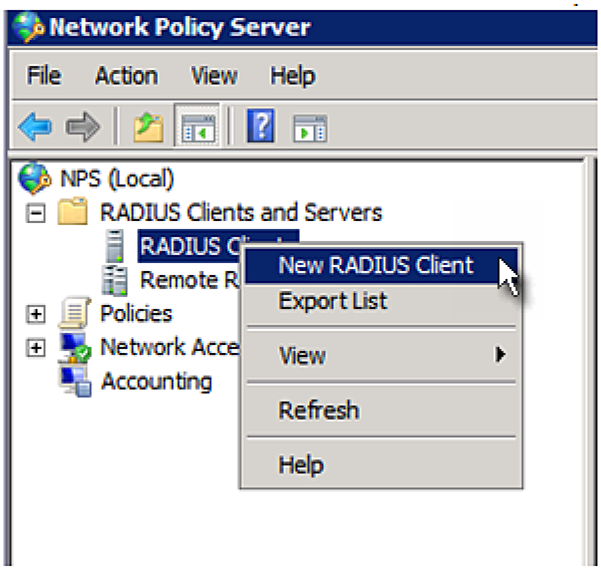
Authentication: 1812,1645

Authentication default ports 1812,1645

Accounting: 1813,1646

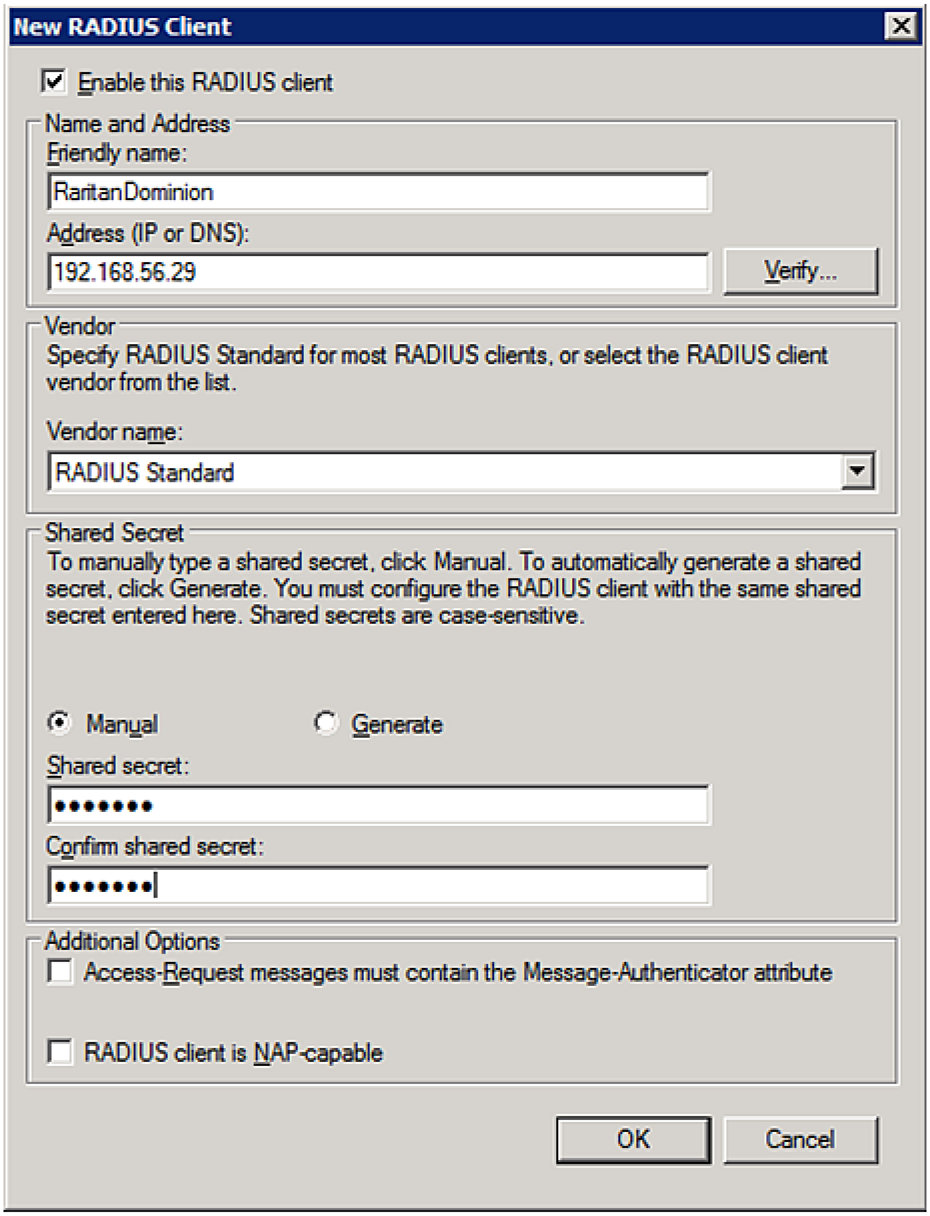
Accounting default ports 1813,1646

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.



New RADIUS Client

☑ Enable this RADIUS client

Name and Address

Friendly name: RaritanDominion

Address (IP or DNS): 192.168.56.29

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••

Confirm shared secret: •••••••

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

5. Click OK.

Step B: Configure Connection Request Policies

You need to configure the following for connection request policies:

a. IP address or host name of the EMX

b. Connection request forwarding method

c. Authentication method(s)

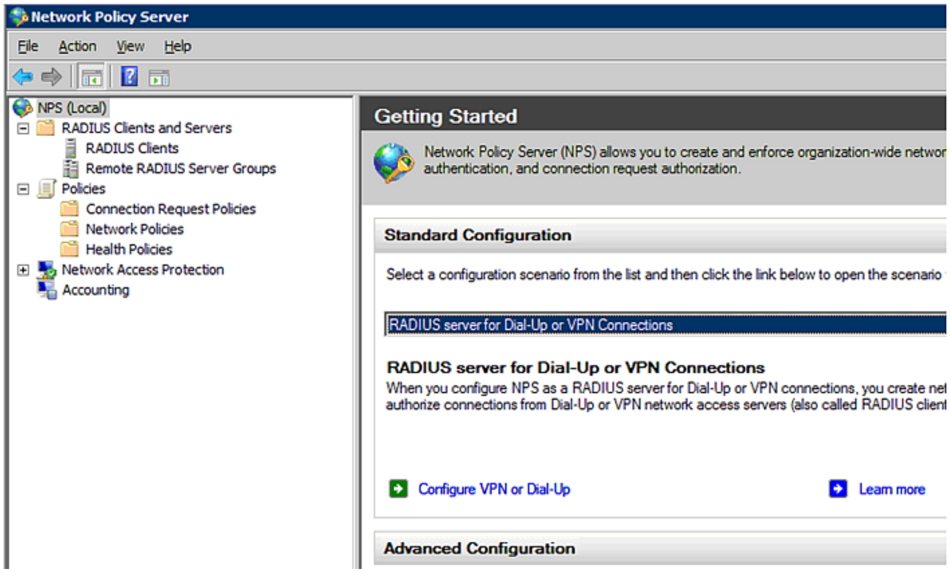
d. Standard RADIUS attributes

In the following illustration, we assume:

- *Local* NPS server is used
- IP address of your EMX: *192.168.56.29*
- RADIUS protocol selected on your EMX: *CHAP*
- Existing role of your EMX: *Admin*

To configure connection request policies:

1. Open the NPS console, and expand the Policies folder.



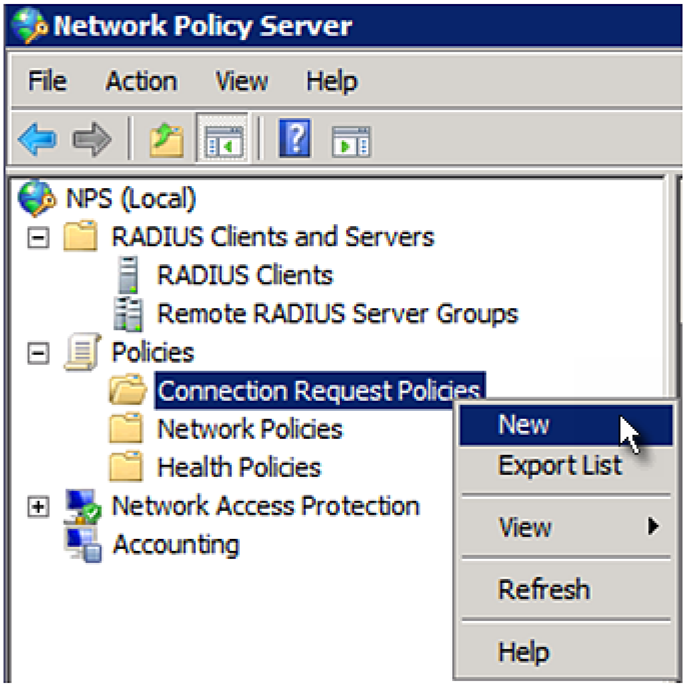
Network Policy Server (NPS) allows you to create and enforce organization-wide networ authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario

RADIUS server for Dial-Up or VPN Connections

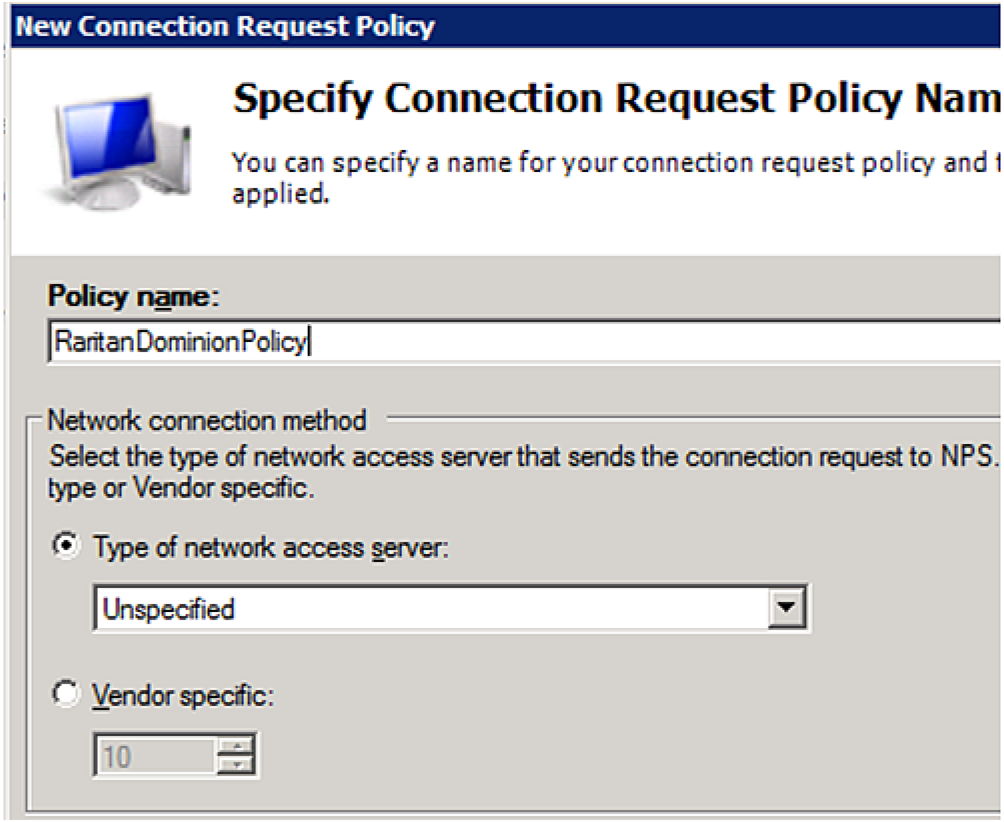
When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create net authorize connections from Dial-Up or VPN network access servers (also called RADIUS client

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.

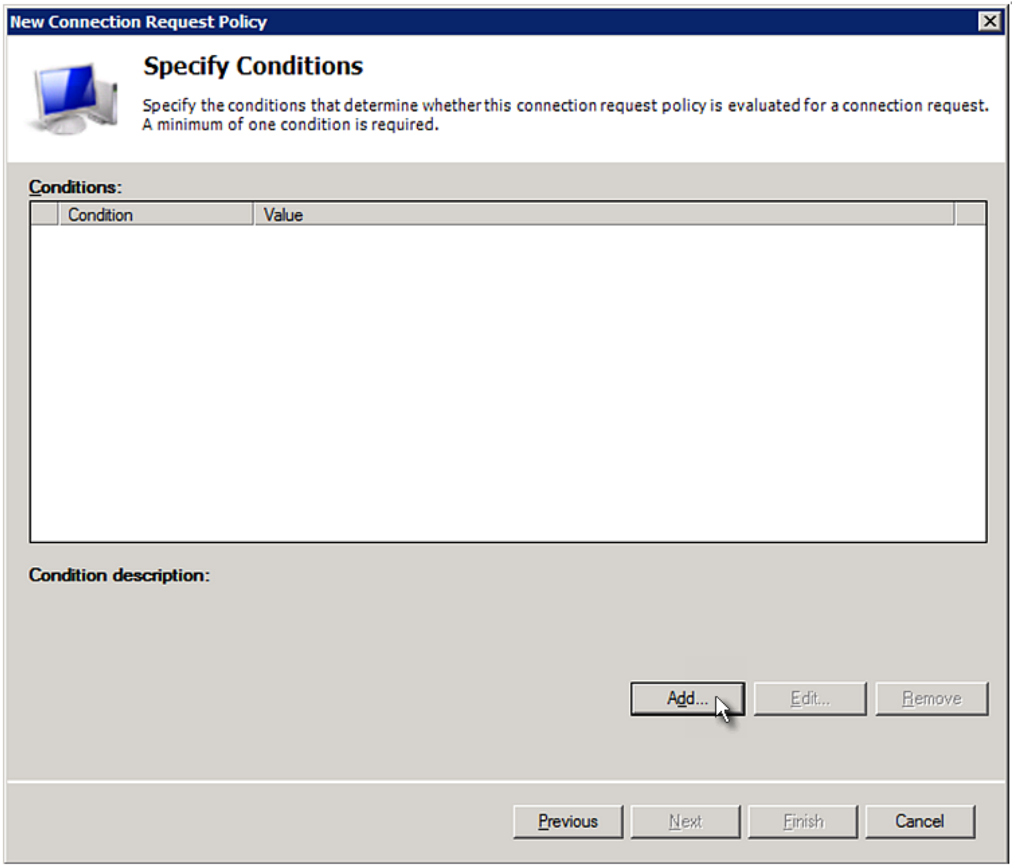
● Type of network access server:

Unspecified

○ Vendor specific:

10

4. Click Next to show the "Specify Conditions" screen. Click Add.



Specify Conditions

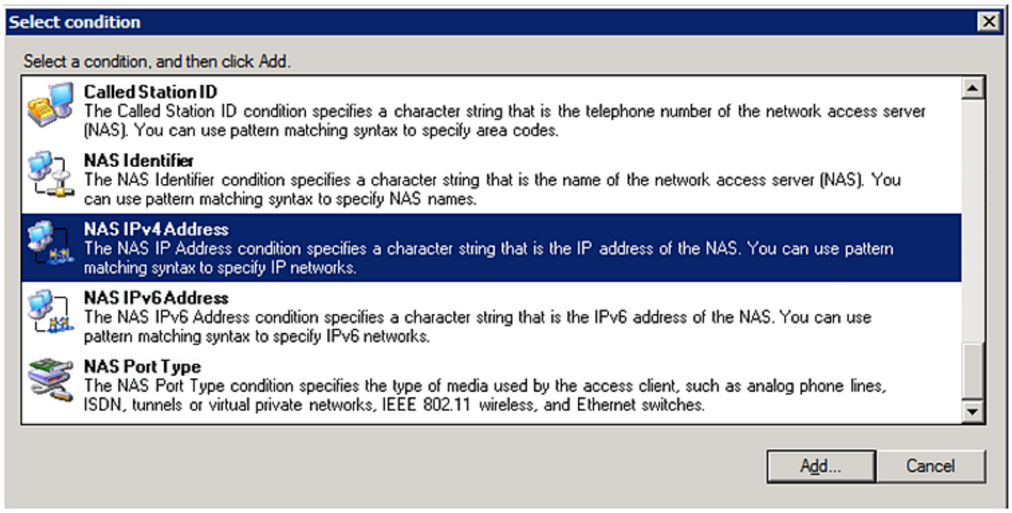
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value

Condition description:

5. The "Select condition" dialog appears. Click Add.



Select a condition, and then click Add.

Called Station ID
The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.

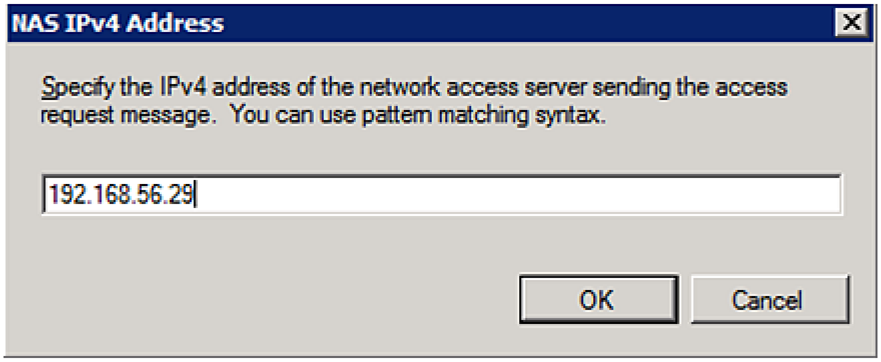
NAS Identifier
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.

NAS IPv4 Address
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

NAS IPv6 Address
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.

NAS Port Type
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

6. The NAS IPv4 Address dialog appears. Type the EMX IP address -- *192.168.56.29*, and click OK.

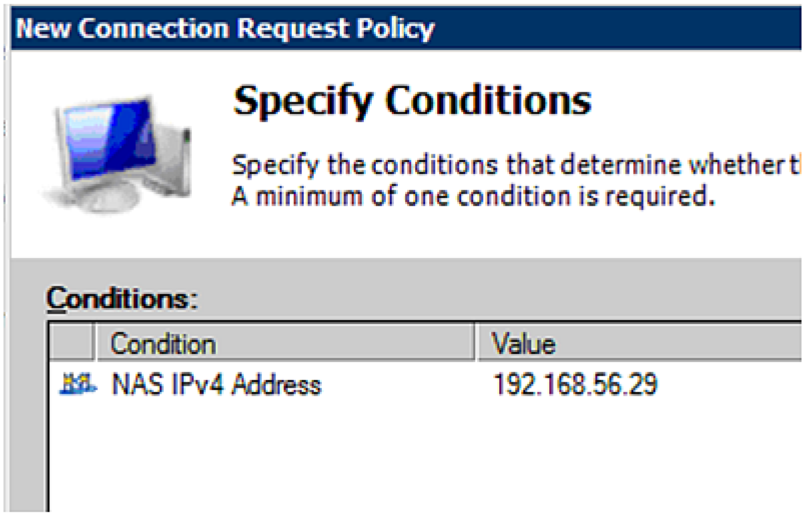


NAS IPv4 Address

Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.

192.168.56.29

7. Click Next in the New Connection Request Policy dialog.



New Connection Request Policy

Specify Conditions

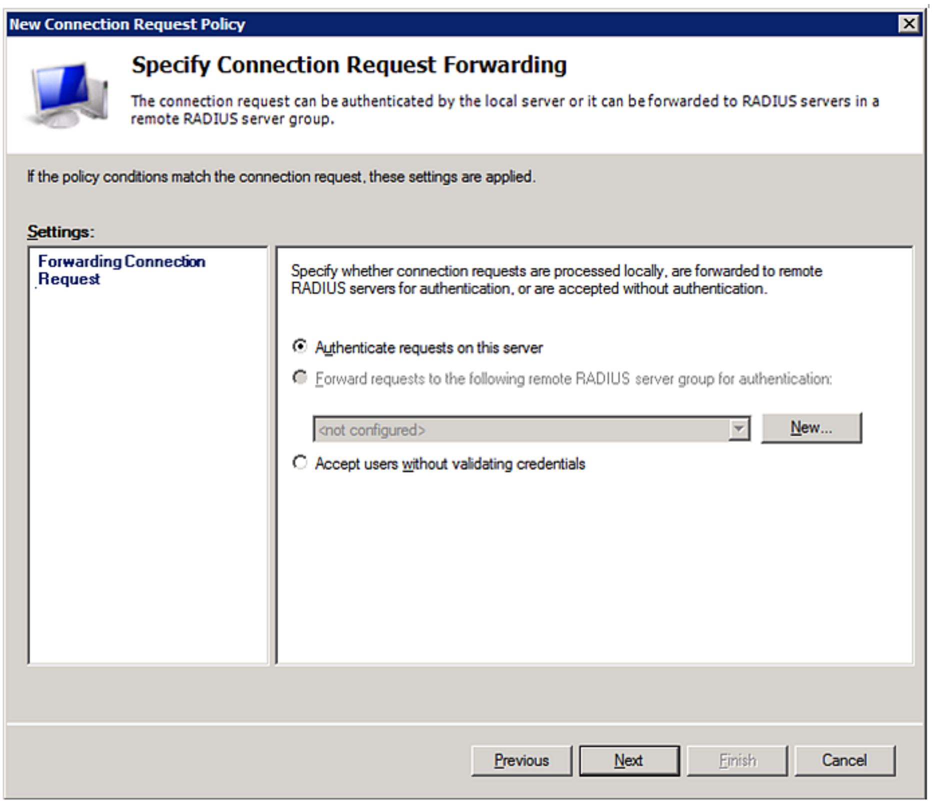
Specify the conditions that determine whether t
A minimum of one condition is required.

Conditions:

Condition	Value
NAS IPv4 Address	192.168.56.29

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.



Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

Forwarding Connection Request

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

● Authenticate requests on this server

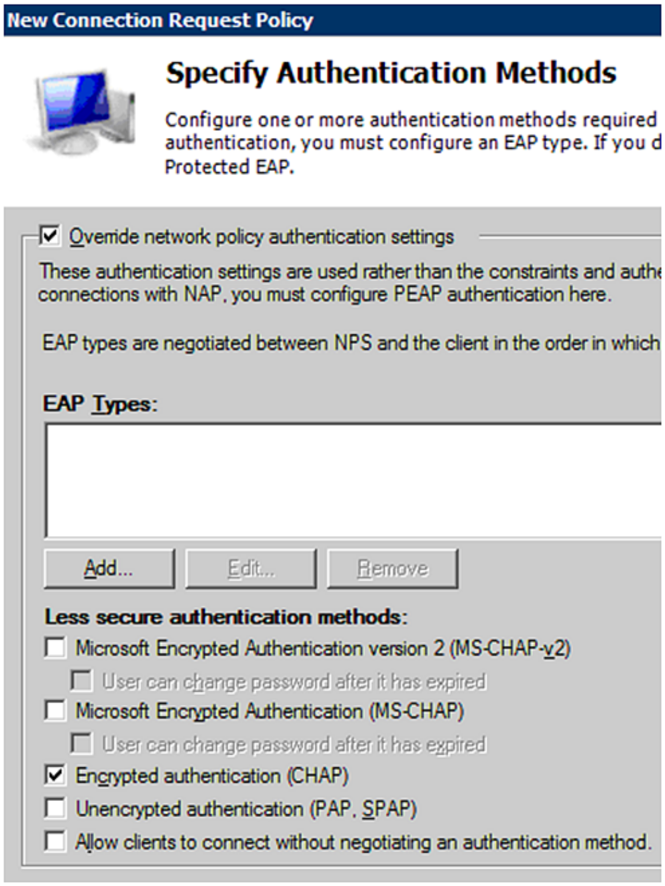
○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials

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."



Specify Authentication Methods

Configure one or more authentication methods required
authentication, you must configure an EAP type. If you d
Protected EAP.

☑ Override network policy authentication settings

These authentication settings are used rather than the constraints and authe
connections with NAP, you must configure PEAP authentication here.

EAP types are negotiated between NPS and the client in the order in which

EAP Types:

Less secure authentication methods:

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

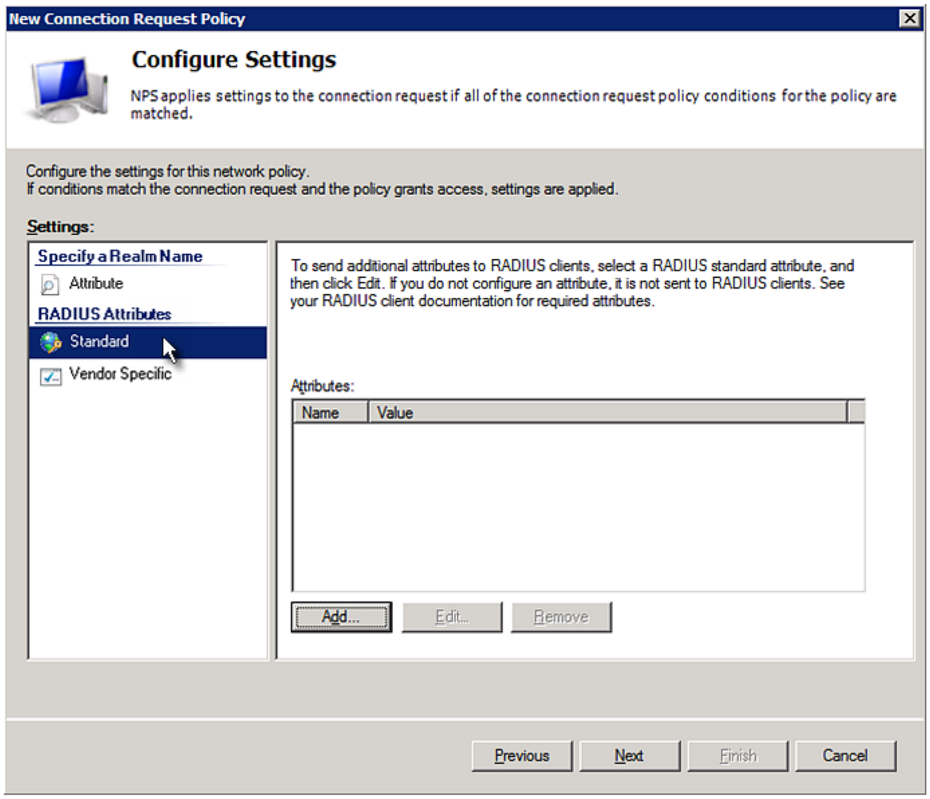
☐ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

☐ Allow clients to connect without negotiating an authentication method.

10. Select Standard to the left of the dialog and then click Add.



New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

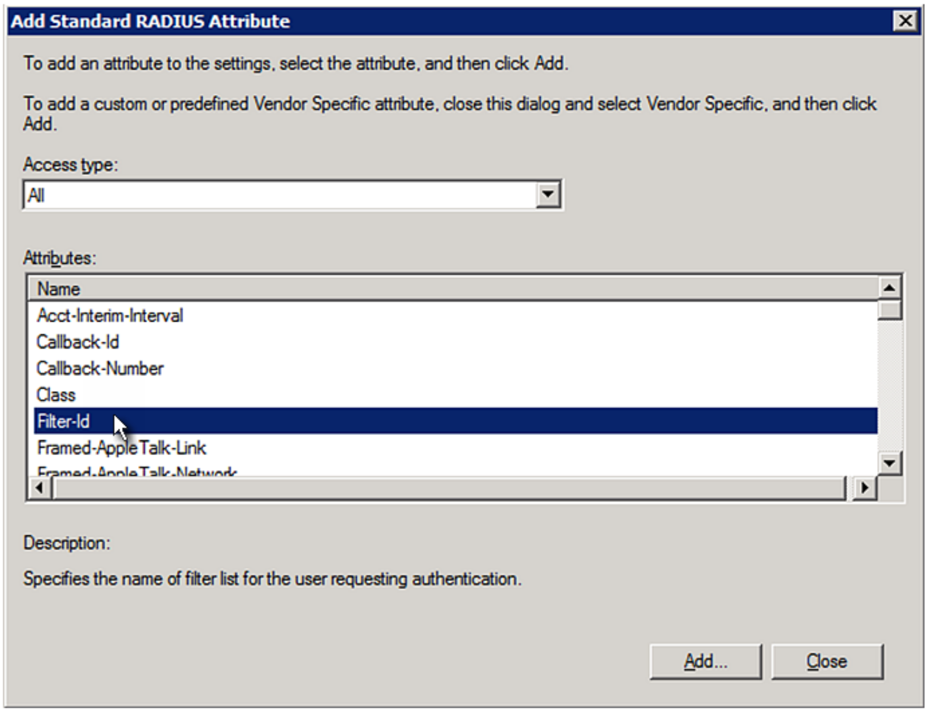
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value

11. Select Filter-Id from the list of attributes and click Add.



Add Standard RADIUS Attribute

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:

All

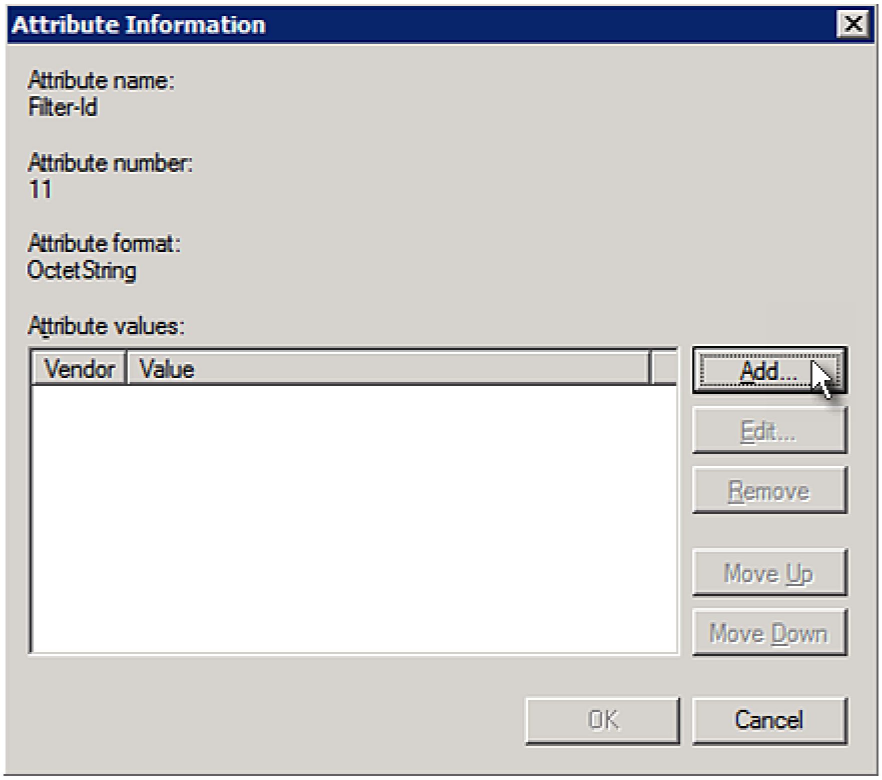
Attributes:

Name
Acct-Interim-Interval
Callback-Id
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network

Description:

Specifies the name of filter list for the user requesting authentication.

12. In the Attribute Information dialog, click Add.



Attribute Information

Attribute name:
Filter-Id

Attribute number:
11

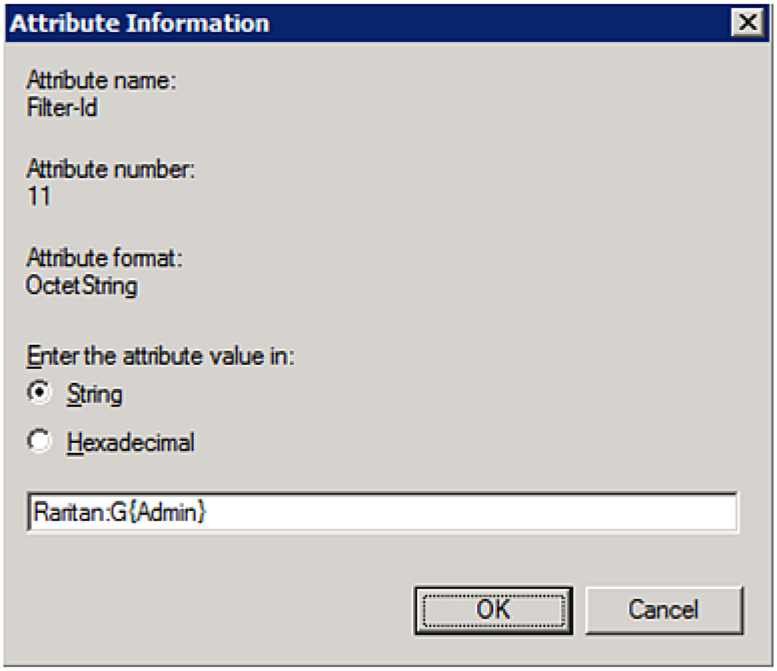
Attribute format:
OctetString

Attribute values:

Vendor	Value

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.



Attribute Information

Attribute name:
Filter-Id

Attribute number:
11

Attribute format:
OctetString

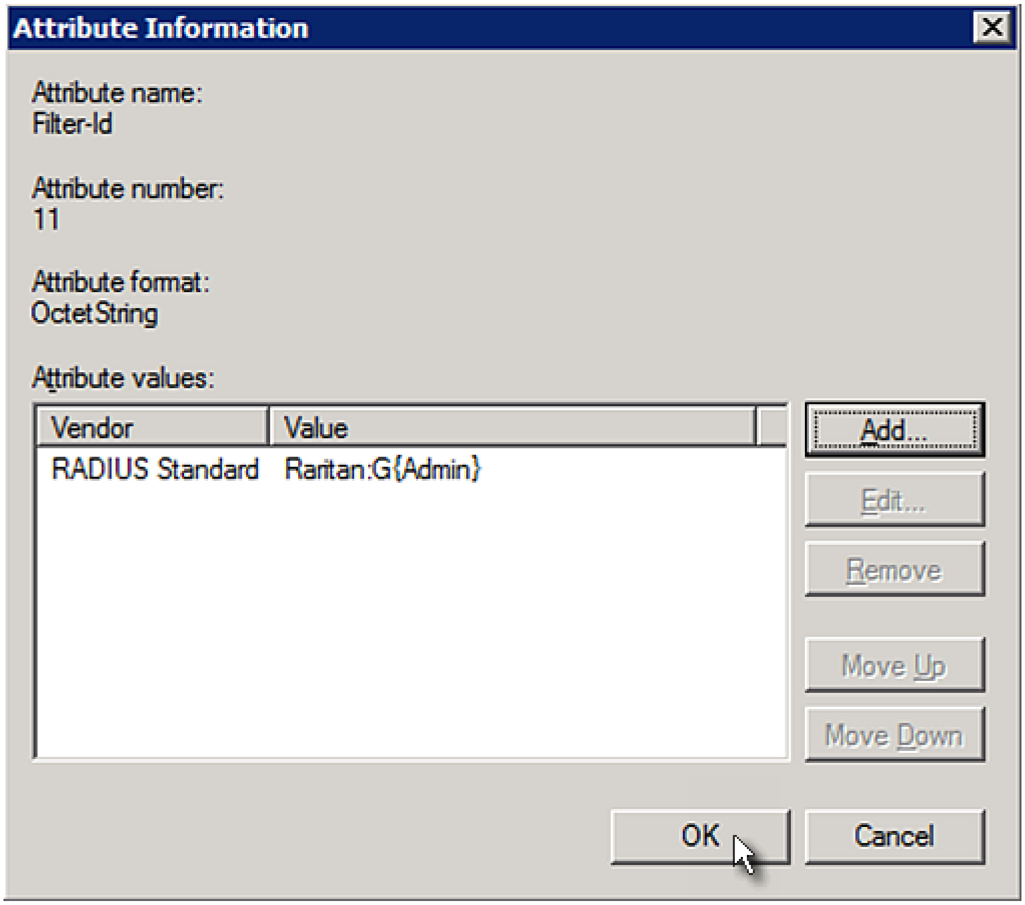
Enter the attribute value in:

● String

○ Hexadecimal

Raritan:G{Admin}

14. The new attribute is added. Click OK.



Attribute Information

Attribute name:
Filter-Id

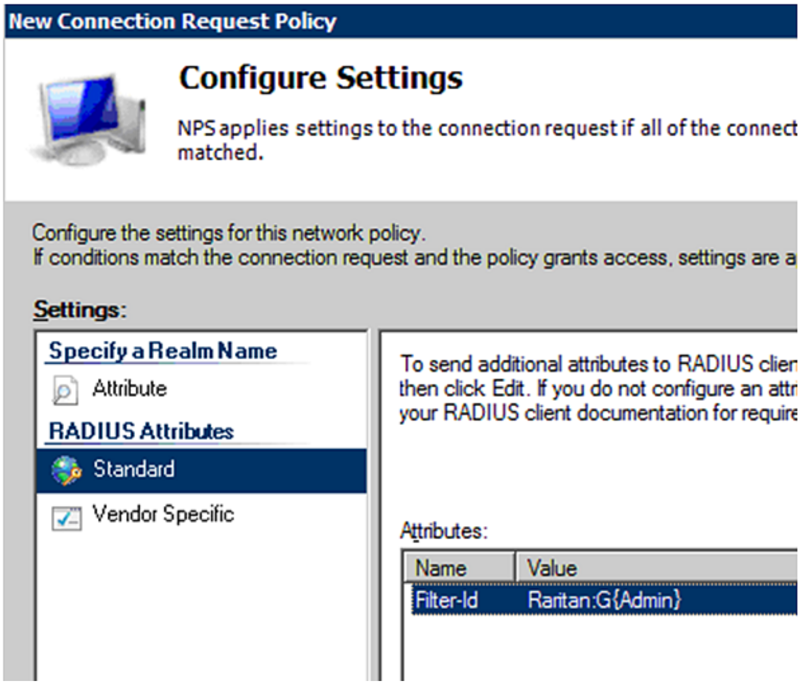
Attribute number:
11

Attribute format:
OctetString

Attribute values:

Vendor	Value
RADIUS Standard	Raritan:G{Admin}

15. Click Next to continue.



New Connection Request Policy

Configure Settings

NPS applies settings to the connection request if all of the connect matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are a

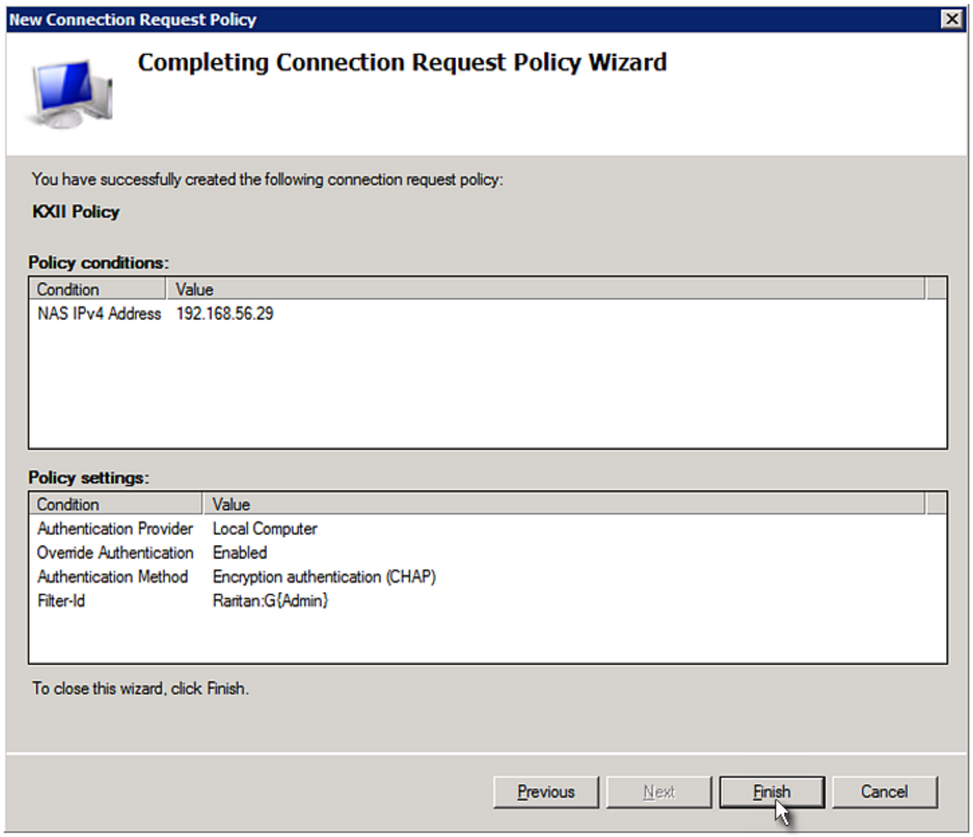
Settings:

To send additional attributes to RADIUS clien then click Edit. If you do not configure an attr your RADIUS client documentation for require

Attributes:

Name	Value
Filter-Id	Raritan:G{Admin}

16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.



Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

KXII Policy

Policy conditions:

Condition	Value
NAS IPv4 Address	192.168.56.29

Policy settings:

Condition	Value
Authentication Provider	Local Computer
Override Authentication	Enabled
Authentication Method	Encryption authentication (CHAP)
Filter-Id	Raritan:G{Admin}

To close this wizard, click Finish.

Step C: Configure a Vendor-Specific Attribute

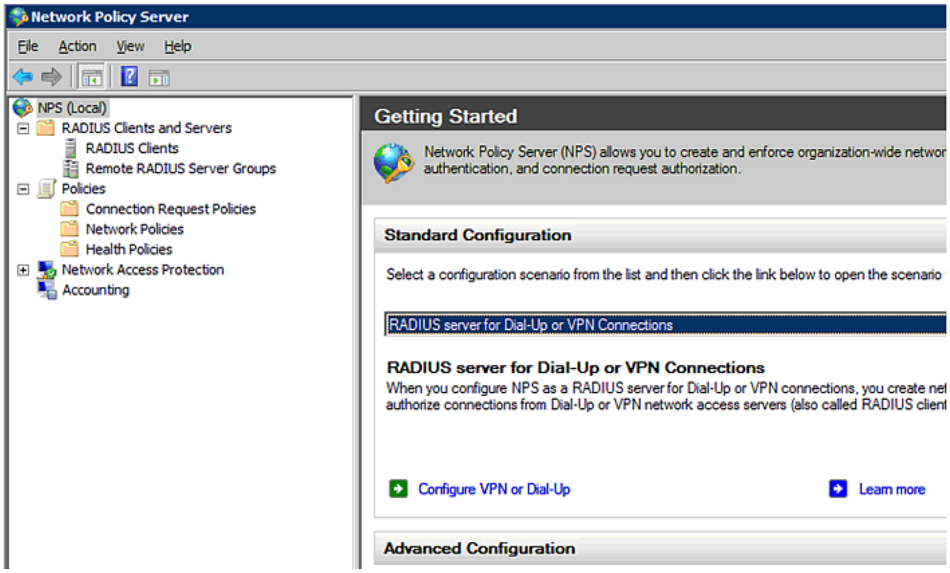
You must specify a vendor-specific attribute (VSA) for Raritan on Windows 2008 NPS. Raritan's vendor code is **13742**.

In the following illustration, we assume:

- There are three roles available on your EMX: *Admin*, *User*, and *SystemTester*.

To configure VSA:

1. Open the NPS console, and expand the Policies folder.



Getting Started

Network Policy Server (NPS) allows you to create and enforce organization-wide networ authentication, and connection request authorization.

Standard Configuration

Select a configuration scenario from the list and then click the link below to open the scenario

RADIUS server for Dial-Up or VPN Connections

RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create net authorize connections from Dial-Up or VPN network access servers (also called RADIUS client

Advanced Configuration

2. Select Connection Request Policies and double-click the policy where you want to add a custom VSA. The policy's properties dialog appears.
3. Click the Settings tab.
4. Select Vendor Specific, and click Add. The Add Vendor Specific Attribute dialog appears.
5. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.
6. Click Add, and the Vendor-Specific Attribute Information dialog appears.
7. Click "Enter Vendor Code" and type *13742*.
8. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).
9. Click Configure Attribute, and then:

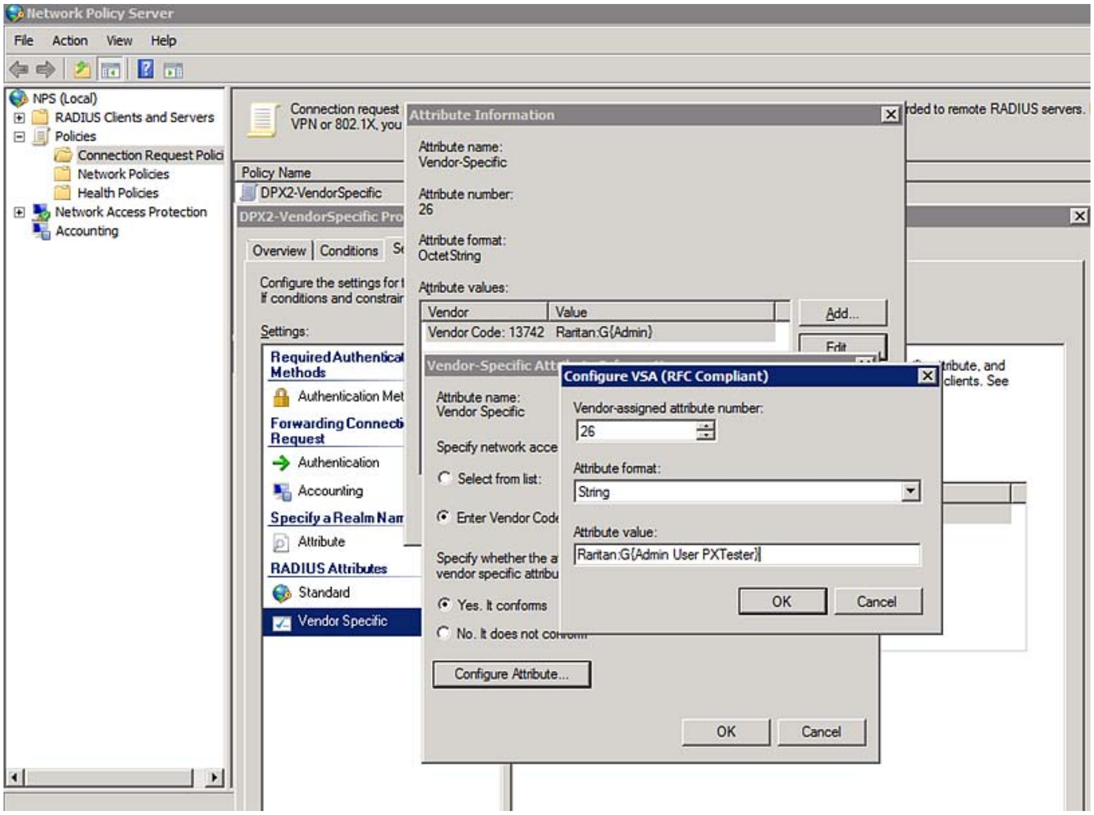
a. Type *26* in the "Vendor-assigned attribute number" field.

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 are specified inside the curved brackets {} -- Admin, User and SystemTester.

Note that different roles must be separated with a space.

10. Click OK.



Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value
Vendor Code: 13742	Raritan:G{Admin}

Attribute name:
Vendor Specific

○ Select from list:

● Enter Vendor Code

● Yes. It conforms

○ No. It does not conform

Vendor-assigned attribute number:
26

Attribute format:
String

Attribute value:
Raritan:G{Admin User PXTester}

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.

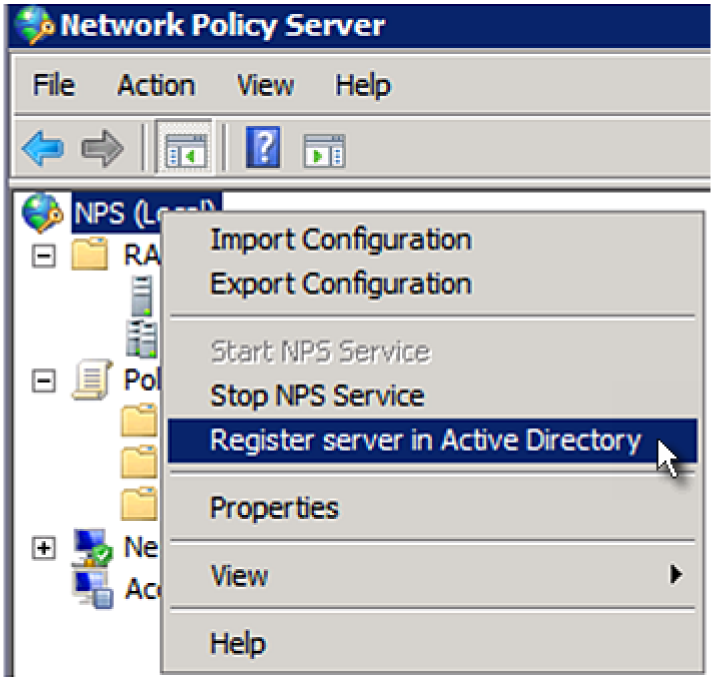
If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

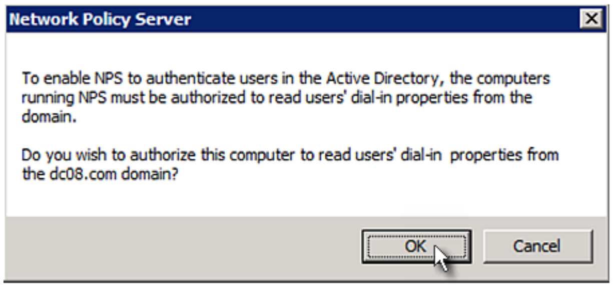
Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

▶ To register NPS:

1. Open the NPS console.
2. Right-click NPS (Local) and select "Register server in Active Directory."



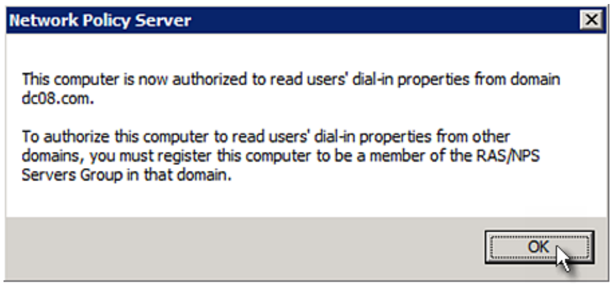
3. Click OK, and then OK again.



Network Policy Server

To enable NPS to authenticate users in the Active Directory, the computers running NPS must be authorized to read users' dial-in properties from the domain.

Do you wish to authorize this computer to read users' dial-in properties from the dc08.com domain?



Network Policy Server

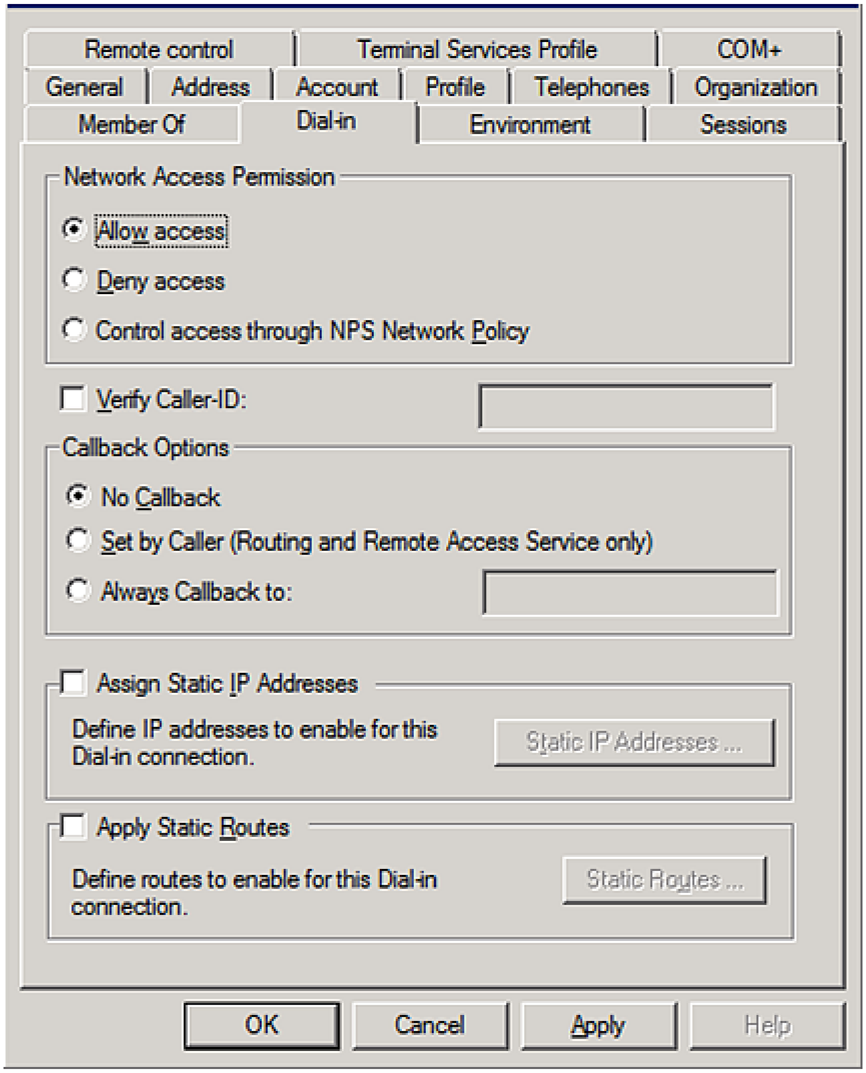
This computer is now authorized to read users' dial-in properties from domain dc08.com.

To authorize this computer to read users' dial-in properties from other domains, you must register this computer to be a member of the RAS/NPS Servers Group in that domain.

▶ To grant EMX users remote access permission:

1. Open Active Directory Users and Computers.
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.



Network Access Permission

● Allow access

○ Deny access

○ Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

□ Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

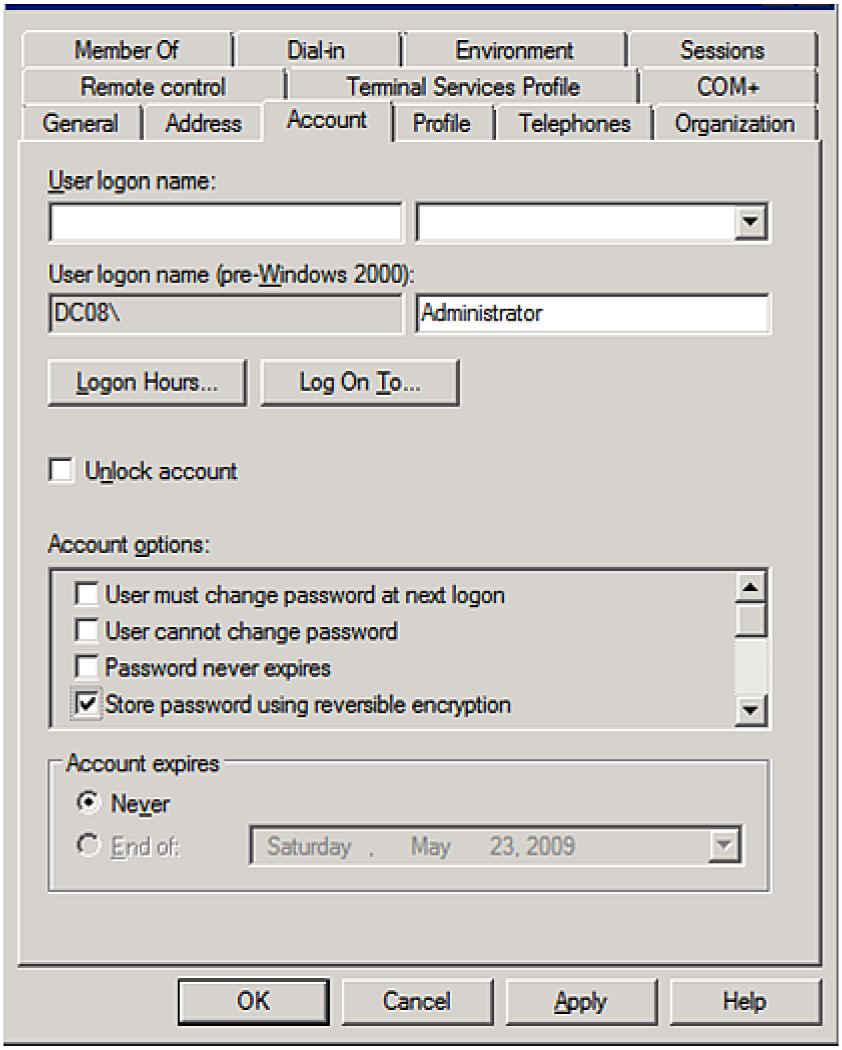
□ Apply Static Routes

Define routes to enable for this Dial-in connection.

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.

3. Click the Account tab and select the "Store password using reversible encryption" checkbox.



User logon name:

User logon name (pre-Windows 2000): DC08\ Administrator

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
☑ Store password using reversible encryption

Account expires

● Never
○ End of: Saturday , May 23, 2009

Non-Windows RADIUS Server

For a non-Windows RADIUS server, such as FreeRADIUS, a vendor-specific dictionary file is required.

Dictionary File

Create a vendor-specific dictionary file for Raritan and add the following information to it. Raritan's vendor code is **13742**.

```
# -*- text -*-
#
# dictionary.raritan
#
#
# Version:     $Id$
#
VENDOR         Raritan                        13742
#
#  Standard attribute
#
BEGIN-VENDOR   Raritan

ATTRIBUTE      Raritan-Vendor-Specific        26    string

END-VENDOR     Raritan
```

Note that "string" in the above contents must be replaced by `Raritan:G{roles}`, where "roles" are one or multiple roles to which the user belongs. For more details, see ***Format of the "string"*** (on page 526).

Format of the "string"

The format of `string` in the dictionary file is:

```
Raritan:G{roles}
```

"roles" inside the curved brackets {} are role names, which comprise one or multiple roles to which the user belongs.

Multiple role names are separated with a space.

▶ Example:

If the user has three roles -- *Admin*, *User* and *SystemTester*, then type:

```
Raritan:G{Admin User SystemTester}
```

Therefore, in Raritan's dictionary file, the attribute line is like the following:

```
ATTRIBUTE   Raritan-Vendor-Specific 26    Raritan:G{Admin User SystemTester}
```

Appendix I Additional EMX Information

In This Chapter

Reserving IP Addresses in Windows 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 Windows® DHCP server, use the EMX device's serial number as the unique ID instead of the MAC address.

▶ IP address reservation procedure:

1. Convert the serial number of your EMX into hexadecimal ASCII codes.

   - For example, if the serial number is `PEG1A00003`, convert each digit to ASCII codes as shown below:

     ```
     P=50
     E=45
     G=47
     1=31
     A=41
     0=30
     3=33
     ```

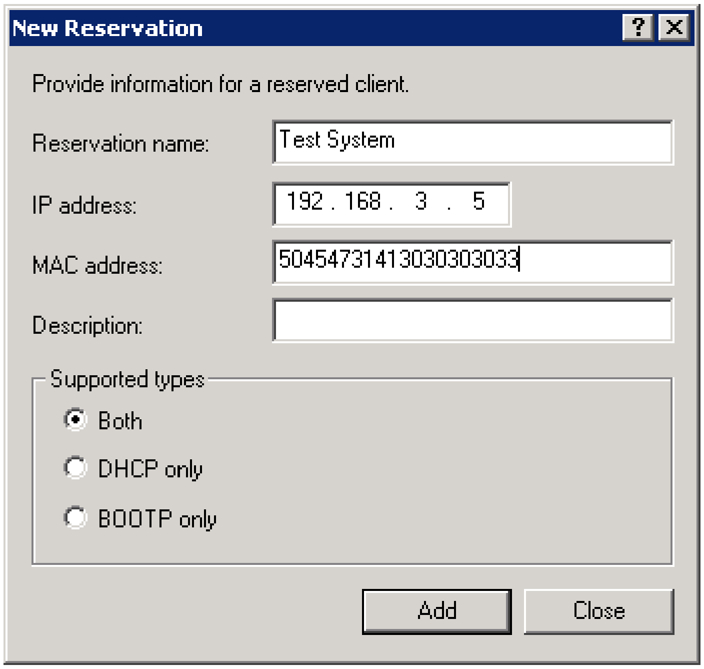
     Therefore, the complete ASCII codes are as follows:

     ```
     PEG1A00003 = 50454731413030303033
     ```

2. In your DHCP server, bring up the New Reservation dialog to reserve the IP address for your EMX.

Field	Description
IP address	Enter the IP address you want to reserve.

Field	Description
MAC address	Enter the ASCII codes of the EMX serial number. Do NOT contain spaces in the ASCII codes. ▪ In this example, enter `5045473141303030303033`
Other fields	Configure them according to your needs.



New Reservation

Provide information for a reserved client.

Reservation name: Test System

IP address: 192 . 168 . 3 . 5

MAC address: 5045473141303030303033

Description:

Supported types

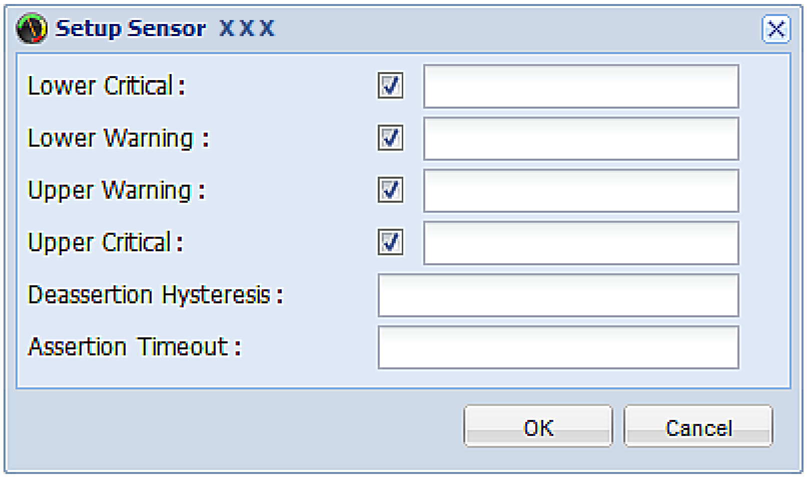
● Both

○ DHCP only

○ BOOTP only

Sensor Threshold Settings

This section explains the thresholds settings in a threshold setup dialog for a numeric internal or external sensor.



Setup Sensor XXX

Lower Critical : ☑

Lower Warning : ☑

Upper Warning : ☑

Upper Critical : ☑

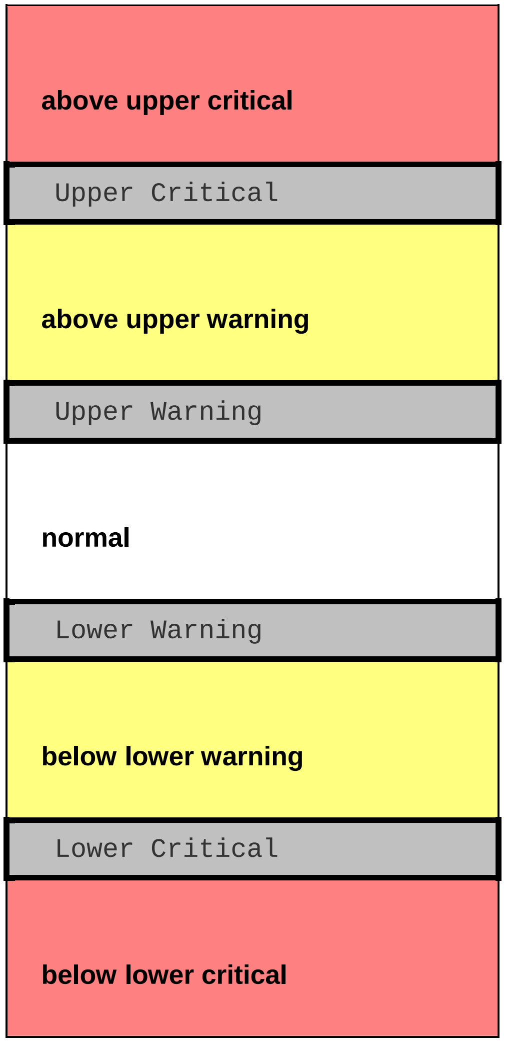
Deassertion Hysteresis :

Assertion Timeout :

Thresholds and Sensor States

A numeric sensor has four threshold settings: 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.



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:

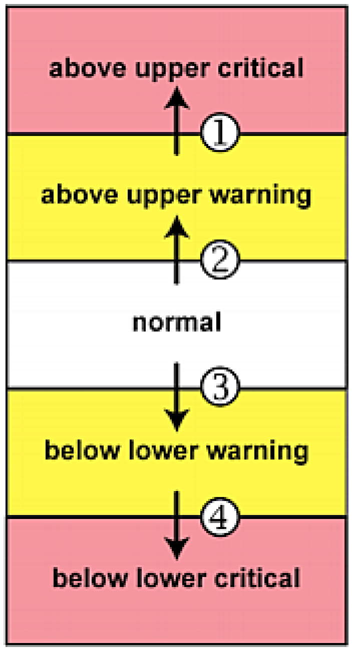
- ***"above upper critical" State*** (on page 255)
- ***"above upper warning" State*** (on page 255)
- ***"below lower critical" State*** (on page 255)
- ***"below lower warning" State*** (on page 255)

"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 "worse" new state. Below are bad state changes that cause the EMX to assert.

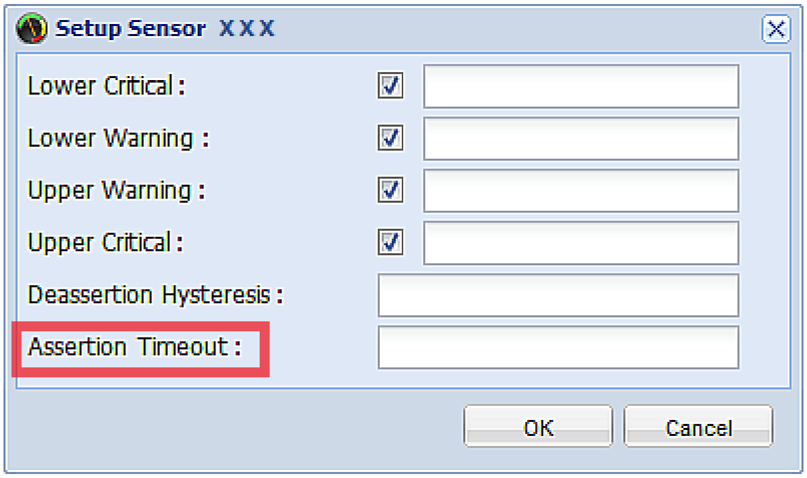


1. above upper warning --> above upper critical
2. normal --> above upper warning
3. normal --> below lower warning
4. below lower warning --> below lower critical

▶ Assertion Timeout:

In the threshold setup dialog, the Assertion Timeout field impacts the "assertion" action. It determines how long a sensor must be in the "worse" new state before the EMX turns on 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. Because the EMX measures each sensor every second, timing of a sample is equal to a second.

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 reading fluctuates 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:

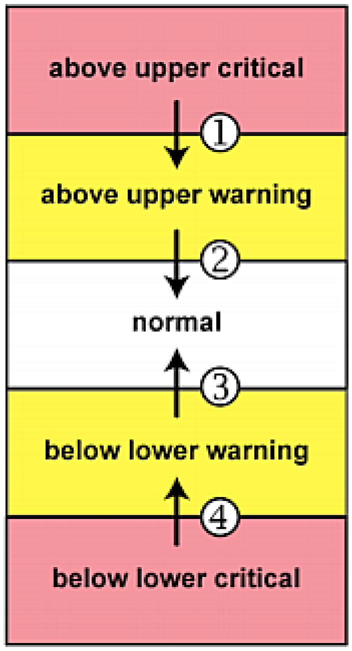
- If the temperature remains above 25 degrees Celsius in the "above upper warning" range for 5 seconds, the EMX turns on the "assertion" action to announce the "above upper warning" state.
- If the temperature drops below 25 degrees Celsius within 5 seconds, the EMX does NOT turn on the "assertion" action.

"To De-assert" and Deassertion Hysteresis

After the EMX asserts a worse state for a sensor, it may de-assert the same state later on.

To de-assert a state:

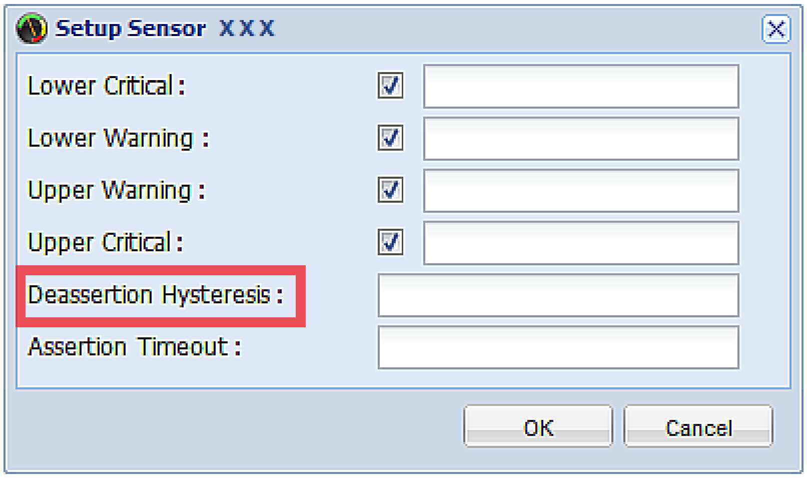
To de-assert a state is to announce the end of the previously asserted worse state. Below are good state changes that cause the EMX to de-assert the previous state.



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 dialog, the Deassertion Hysteresis field determines a new level to turn on the "deassertion" action.



Lower Critical : ☑
Lower Warning : ☑
Upper Warning : ☑
Upper Critical : ☑
Deassertion Hysteresis :
Assertion Timeout :

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 hits 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 value of the decrease or increase is exactly the hysteresis value.

For example:

If Deassertion Hysteresis = 2,

- 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 reading fluctuates 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 turn on the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the EMX turns on 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.

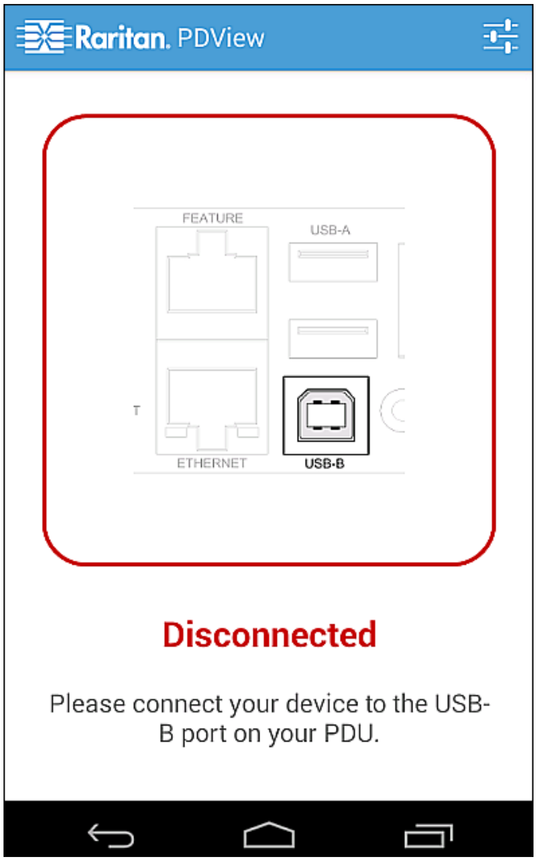
▶ Requirements for using PDView:

- 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 a 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 for Android devices.



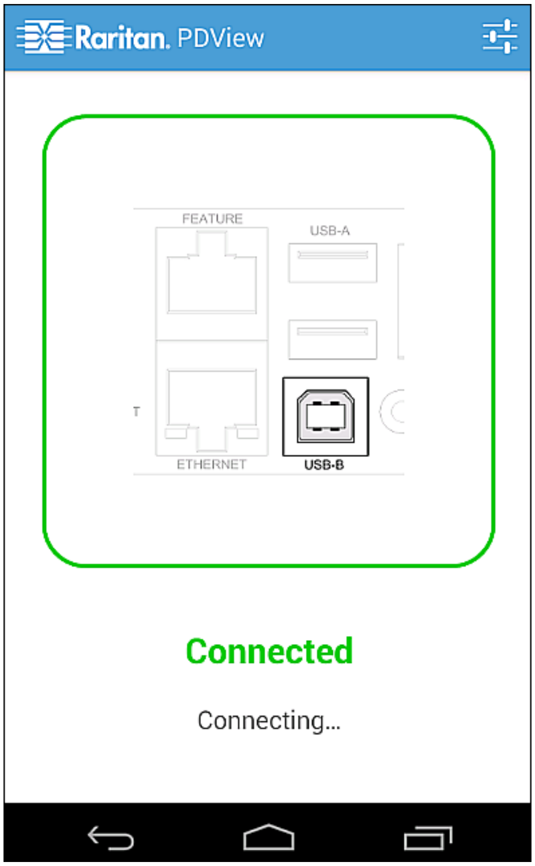
Disconnected

Please connect your device to the USB-B port on your PDU.

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
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.

Truncated Data in the Web Interface

Some fields of the EMX web interface can accommodate data entry up to 256 characters. When the data entered is too long, it may be truncated due to some or all of the following factors:

- Screen resolution
- Font size
- Font type
- Size of different characters

Current web browser technology cannot break or wrap these fields with long inputs.

The solution for this issue includes:

- Increase of the screen resolution
- Application of smaller font size
- Use of other interfaces, such as the CLI or SNMP, to view the data in these fields

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.

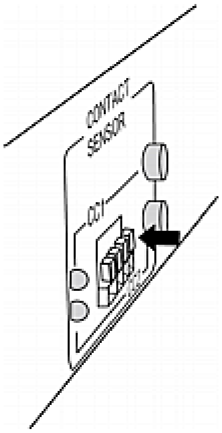
It is not guaranteed that all third-party detectors/switches are compatible with the EMX. You need to test the compatibility after installing them.

Note: If you are using an EMX2-888 with a removable terminal module, see **Connecting Contact Closure Sensors to EMX2-888** *(on page 77).*

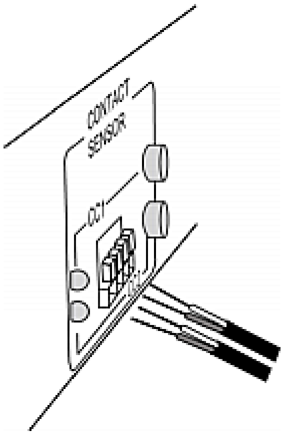
► To connect sensors to old EMX2-888 contact closure terminals:

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.

Appendix J Integrating Asset Management Sensors with Other Products

In This Chapter

Asset Management Sensors and Raritan PDUs

Asset sensors also work with the following Raritan power distribution units (PDUs) or transfer switches:

- PX2 PDUs
- PX3 PDUs
- PX3TS transfer switches

For information on setting up asset sensors to work with each product, refer to its User Guide or Online Help on the Raritan website's ***Support page*** (***http://www.raritan.com/support/***).

Asset Management Sensors and dcTrack

If any asset sensors 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 sensors, see **Connecting Asset Management Sensors** *(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 sensor. Power IQ then generates a connect or disconnect event. When dcTrack polls Power IQ, the connect/disconnect 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 sensor 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 sensor 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 sensor 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 details on dcTrack as well as how asset sensors work with dcTrack, contact Sunbird Professional Services and Support from the http://support.sunbirddcim.com.

Index

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-5795-3170
Email: support.japan@raritan.com

Europe

Europe

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom

Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France

Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany

Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com