Raritan.

A brand of **legrand**

Smart Rack Controller

User Guide

Xerus™ Firmware v3.6.0

FCC Information

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

VCCI Information (Japan)

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。　　　　VCCI－A

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

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

Contents

Chapter 7   Using SNMP   346

Chapter 8   Using the Command Line Interface   355

Raritan.
A brand of legrand

Raritan.
A brand of ☐legrand®

Chapter 1   Introduction

In This Chapter

Overview

Raritan's Smart Rack Controller (SRC) provides a rack management solution that combines the capabilities of environmental monitoring, asset management, image surveillance, event notifications and support for Schroff® heat exchangers.

In addition, you can even control the access to cabinets with Raritan's door handles (or SmartLock kit).

Important: Asset management feature and door handles (or SmartLock kit) are mutually exclusive. You cannot have both devices connected simultaneously.

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

At least one Raritan DX or DX2 environmental sensor package is required for this feature.

After connecting Raritan environmental sensor package(s) to SRC, you can remotely monitor surrounding conditions in the data center, such as temperature or humidity, or control a system if actuators are connected.

Note: SRC does NOT support these other Raritan environmental sensor packages: DPX, DPX2, DPX3 (except for the DPX3-ENVHUB4 sensor hub).

▶ **Cabinet access control:**

Raritan's door handles or SmartLock kit is required, which is model dependent.

- You only need two door handles when your SRC model has onboard door handle ports, such as SRC-0102.

  If you want to increase the number of door handles from two to four, you can purchase a SmartLock kit and then connect it to this SRC's SENSOR port.

- You must purchase the SmartLock kit if your model does NOT have onboard door handle ports, such as SRC-0100.

Raritan's SmartLock kit contains one DX2-DH2C2 and a pair of door handles.

After properly connecting and configuring door handles or the SmartLock kit, you can control the access to the selected cabinet via SRC.

▶ **Asset management:**

You can remotely track the location of IT equipment after tagging IT devices electronically. This feature is especially useful when there are a number of IT devices to administer.

The following 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 strips (asset strips)*: Each asset strip transmits the tag and position information to SRC.

▪ *An SRC device*: You can remotely locate each tagged IT device through SRC.

▶ **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 SRC.

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:**

SRC 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.

Raritan.
A brand of legrand®

Product Models

There are two SRC models:

- SRC-0100
- SRC-0102

They are functionally identical except that SRC-0100 does NOT have onboard door handle ports and contact closure terminals while the other model has them.

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

SRC-0100

SRC-0100 has the following ports and components:
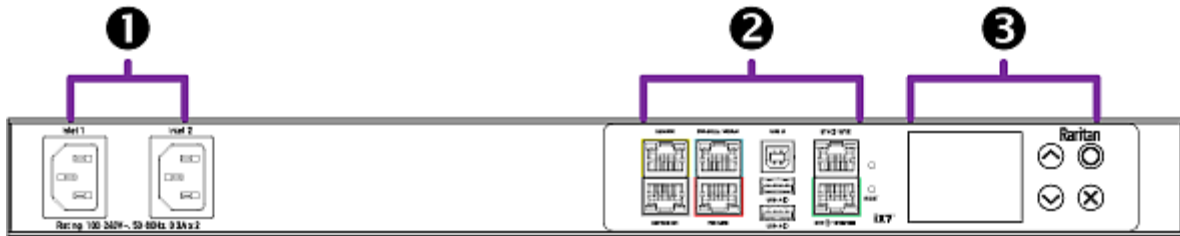
To control access to a cabinet via this model, you must purchase Raritan's SmartLock kit.

▶ ❶ **DUAL INLETS:**

Dual inlets can supply redundant power to this model.

▶ ❷ **STANDARD CONNECTION PORTS:**

- CONSOLE/MODEM port x 1 (blue)
- Sensor port x 1 (yellow)
- USB-A port x 2
- USB-B port x 1
- Feature port x 1 (red)
- Ethernet port x 2 (green and white)

For details, see **Connection Ports** (on page 67).

Note: Expansion port is reserved for future use so it does NOT function now.

▶ ❸ **FRONT PANEL LCD and CONTROL BUTTONS:**

Front panel LCD and buttons let users view real-time device information and/or alerts without logging in to the SRC software. See **Dot-Matrix LCD Display** (on page 70).

SRC-0102

SRC-0102 has the following ports and components:

▶ ❶ **DUAL INLETS:**

Dual inlets can supply redundant power to this model.

▶ ❷ **ONBOARD DOOR HANDLE PORTS and CONTACT CLOSURE TERMINALS:**

These ports support the cabinet access control feature and contact closure sensors. See **Onboard Door Handle Ports and Contact Closure Terminals** (on page 69).
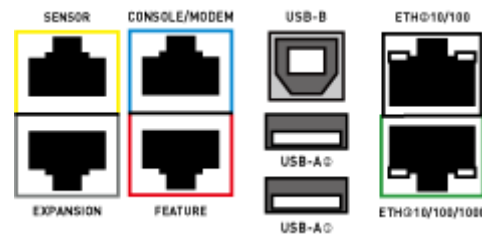
▶ ❸ **STANDARD CONNECTION PORTS:**

- CONSOLE/MODEM port x 1 (blue)
- Sensor port x 1 (yellow)
- USB-A port x 2
- USB-B port x 1
- Feature port x 1 (red)
- Ethernet port x 2 (green and white)

For details, see **Connection Ports** (on page 67).

Note: Expansion port is reserved for future use so it does NOT function now.

▶ ④ **FRONT PANEL LCD and CONTROL BUTTONS:**

Front panel LCD and buttons let users view real-time device information and/or alerts without logging in to the SRC software. See **Dot-Matrix LCD Display** (on page 70).

Package Contents

The following lists the equipment shipped with SRC. If anything is missing or damaged, contact the local dealer or Raritan Technical Support for help.

- One SRC device
- Bracket pack and screws

Quick Setup Guide

Optional Accessories

Part or all of the following equipment is shipped on demand only.

- Asset management strips and asset tags
- Door handles or SmartLock kit
- DX and/or DX2 environmental sensor package(s)
- DPX3-ENVHUB4 sensor hubs

Warning: SRC does NOT support these other Raritan environmental sensor packages: DPX, DPX2, DPX3 (except for the DPX3-ENVHUB4 sensor hub).

APIPA and Link-Local Addressing

SRC supports Automatic Private Internet Protocol Addressing (APIPA).

With APIPA, your SRC 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 SRC using the link-local address/host name. Those in a different subnet cannot access it.

Exception: SRC in the Port Forwarding mode does not support APIPA. See **Setting the Cascading Mode** *(on page 177).*

Once the SRC 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 SRC, but no IP address is assigned to the SRC.

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

  Note: Configuration by connecting the SRC to a computer using a network cable is an application of this scenario. See **Connecting the SRC to a Computer** *(on page 21).*

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

► **Link-local addressing:**

- *IPv4 address*:

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

- *IPv6 address*:

  A link-local IPv6 address is available only after IPv6 is enabled on the SRC. See **Configuring Network Settings** (on page 160).

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

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

► **Retrieval of the link-local address:**

- See **Device Info** (on page 80).

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 SRC for cabling and equipment connections.

Chapter 2   Rackmount

There are two ways to mount an SRC device, using the same Raritan rackmount brackets.
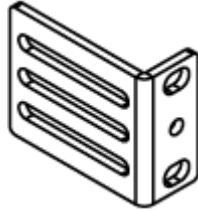
- *1U Rackmount Method* (on page 8)

  SRC is mounted like a 1U device in the rack.

- *0U Rackmount Method* (on page 9)

  SRC is mounted like a 0U device in the rack.

In This Chapter

1U Rackmount Method

► **To mount SRC like a 1U device:**

1. Align the two edge slots of the L-bracket with two of the screw holes on one end of the SRC device.

2. Screw the L-bracket to the device and ensure the bracket is fastened securely.
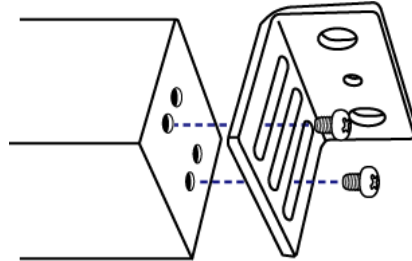
3. Repeat Steps 1 to 2 to screw another L-bracket to the other end of the device.

4. After both L-brackets are installed, fasten the device to the rack, using rack screws, through two identical round holes of each L-bracket.

0U Rackmount Method
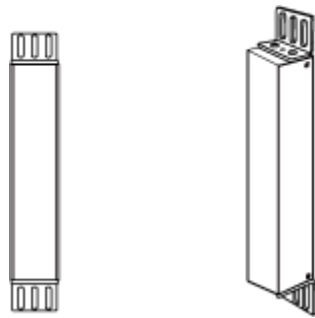
▶ **To mount SRC like a 0U device:**

1. Align the two round holes of the L-bracket with two of the screw holes on the top of the SRC device.

2. Screw the L-bracket to the device and ensure the bracket is fastened securely.
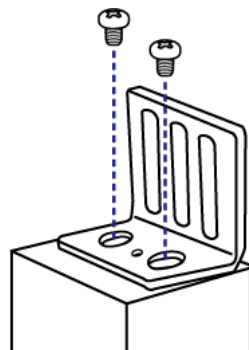
3. Repeat Steps 1 to 2 to screw another L-bracket to the other end of the device.

4. After both L-brackets are installed, fasten the device to the rack, using rack screws, through slots of each L-bracket.

Chapter 3   Initial Installation and Configuration

This chapter explains how to install your SRC and configure it for network connectivity.

In This Chapter

Connecting SRC to Power

SRC supports redundant power with two inlets. See **Product Models** (on page 3).

You can connect only one or both inlets to proper power sources.

1. Connect each SRC to an appropriately rated branch circuit. Refer to the label or nameplate affixed to your SRC for appropriate input ratings or range of ratings.

2. When a SRC powers up, it proceeds with the power-on self test and software loading for a few moments.

3. When the software has completed loading, the front panel display illuminates.

Connecting the SRC to Your Network

To remotely administer the SRC, you must connect the SRC to your local area network (LAN). SRC can be connected to a wired or wireless network.

*Note: If your SRC will work as a master device in the bridging mode, you must make a wired connection. See **Cascading Multiple SRC Devices for Sharing Ethernet Connectivity** (on page 24).*

Ethernet port of SRC must be enabled for the described connection to work properly, which has been enabled per default. See **Wired Network Settings** (on page 161).

▶ **To make a wired connection:**

1. Connect a standard network patch cable to either or both Ethernet ports on the SRC.

   ▪ The two Ethernet ports must be connected to different subnets. See **Dual Ethernet Connection** (on page 14).

- The "green" Ethernet port labeled "ETH①10/100/1000" supports up to 1000 Mbps so it is highly recommended for network connection.

2. Connect the other end of the cable to your LAN.

Below illustrates the ETHERNET ports. Note that the port locations on your SRC may differ.
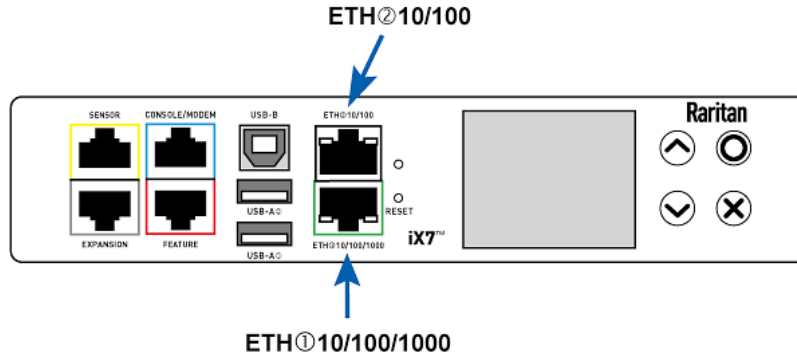
Warning: Accidentally plugging an RS-232 RJ-45 connector into the Ethernet port can cause permanent damage(s) to the Ethernet hardware.

► **To make a wireless connection:**

Do one of the following:

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

See *USB Wireless LAN Adapters* (on page 12) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

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

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

Supported Wireless LAN Configuration

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

Tip: Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the SRC. See *USB Wireless LAN Adapters* **(on page 12).**

Note: You must configure SRC to enable its wireless LAN interface. See the topic titled *Configuring Network Settings* **(on page 160) in the User Guide.**

Dual Ethernet Connection

One SRC device has two Ethernet (LAN) ports:

- ETH①10/100/1000 (marked in *green*) supports up to 1000 Mbps. This is "ETH1".
- ETH②10/100 (marked in *white*) supports up to 100 Mbps. This is "ETH2".

For more information on the two ports, see **Connection Ports** (on page 67).

You can connect both ports to *different* subnets (networks) and therefore obtain two IP addresses for wired networking. It is strongly recommended that you DO NOT connect both ports to the same subnet to avoid potential issues. Contact your IT department if you are not sure whether the two Ethernet ports are connecting to the same or different subnets.

Exception: A USB-cascading chain must connect to "only one" network. Do NOT connect both Ethernet ports of any SRC master or slave device to the LAN. See **Cascading Multiple SRC Devices for Sharing Ethernet Connectivity** *(on page 24).*

▶ **Check list when connecting both ports to the networks:**

- Both Ethernet interfaces are connecting to different subnets.
- Both Ethernet interfaces have been enabled. By default both are enabled. See **Device Info** (on page 80) and **Ethernet Interface Settings** (on page 164).
- Both Ethernet interfaces are configured with proper IPv4 and/or IPv6 settings. See **Wired Network Settings** (on page 161).
  - It is NOT required that the two Ethernet interfaces share similar network settings. For example, you can enable IPv4 settings in one interface but enable IPv6 settings in the other, or apply static IP to one but DHCP IP to the other.
- The cascading mode is disabled. By default it is disabled. See **Setting the Cascading Mode** (on page 177).

Configuring the SRC

You can initially configure the SRC via one of the following:

- A TCP/IP network that supports DHCP
- A mobile device with PDView installed
- A computer physically connected to the SRC

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

1. Connect the SRC to a DHCP IPv4 network. See **Connecting the SRC to Your Network** (on page 11).
2. Retrieve the DHCP-assigned IPv4 address. Use the front panel LCD display to retrieve it. See **Device Info** (on page 80).

3. Launch a web browser to configure the SRC. See *Login* (on page 89).

▶ **Configuration via a connected mobile device:**

1. Download the PDView app to your mobile device. See *Connecting a Mobile Device to SRC* (on page 15).
2. Connect the mobile device to SRC via USB.
3. Launch PDView to configure the SRC.

▶ **Configuration via a connected computer:**

1. Connect the SRC to a computer. See *Connecting the SRC to a Computer* (on page 21).
2. Use the connected computer to configure the SRC via the command line or web interface.
   - Command line interface: See *Initial Network Configuration via CLI* (on page 630).
   - Web interface: Launch the web browser on the computer, and type the link-local IP address or *pdu.local* to access the SRC. See *Login* (on page 89).

     For link-local IP address retrieval, see *Device Info* (on page 80).

Tip: To configure a number of SRC devices quickly, see **Bulk Configuration Methods** *(on page 23).*

Connecting a Mobile Device to SRC

Raritan's PDView is a free app that turns your iOS or Android mobile device into a local display for SRC.

PDView is especially helpful when your SRC is not connected to the network but you need to check the SRC status, retrieve its information, or change its settings.

▶ **Requirements for using PDView:**

- SRC is running any firmware version.
- If using an Android device, it must support USB "On-The-Go" (OTG).
- An appropriate USB cable is required. For information, refer to Step B below.

▶ **Step A: Download and install PDView**

1. Visit either Apple App or Google Play Store.

▪ *https://itunes.apple.com/app/raritan-pdview/id780382738*

▪ *https://play.google.com/store/apps/details?id=com.raritan.android.pd view*

2. Install PDView.

▶ **Step B: Connect the mobile device to SRC**

1. Get an appropriate USB cable for your mobile device.

   ▪ *iOS*: Use the regular USB cable shipped with your iOS mobile device.

   ▪ *Android*: Use an **USB OTG** adapter cable.

2. Connect the mobile device to the appropriate USB port on the SRC.

   ▪ *iOS*: USB-A port.

   ▪ *Android*: USB-B port
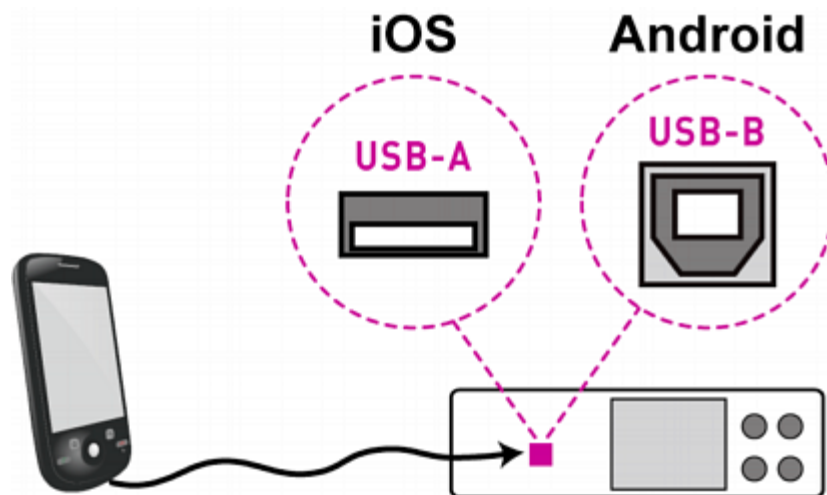
▶ **Step C: Launch PDView to access the SRC**

1. Launch the PDView app from your mobile device. Below illustrate iPad's PDView screens.

a. The "Disconnected" message displays first when PDView has not detected the SRC yet.

A diagram in PDView indicates the appropriate USB port your mobile device should connect according to your mobile operating system.
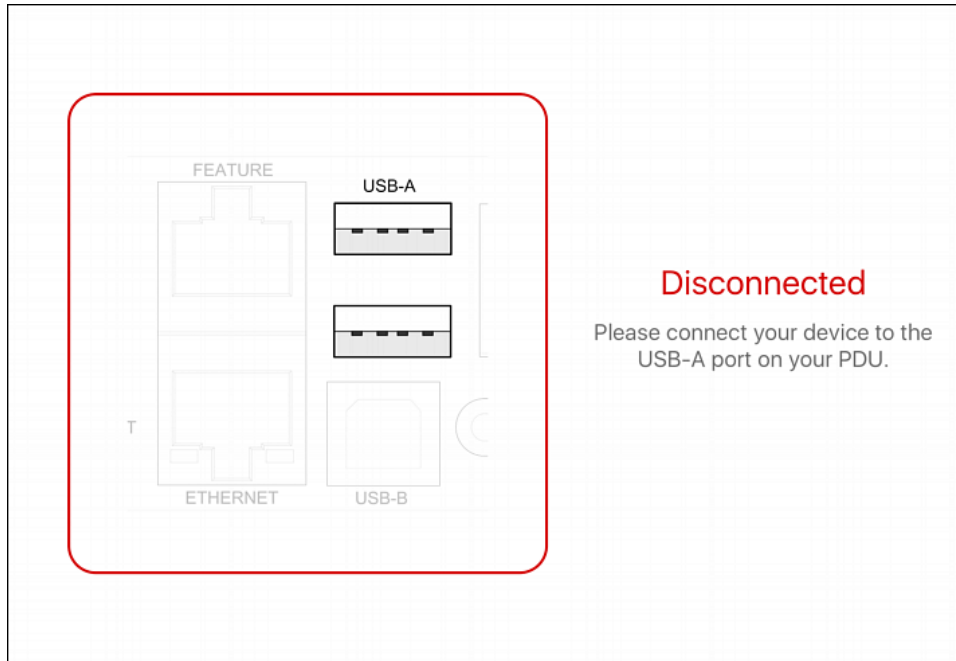
Note: PDView also shows the 'Disconnected' status during the firmware upgrade. If so, wait until the firmware upgrade finishes.

b. The PDView shows the "Connected" message when it detects the connected SRC.
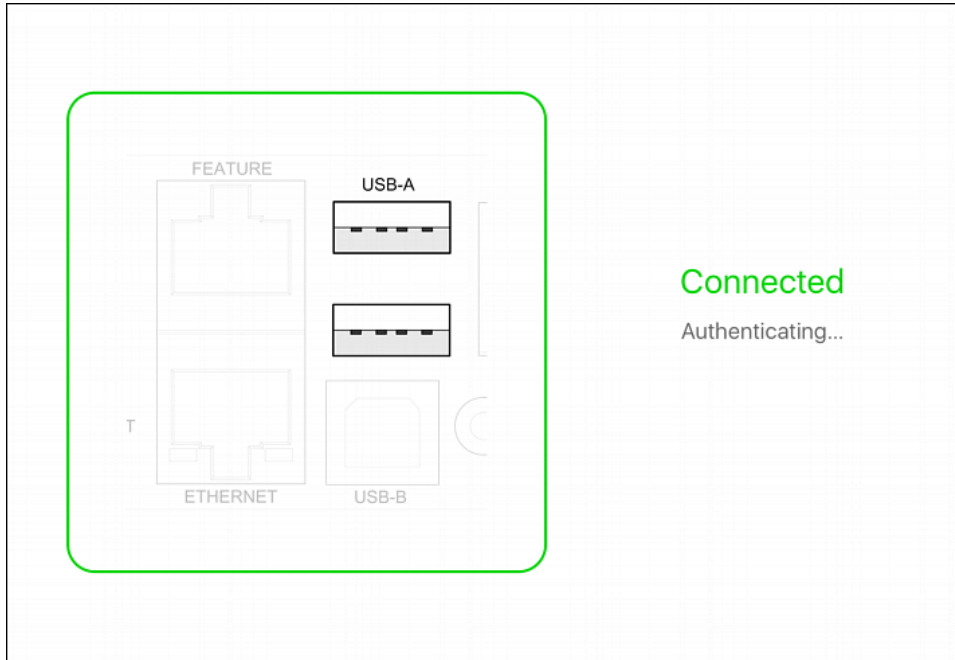
2. If the factory-default user credentials "admin/raritan" remain unchanged, PDView automatically logs in to the web interface of SRC.

   If they have been changed, the login screen displays instead and you must enter appropriate user credentials for login.

3. The web interface opens. Now you can view or modify the data of SRC.

   ▪ The web interface prompts you to change the password if this is the first time you log in.

*Tip: You can store the updated "admin" or other user credentials in PDView so that automatic login always functions properly upon detection of the SRC. See **Saving User Credentials for PDView's Automatic Login** (on page 19).*

Saving User Credentials for PDView's Automatic Login

When PDView detects SRC for the "first" time, it automatically attempts to log in with the factory-default user credentials -- *admin* (user name) and *raritan* (password).

If you have modified the factory-default user credentials, PDView's automatic login fails and the login screen displays for you to manually enter user credentials.

To make automatic login work again, you can save the modified admin credentials or any custom user credentials in PDView. A maximum of 5 user credentials can be saved, and PDView will try these credentials one by one until the login succeeds.

The following procedure illustrates iPad only, but the procedure applies to any iOS or Android mobile devices.

▶ **To save user credentials in PDView:**

1. Make sure your mobile device is NOT connected to the SRC so that PDView does NOT perform the automatic login feature after it is launched.

2. Launch PDView on your mobile device.

3. Tap the top-right icon (iOS) or (Android).
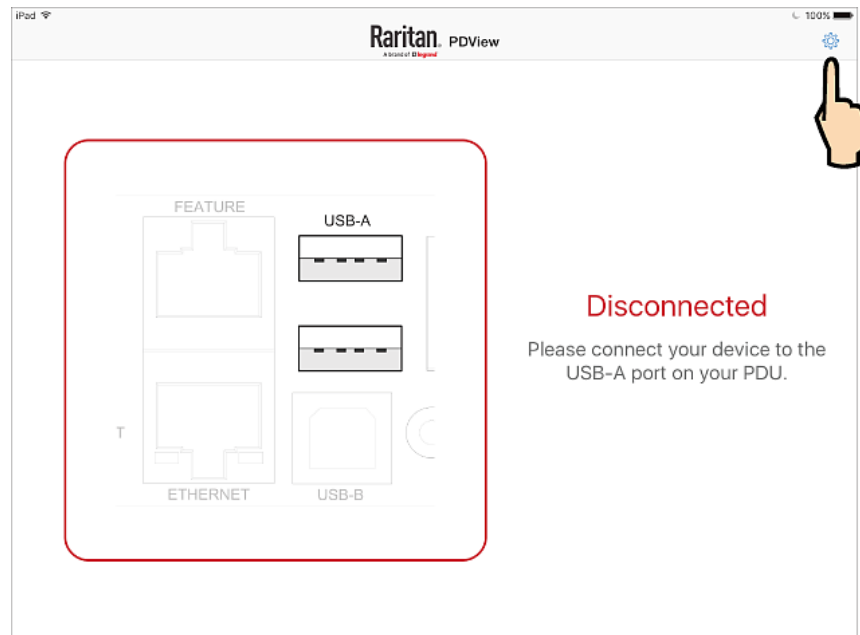
4. The user credentials setup page opens.

- Per default, three administrator user credentials are pre-configured for three companies' products:
  - *Raritan*
  - *Legrand*
  - *ServerTech (Server Technology)*

5. Modify existing user credentials or type new ones, and tap Save.
   - The pre-configured admin credentials can be removed or overwritten to meet your needs.

Connecting the SRC to a Computer

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

- Ethernet ports
- USB-B port
- RS-232 serial port (RJ-45)
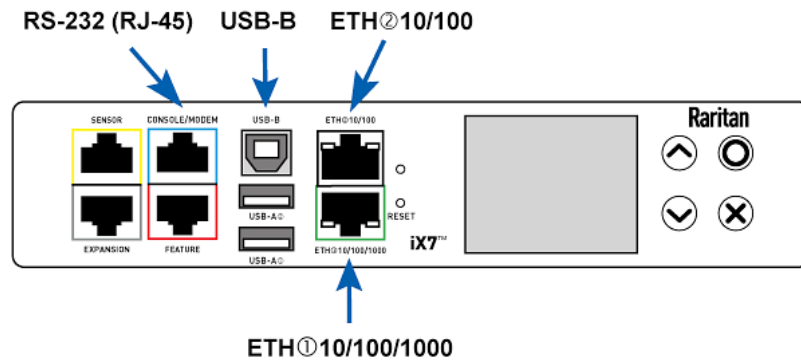
To use the command line interface (CLI) for configuration, establish an RS-232 or USB connection.

To use a web browser for configuration, make a network connection to the computer. The SRC 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*

See **APIPA and Link-Local Addressing** (on page 6).

Establish one of the following connections to a computer. Ethernet port of SRC must be enabled for the described connection to work properly, which has been enabled per default.

▶ **Direct network connection:**

1. Connect one end of a standard network patch cable to either Ethernet port of the SRC.
2. Connect the other end to a computer's Ethernet port.
3. On the connected computer, launch a web browser to access the SRC, using either link-local addressing: *pdu.local* or *169.254.x.x*. See **Login** (on page 89).

▶ **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 629).

2. Connect a USB cable between a computer's USB-A port and the USB-B port of SRC.

3. Perform *Initial Network Configuration via CLI* (on page 630).

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

▶ **Serial connection for "RJ-45" RS-232 connector:**

1. Connect the RJ-45 end of the RJ45-to-DB9 adapter cable to the RJ-45 port labeled CONSOLE / MODEM on SRCCabinet Live Chart.

   ▪ See *RJ45-to-DB9 Cable Requirements for Computer Connections* (on page 22).

2. Connect the DB9 end to your computer's RS-232 port (COM).

3. Perform *Initial Network Configuration via CLI* (on page 630).

RJ45-to-DB9 Cable Requirements for Computer Connections

An RJ45-to-DB9 adapter/cable is required for connecting the **SRC** to a computer, if the use of a USB cable is not wanted.

A third party RJ45-to-DB9 adapter/cable needs to meet the following requirements.

- RJ-45 to "DB9 female"
- RX/TX and according control pins are CROSSED

The widespread blue Cisco RJ-45 to DB9 adapter cable is highly recommended, which has the following pin assignments:

DB9 pin signal	DB9 pin No.	RJ-45 pin No.	RJ-45 pin signal
CTS	8	1	RTS
DSR	6	2	DTR
RxD	2	3	TxD
GND	5	4	GND
GND	5	5	GND
TxD	3	6	RxD
DTR	4	7	DSR
RTS	7	8	CTS
DCD	1 (Not connected)	N/A	
RI	9 (Not connected)		

Note: The blue Cisco RJ-45 to DB9 adapter cable CANNOT be used for connecting a modem. See **RJ45-to-DB9 Cable Requirements for Modem Connections** *(on page 610).*

Bulk Configuration Methods

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

▶ **A bulk configuration file downloaded from SRC:**

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

  See **Bulk Configuration** (on page 313).

▶ **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 SRC devices after connecting them to the network.

  See **Bulk Configuration or Firmware Upgrade via DHCP/TFTP** (on page 527).

▶ **Curl command:**

- *Requirement*: Two files are required -- one is a configuration file in TXT and the other is a devices list file in CSV. See **config.txt** (on page 520) and **devices.csv** (on page 522).
- *Procedure*: Upload both files to all of SRC devices one by one, using the appropriate curl command.

  See **Upload via Curl** (on page 553).

▶ **SCP or PSCP command:**

- *Requirement*: Two files are required -- one is a configuration file in TXT and the other is a devices list file in CSV.
- *Procedure*: Upload both files to all of SRC devices one by one, using the appropriate SCP or PSCP command.

  See **Uploading or Downloading Raw Configuration Data** (on page 505).

▶ **A USB flash drive:**

- *Requirement*: A FAT32- or supperfloppy-formatted USB flash drive containing two special configuration files and one devices list file is required.

- *Procedure*: Plug this USB drive into the SRC. 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 513).

Cascading Multiple SRC Devices for Sharing Ethernet Connectivity

Important: To upgrade an existing Raritan USB-cascading chain from any pre-3.3.10 firmware version to version 3.3.10 or later, follow the *Upgrade Sequence in an Existing Cascading Chain* **(on page 310).**

You can have multiple SRC devices share one Ethernet connection by cascading them via one of the interfaces below:

- USB interface
- Ethernet interface

The first one in the cascade is the master device and all the other devices follow it in the cascade. Only the master device is physically connected to the LAN -- wired or wireless.

Each device in the cascade is accessible over the network, with Bridging or Port-Forwarding cascading mode activated on the master device. See *Setting the Cascading Mode* (on page 177).

- **Bridging**: Each device in the cascading chain is accessed with a different IP address.

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

▶ **Basic cascading restrictions:**

- All devices in the chain must run "compatible" firmware versions.
  - ▪ Firmware version 3.3.10 or later is NOT compatible with pre-3.3.10 firmware versions in terms of the cascading feature so all Raritan devices in the cascading chain must run version 3.3.10 or later.

- The cascading mode of all devices in the chain must be the same.

- In the Bridging mode, the master device can have "only one" connection to the network. DO NOT connect both Ethernet ports to the network(s) unless your network has the R/STP protocol enabled.

  Note: The Port Forwarding mode does NOT have this restriction. In this mode, you can enable two wired and one wireless network connections.

- Do NOT connect cascaded devices other than master to the LAN or WLAN.
- (WIFI only) You must use Raritan's USB WIFI wireless LAN adapter instead of other WIFI adapters for wireless network connection.

▶ *Troubleshooting:*

When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain. See **Cascading Troubleshooting** (on page 624).

Cascading All Devices via USB

You must set the cascading mode before establishing the chain. See *Setting the Cascading Mode* (on page 177).

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

Both cascading modes support a maximum of 16 devices in a chain.

The following diagram illustrates SRC devices cascaded via USB.
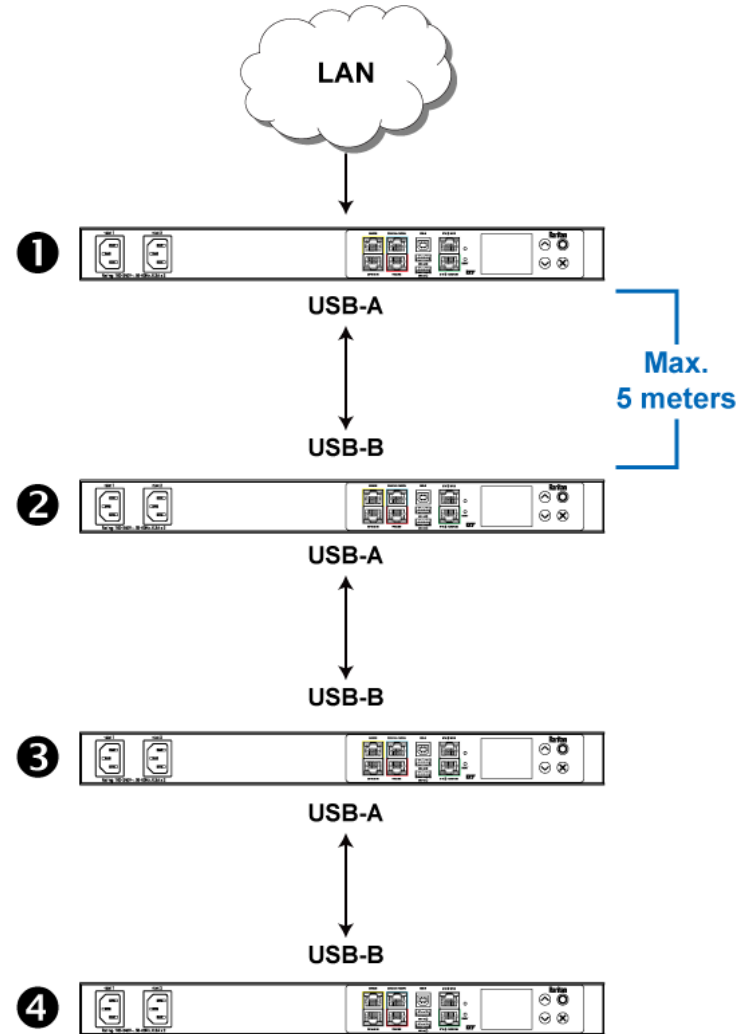
Number	Device role
➊	Master device
➋	Slave 1
➌	Slave 2

Number	Device role
④	Slave 3

▶ **To cascade SRC devices via USB:**

1. Make sure all Raritan devices are running firmware version 3.3.10 or later.

2. Choose the appropriate one as the master device.

   - When the Port Forwarding mode over "wireless LAN" is intended, the master device must be a Raritan product with two USB-A ports, such as PX3, Smart Rack Controller, EMX2-888, PX3TS or BCM2.

3. Log in to all devices one by one and select the same cascading mode.

   - **Bridging mode**:

     Set the cascading mode of all devices to Bridging.

   - **Port Forwarding mode**:

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

   See **Setting the Cascading Mode** (on page 177).

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

   - **Bridging mode**:

     Use a standard network patch cable (CAT5e or higher).

   - **Port Forwarding mode**:

     Use a standard network patch cable and/or a Raritan USB WIFI wireless LAN adapter. For information on the Raritan USB WIFI adapter, see **USB Wireless LAN Adapters** (on page 12).

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

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

7. Repeat the same step to connect more slave devices. You can cascade up to 15 slave devices.

8. (Optional) Configure or change the network settings of the master and/or slave devices as needed. See **Configuring Network Settings** (on page 160).

   - **Bridging mode**: Each cascaded device has its own network settings.

     For example, you can have some devices use DHCP-assigned IP addresses and the others use static IP addresses.

   - **Port Forwarding mode**: Only the master device's network settings should be configured.

▶ **A tip for USB cascading:**

The "USB-cascading" chain can be a combination of diverse Raritan products that support the USB-cascading feature, including PX3, PXC, Smart Rack Controller, transfer switch, PX2, BCM and EMX.

Extended Cascading with SRC Devices

SRC supports cascading via either Ethernet or USB ports. This is because they have "two" Ethernet ports.

You can use either Ethernet port on the SRC PDU for cascading.

You must set the cascading mode before establishing the chain. See *Setting the Cascading Mode* (on page 177).

Both cascading modes support a maximum of 16 devices in a chain.

When establishing a Port-Forwarding chain, make sure you follow the guidelines described in the section titled *Restrictions of Port-Forwarding Connections* (on page 32).

You can mix Ethernet and USB cascading in the SRC PDU chain if preferred. The following diagram illustrates such a chain.

The distance between two Ethernet-cascaded devices can be up to 100 meters, while the distance between two USB-cascaded devices supports up to 5 meters only.
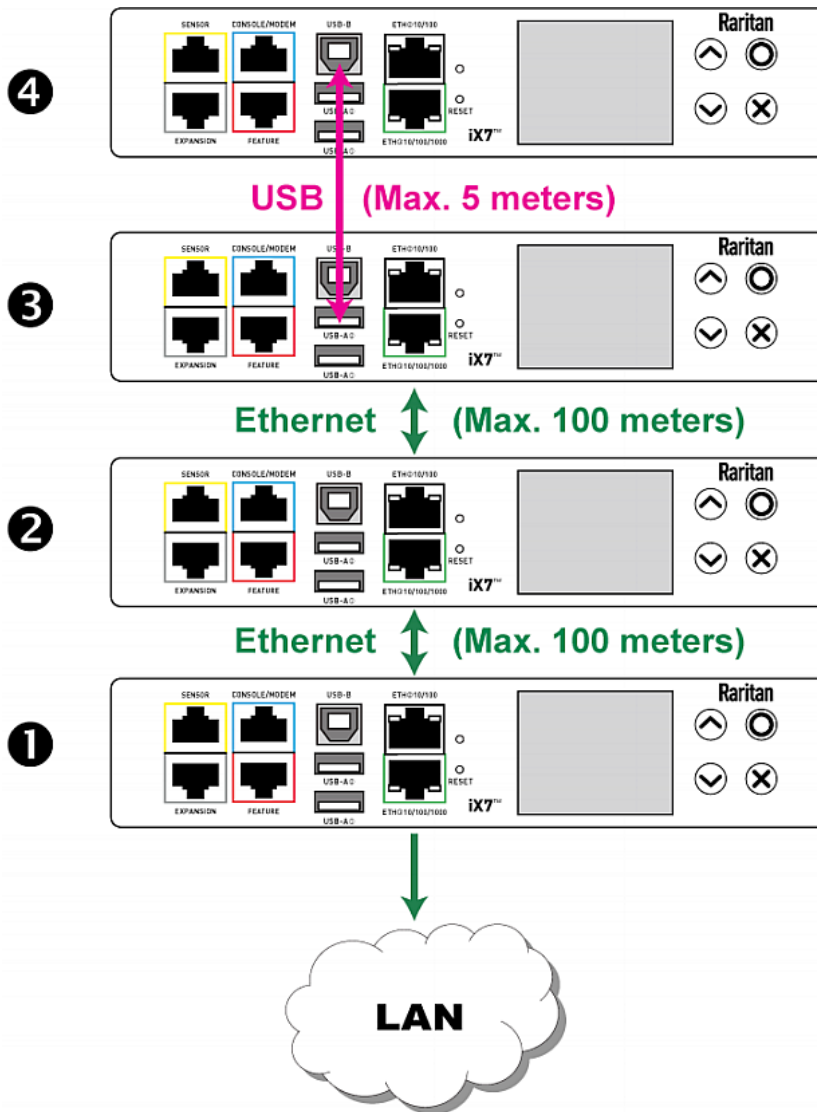
Number	Device role
❶	Master device
❷	Slave 1
❸	Slave 2
❹	Slave 3

For instructions on USB cascading, see *Cascading All Devices via USB* (on page 26).

▶ **Suggestions for extended cascading:**

- Ethernet cascading is recommended because of the longer distance, lower latency and more reliable connection it supports.
- The "green" ETH1 port (ETH⏻10/100/1000) on a Raritan master device is recommended for network connection because it supports up to 1000 Mbps.

▶ **To cascade SRC PDUs via Ethernet ports:**

1. Make sure all Raritan devices are running firmware version 3.3.10 or later.
2. Choose one SRC as the master device.
3. Log in to all devices one by one and select the same cascading mode.
    - **Bridging mode**:

      Set the cascading mode of all devices to Bridging.
    - **Port Forwarding mode**:

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

   See *Setting the Cascading Mode* (on page 177).
4. Connect the master device to the LAN, using a method below.
    - **Bridging mode**:

      Use a standard network patch cable (CAT5e or higher).
    - **Port Forwarding mode**:

      Use a standard network patch cable and/or a Raritan USB WIFI wireless LAN adapter. For information on the Raritan USB WIFI adapter, see *USB Wireless LAN Adapters* (on page 12).
5. Connect the available Ethernet port of the master device to either Ethernet port of another SRC via a standard network patch cable. This additional SRC device is Slave 1.
6. Connect Slave 1's available Ethernet port to either Ethernet port of another SRC via a standard network patch cable. The second additional device is Slave 2.
7. Repeat the same step to connect more SRC PDUs. You can cascade up to 15 slave devices.
8. (Optional) Configure or change the network settings of the master and/or slave devices as needed. See *Configuring Network Settings* (on page 160).
    - **Bridging mode**: Each cascaded device has its own network settings.

      For example, you can have some devices use DHCP-assigned IP addresses and the others use static IP addresses.
    - **Port Forwarding mode**: Only the master device's network settings should be configured.

▶ **Recommendations for cascade loops:**

You can connect both the first and the last PDU to your network (cascade loop) under the following conditions:

a. The remaining network MUST use R/STP to avoid network loops.

AND

Both the first and the last PDUs MUST either attach to the same switch or, if they are attached to two separate switches, you must configure both ports of these switches so that the STP costs are high. This prevents the STP protocol from sending unrelated traffic through the PDU cascade, which can cause bottlenecks that lead to connectivity issues in the whole network.

Restrictions of Port-Forwarding Connections

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

- Each cascaded device, except for the master device, must have only one upstream device.

- Each cascaded device, except for the last slave device, must have only one downstream device.

- Use only one cable to cascade two devices. That is, NO simultaneous connection of USB and Ethernet cables between two cascaded devices.

The following diagrams illustrate cascading connections that are NOT supported.

▶ **UNSUPPORTED connections:**

- One cascaded device has two upstream devices via Ethernet cables.

Raritan.
A brand of legrand
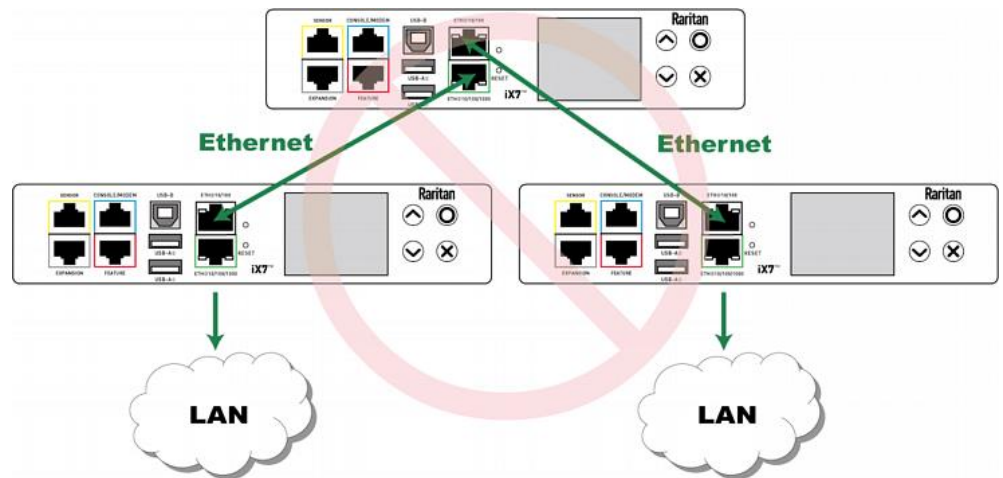
- One cascaded device has two upstream devices via Ethernet and USB cables.
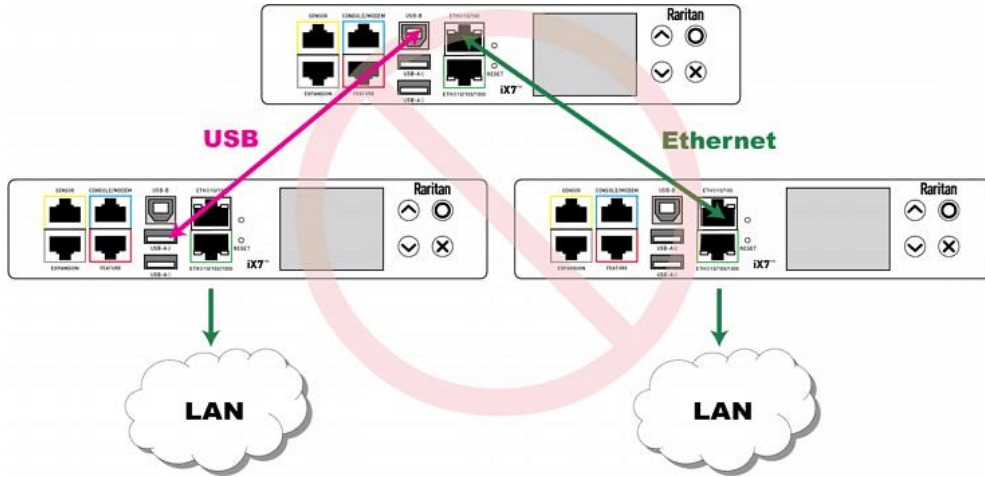
- One cascaded device has two downstream devices.
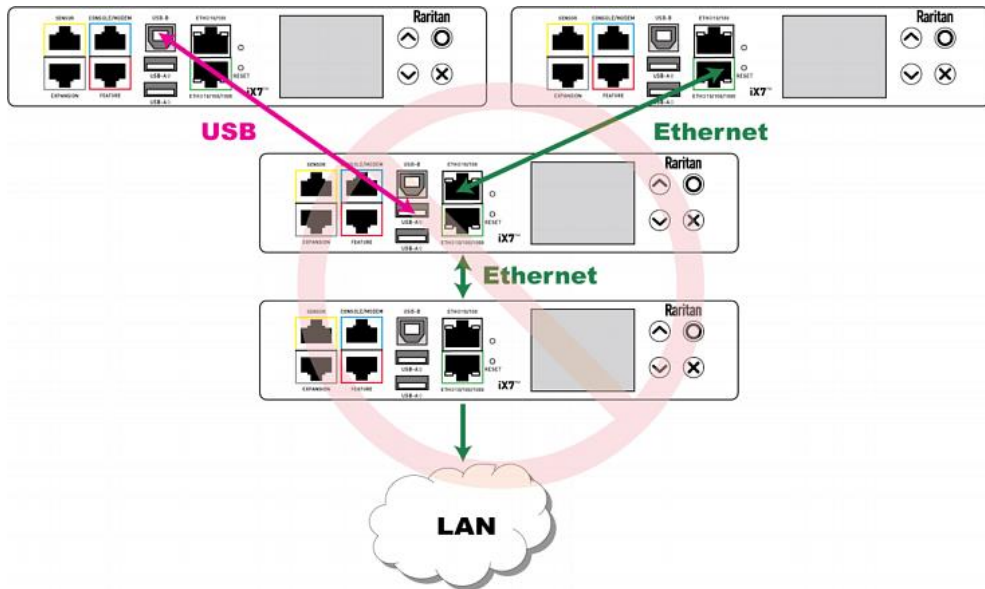
- One device is connected to another device via two cascading cables - USB and Ethernet cables.
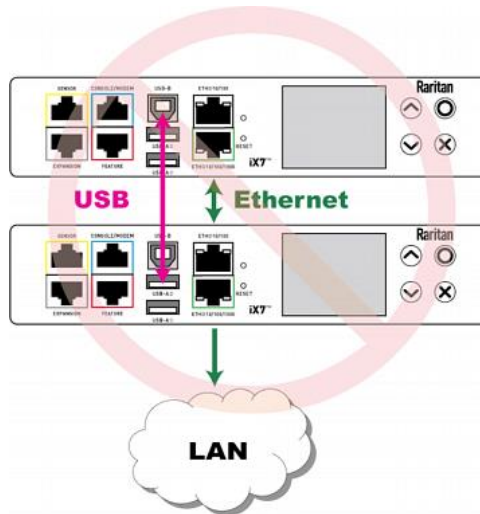
Chapter 4   Connecting External Equipment (Optional)

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

In This Chapter

Connecting Raritan Environmental Sensor Packages

Raritan's **DX** or **DX2** environmental sensor packages are required for SRC to detect the surrounding condition like the temperature, or to control a system like door handles.

> Warning: SRC does NOT support these other Raritan environmental sensor packages: DPX, DPX2, DPX3 (except for the DPX3-ENVHUB4 sensor hub). If you need a Raritan sensor hub for connecting DX or DX2, only DPX3-ENVHUB4 is supported by SRC. See *Using an Optional DPX3-ENVHUB4 Sensor Hub* (on page 40).

For detailed information on each sensor package, refer to the Environmental Sensors and Actuators Guide (or Online Help) on Raritan website's *Support page* (*http://www.raritan.com/support/*).

A DX or DX2 environmental sensor package may comprise sensors only or a combination of sensors and actuators.

SRC can manage a maximum of 32 sensors and/or actuators per SENSOR port.

Total number of supported sensors/actuators is model dependent.

Model	Number of sensors/actuators that can be managed
SRC-0100	32
SRC-0102	38, which is the sum of the following. ▪ Supports 32 managed sensors/actuators per sensor port ▪ Contains 6 sensors of onboard door handle ports and contact closure terminals

The supported maximum cabling distance is 98 feet (30 meters), except for DX2-DH2C2, which supports 29 feet (9 meters).

Identifying the Sensor Port

Warning: If you purchase Raritan's environmental sensor packages, make sure you connect them to the correct port on the SRC, or damages may be caused to SRC and/or connected sensor packages.

▶ **How to identify the SENSOR port:**

• The correct port is labeled SENSOR.

• The SENSOR port is marked with YELLOW color, as shown below.
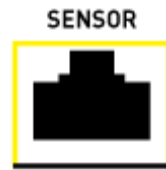
DX2 Sensor Packages

You can cascade up to 12 DX2 sensor packages.

When cascading DX2, remember that the SRC only supports a maximum of 32 sensors and/or actuators. For the total number of sensors/actuators supported by each model, see **Connecting Raritan Environmental Sensor Packages** (on page 36).

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 SRC.

Tip: To manage the last several sensors/actuators after 32nd function, you can release some "managed" sensors or actuators, and then manually bring the last several sensors/actuators into management. See **Peripherals** *(on page 108).*
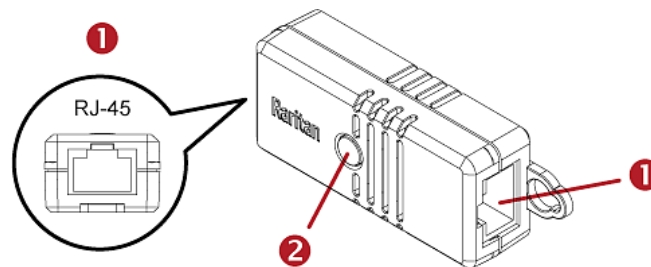
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DX2 sensor package.
❷	LED, which indicates the sensor package's status

▶ **Connect DX2 to the SRC:**

1. Connect a standard network patch cable (CAT5e or higher) to either RJ-45 port on a DX2 sensor package.

2. If you want to cascade DX2 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 DX2 package.

   b. Plug the other end into either RJ-45 port on an additional DX2 package.

   Repeat the same steps to cascade more DX2 packages.

   Exception: You CANNOT cascade DX2-DH2C2 packages. Only one DX2-DH2C2 can be connected to the SENSOR port of any SRC model.
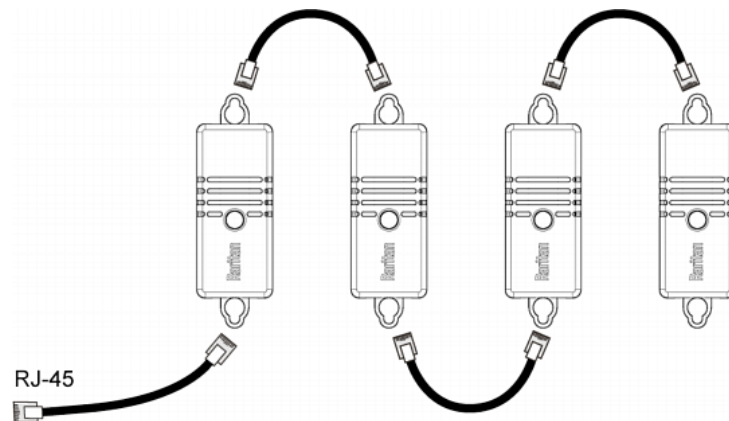
RJ-45

3. Connect the first DX2 sensor package to the SRC by plugging its cable's connector into the RJ-45 SENSOR port of the SRC.

Warning: DX2-DH2C2 and asset management strip(s) are mutually exclusive so do NOT connect both of them to the SRC simultaneously.

DX2-DH2C2

DX2-DH2C2 is one of DX2 environmental sensor package.

It is designed for cabinet access control so it is included in Raritan's SmartLock kit. For information on how to connect door handles and/or contact closure sensors, refer to:

- *Connecting a SmartLock Kit to DX2-DH2C2* (on page 43)
- *Connecting Contact Closure Detectors to DX2-DH2C2* (on page 47)

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 and Actuators 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 SRC 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 SRC.

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

Tip: To manage the last several sensors/actuators after 32nd function, you can release some "managed" sensors or actuators, and then manually bring the last several sensors/actuators into management. See **Peripherals** *(on page 108).*
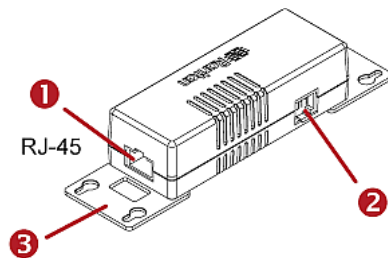
Numbers	Components
❶	RJ-45 ports, each of which is located on either end of a DX sensor package.
❷	RJ-12 port, which is reserved for future use and now blocked.
❸	Removable rackmount brackets.

▶ **Connect DX to the SRC:**

1. Connect a standard network patch cable (CAT5e or higher) to either RJ-45 port on a DX sensor package.

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.

    Exception: You CANNOT cascade DX-PD2C5 sensor packages. One SRC supports only one DX-PD2C5.
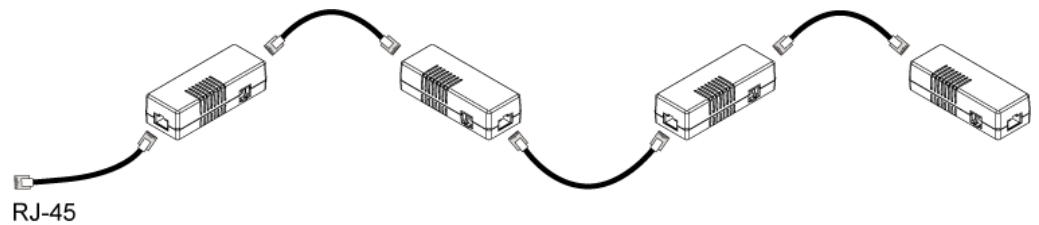
RJ-45

3. Connect the first DX sensor package to the SRC by plugging its cable's connector into the RJ-45 SENSOR port of the SRC.

    Warning: DX-PD2C5 or DX2-DH2C2 (or door handles), and asset management strip(s) are mutually exclusive so do NOT connect both of them to the SRC simultaneously.

Using an Optional DPX3-ENVHUB4 Sensor Hub

A Raritan DPX3-ENVHUB4 sensor hub increases the number of sensor ports for the SRC.

Note that the sensor hub SRC supports is DPX**3**-ENVHUB4 instead of the old hub DPX-ENVHUB4.

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

1. Connect the DPX3-ENVHUB4 sensor hub to the SRC using a standard network patch cable (CAT5e or higher).

    a. Plug one end of the cable into the IN port (Port 1) of the hub.

    b. Plug the other end of the cable into the RJ-45 SENSOR port of the SRC.

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

Raritan.
A brand of legrand

This diagram illustrates a configuration with a sensor hub connected.
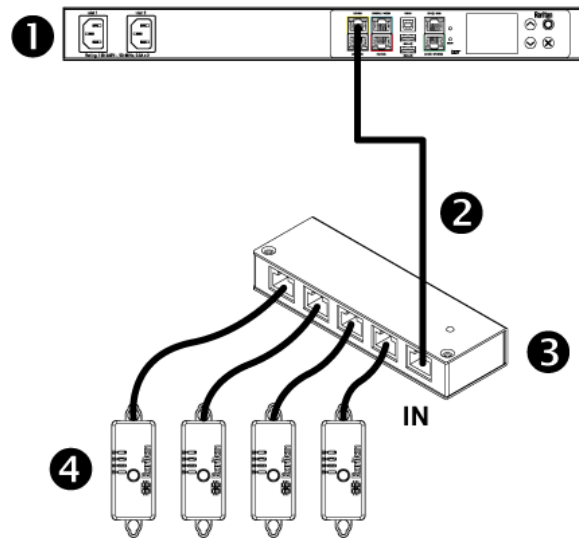
❶	SRC
❷	A standard network cable
❸	DPX3-ENVHUB4 sensor hub
❹	Any Raritan sensor packages

Connecting Door Handles or a SmartLock Kit

Raritan's door handles or SmartLock kits are required for SRC to control the access to a cabinet.

Depending on your SRC model, you may have to purchase either only door handles or a full SmartLock kit from Raritan.

Raritan's SmartLock kit contains one DX2-DH2C2 and a pair of door handles.

Note: For details, refer to the user documentation accompanying the SmartLock kit or download it from Raritan's **Support page (http://www.raritan.com/support/)**.

To detect the cabinet's door status, you need to connect third-party contact closure detectors, which are optional.

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

- For SRC without onboard door handle ports, such as SRC-0100, you need a SmartLock kit. See **Connecting a SmartLock Kit to DX2-DH2C2** (on page 43).

- For SRC with onboard door handle ports, such as SRC-0102, you can only purchase and connect Raritan's door handles instead of a SmartLock kit. See **Connecting Raritan's Door Handles to SRC Onboard Ports** (on page 45).

  Such models support a maximum of four door handles. Therefore, you can purchase a SmartLock kit and connect it to your SRC if you want your SRC to support up to four door handles.

Limitations

Read the restrictions below before connecting door handles or a SmartLock kit (that is, DX2-DH2C2 kit) to SRC.

- Up to one DX2-DH2C2 can be connected per SENSOR port of SRC.

  - SRC-0100 supports a maximum of 2 door handles by connecting one DX2-DH2C2.

  - SRC-0102 has two onboard door handle ports so it supports a maximum of 4 door handles. You can connect two door handles to onboard door handle ports and connect one DX2-DH2C2 to its SENSOR port.

- Only the door handles sold with DX2-DH2C2 are supported.

- No hot plugging or hot swapping with door handles when they are directly or indirectly connected to a *powered* SRC.

  - That is, no connection or disconnection of door handles when they are powered.

- The maximum cabling length for door handles or SmartLock kit is 29 feet (9 meters). For details, refer to the following diagram.
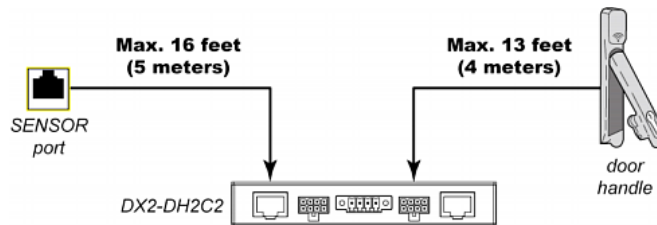
Connecting a SmartLock Kit to DX2-DH2C2

You need a SmartLock kit if your SRC does NOT include a built-in DX2-DH2C2, such as SRC-0100.

▶ **Overview:**

No.	Component	Function
❶	Two pairs of contact closure sensor terminals	Connect to third-party contact closure detectors/switches for detecting the door open/closed status.
❷	Two door handle ports	Connect to the standard category cable of the door handle. The two door handles are usually attached to different doors of the same cabinet.

No.	Component	Function
❸	Two RJ-45 ports	Connect a standard network patch cable for either or both purposes below: • Connect to the **SENSOR** port (yellow) of SRC. • Cascade DX2 sensor package(s). See **DX2 Sensor Packages** (on page 37). *Exception: You CANNOT cascade DX2-DH2C2 packages.*

▶ **Connection procedure:**

1. Connect supported door handles to DX2-DH2C2.
   - ▪ (Optional) Connect contact closure detectors/switches for detecting door status to DX2-DH2C2. See **Connecting Contact Closure Detectors to DX2-DH2C2** (on page 47).

2. Connect DX2-DH2C2 to the SENSOR port of SRC. Always connect DX2-DH2C2 directly to the sensor port. If you are cascading with other sensors, the DX2-DH2C2 must be in the first position, directly connected to the sensor port.

Connecting Raritan's Door Handles to SRC Onboard Ports

You only need to purchase door handles if your SRC has a built-in DX2-DH2C2, such as SRC-0102.

▶ **SRC door handle ports and terminals:**

No.	Component	Function
❶	Two pairs of contact closure sensor terminals	Connect to third-party contact closure detectors/switches for detecting the door open/closed status.
❷	Two door handle ports	Connect to the standard category cable of the door handle
		The two door handles are usually attached to

45

No.	Component	Function
		different doors of the same cabinet.

▶ **Connection procedure:**

1. Connect Raritan door handles to onboard door handle ports of SRC.

2. (Optional) Connect contact closure detectors/switches for detecting door status to contact closure terminals of SRC. See *Connecting Contact Closure Detectors to SRC Onboard Terminals* (on page 48).

Connecting Contact Closure Detectors

If you connect any door handles or SmartLock kit to SRC to control the access to any cabinet, you can also connect third-party contact closure detectors/switches to detect whether the doors of the same cabinet are open or closed.

Note that contact closure detectors/switches are NOT required for cabinet access control.

Both DX2-DH2C2 and SRC's contact closure terminals contain two contact closure channels, each of which comprises two termination points. Therefore, you can connect at least two contact closure detectors/switches per unit.

*   To connect contact closure detectors/switches to DX2-DH2C2, see *Connecting Contact Closure Detectors to DX2-DH2C2* (on page 47).

*   To connect contact closure detectors/switches to onboard CC terminals on the SRC, see *Connecting Contact Closure Detectors to SRC Onboard Terminals* (on page 48).

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

Raritan.
A brand of ⬛legrand®

Connecting Contact Closure Detectors to DX2-DH2C2

► **Overview:**

No.	Component	Function
❶	Two pairs of contact closure sensor terminals	See the table in the topic titled *Connecting a SmartLock Kit to DX2-DH2C2* (on page 43).
❷	Two door handle ports	
❸	Two RJ-45 ports	

► **Connection procedure:**

1. Connect contact closure sensors to the terminals. See **Connecting Detectors/Switches to Contact Closure Terminals** (on page 49).

2. Connect DX2-DH2C2 to the SENSOR port of SRC.

Connecting Contact Closure Detectors to SRC Onboard Terminals

► **Overview:**
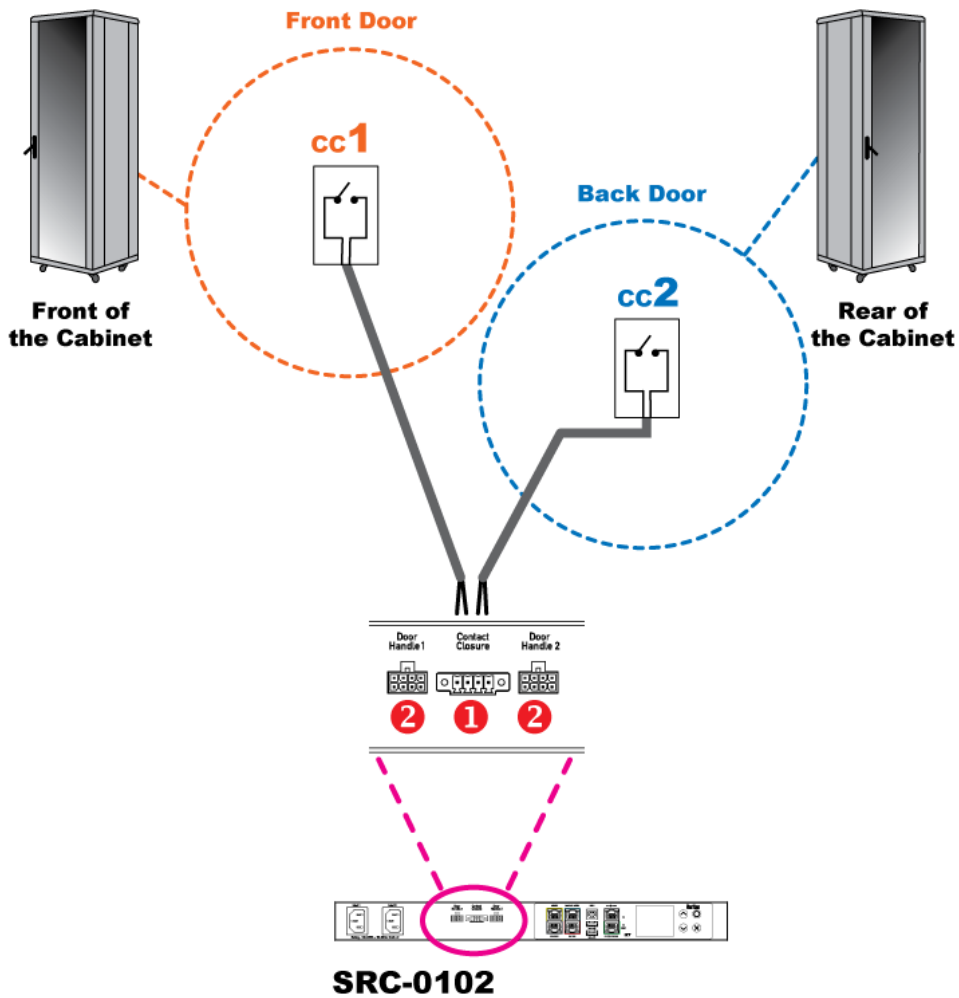
No.	Component	Function
❶	Two pairs of contact closure sensor terminals	See the table in the topic titled **Connecting Raritan's Door Handles to SRC Onboard Ports**

No.	Component	Function
❷	Two door handle ports	(on page 45).

▶ **Connection procedure:**

1. First turn the SRC upside down.
2. Connect contact closure sensors to the terminals. See *Connecting Detectors/Switches to Contact Closure Terminals* (on page 49).

Connecting Detectors/Switches to Contact Closure Terminals

No matter it is DX2-DH2C2 or the SRC device with onboard door handle ports, the location of contact closure terminals are always located between the two door handle ports as illustrated below.
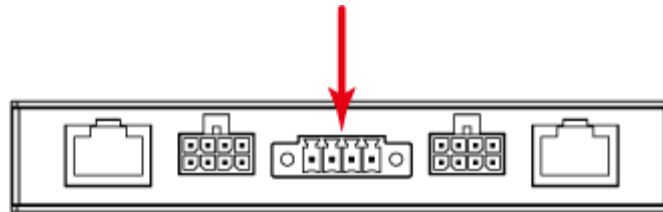
DX2-DH2C2 comprises two parts: sensor box and terminal module. The terminal module is detachable so it is convenient to connect/disconnect discrete detectors/switches. SRC with onboard door handle ports also have this terminal module.
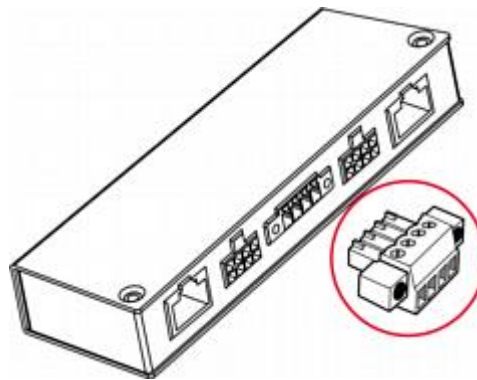
The following illustrates the procedure of connecting contact closure detectors/switches to DX2-DH2C2. This procedure can also apply to SRC onboard contact closure terminals but you have to turn the terminal module upside down so that you can see the four screws for four termination points.
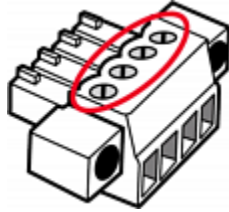
▶ **To make connections after the terminal module is separated:**

1. Loosen the screws at two sides of the terminal module.

   Note: The two screws are not removable so just loosen them.
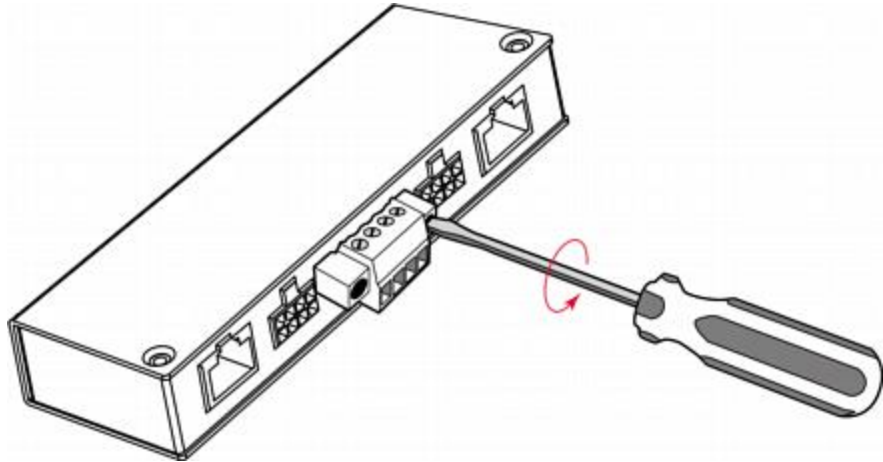
2. Separate the terminal module from the sensor box.
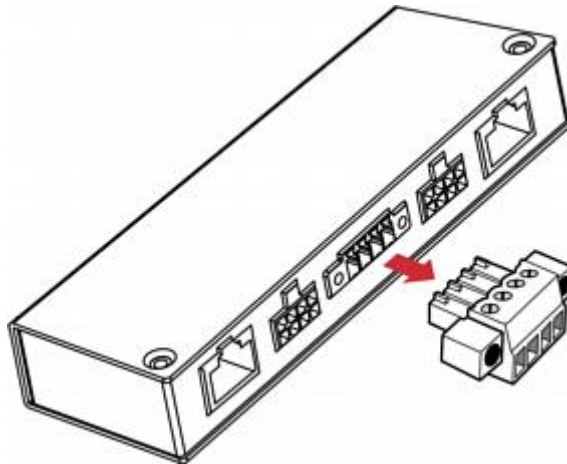
3. Strip the insulation around 12 mm from the end of each wire of discrete detectors/switches.

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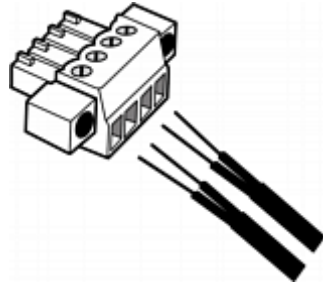
5. Use a screwdriver with a 2.5 mm wide shaft to tighten the screws above each termination point to secure the wires, using a torque of 0.196 N·m (2 kgf·cm).

   Note: If your terminal module is separated from SRC, you must flip it to secure the four screws.
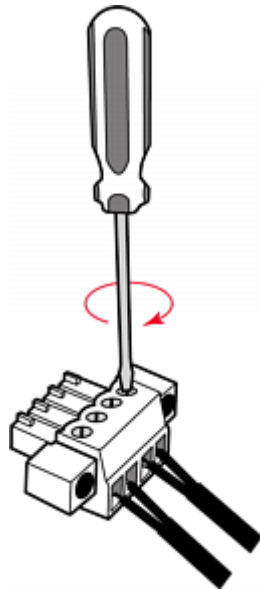
6. After connecting detectors/switches to the terminal module, plug the terminal module back into the sensor box, and then tighten the screws at two sides of the terminal module.
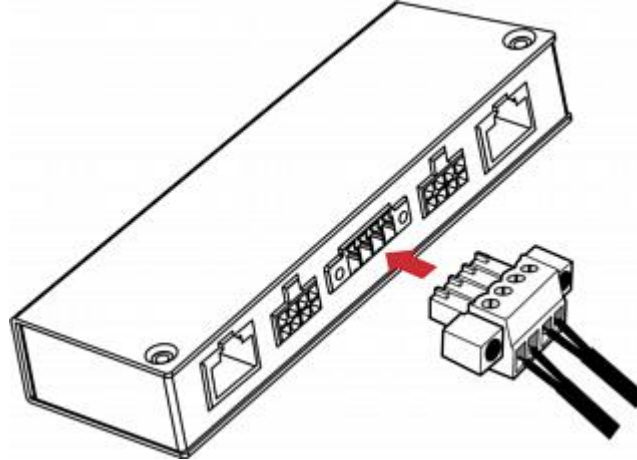
▶ **To make connections when the terminal module is attached:**

You can also connect a detector/switch when the terminal module remains attached to the sensor box. For detailed information on the insulation and torque, refer to the above procedure.

1. Strip the insulation of each wire of both detectors/switches, and insert them to the termination points.
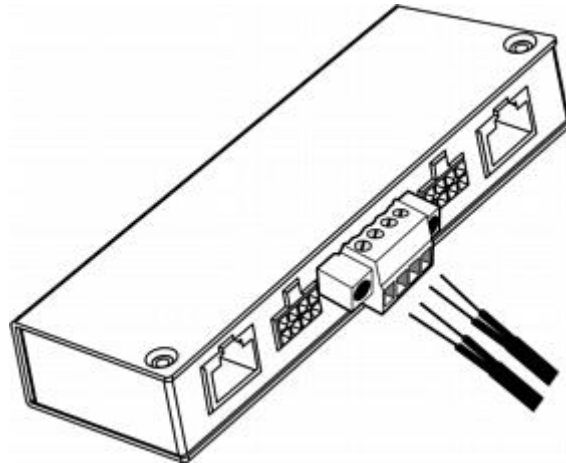
2. Tighten the screws above each termination point to secure wires.

Raritan.
A brand of ☐ legrand®

- If you are attaching wires to SRC onboard contact closure terminals, turn it upside down to tighten the screws.
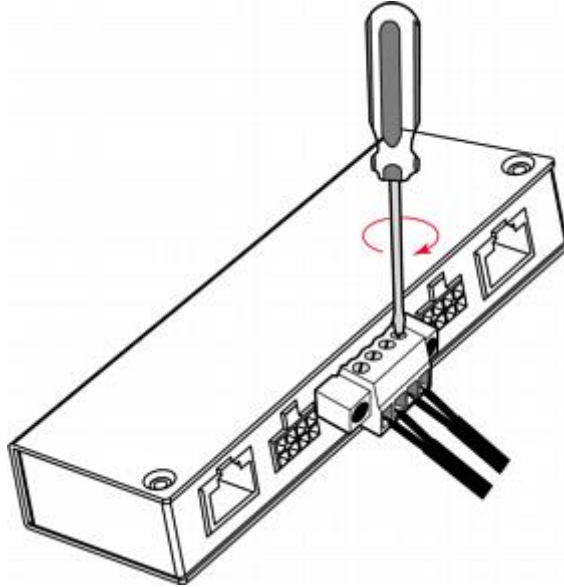
Connecting Asset Management Strips

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

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

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

Warning: DX-PD2C5 or DX2-DH2C2 (or door handles), and asset management strip(s) are mutually exclusive so do NOT connect both of them to the SRC simultaneously.

Combining Regular Asset Strips

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

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

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

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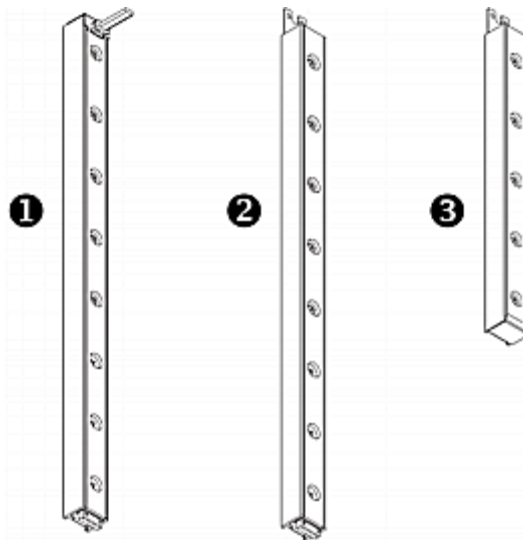
❶	8U MASTER asset strip with 8 tag ports
❷	8U SLAVE asset strip with 8 tag ports
❸	5U "ending" SLAVE asset strip with 5 tag ports

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

▶ **To assemble asset strips:**

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

Raritan.
A brand of ☐ legrand

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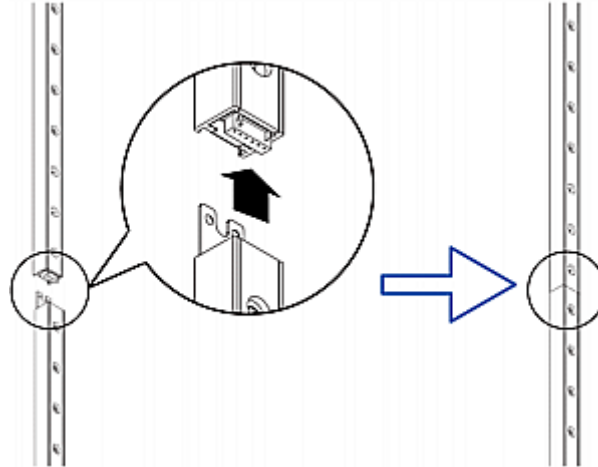
2. Connect another 8U slave strip to the one being attached to the master strip in the same manner as Step 1.

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

   - The final slave strip can be 8U or 5U, depending on the actual height of your rack.

   - Connect the "ending" asset strip as the final one in the assembly.

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

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

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

Introduction to Asset Tags

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

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

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

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

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

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

Connecting Regular Asset Strips to SRC

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

The SRC supplies power to the connected asset strips.

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

Note: To configure asset strips after finishing the asset strip connection, see **Asset Strip** *(on page 132).*

Connecting Asset Tags to SRC

The following asset tag connection procedure applies to all SRC models.

Note that the maximum cabling distance supported for each connected asset strip assembly is 10 meters.

▶ **To connect a regular asset strip assembly to SRC:**

1. Assemble regular asset strips according to your needs. See *Combining Regular Asset Strips* (on page 54).

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 56).

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

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

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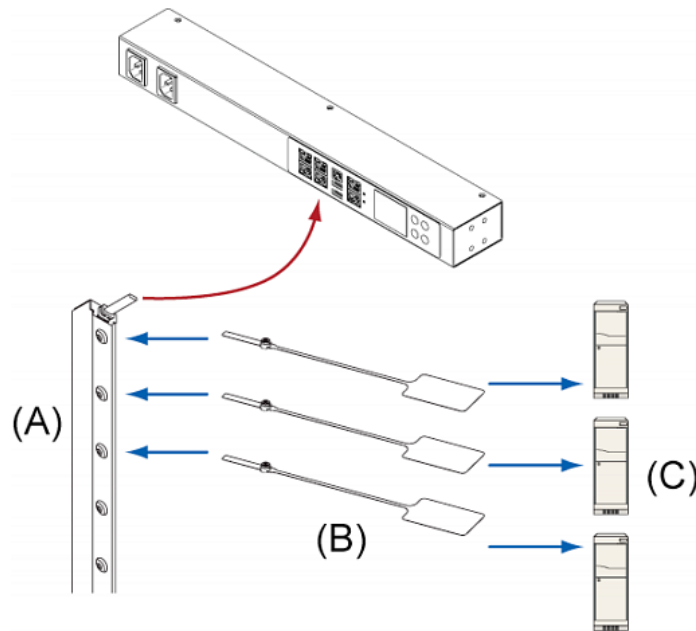
(A)	MASTER asset strip
(B)	Asset tags
(C)	IT devices

Connecting Blade Extension Strips

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

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

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

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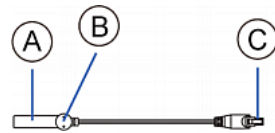
A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

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

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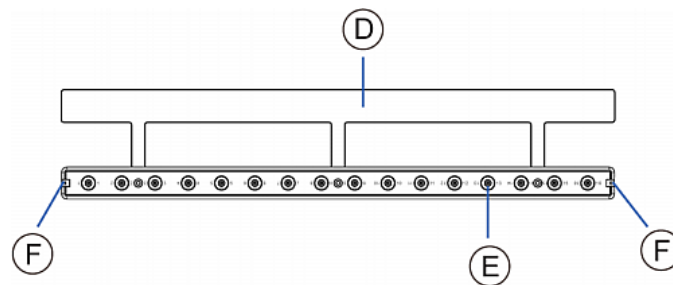
D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

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

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

1. Connect the tag connector cable to the blade extension strip.

   ▪ Plug the cable's connector into the socket at either end of the blade extension strip.
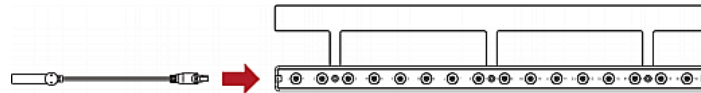
2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.
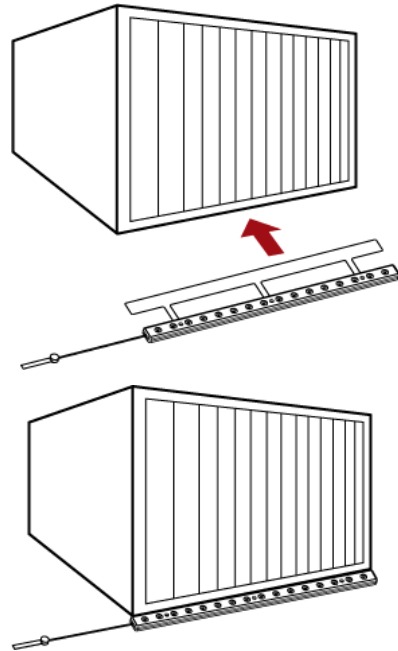
3. Connect one end of an asset tag to a blade server and the other end to the blade extension strip.

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

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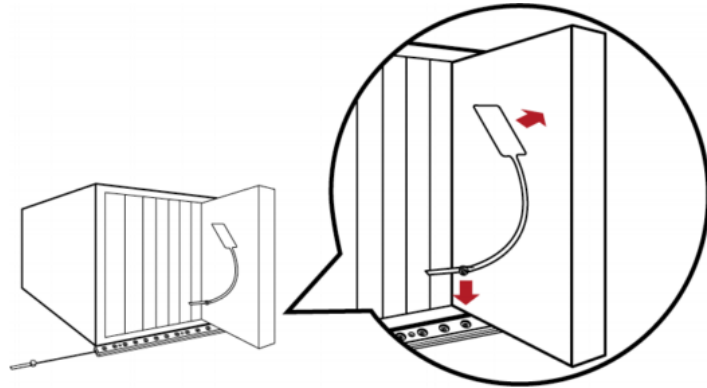
4. Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.

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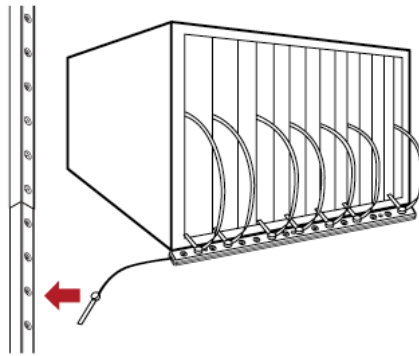
6. Repeat the above steps to connect additional blade extension strips. Up to 128 asset tags on blade extension strips are supported per FEATURE port.

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

Connecting Composite Asset Strips (AMS-Mx-Z)

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

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

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

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

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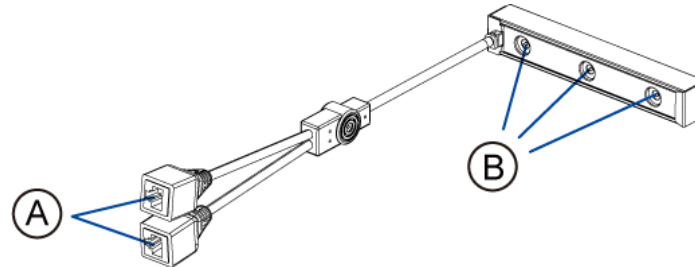
A	Two RJ-45 connectors
B	Tag ports

Important: DO NOT hot swap or hot plug any AMS-Mx-Z in a composite asset strip chain after connecting the chain to the SRC device. Doing so may cause the device's FEATURE port to malfunction.

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

If there are only 2 or 3 IT devices to track, you can connect only one AMS-M2-Z or AMS-M3-Z to the SRC device. In this case, go to step 2. If there are more than 2 or 3 IT devices, you need to daisy chain multiple composite asset strips and start from step 1.

1. (Optional) Daisy chain multiple composite asset strips.

   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 first composite asset strip.

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

   d. Repeat the same steps to connect more composite asset strips. See **Daisy-Chain Limitations of Composite Asset Strips** (on page 62) for the maximum number of composite asset strips supported per chain.

   Note: Different types of composite asset strips can be mixed in a chain.

2. Connect the composite asset strip(s) to the SRC device via a standard network patch cable (CAT5e or higher).

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

   ▪ For a composite asset strip chain, connect the cable to the "Input" port of the first asset strip.

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

3. Affix an asset tag to the IT device. Then connect this asset tag to the composite asset strip by plugging the tag connector into the tag port on the composite asset strip. For details, see **Connecting Regular Asset Strips to SRC** (on page 56).

4. (Optional) For a chain, it is highly recommended using the cable ties to help hold the weight of all connecting cables.

AMS-M2-Z
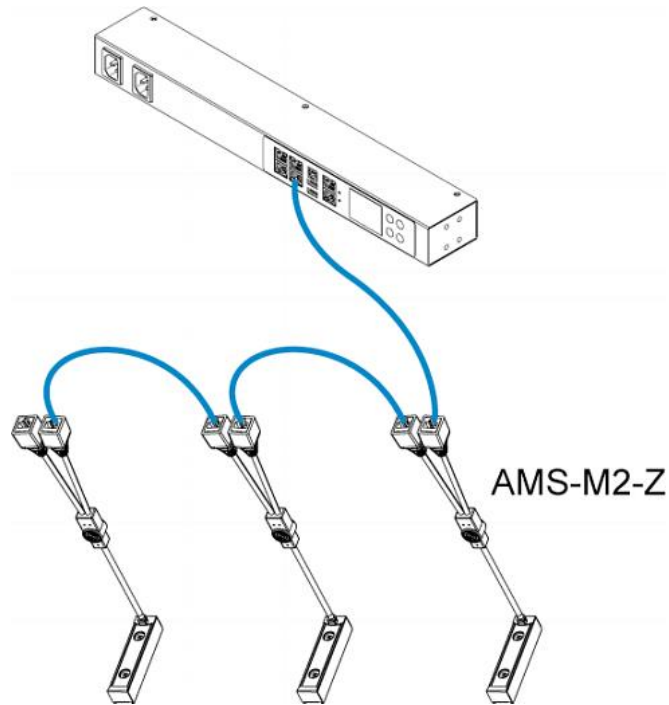
5. Repeat Step 3 to connect IT devices to the other composite asset strips in the chain.

Daisy-Chain Limitations of Composite Asset Strips

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

- The maximum cable length between composite asset strips is 2 meters, but the total cable length cannot exceed 10 meters.

- The maximum number of composite asset strips that can be daisy chained depends on the Raritan product you purchased.

- It is NOT supported to hot swap or hot plug any AMS-Mx-Z in a composite asset strip chain that has been connected to Raritan's PDU, SRC, or PMC. Therefore, first disconnect the chain from the device when you need to swap or add any AMS-Mx-Z to the chain.

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

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

Note: In case you hot swap or hot plug any AMS-Mx-Z in a chain, causing the FEATURE port of the SRC to malfunction, you can power cycle or reset the SRC to restore the FEATURE port.

Connecting a Logitech Webcam

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

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

- Logitech® HD pro C920
- Logitech® Webcam® Pro 9000, Model 960-000048

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

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

The SRC supports up to two webcams. After connecting a webcam, you can retrieve visual information from anywhere through the SRC web interface.

For more information on the Logitech webcam, refer to the user documentation accompanying it.

▶ **To connect a webcam:**

1. Connect the webcam to the USB-A port on the SRC. The SRC 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 SRC web interface after the connection is complete. See *Configuring Webcams and Viewing Live Images* (on page 326).

Connecting a GSM Modem

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

- MC52iT
- MC55iT
- EHS6T

See **Available Actions** (on page 238) for more information on SMS messages.

Note: SRC cannot receive SMS messages.

▶ **To connect the GSM modem:**

1. Connect the GSM modem to the serial port labeled CONSOLE / MODEM on the SRC.
   - A third party RJ-45 to "DB9 male" adapter/cable is required for this connection. See **RJ45-to-DB9 Cable Requirements for Modem Connections** (on page 610).
2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.
3. Configure the GSM modem settings in the SRC to specify the modem's SIM PIN number and the recipient phone number. See **Configuring the Serial Port** (on page 290).

Connecting an Analog Modem

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

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

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

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

Note that the SRC 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 SRC.

- A third party RJ-45 to "DB9 male" adapter/cable is required for this connection. See *RJ45-to-DB9 Cable Requirements for Modem Connections* (on page 610).

You need to enable the modem dial-in support to take advantage of this feature, see *Configuring the Serial Port* (on page 290).

Connecting an External Beeper

The SRC 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 SRC to switch on or off the external beeper when specific events occur. See *Event Rules and Actions* (on page 224).

▶ **To connect an external beeper:**

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

Connecting a Modbus RTU Device or Bus

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

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

1. Connect a Modbus RTU device, or a Modbus bus with multiple RTU devices, to the SRC 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 SRC.
2. On the SRC, enable and properly configure the Modbus Gateway feature. See *Changing Modbus Settings* (on page 192).

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

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

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

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

  If the Modbus TCP client does not support unit identifier addressing, refer to *Changing Modbus Settings* (on page 192).

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

Chapter 5   Introduction to SRC Components

This chapter explains how to use the SRC device, including:

- Introduction to connection ports
- Operation of the front panel display
- The internal beeper's behavior
- The reset button

In This Chapter

Connection Ports

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

Standard Ports

All SRC models have the following 9 standard ports.

Port	Used for...
USB-B	- Cascading SRC devices for sharing a network connection. See **Cascading All Devices via USB** (on page 26). - Establishing a USB connection between a computer and the SRC for: - Using the command line interface. - Performing the disaster recovery. Contact Raritan Technical Support for instructions. - Connecting to an Android mobile device for viewing or configuring the SRC. - See **Connecting a Mobile Device to SRC** (on page 15).

Port	Used for...
USB-A	**This is a "host" port, which is powered, per USB 2.0 specifications.** • Connecting to an iOS mobile device for viewing or configuring the SRC. See **Connecting a Mobile Device to SRC** (on page 15). • Connecting a USB device, such as a Logitech® webcam or wireless LAN adapter. • Cascading SRC devices for sharing a network connection.
FEATURE	Connection to one of the following devices: ▪ A Raritan access product, such as Dominion KX III KVM switch, with the use of a power CIM. ▪ 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. ▪ A Raritan asset management strip, which allows you to track the locations of IT devices on the rack. See **Connecting External Equipment (Optional)** (on page 35). Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.
CONSOLE/ MODEM **(RJ-45)**	Establishing a serial connection between the SRC and a computer or modem. You need a third-party RJ-45 to DB9 adapter/cable for the connection(s). Note that the RJ-45 to DB9 adapter/cable for connecting a computer is different from the one for connecting a modem. For details, refer to: ▪ **RJ45-to-DB9 Cable Requirements for Computer Connections** (on page 22) ▪ **RJ45-to-DB9 Cable Requirements for Modem Connections** (on page 610)
SENSOR **(RJ-45)**	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.

Raritan.
A brand of ☐ legrand®

Port	Used for...
ETH①10/100/1000, ETH②10/100/1000	SRC has two Ethernet ports. Connecting the SRC to your company's network via a standard network patch cable (Cat5e/6). This connection is necessary to administer or access the SRC remotely. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. You can use either Ethernet port for network connection or cascading. See *Extended Cascading with SRC Devices* (on page 29). *Note: Network connection to this port is not required if wireless connection is preferred, or if the SRC is a slave device in the cascading configuration.*
EXPANSION	• NO function now • Reserved for future use

Onboard Door Handle Ports and Contact Closure Terminals

Only specific SRC models like SRC-0102 have onboard door handle ports and contact closure terminals. See *Product Models* (on page 3).

These ports are functionally identical to DX2-DH2C2.

Port	Description
Door handle ports	You can connect a maximum of two door handles supported by DX2-DH2C2 for cabinet access control. ▪ See *Connecting Raritan's Door Handles to SRC Onboard Ports* (on page 45). Note that door handles and asset strips are mutually exclusive so you CANNOT connect them simultaneously.
Contact closure terminals	You can connect a maximum of two contact closure sensors to monitor a selected door's status. ▪ See *Connecting Contact Closure Detectors to SRC Onboard Terminals* (on page 48).

Dot-Matrix LCD Display

An SRC model comes with a dot-matrix LCD display.

Automatic and Manual Modes

After powering on or resetting the SRC, the front panel LCD display first shows some dots, then Raritan logo and finally enters the automatic mode.

▶ **Automatic mode without alerts available:**

In this mode, the LCD display cycles through the sensor/actuator information as long as there are no alerts.

If there are no sensors/actuators managed, the display shows this message instead: *No managed devices*.

You can look into detailed information by selecting a specific sensor/actuator using ⌃ / ⌄ and ⬤. For operation details, see **Peripherals** (on page 76).

▶ **Manual mode:**

To view more information of your SRC, enter the manual mode.

Press ⬤ or ✖ to enter the manual mode, where the Main Menu is first displayed. See **Main Menu** (on page 72).

To return to the automatic mode, press ✖ once or multiple times.

▶ **When an alert exists:**

- In the automatic mode, when an alert occurs, the LCD display stops cycling through information, and warns you by showing the alerts notice in a yellow or red background. See **Alerts Notice in a Yellow or Red Screen** (on page 85).

  To enter the manual mode, press ✖.

- In the manual mode, both the top and bottom bars will turn yellow or red to indicate the presence of any alert. See **Operating the Dot-Matrix LCD Display** (on page 71).

Control Buttons
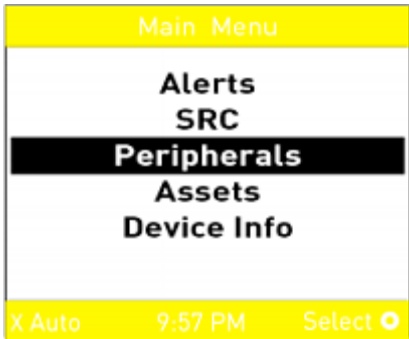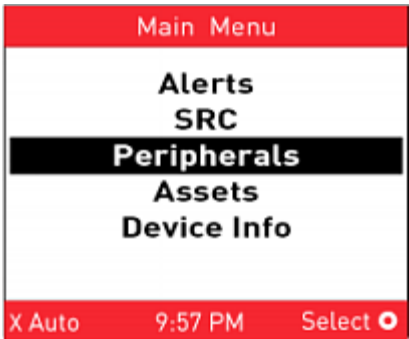
Use the control buttons to navigate to the menu in the manual mode.

Button	Function
⌃	Up
⌄	Down
◉	OK
⊗	Back -- OR -- Switch between automatic and manual modes

Operating the Dot-Matrix LCD Display

Enter manual mode when you want to operate the dot-matrix LCD display. You can use the dot-matrix LCD display to:

- Show information of the SRC, built-in components, or connected peripheral devices
- Control actuators if any

▶ **Color changes of the display's top and bottom bars:**

- In the manual mode, both the top and bottom bars will turn yellow or red to indicate the presence of any alert. For color definitions, see *Yellow- or Red-Highlighted Sensors* (on page 115).

Screen with yellow bars	Screen with red bars
All alerts enter the warning level only.	Partial or all alerts enter the critical level.

- Both bars turn black when there are NO alerts.

Screen with black bars
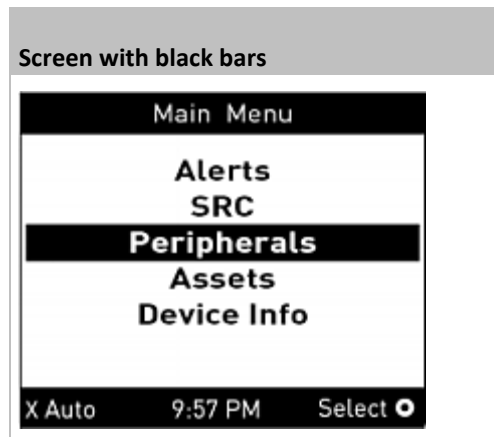
Main Menu

The Main Menu contains 5 menu commands.

Control buttons that can be used and the system time are shown at the bottom of the LCD display.
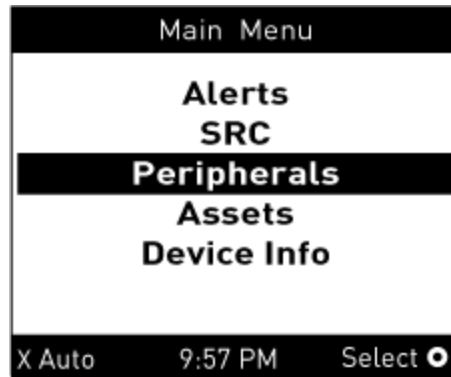
If any alerts exist, the top and bottom bars on the LCD display change the color from black to yellow or red. See **Operating the Dot-Matrix LCD Display** (on page 71).

Menu command	Function
Alerts	Indicates all alerted sensors, if any. See **Alerts** (on page 73).
SRC	Shows the internal beeper's state, and, if it is on, the reason for turning on. See **SRC** (on page 75).
Peripherals	Shows the information of connected Raritan environmental sensors or actuators, such as the temperature sensor. You can turn on or off a connected actuator with this command. See **Peripherals** (on page 76).
Assets	Shows the asset management information if Raritan asset management equipment is connected to your SRC. See **Assets** (on page 79).
Device Info	Shows the device information, such as IP and MAC address. See **Device Info** (on page 80).

Note: To return to the automatic mode, press ⊗. See **Automatic and Manual Modes** (on page 70).

Alerts

The "Alerts" menu command shows a list of the following alerted sensors, including both internal and external sensors.

- Any numeric sensor that enters the warning or critical range if the thresholds have been enabled
- State sensors that enter the alarmed state

Tip: The same information is available in the web interface's Dashboard. See **Dashboard - Alerted Sensors** (on page 103).

If there are no alerted sensors, the LCD display shows the message "No Alerts."

▶ **To view alerted sensors:**

1. Press ⌃ or ⌄ to select "Alerts" in the Main Menu, and press ◎.
2. Alerted sensors, if any, are highlighted in either red or yellow. For color definitions, see **Yellow- or Red-Highlighted Sensors** (on page 115).

▪ The top and bottom bars on the LCD display may be yellow or red, depending on the type(s) of available alerts. See **Operating the Dot-Matrix LCD Display** (on page 71).

Number	Description
❶	Alarm names.
❷	The time the alarm occurred. If the alarm occurred at least two times, then more information is shown. ▪ Number of alarms ▪ The first occurrence time ▪ The last occurrence time
❸	Alerted sensor names.
❹	Sensor readings and/or states. A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only. Available states are listed below. For further information, see **Sensor/Actuator States** (on page 118). ▪ Alarmed ▪ Lower Critical = below lower critical ▪ Lower Warning = below lower warning ▪ Upper Warning = above upper warning ▪ Upper Critical = above upper critical ▪ Open (only available for Raritan PDUs with overcurrent protectors)
❺	The 'Details' command appears for alarms only. ▪ If your Alert List comprises alerted sensors only, then 'Details' is not shown.

3. Press ⌃ or ⌄ to view additional pages. When there are multiple pages, page numbers appear in the top-right corner of the display.

SRC

The "SRC" menu command shows the internal beeper state.

Tip: The internal beeper state information is also available in the SRC web interface. See **SRC** *(on page 106).*

▶ **To view or configure SRC information:**

1. Press ⌃ or ⌄ to select "SRC" in the Main Menu, and press ◉.
2. The internal beeper state is shown: Active or Off.
   - In the Active state, the reason of turning on the beeper is indicated, and the top/bottom bars turn red.

   - To mute the beep sound immediately, press ◉. See **Muting the Internal Beeper** (on page 75).

3. Press ⌄ to show the status of the 12V power supply to the controller. For details on this sensor, see **+12V Power Supply Sensor** (on page 107).

4. To return to the Main Menu, press ✖.

Muting the Internal Beeper

After enabling the internal beeper's mute control function, you can choose to mute the beeper via the front panel whenever the beeper sounds for an alarm.

By default, the beeper's mute control feature via front panel is enabled.

Tip: To disable this feature, see **Front Panel Settings** *(on page 289).*

▶ **To mute the internal beeper during an alarm:**

1. Press ⌃ or ⌄ to select "SRC" in the Main Menu, and press ◉.

2. Press ◉. A confirmation message appears.

3. Press ⌃ to select Yes and then press ◉.

4. The beeper stops beeping, and the Beeper State shows "Active (Muted)".

Note that the alarmed state remains unchanged yet for the moment.

Peripherals

If there are no Raritan environmental sensor packages connected to your SRC, the LCD display shows the message "*No managed devices*" for the "Peripherals" menu command.

If you have enabled the front panel actuator control function, you can switch on or off a connected actuator using the LCD display. See **Miscellaneous** (on page 297).

▶ **To show environmental sensor or actuator information:**

1. Press ⊙ or ⊙ to select "Peripherals" in the Main Menu, and press ⊙.

2. The display shows a list of environmental sensors/actuators.

   ▪ If the desired sensor or actuator is not visible, press ⊙ or ⊙ to scroll up or down.

   ▪ When the list exceeds one page, the currently-selected sensor/actuator's ID number and total of managed sensors/actuators are indicated in the top-right corner of the display.

   ▪ If any sensor enters the warning, critical, or alarmed state, like 'Tamper Detector 1' shown below, it is highlighted in yellow or red. For color definitions, see **Yellow- or Red-Highlighted Sensors** (on page 115).

     The top and bottom bars also turn yellow or red. See **Operating the Dot-Matrix LCD Display** (on page 71).
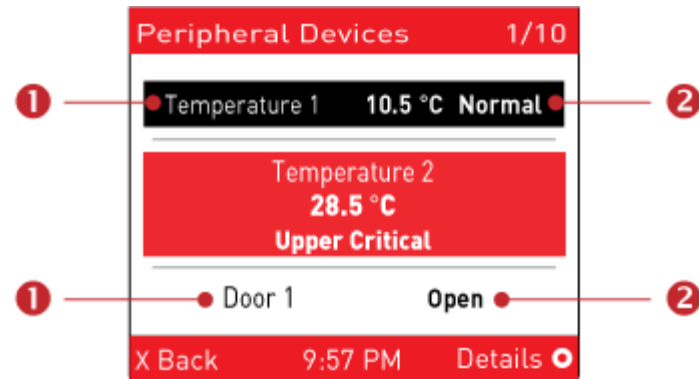
Number	Description
❶	Sensor or actuator names.

Number	Description
❷	Sensor or actuator states as listed below. For further information, see ***Sensor/Actuator States*** (on page 118). ▪ *n/a* = unavailable ▪ *Normal* ▪ *Alarmed* ▪ *Lower Critical* = below lower critical ▪ *Lower Warning* = below lower warning ▪ *Upper Warning* = above upper warning ▪ *Upper Critical* = above upper critical ▪ *On* ▪ *Off* ▪ *Open* ▪ *Closed* A numeric sensor shows both the reading and state. A state sensor or actuator shows the state only.

3. To view an environmental sensor or actuator's detailed information, press ⌃ or ⌄ to select that sensor or actuator, and press ◎.
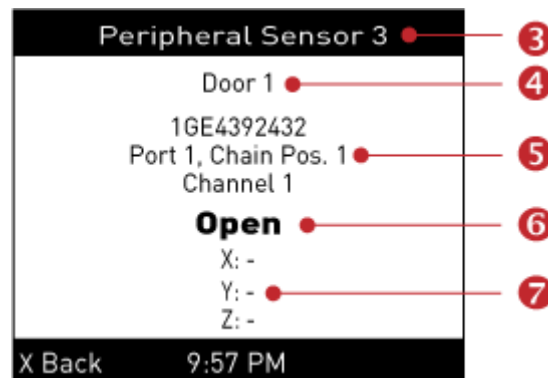
Number	Description
❸	The ID number assigned to this sensor or actuator. ▪ A sensor shows "Peripheral Sensor x" (x is the ID number) ▪ An actuator shows "Peripheral Actuator x"
❹	Sensor or actuator name.

Number	Description
❺	The following information is listed. ▪ Serial number ▪ Chain position, which involves the following information: ▪ *Port <N>*: <N> is the number of the sensor port where this sensor or actuator is connected. This number is always 1 for SRC. ▪ *Chain Pos. <n>*: <n> is the sensor or actuator's position in a sensor daisy chain. *Note: Only Raritan's DX, DX2, DPX2 and DPX3 series provide the chain position information.* ▪ If this sensor or actuator is on a sensor package with multiple channels, such as DX2-DH2C2, its channel number is indicated as "Channel x", where x is a number.
❻	Depending on the sensor type, any of the following information is displayed: ▪ State of a state sensor: *Normal*, *Alarmed*, *Open* or *Closed*. ▪ State of an actuator: *On* or *Off*. ▪ Reading of a numeric sensor.
❼	X, Y, and Z coordinates which you specify for this sensor or actuator. See **Individual Sensor/Actuator Pages** (on page 124).

▶ **To switch on or off an actuator:**

1. Follow the above steps 1 to 3 to select an actuator.

```
        Peripheral Actuator 6
        Door Handle Lock 1
           1GE8200098
      Port 1, Chain Pos. 1
            Channel 1
           Closed
             X: –
             Y: –
             Z: –
  X Back      9:57 PM     Switch ⦿
```

Raritan.
A brand of ❑legrand
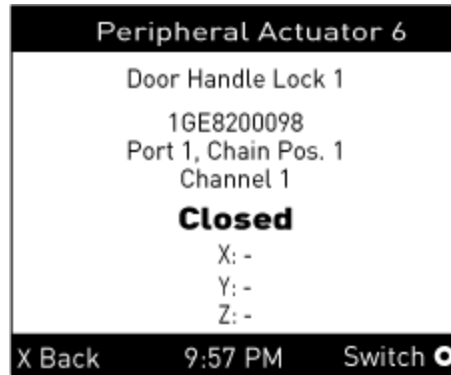
2. Press ⬤ to turn on or off the actuator. A confirmation message similar to the following is shown.

```
Peripheral Actuator 6

Do you really want to
switch off Door Handle
Lock 1?

        Yes

        No

X Back       9:57 PM
```
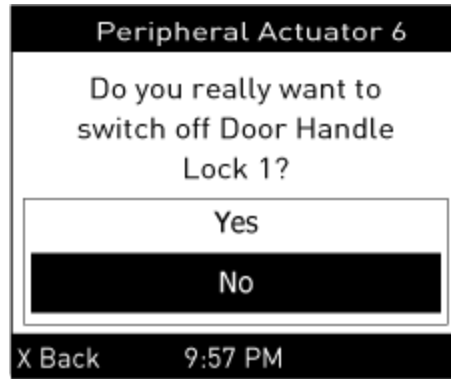
3. Press ⌃ or ⌄ to select Yes or No, and then press ⬤.

4. Verify that the actuator status shown on the LCD display has been changed.

Assets

If there are no Raritan asset management strips connected, the LCD display shows the message "No asset strips connected" for the "Assets" menu command.

After connecting asset strips, only the information of the rack units where asset tags have been detected is shown on the LCD display.

▶ **To show asset strip information:**

1. Press ⌃ or ⌄ to select "Assets" in the Main Menu, and press ⬤.

2. The display shows the available asset strip, and indicates how many rack units and tags are detected on this strip.

   ▪ The number of tags includes both the tags attached to the asset strip and those attached to the blade extension strip, if any.

3. Press ⬤ to show this asset strip's details, including:

   ▪ State - strip status.

   ▪ Main Tags - number of the tags attached to the asset strip.

   ▪ Blade Tags - number of the tags attached to the blade extension strip(s), if any.

   Note: The 'Blade Tags' information appears only when there are tags detected on the connected blade extension strip.

   ▪ Type - the asset strip type.

   ▪ Numbering - the numbering mode. See **Asset Strip** (on page 132).

   ▪ Offset - the starting number of the rack unit numbering.

- Orientation - the strip's orientation.

4. Press ⊙ again to show a list of available tags and their information.

   - When the list exceeds one page, the currently-selected main tag and total of available main tags are indicated in the top-right corner of the display.

   - If the desired tag is not visible, press ⌃ or ⌄ to scroll up or down.

5. If any blade extension strip is connected to this asset strip, select it and Press ⊙ to view a list of available tags and asset IDs on this extension strip.

Device Info

The display shows the device's information, network and IPv4/IPv6 settings through various pages. Page numbers are indicated in the top-right corner of the LCD display.

▶ **To show the device information:**

1. Press ⌃ or ⌄ to select "Device Info" in the Main Menu, and press ⊙.

   Device information similar to the following diagram displays.

2. Device information like the device name, model name, firmware version, and so on is displayed.
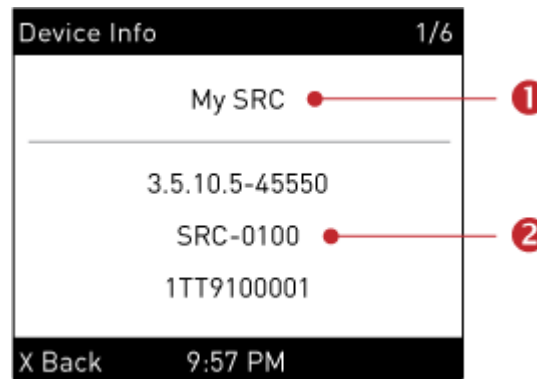
Number	Description
❶	Device name.
❷	Firmware version, model name and serial number

3. Press ⌄ to show the Network Common page.

Network Common   2/6

DNS Servers
192.168.80.80   ❹
192.168.80.83

Default Gateways
192.168.84.255   ❺

X Back   9:57 PM
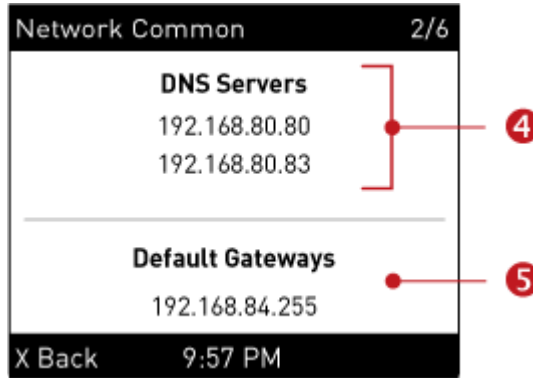
Number	Description
❹	DNS servers.
❺	Default gateways.

4. Press ⌄ to show the Network Cascading page.

Network Cascading   3/6

No Cascading   ❻

X Back   9:57 PM

Number	Description
❻	Cascading status, which can be one of the following:

Cascading status, which can be one of the following:

- No Cascading: This device's cascading mode is set to None. See **Setting the Cascading Mode** (on page 177).
- Network Bridge Enabled: This device's cascading mode is set to Bridging. Its IP address is also displayed on this page.
- Port Forwarding Master: This device's cascading mode is set to Port Forwarding, and it is a master device.
  - Slave Connected: Indicates whether the presence of a slave device is detected - *yes* or *no*.
- Port Forwarding Slave: This device's cascading mode is set to Port Forwarding, and it is a slave device.
  - Slave Connected: Indicates whether the presence of a slave device is detected - *yes* or *no*.
  - Cascade Position: Indicates the position of a slave device in the Port Forwarding mode. 1 represents Slave 1, 2 represents Slave 2, and so on.
  - A port forwarding slave device will also display the master device's IP address on this page.

5. Press ⌄ to show the Ethernet pages.

Raritan.
A brand of ☐legrand'

6. A SRC has two Ethernet pages -- ETH1 and ETH2.

Number	Description
7	Ethernet interface information, including: ▪ MAC address. ▪ Speed. ▪ Full or half duplex.
8	IPv4/IPv6 network information, including: ▪ Network configuration: DHCP (or Automatic), or Static. Static represents Static IP. ▪ IP address. ▪ Prefix length, such as "/24". *Note: If you disable any Ethernet interface, a message 'Interface Disabled' is shown. See* **Ethernet Interface Settings** *(on page 164).*

If you do not enable IPv4/IPv6 settings, an 'IPv4 (or IPv6) Disabled' message is displayed.

7. Press ⌄ to show the WIRELESS page.

Number	Description
⑨	If NO supported WLAN adapter is plugged or detected, the message "No Adapter Detected" is shown.
	If a supported WLAN adapter is detected and configured properly, wireless network information is shown instead, including:
	▪ MAC address
	▪ SSID
	▪ IPv4/IPv6 network information -- for detailed explanation, refer to number ⑧

8. To return to the Main Menu, press ✖.

Alerts Notice in a Yellow or Red Screen

In the automatic mode, if an alert occurs, the LCD display automatically shows a yellow or red screen which indicates the total number of alerted sensors and information of the latest transitions.

- When all alerted sensors enter the warning levels, the screen's background turns yellow.

- When at least one of the alerted sensors enters the critical level or there is any "alarm", the screen's background turns red.

For color definitions, see *Yellow- or Red-Highlighted Sensors* (on page 115).

The following illustrates the alerts notices in red.
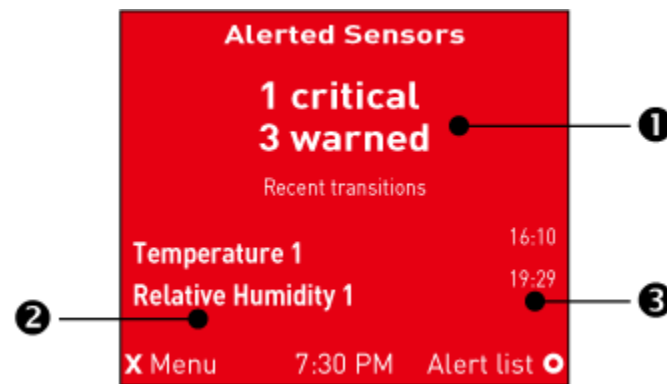
Number	Description
❶	The total of alerted sensors in critical and warning levels.
❷	A list of final alerted sensors that changed their readings or states.
❸	The final time that each alerted sensor changed its readings or states.

▶ **When there is any alarm present:**

The LCD display looks similar to the above diagram except that it shows the alarm(s) and the available command in the bottom-right corner is 'Actions' instead of 'Alert list'.
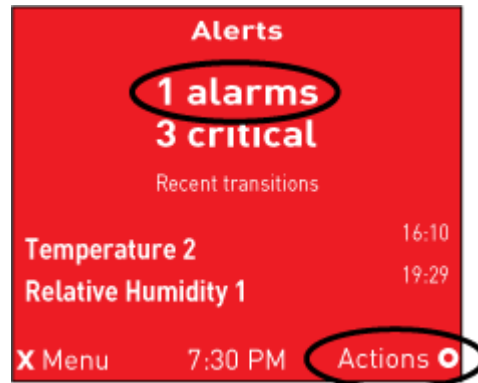
▶ **Available operations:**

- For the notice listing alerted sensors only, press ⊚ to view a list of all alerted sensors. See **Alerts** (on page 73).

- For the notice where at least an alarm is present, press ⊚. Then do the following:

  a. Two options display. Press ⌃ or ⌄ to select either option, and press ⊚.
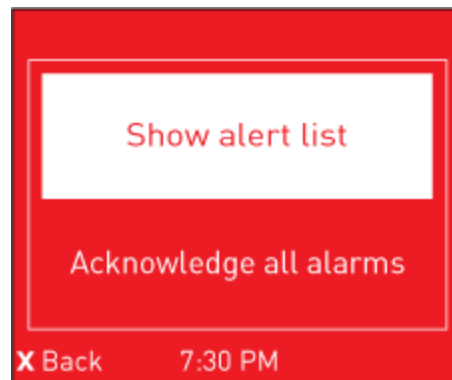
- *Show alert list*: This option lists all of alerted sensors and alarms. You still can choose to acknowledge alarms after viewing the list. See **Alerts** (on page 73).

- *Acknowledge all alarms*: This option immediately acknowledges all existing alarms, without showing the list of alarms.

b. (Optional) If 'Acknowledge all alarms' is selected in the above step, a confirmation prompt similar to the diagram below appears. Press ⌃ or ⌄ to confirm or abort the operation, and press ⏺.
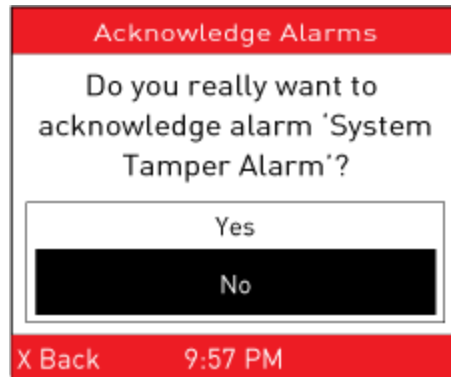
Showing the Firmware Upgrade Progress

When upgrading the SRC, the firmware upgrade progress will be displayed as a percentage on the LCD display, similar to the following diagram.

In the end, a message appears, indicating whether the firmware upgrade succeeds or fails.

Reset Button

The reset button is located inside the small hole labeled RESET near the display panel.
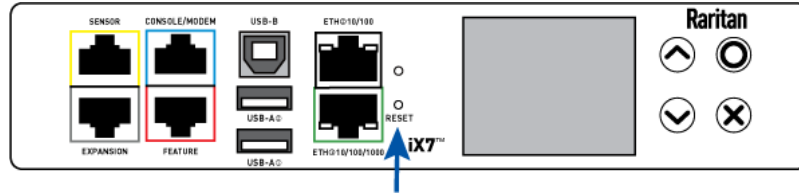
- Pressing this reset button restarts the SRC software.
- The SRC can be reset to its factory default values using this button when a serial connection is available. See **Resetting to Factory Defaults** (on page 556).

Beeper

The SRC 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 224).

Tip: To remotely check this beeper's state via the web interface, see **SRC** *(on page 106).*

Chapter 6   Using the Web Interface

This chapter explains how to use the web interface to administer the SRC.

In This Chapter

Supported Web Browsers

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

Login, Logout and Password Change

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

After login, you can create user accounts for other users. See *Creating Users* (on page 148).

Login

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

▶ **To log in to the web interface:**

1. Open a browser and type the IP address of your SRC.

- 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 6).
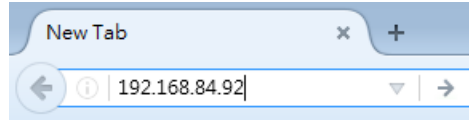
Tip: You can also enter the desired page's URL so that you can immediately go to that page after login. See **Quick Access to a Specific Page** *(on page 100).*

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

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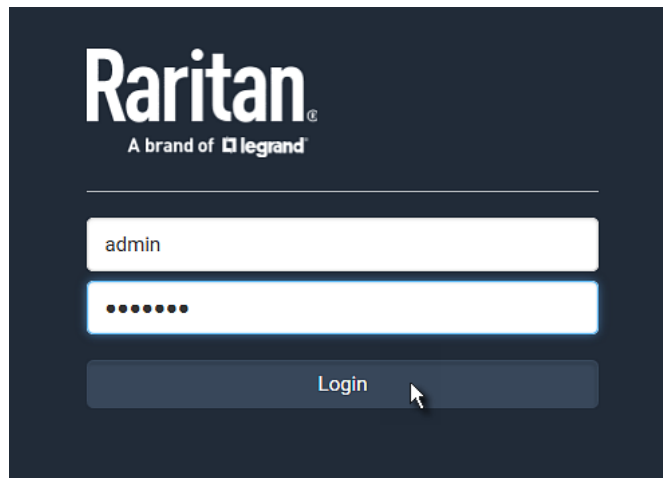
4. (Optional) If a security agreement is displayed, accept it. Otherwise, you cannot log in.

Note: To configure the security agreement, see **Enabling the Restricted Service Agreement** *(on page 218).*

5. Click Login or press Enter. The web interface of SRC opens.

Depending on your hardware configuration, your web interface shown onscreen may look slightly different from the image below.

Note: The address to access a slave device in the Port Forwarding mode via non-standard ports is a combination of a protocol (http:// or https://), an IP address and a port number. See **Port Forwarding Examples** *(on page 182).*

Changing Your Password

You need appropriate permissions to change your password. Refer to the following for details.

To change other users' passwords, Administrator Privileges are required instead. See *Editing or Deleting Users* (on page 151).

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

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

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

Users without permissions listed must change password.

Note: This password change request also appears if the 'force password change' is enabled in the user account setting. See **Creating Users** *(on page 148).*

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

You must have the Change Own Password permission to change your own password. See *Creating Roles* (on page 153).

1. Choose User Management > Change Password.
2. First type the current password, and then the new password twice. Passwords are case sensitive.

- A password comprises 4 to 64 characters.

Change Password - admin

Old Password	required
Confirm password	required
New password	required

✔ Save

Remembering User Names and Passwords

SRC supports the password manager of common web browsers, including:

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

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

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

SRC does NOT support other browser password managers.

Logout

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

▶ **To log out without closing the web browser:**
- Click "Logout" on the top-right corner.

    -- OR --

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

▶ **To log out by closing the web browser:**
- Click ⊠ on the top-right corner of the window.

    -- OR --

- Choose File > Close, or File > Exit.

Web Interface Overview

The web interface consists of four areas as shown below.

▶ **Operation:**

1. Click any menu or submenu item in the area of ❶.

2. That item's data/setup page is then opened in the area of ❷.

3. Now you can view or configure settings on the opened page.

4. To return to the main menu and the Dashboard page, click on the top-left corner.
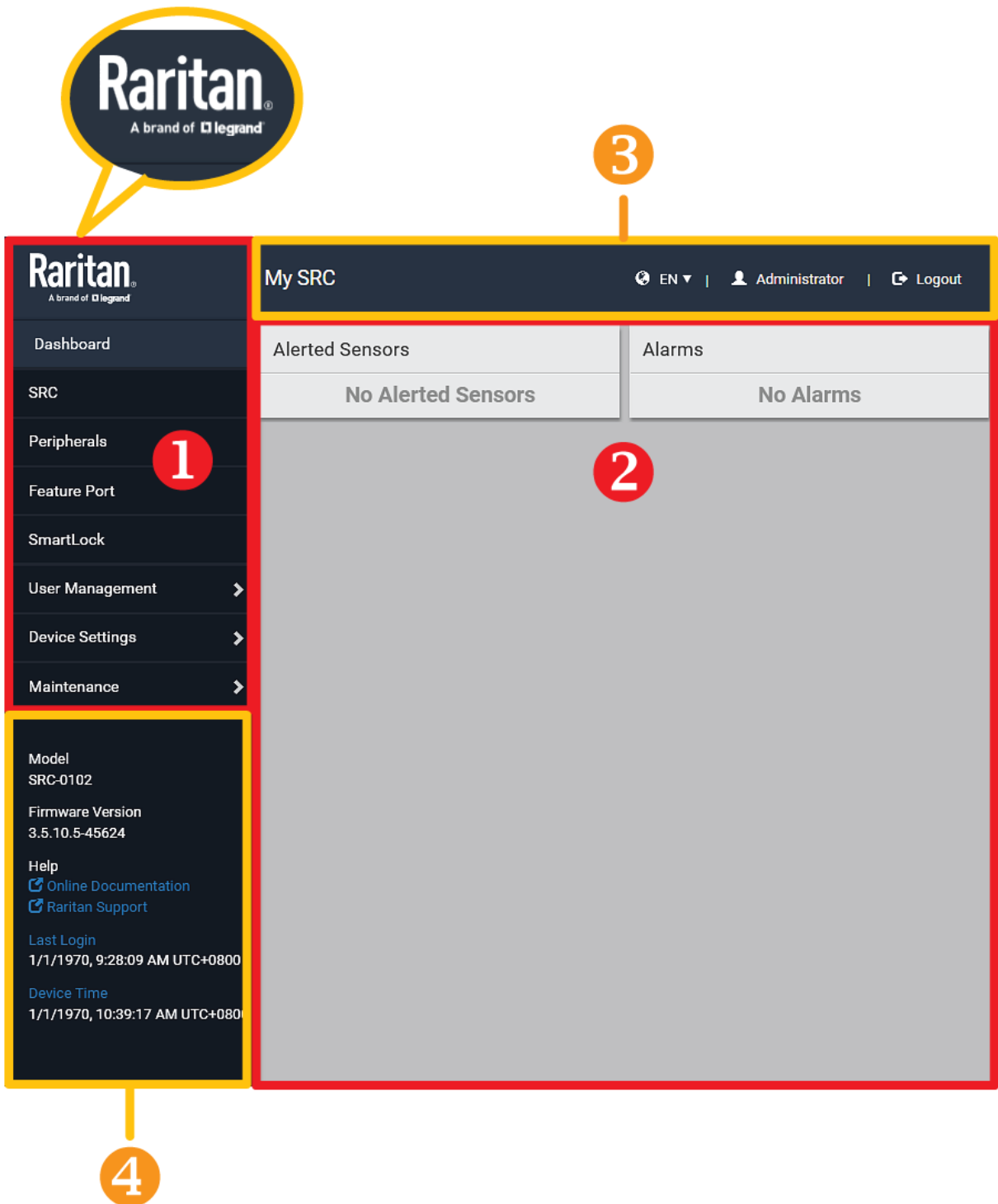
Number	Web interface element
❶	*Menu* (on page 98)
❷	Data/setup page of the selected menu item.
❸	▪ Left side: - SRC device name. *Note: To customize the device name, see* **SRC** *(on page 106).* ▪ Right side: - Displayed language, which is English (EN) by default. You can change it. - Your login name, which you can click to view your user account settings. - Logout button.
❹	From top to bottom -- ▪ Your SRC model. ▪ Current firmware version. ▪ **Online Documentation**: link to the online help of SRC. - See **Browsing through the Online Help** (on page 644). ▪ **Raritan Support**: link to Raritan Technical Support webpage. ▪ Date and time of your user account's last login. - Click **Last Login** to view your login history. ▪ SRC system time, which is converted to the time zone of your computer or mobile device. - Click **Device Time** to open the Date/Time setup page.

Menu

Depending on your model and hardware configuration, your SRC may show all or some menu items shown below.
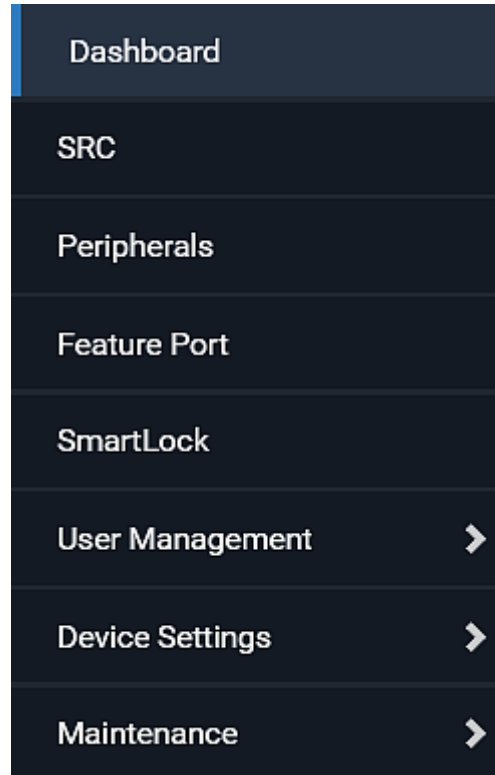
Menu	Information shown
Dashboard	Summary of the SRC status, which shows a list of alerted sensors and alarms, if any. See **Dashboard** (on page 102).
SRC	Device data and settings, such as the device name and MAC address. See **SRC** (on page 106).
Peripherals	Status and settings of Raritan environmental sensor packages, if connected. See **Peripherals** (on page 108).

Menu	Information shown
Feature Port The name 'Feature Port(s)' will be replaced with one of the device names listed to the right	Status and settings of the device connected to the Feature port(s), which can be one of the following. ▪ Asset Strip ▪ External Beeper ▪ LHX 20 ▪ SHX 30 ▪ LHX 40 See **Feature Port** (on page 130).
Webcams	The 'Webcams' menu item appears when there is any webcam(s) connected to the SRC, or when there are snapshots saved onto the SRC already. Webcam live snapshots/video and webcam settings. See **Webcam Management** (on page 324).
SmartLock -- *and/or* -- Card Readers	**Scenario (1):** If your SRC has onboard door handle ports, such as SRC-0102, 'SmartLock' or both menu items appear. **Scenario (2):** If your SRC does NOT have onboard door handle ports, such as SRC-0100, then it does NOT show either item by default. Either or both menu items appear only when you connect Raritan's SmartLock kit to this product. For details, refer to the user documentation accompanying the SmartLock kit or download it from Raritan's **Support page** (*http://www.raritan.com/support/*). ▪ **SmartLock**: Configures and controls the door handles connected to this product via DX2-DH2C2. Note that this page is not available if connecting the door handles to other Raritan sensors than DX2-DH2C2. ▪ **Card Readers**: Lists the card readers connected to SRC directly or indirectly. See **SmartLock and Card Reader** (on page 337).
User Management	Data and settings of user accounts and groups, such as password change. See **User Management** (on page 147).
Device Settings	Device-related settings, including network, security, system time, event rules and more. See **Device Settings** (on page 158).
Maintenance	Device information and maintenance commands, such as firmware upgrade, device backup and reset. See **Maintenance** (on page 299).

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

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

- Click the topmost link with the symbol **<**. For example, click .
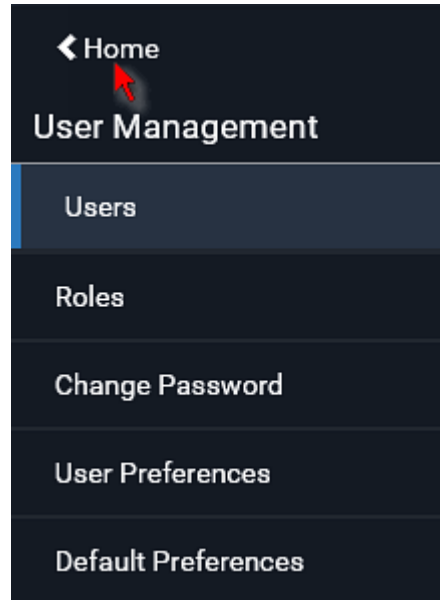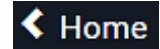
- Click on the top-left corner to return to the main menu.

Quick Access to a Specific Page

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

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

► **URL examples:**

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

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

Sorting a List

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

▶ **Illustration -- Event Log:**

1. By default, the Event Log is sorted in the descending order based on the ID column. Therefore, the arrow ▼ is displayed adjacent to the ID header.

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

ID ▼	Timestamp	Event Class
665	7/24/2017, 3:14:43 AM Eastern Daylight Time	User Activity
664	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor
663	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor
662	7/24/2017, 2:42:35 AM Eastern Daylight Time	Sensor

3. The arrow turns to ▲, indicating the list is sorted in the "ascending" order.

ID ▲

4. To resort the list based on a different column, click a different column header. In this example, the 'Event Class' column is clicked.

ID ▲	Timestamp	Event Class	Event

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

ID	Timestamp	Event Class ▲	Event

Dashboard

The Dashboard page contains two sections.

Number	Section	Information shown
❶	Alerted Sensors	▪ When no sensors enter the alarmed state, this section shows the message "No Alerted Sensors." ▪ When any sensor enters the alarmed state, this section lists all of them. See **Dashboard - Alerted Sensors** (on page 103).
❷	Alarms	This section can show data only after you have set event rules requiring users to take the acknowledgment action. ▪ When there are no unacknowledged events, this section shows the message "No Alarms." ▪ When there are unacknowledged events, this section lists all of them. See **Dashboard - Alarms** (on page 104).

▶ **The Hardware Failures section:**

If SRC detects any internal hardware issues, a section labeled "Hardware Failures" will appear on the Dashboard page, listing all of current hardware issues.

This section does NOT display as long as there are no hardware failures present. See **Hardware Issue Detection** (on page 321).

Dashboard - Alerted Sensors

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

To view detailed information or configure each alerted sensor, you can click each sensor's name to go to individual sensor pages. See *Individual Sensor/Actuator Pages* (on page 124).

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 101).

▶ **Summary in the section title:**

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

For example:

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

    - Numeric sensors enter the critical state.

    - State sensors enter the alarmed state.

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

▶ **List of alerted sensors:**

Two icons are used to indicate various sensor states.

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

For details, see *Sensor/Actuator States* (on page 118).

Dashboard - Alarms

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

*Note: For information on event rules, see **Event Rules and Actions** (on page 224).*

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

▶ **To acknowledge an alarm:**

- Click Acknowledge, and that alarm then disappears from the Alarms section.

This table explains each column of the alarms list.

Field	Description
Name	Custom name of the Alarm action.
Reason	The first event that triggers the alert.
First Appearance	Date and time when the event indicated in the Reason column occurred for the first time.
Last Appearance	Date and time when the event indicated in the Reason column occurred for the last time.
Count	Number of times the event indicated in the Reason column has occurred.
More Alerts	This field appears only when there are more than one types of events triggering this alert. If there are other types of events (that is, other reasons) triggering the same alert, the total number of additional reasons is displayed. You can click it to view a list of all events.

The date and time shown on the SRC web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of SRC to your computer or mobile device.

Tip: You can also acknowledge all alarms by operating the LCD display. Refer to **Alerts Notice in a Yellow or Red Screen** *(on page 85).*

SRC

The SRC device's generic information and SRC settings are available on the SRC page.

To open the SRC page, click 'SRC' in the **Menu** (on page 98).

▶ **Device information shown:**

- Firmware version
- Serial number
- MAC address
- *Internal Beeper State* (on page 106)
- Status of *+12V Power Supply Sensor* (on page 107)

▶ **To configure global settings:**

1. Click Edit Settings.
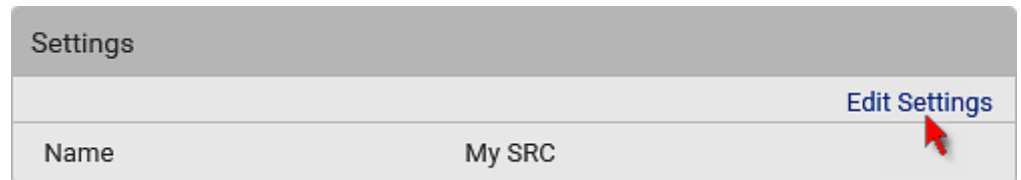
2. Customize the Name field.
3. Click Save.

Internal Beeper State

The SRC page indicates the internal beeper state.
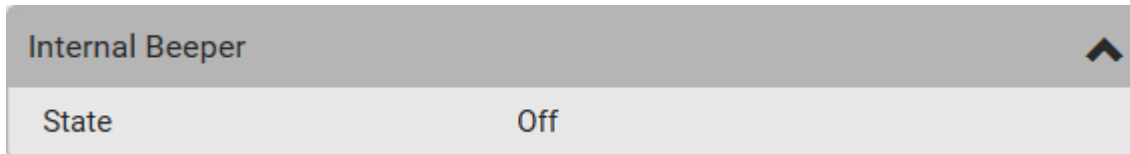
▶ **Available beeper states:**

States	Description
Off	The beeper is turned off.
Active	The beeper is turned on.

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

See *Event Rules and Actions* (on page 224).

+12V Power Supply Sensor

The SRC's controller receives DC 12V power from its inlet. A sensor monitors the power supply status and indicates it on the SRC page.

State	Description
OK	The SRC controller is receiving power from its own inlet.
fault	The SRC controller cannot receive power from its own inlet because of a power failure on the inlet or a broken 12V power supply.
unavailable	The communication with the 12V power supply sensor is lost.

▶ **Alternatives for checking the 12V power supply status:**

- Dot-matrix LCD panel. See *SRC* (on page 75).
- CLI command: `show src details`. See *Using the Command Line Interface* (on page 355).

Peripherals

> Only DX and DX2 environmental sensor packages are supported. SRC does NOT support these other Raritan environmental sensor packages: DPX, DPX2, DPX3 (except for the DPX3-ENVHUB4 sensor hub).

If there are Raritan environmental sensor packages connected to the SRC, they are listed on the Peripherals page. See *Connecting Raritan Environmental Sensor Packages* (on page 36).

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

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

SRC communicates with *managed* sensors/actuators only and retrieves their data. It does not communicate with unmanaged ones. See *Managed vs Unmanaged Sensors/Actuators* (on page 117).

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

Model	Number of sensors/actuators that can be managed
SRC-0100	32
SRC-0102	38, which is the sum of the following. ▪ Supports 32 managed sensors/actuators per sensor port ▪ Contains 6 sensors of onboard door handle ports and contact closure terminals

Note: To disable the automatic management function, refer to the final table in this section. You need to manually manage a sensor/actuator only when it is not under management.

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

Open the Peripheral Devices page by clicking Peripherals in the *Menu* (on page 98). Then you can:

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

Peripheral Devices						⏻ On ⏻ Off ☑ ⋮	
# ▲	Name	Reading	State	Type	Serial Number	Position	Actuator
1	Temperature 1	24.0 °C	normal	Temperature	QMTemu0005	Port 1, Chain Position 5	
2	Temperature 2	24.0 °C	normal	Temperature	QMSemu0004	Port 1, Chain Position 4	
3	Relative Humidity 1	42 %	normal	Humidity	QMSemu0004	Port 1, Chain Position 4	
4	On/Off 1		normal	Contact Closure	QU7emu0003	Port 1, Chain Position 3, Channel 1	
5	On/Off 2		normal	Contact Closure	QU7emu0003	Port 1, Chain Position 3, Channel 2	

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

Peripheral Devices

# ▲	Name
1	Temperature 1
2	Temperature 2
3	Relative Humidity 1
4	On/Off 1

If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 101).

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

If any sensor enters an alarmed state, it is highlighted in yellow or red. See *Yellow- or Red-Highlighted Sensors* (on page 115). An actuator is never highlighted.

Column	Description
Name	By default the SRC assigns a name comprising the following two elements to a newly-managed sensor/actuator. ▪ Sensor/actuator type, such as "Temperature" or "Dry Contact." ▪ Sequential number of the same sensor/actuator type, like 1, 2, 3 and so on. You can customize the name. See *Individual Sensor/Actuator Pages* (on page 124).

Column	Description
Reading	Only managed 'numeric' sensors show this data, such as temperature and humidity sensors.
State	The data is available for all sensors and actuators. See **Sensor/Actuator States** (on page 118).
Type	Sensor or actuator type.
Serial Number	This is the serial number printed on the sensor package's label. It helps to identify your Raritan sensors/actuators. See **Finding the Sensor's Serial Number** (on page 119).
Position	The data indicates where this sensor or actuator is located in the sensor chain. See **Identifying the Sensor Position and Channel** (on page 120).
Actuator	Indicates whether this sensor package is an actuator or not. If yes, the symbol ✔ is shown.

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

When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed sensor/actuator, see **Managing One Sensor or Actuator** (on page 122). To release any one, follow this procedure.

1. Click ☑ to make checkboxes appear in front of sensors/actuators.

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

2. Select multiple sensors/actuators.
   - To release sensors/actuators, you must select "managed" ones only. See **Sensor/Actuator States** (on page 118).
   - To manage sensors/actuators, you must select "unmanaged" ones only.

- To select ALL sensors/actuators, select the topmost checkbox in the header row.

Peripheral Devices

✔	# ▲	Name
☐	1	Temperature 1
☐	2	Temperature 2
☐	3	Relative Humidity 1

3. To release selected ones, click ⋮ > Release.

    To manage them, click ⋮ > Manage.

    - The management action triggers a "Manage Peripheral Device" dialog. Simply click Manage if you are managing *multiple* sensors/actuators.

Manage Peripheral Device

- ● Automatically assign a sensor number
- ○ Manually select a sensor number

Sensor 1 (unused) ▼

Cancel   Manage

- If you are managing only *one* sensor/actuator, you can choose to assign an ID number by selecting "Manually select a sensor number." See ***Managing One Sensor or Actuator*** (on page 122).

4. Now released sensors/actuators become "unmanaged."

    Managed ones show one of the managed states.

▶ **To configure sensor/actuator-related settings:**

1. Click ⋮ > Peripheral Device Setup.

2. Now you can configure the fields.

    - Click ▼ to select an option.
    - Adjust the numeric values.

▪ Select or deselect the checkbox.

Field	Function	Note
Peripheral device Z coordinate format	Determines how to describe the vertical locations (Z coordinates) of Raritan environmental sensor packages. ▪ *Options: Rack units and Free-form* See ***Z Coordinate Format*** (on page 129).	To specify the location of any sensor/actuators in the data center, see ***Individual Sensor/Actuator Pages*** (on page 124).
Peripheral device auto management	Enables or disables the automatic management feature for Raritan environmental sensor packages. ▪ *The default is to enable it.*	See ***How the Automatic Management Function Works*** (on page 122).
Altitude	Specifies the altitude of SRC above sea level when a Raritan's differential air pressure sensor is attached. ▪ *Range: -425 to 3000 meters (-1394 to 9842 feet)* ▪ *Note that it can be a negative value down to -425 meters (-1394 feet) because some locations are below the sea level.*	▪ The device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 623). ▪ The default altitude measurement unit is meter. See ***Setting Default Measurement Units*** (on page 157). ▪ You can have the measurement unit vary between meter and foot according to user credentials. See ***Setting Your Preferred Measurement Units*** (on page 156).
Active powered dry contact limit	Determines the maximum number of "active" powered dry contact actuators that is permitted concurrently. ▪ *Range: 0 to 24* ▪ *Default: 1*	▪ An "active" actuator is the one that is turned ON, or, if with a door handle connected, is OPENED. ▪ This setting only applies to "powered dry contact" (PD) actuators rather than normal "dry contact" actuators. ▪ You need either 'Change Peripheral Device Configuration' privilege or 'Administrator Privileges' to change its upper limit. ▪ To turn on/off the connected actuators, see ***Peripherals*** (on page 108).

3. Click Save.

4. To return to the sensor list on the Peripheral Devices page, click "Peripheral Devices" on the top.

Raritan.
A brand of ∎legrand

◄ Peripheral Devices | Setup

► **To configure default threshold settings:**

Note that any changes made to default threshold settings not only re-determine the initial threshold values that will apply to newly-added sensors but also the threshold values of the already-managed sensors where default thresholds are being applied. See *Individual Sensor/Actuator Pages* (on page 124).

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

Peripheral Device Default Thresholds

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

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

Lower critical	✔ 10	°C
Lower warning	✔ 15	°C
Upper warning	✔ 30	°C
Upper critical	✔ 35	°C
Deassertion hysteresis	1	°C
Assertion timeout	0	Samples
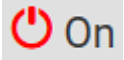
> For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** (on page 614).
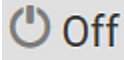
4. Click Save.

Tip: To customize the threshold settings on a per-sensor basis, go to **Individual Sensor/Actuator Pages** *(on page 124).*

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

1. Select one or multiple actuators which are *in the same status -* on or off.

2. To select multiple actuators, click [checkbox icon] to make checkboxes appear and then select desired actuators.

3. Click the desired button.

[On icon] : Turn ON.

[Off icon] : Turn OFF.

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. To change this limitation of "powered dry contact" actuators, modify the active powered dry contact setting. See **Peripherals** *(on page 108).*

4. Confirm the operation when prompted.

If you select a DX2-DH2C2 door handle lock, then the Open and Close buttons appear. For detailed operations, see **Door Handle Status and Control** (on page 342).

Tip: If intending to control the actuator via the front panel, see **Front Panel Settings** *(on page 289).*

Yellow- or Red-Highlighted Sensors

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

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

For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** (on page 614).

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

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

Sensor status	Color	States shown in the interface	Description
Unknown		unavailable	Sensor state or readings cannot be detected.
		unmanaged	Sensors are not being managed. See **Managed vs Unmanaged Sensors/Actuators** (on page 117).
Normal		normal	▪ Numeric or state sensors are within the normal range. -- OR -- ▪ No thresholds have been enabled for numeric sensors.
Warning		above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
		below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
Critical		above upper critical	Upper Critical threshold < "R"
		below lower critical	"R" < Lower Critical threshold
Alarmed		alarmed	State sensors enter the abnormal state.

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

Managed vs Unmanaged Sensors/Actuators

To manually manage or unmanage/release a sensor or actuator, see *Peripherals* (on page 108).

▶ **Managed sensors/actuators:**

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

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

- They show one of the managed states. See *Sensor/Actuator States* (on page 118).
- For managed 'numeric' sensors, their readings are retrieved and displayed. If any numeric sensor is disconnected or its reading cannot be retrieved, it shows "unavailable" for its reading.

▶ **Unmanaged sensors/actuators:**

- SRC does NOT communicate with unmanaged sensors/actuators so their data is not retrieved.
- Unmanaged sensors/actuators are listed only when they are physically connected to SRC.

  They disappear when they are no longer connected.
- They do *not* have an ID number.
- They show the "unmanaged" state.

Sensor/Actuator States

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

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

Sensors will be highlighted in yellow or red when they enter abnormal states. See *Yellow- or Red-Highlighted Sensors* (on page 115).

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

▶ **Managed sensor states:**

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

State	Description
normal	▪ For numeric sensors, it means the readings are within the normal range. ▪ For state sensors, it means they enter the normal state.
below lower critical	"R" < Lower Critical threshold
below lower warning	Lower Critical threshold <= "R" < Lower Warning threshold
above upper warning	Upper Warning threshold < "R" <= Upper Critical threshold
above upper critical	Upper Critical threshold < "R"
alarmed	The state sensor enters the abnormal state.
unavailable	▪ Communication with the managed sensor is lost. -- OR -- ▪ DX2 and DX sensor packages are upgrading their sensor firmware.

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

▶ **Managed actuator states:**

State	Description
on	The actuator is turned on.
off	The actuator is turned off.
unavailable	▪ Communication with the managed actuator is lost. -- OR -- ▪ DX2 or DX sensor packages are upgrading their sensor firmware.

▶ **Unmanaged sensor/actuator states:**

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

Note: Unmanaged sensors or actuators will disappear from the web interface after they are no longer physically connected to the SRC. To manage a sensor/actuator, go to **Peripherals** *(on page 108).*

Finding the Sensor's Serial Number

A DX2 and DX sensor package has a serial number tag attached to its rear side.

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

Identifying the Sensor Position and Channel

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

- DX and DX2 series show both the sensor port number and its position in a sensor chain.

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

- If a Raritan DPX3-ENVHUB4 sensor hub is involved, the hub port information is also indicated for DX2 and DX.

   For example, *Hub Port 3*.

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

   For example, *Channel 1*.

▶ **Sensor/actuator position examples:**

Example	Physical position
Port 1, **Chain Position 4**	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 4th sensor package of the sensor chain.
Port 1, **Chain Position 3,** **Channel 2**	▪ Connected to the sensor port #1. ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain. ▪ It is the 2nd channel of the sensor package.
Port 1, **Chain Position 1,** **Hub Port 2,** **Chain Position 3**	▪ Connected to the sensor port #1. ▪ Connected to the 2nd port of the DPX3-ENVHUB4 sensor hub, which shows the following two pieces of information: 　▪ The hub's position in the sensor chain -- "Chain Position 1" 　▪ The hub port where this particular sensor package is connected -- "Hub Port 2" ▪ The sensor/actuator is located in the 3rd sensor package of the sensor chain connected to the hub's port 2.

How the Automatic Management Function Works

This setting is configured on **Peripherals** (on page 108).

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

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

Below lists the upper limit of each model.

Model	Number of sensors/actuators that can be managed
SRC-0100	32
SRC-0102	38, which is the sum of the following. ▪ Supports 32 managed sensors/actuators per sensor port ▪ Contains 6 sensors of onboard door handle ports and contact closure terminals

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

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

You must manually manage new sensors/actuators. See **Peripherals** (on page 108).

Managing One Sensor or Actuator

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

Tip: When the total of managed sensors/actuators reaches the maximum value, you cannot manage additional ones. The only way to manage any sensor/actuator is to release or replace the managed ones. To replace a managed one, assign an ID number to it by following the procedure below. To release any one, see **Peripherals** *(on page 108).*

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

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

2. The Manage Peripheral Device dialog appears.

Manage Peripheral Device

- ● Automatically assign a sensor number
- ○ Manually select a sensor number

Sensor 1 (unused) ▼

Cancel | Manage

▪ To let SRC randomly assign an ID number to it, select "Automatically assign a sensor number."

This method does not release any managed sensor or actuator.

▪ To assign a desired ID number, select "Manually select a sensor number." Then click ▼ to select an ID number.

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

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

3. Click Manage.

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

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

▪ A relative humidity value is measured in percentage (%).

▪ An absolute humidity value is measured in grams per cubic meter (g/m^3).

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

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

Individual Sensor/Actuator Pages

A sensor's or actuator's data/setup page is opened after clicking any sensor or actuator name on the Peripheral Devices page. See *Peripherals* (on page 108).

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

Threshold settings, if enabled, help you identify whether any numeric sensor enters the warning or critical level. See *Yellow- or Red-Highlighted Sensors* (on page 115). In addition, you can have SRC automatically generate alert notifications for any warning or critical status. See *Event Rules and Actions* (on page 224).

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

1. Click Edit Thresholds.

Tip: The date and time shown on the SRC web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of SRC to your computer or mobile device.

2. Select or deselect 'Use default thresholds' according to your needs.

- To have this sensor follow the default threshold settings configured for its own sensor type, select the 'Use default thresholds' checkbox.

  The default threshold settings are configured on the page of **Peripherals** (on page 108).

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

Note: For concepts of thresholds, deassertion hysteresis and assertion timeout, see **Sensor Threshold Settings** *(on page 614).*

3. Click Save.

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

1. Click Edit Settings.

Settings	
	Edit Settings
Name	Temperature 1
Description	
Location (X)	
Location (Y)	
Location (Z: Rack Units)	

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

Fields	Description
Name	A name for the sensor or actuator.
Description	Any descriptive text you want.
Location (X, Y and Z)	Describe the sensor's or actuator's location in the data center by typing alphanumeric values for the X, Y and Z coordinates. See *Sensor/Actuator Location Example* (on page 130). If the term "Rack Units" appears in parentheses in the Z location, you must type an integer number. The Z coordinate's format is determined on the page of *Peripherals* (on page 108).
Alarmed to Normal Delay	This field is available for the DX-PIR presence detector only. It determines the wait time before the SRC announces that the presence detector is back to normal after it already returns to normal. Adjust the value in seconds.
Binary Sensor Subtype	This field is available for any Raritan contact closure sensor except for DX2-DH2C2's contact closure sensors. Determine the sensor type of your contact closure detector. ▪ *Contact Closure* detects the door lock or door open/closed status. ▪ *Smoke Detection* detects the appearance of smoke. ▪ *Water Detection* detects the appearance of water on the floor. ▪ *Vibration* detects the vibration of the floor.

Fields	Description
Sensor Polarity	This field is available for DX2-CC2 contact closure sensors only.
	Determine the normal state of your DX2-CC2.
	▪ *Normal Open:* The open status of the connected detector/switch is considered normal. An alarm is triggered when the detector/switch turns closed.
	▪ *Normal Closed:* The closed status of the connected detector/switch is considered normal. An alarm is triggered when the detector/switch turns opened.

▶ **To view a numeric sensor's chart**

This sensor's data within the past tens of minutes is shown in the chart. Note that only a numeric sensor has this diagram. State sensors and actuators do not have such data.

- To retrieve the exact data at a particular time, hover your mouse over the data line in the chart. Both the time and data are displayed as illustrated below.
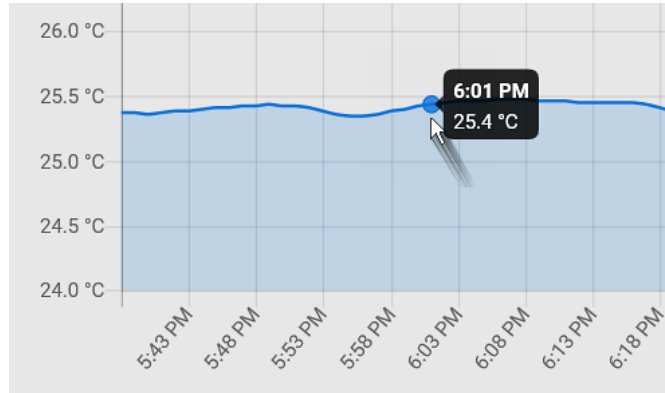
▶ **To turn on or off an actuator:**

1. Click the desired control button.

: Turn ON.

: Turn OFF.

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

Note: Per default you can turn on as many dry contact actuators as you want, but only one "powered dry contact" actuator can be turned on at the same time. To change this limitation of "powered dry contact" actuators, modify the active powered dry contact setting. See **Peripherals** *(on page 108).*

▶ **Other operations:**

You can go to another sensor's or actuator's data/setup page by clicking the selector ⬍ on the top-left corner.

Z Coordinate Format

Z coordinates refer to vertical locations of Raritan's environmental sensor packages. You can use either the number of rack units or a descriptive text to describe Z coordinates.

For a Z coordinate example, see **Sensor/Actuator Location Example** (on page 130).

▶ **To configure Z coordinates:**

1. Determine the Z coordinate format on **Peripherals** (on page 108). Available Z coordinate formats include:

Format	Description
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.

129

Format	Description
Free-form	Any alphanumeric string can be used for specifying the Z coordinate. The value comprises 0 to 24 characters.

2. Configure Z coordinates on the **Individual Sensor/Actuator Pages** (on page 124).

Sensor/Actuator Location Example

Use the X, Y and Z coordinates to describe each sensor's or actuator's physical location in the data center. See **Individual Sensor/Actuator Pages** (on page 124).

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

▶ **Example:**

X = Brown Cabinet Row

Y = Third Rack

Z = Top of Cabinet

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

- X and Y: They can be any alphanumeric values comprising 0 to 24 characters.

- Z: When the Z coordinate format is set to *Rack units*, it can be any number ranging from 0 to 60. When its format is set to *Free-form*, it can be any alphanumeric value comprising 0 to 24 characters. See **Peripherals** (on page 108).

Feature Port

The FEATURE port supports connection to the following devices.

Device	Description
Asset Strip	Raritan asset strips
External Beeper	An external beeper with the RJ-45 socket.
LHX 20	Schroff® LHX-20 heat exchanger.
SHX 30	Schroff® SHX-30 heat exchanger.
LHX 40	Schroff® LHX-40 heat exchanger.
Power CIM	Only Raritan PDUs support the connection to a Raritan power CIM or digital KVM. SRC does NOT support this feature so you can ignore this option.

When the SRC detects the connection of any listed device, it replaces 'Feature Port' in the menu with that device's name and shows that device's data/settings instead. See **Asset Strip** (on page 132), **External Beeper** (on page 140), **Schroff LHX/SHX** (on page 141) and Power CIM.

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

Open the Feature Port page by clicking it in the **Menu** (on page 98). From this page, you can enable or disable this port's detection capability, or force it to show a specific device's data/settings even though no device is detected.

*Note: You must enable the LHX/SHX support for the SRC to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See **Miscellaneous** (on page 297).*

▶ **To configure the feature port:**

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

> **Feature Port Setup**
>
> Port: 1
> Device Type: Asset Strip
> Detection Mode:
>
> | Auto ▼ |
>
> Cancel   Save

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

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

*Note: 'LHX 20', 'SHX 30', and 'LHX 40' are not available when the support of LHX/SHX heat exchangers is disabled. See **Miscellaneous** (on page 297).*

Asset Strip

After connecting and detecting Raritan asset management strips (asset strips), the SRC shows 'Asset Strip' in place of 'Feature Port' in the menu.

Note: For connection instructions, see **Connecting Asset Management Strips** *(on page 53).*

To open the Asset Strip page, click it in the **Menu** (on page 98). On this page, you can configure the rack units of asset strips and asset tags. A rack unit refers to a tag port on the asset strips. The "Change Asset Strip Configuration" permission is required.

For the functionality of this icon ⁝ on the top-right corner, see **Feature Port** (on page 130).

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

1. Click Edit Settings.

Settings	⌃
	Edit Settings
Name	
Number of rack units	48
Numbering mode	Bottom-up
Numbering offset	1
Orientation	Bottom connector
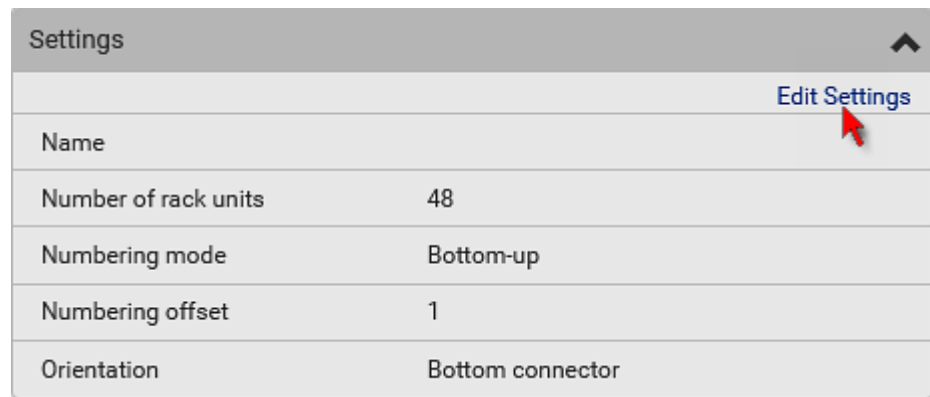
2. Make changes to the settings by directly typing a new value, or clicking that field to select a different option.

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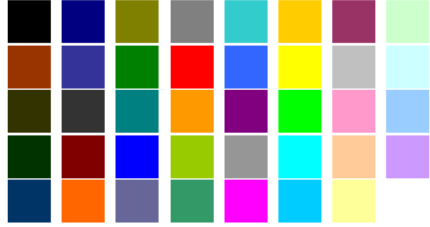
Field	Description
Numbering mode	The rack unit numbering method in a rack/cabinet. ▪ *Top-Down*: The numbering starts from the highest rack unit of a rack/cabinet. ▪ *Bottom-Up*: The numbering starts from the lowest rack unit of a rack/cabinet.
Numbering offset	The start number in the rack unit numbering.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

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

▪ Click a color in the color palette.

- Type the hexadecimal RGB value of the color, such as #00FF00.
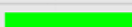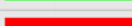
3. Click Ok. The rack unit numbering and LED color settings are immediately updated on the Rack Units list illustrated below.

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

- A blade extension strip and a *programmable* tag are marked with the word 'programmable' in the Asset/ID column. You can customize their Asset IDs. For instructions, refer to this section's last procedure below.

- If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 101).

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

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

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

Setup of Rack Unit 3

Name

Operation Mode

Auto (based on Tag) ▼

LED Mode

On ▼

LED Color

| Cancel | Save |

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

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

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

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

A blade extension strip, like an asset strip, has multiple tag ports. An extension strip is marked with a grayer color on the Asset Strip page, and its tag ports list is collapsed by default.

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

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

Rack Units							
							Program Asset IDs
Rack unit ▲	Index	Slot	Name	Asset / ID	Operation Mode	LED Mode	LED Color
1	1			000015B914BB	Auto	On	🟩
2	2	1-16 ∧		0000ABC12345 (programmable)	Auto	On	🟩
3	3			000015B9152E	Auto	On	🟩
4	4				Auto	On	🟥

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

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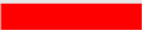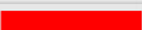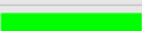
■ To hide the blade extension slots list, click **1-N ✔** .

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

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

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

1. Click Program Asset IDs.

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

2. In the Asset/ID column, enter the customized asset IDs by typing values or scanning the barcode.

   ▪ When using a barcode reader, first click the desired rack unit, and then scan the asset tag. Repeat this step for all desired rack units.

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

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

3. Verify the correctness of customized asset IDs and modify as needed.
4. Click Apply at the bottom of the page to save changes.
   - Or click Cancel to abort changes.

Tip: Another way to abort changes is to click Rack Units. Refer to the diagram below.

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

Raritan.
A brand of ▢legrand'

139

Asset Strip Automatic Firmware Upgrade

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

During the firmware upgrade, the following events take place:

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

External Beeper

After connecting and detecting a supported external beeper, the SRC shows 'External Beeper' in place of 'Feature Port' in the menu.

Note: For connection instructions, see **Connecting an External Beeper** *(on page 65).*

To open the External Beeper page, click it in the **Menu** (on page 98). This page shows an external beeper's status, including:

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

For the functionality of this icon ⋮ on the top-right corner, see **Feature Port** (on page 130).

Schroff LHX/SHX

You must enable the LHX/SHX support for the SRC to detect the presence of a supported Schroff® LHX/SHX heat exchanger. See **Miscellaneous** (on page 297).

After enabling the LHX/SHX support and connecting a supported Schroff® LHX/SHX heat exchanger to the SRC, the SRC shows the connected device type in place of 'Feature Port' in the menu -- LHX 20, LHX 40 or SHX 30.

Note: For connection instructions, see Connecting a Schroff LHX/SHX Heat Exchanger.

To open the LHX/SHX page, click 'LHX 20', 'LHX 40' or 'SHX 30' in the **Menu** (on page 98). Then you can monitor and administer the connected LHX/SHX device with the following.

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

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

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

For the functionality of this icon ⋮ on the top-right corner, see **Feature Port** (on page 130).

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

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

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

Operational State	critical ❗
Switch State	⏻ On

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

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

LHX 40 (1)	⏻ On ⏻ Off ⚙
Information	
	Schroff®
Model	LHX 40
Firmware Version	0x3d
Operational State	critical ❗
Switch State	⏻ On
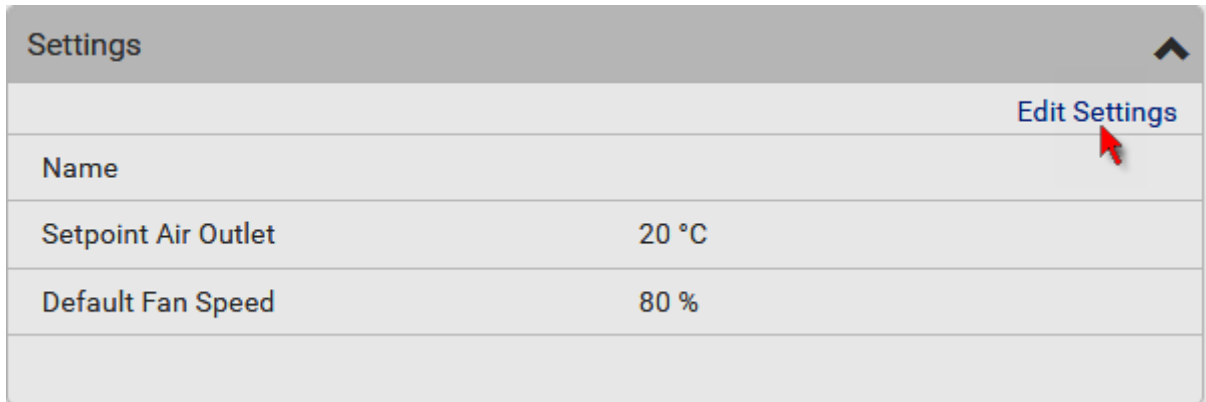
⏻ On : Power ON.

⏻ Off : Power OFF.

2. Confirm the operation on the confirmation message.

Raritan.
A brand of legrand®

▶ **To configure LHX/SHX settings:**

1. Click Edit Settings.

Settings	
	Edit Settings
Name	
Setpoint Air Outlet	20 °C
Default Fan Speed	80 %

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

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

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

   a. Click the desired sensor.

b. Click Edit Thresholds.

Sensors		
		Edit Thresholds
Name	**Reading**	**Status**
Temperature Air Outlet (F1)	19.9 °C	normal
Temperature Air Outlet (F2)	19.9 °C	normal
Temperature Air Inlet (F3)	25.9 °C	normal
Temperature Air Inlet (F4)	25.9 °C	normal
Temperature Water Inlet (F6)	26.6 °C	normal
Fan Speed (M1)	2844 rpm	normal
Fan Speed (M2)	3035 rpm	normal
Fan Speed (M3)	2837 rpm	normal
Fan Speed (M4)	3008 rpm	normal
Fan Speed (M5)	2682 rpm	normal
Fan Speed (M6)	2855 rpm	normal
Fan Speed (M7)	2907 rpm	normal
Door Contact	0	closed

c. Enable and set the desired thresholds and deassertion hysteresis.

Note that assertion timeout is NOT available on LHX/SHX.

d. Click Save.

3. After thresholds are enabled, sensors may be highlighted in yellow or red if they enter the warning or critical range. See *Yellow- or Red-Highlighted Sensors* (on page 115).

*Tip: You can also create event rules to notify you of the warning or critical levels. See **Event Rules and Actions** (on page 224).*

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

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

1. Locate the Alert States section.

2. If any LHX sensors fail, they are indicated. Click Acknowledge to acknowledge the sensor failure.

Alert States	︿
Fans	M2, M4, M5 failure
Acknowledge Alert Status	Acknowledge Show Event Log
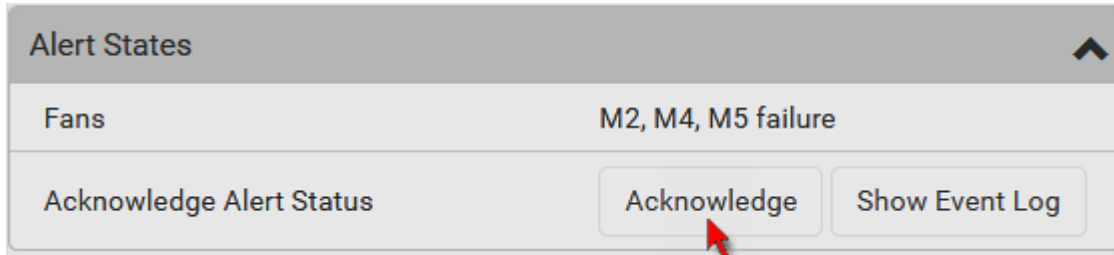
3. To view the history of LHX events, click Show Event Log to go to the Event Log page.

► **Operation time statistics:**

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

Available time units in the statistics --

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

Statistics	︿
Operating Hours (Varistar LHX)	7 h
Operating Hours (Fan 1)	6 h
Operating Hours (Fan 2)	6 h
Operating Hours (Fan 3)	6 h
Operating Hours (Fan 4)	3 h
Operating Hours (Fan 5)	3 h
Operating Hours (Fan 6)	0 h
Operating Hours (Fan 7)	0 h

► **Request maximum cooling:**

Only SHX 30 supports this feature. See *SHX Request Maximum Cooling* (on page 146).

SHX Request Maximum Cooling

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

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

▶ **To perform maximum cooling:**

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

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

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

▶ **To stop maximum cooling:**

- Click Cancel Maximum Cooling.

User Management

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

SRC is shipped with one built-in administrator account: **admin**, which is ideal for initial login and system administration. You cannot delete 'admin' or change its permissions, but you can and **should** change its password.

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

Click 'User Management' in the **Menu** (on page 98), and the following submenu displays.
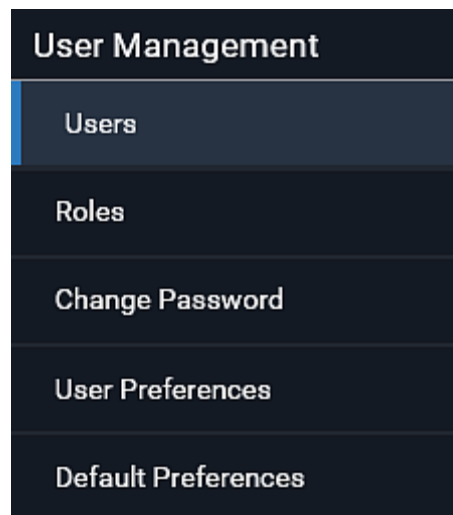
Submenu command	Refer to...
Users	**Creating Users** (on page 148)
Roles	**Creating Roles** (on page 153)
Change Password	**Changing Your Password** (on page 92)
User Preferences	**Setting Your Preferred Measurement Units** (on page 156)
Default Preferences	**Setting Default Measurement Units** (on page 157)

Creating Users

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

To add users, choose User Management > Users > .

▶ **User information:**

Field/setting	Description
User name	The name the user enters to log in to the SRC. • 4 to 32 characters • Case sensitive • Colon character and 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 128 characters • Case sensitive
Enable	When selected, the user can log in to the SRC.
Force password change on next login	When selected, a password change request automatically appears the next time the user logs in. For details, see **Changing Your Password** (on page 92).

▶ **SSH:**

You need to enter the SSH public key only if the public key authentication for SSH is enabled. See **Changing SSH Settings** (on page 191).

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

▶ **SNMPv3:**

The SNMPv3 access permission is disabled by default.

Field/setting	Description
Enable SNMPv3	Select this checkbox when intending to permit the SNMPv3 access by this user.
	*Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring SNMP Settings** (on page 188).*
Security level	Click the field to select a preferred security level from the list: ▪ None: No authentication and no privacy. This is the default. ▪ Authentication: Authentication and no privacy. ▪ Authentication & Privacy: Authentication and privacy.

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

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

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

Field/setting	Description
Same as authentication password	Select this checkbox if the privacy password is identical to the authentication password. To specify a different privacy password, disable the checkbox.

Field/setting	Description
Password, Confirm password	Type the privacy password if the 'Same as Authentication Password' checkbox is deselected. The password must consist of 8 to 32 ASCII printable characters.

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

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

▶ **Preferences:**

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

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

Note: Users can change the measurement units at any time by setting their own preferences. See **Setting Your Preferred Measurement Units** *(on page 156).*

▶ **Roles:**

Select one or multiple roles to determine the user's permissions.

To select all roles, select the topmost checkbox in the header row. However, a user can have a maximum of 32 roles only.

If the built-in roles do not satisfy your needs, add new roles by clicking

. This newly-created role will be then automatically assigned to the user account currently being created. See **Creating Roles** (on page 153).

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change SRC Configuration • View Event Settings • View Local Event Log

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

Editing or Deleting Users

To edit or delete users, choose User Management > Users to open the Users page, which lists all users.

In the Enabled column:

- ✔ : The user is enabled.
- ✖ : The user is disabled.

If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 101).

▶ **To edit or delete a user account:**

1. On the Users page, click the desired user. The Edit User page for that user opens.

2. Make changes as needed.

   - For information on each field, see **Creating Users** (on page 148).

   - To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password remains unchanged.

   - To delete this user, click 🗑 , and confirm the operation.

3. Click Save.

▶ **To delete multiple user accounts:**

1. On the Users page, click 🗹 to make checkboxes appear in front of user names.

   Tip: To delete only one user, you can simply click that user without making the checkboxes appear. Refer to the above procedure.

2. Select one or multiple users.

   - To select all roles, except for the admin user, select the topmost checkbox in the header row.

3. Click ![trash icon].

4. Click Delete on the confirmation message.

Creating Roles

A role is a combination of permissions. Each user must have at least one role.

The SRC provides two built-in roles.

Built-in role	Description
Admin	Provide full permissions.
Operator	Provide frequently-used permissions, including: • Acknowledge Alarms • Change Own Password • Change SRC Configuration • View Event Settings • View Local Event Log

If the two do not satisfy your needs, add new roles. SRC supports up to 64 roles.

▶ **To create a role:**
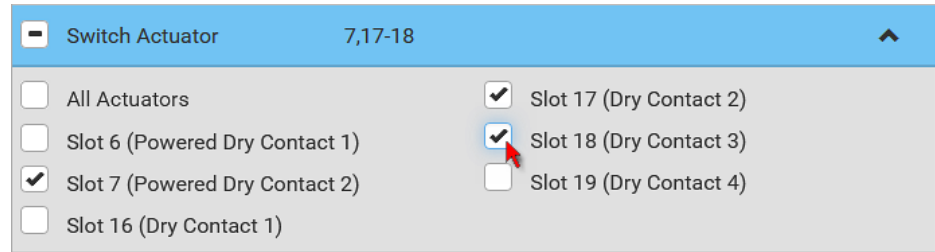
1. Choose User Management > Roles > ![add user icon].

2. Assign a role name.

   ▪ 1 to 32 characters long

   ▪ Case sensitive

   ▪ Spaces are permitted

3. Type a description for the role in the Description field.

4. Select the desired privilege(s).

   ▪ The 'Administrator Privileges' includes all privileges.

   ▪ The 'Unrestricted View Privileges' includes all 'View' privileges.

5. If any privilege requires the argument setting, the symbol [icon] displays in the rightmost edge of that privilege's row. To select such a privilege:

   a. Click on that privilege's row to display a list of available arguments for that privilege.

   b. Select the desired arguments.

      ▪ To select all arguments, simply select the checkbox labeled 'All XXX'.

   Tip: The other way to select all arguments is to select that privilege's checkbox while the arguments list is not expanded yet.

   For example, you can specify the actuators that users can switch on/off as shown below. To select all actuators, select the 'All Actuators' checkbox instead.

6. Click Save.

Now you can assign the role to any user. See **Creating Users** (on page 148) or **Editing or Deleting Users** (on page 151).

Editing or Deleting Roles

Choose User Management > Roles to open the Roles page, which lists all roles.

If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 101).

The Admin role is not user-configurable so the lock icon displays, indicating that you are not allowed to configure it.

▶ **To edit a role:**

1. On the Roles page, click the desired role. The Edit Role page opens.

2. Make changes as needed.
   - The role name cannot be changed.
   - To delete this role, click , and confirm the operation.

3. Click Save.

▶ **To delete any roles:**

1. On the Roles page, click to make checkboxes appear in front of roles.

   Tip: To delete only one role, you can simply click that role without making the checkboxes appear. Refer to the above procedure.

2. Select one or multiple roles.

      ▪   To select all roles, except for the Admin role, select the topmost checkbox in the header row.

3. Click ![trash icon] on the top-right corner.

4. Click Delete on the confirmation message.

Setting Your Preferred Measurement Units

You can change the measurement units shown in the SRC user interface according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users on the Edit User page. See **Editing or Deleting Users** *(on page 151).*

Measurement unit changes only apply to the web interface and command line interface.

Setting your own preferences does not change the default measurement units. See **Setting Default Measurement Units** (on page 157).

▶ **To select the measurement units you prefer:**

1. Choose User Management > User Preferences.

2. Make changes as needed.

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

3. Click Save.

Setting Default Measurement Units

Default measurement units are applied to all SRC user interfaces across all users, including users accessing the SRC via external authentication servers.

For a list of affected user interfaces, see *User Interfaces Showing Default Units* (on page 157). The front panel display also shows the default measurement units.

Note: The preferred measurement units set by any individual user or by the administrator on a per-user basis will override the default units in the web interface and command line interface. See **Setting Your Preferred Measurement Units** *(on page 156) or* **Creating Users** *(on page 148).*

▶ **To set up default user preferences:**

1. Click User Management > Default Preferences.
2. Make changes as needed.

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

3. Click Save.

User Interfaces Showing Default Units

Default measurement units will apply to the following user interfaces or data:

- Web interface for "newly-created" local users when they have not configured their own preferred measurement units. See *Creating Users* (on page 148).
- Web interface for users who are authenticated via LDAP/Radius servers.
- The sensor report triggered by the "Send Sensor Report" action. See *Send Sensor Report* (on page 248).
- Front panel LCD display.

Device Settings

Click 'Device Settings' in the **Menu** (on page 98), and the following submenu displays.
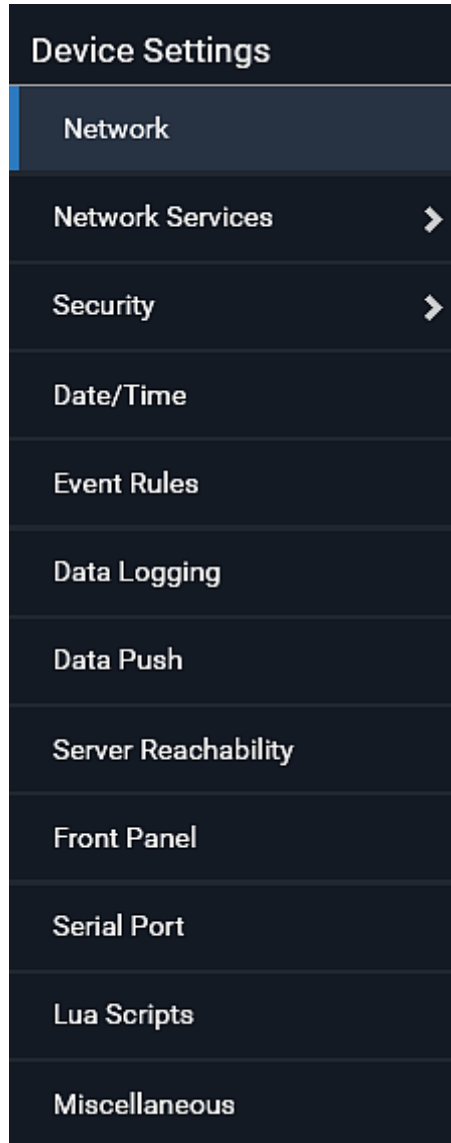
Menu command	Submenu command	Refer to...
Network		*Configuring Network Settings* (on page 160)
Network Services	HTTP	*Changing HTTP(S) Settings* (on page 186)
	SNMP	*Configuring SNMP Settings* (on page 188)

Menu command	Submenu command	Refer to...
	SMTP Server	*Configuring SMTP Settings* (on page 190)
	SSH	*Changing SSH Settings* (on page 191)
	Telnet	*Changing Telnet Settings* (on page 192)
	Modbus	*Changing Modbus Settings* (on page 192)
	Server Advertising	*Enabling Service Advertising* (on page 195)
Security	IP Access Control	*Creating IP Access Control Rules* (on page 197)
	Role Based Access Control	*Creating Role Based Access Control Rules* (on page 201)
	TLS Certificate	*Setting Up a TLS Certificate* (on page 203)
	Authentication	*Setting Up External Authentication* (on page 208)
	Login Settings	*Configuring Login Settings* (on page 215)
	Password Policy	*Configuring Password Policy* (on page 217)
	Service Agreement	*Enabling the Restricted Service Agreement* (on page 218)
Date/Time		*Setting the Date and Time* (on page 220)
Event Rules		*Event Rules and Actions* (on page 224)
Data Logging		*Setting Data Logging* (on page 277)
Data Push		*Configuring Data Push Settings* (on page 278)
Server Reachability		*Monitoring Server Accessibility* (on page 285)
Front Panel		*Front Panel Settings* (on page 289)
Serial Port		*Configuring the Serial Port* (on page 290)
Lua Scripts		*Lua Scripts* (on page 291)
Miscellaneous		*Miscellaneous* (on page 297)

Configuring Network Settings

Configure wired, wireless, and Internet protocol-related settings on the Network page after **Connecting the SRC to Your Network** (on page 11).

You can enable both the wired and wireless networking on SRC so that it has multiple IP addresses -- wired and wireless IP. For example, you can obtain one IPv4 and/or IPv6 address by enabling one Ethernet interface, and obtain one more IPv4 and/or IPv6 address by enabling/configuring the wireless interface. This also applies when SRC enters the port forwarding mode so that SRC has more than one IPv4 or IPv6 address in the port forwarding mode.

However, SRC in the BRIDGING mode obtains "only one" IP address for wired networking. Wireless networking is NOT supported in this mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

▶ **To set up the network settings:**

1. Choose Device Settings > Network.

2. To use DHCP-assigned DNS servers and gateway instead of static ones, go to step 3. To manually specify DNS servers and default gateway, configure the Common Network Settings section. See **Common Network Settings** (on page 163).

   ▪ Static routes and cascading mode are also in this section. You need to configure them only when there are such local requirements. See **Setting the Cascading Mode** (on page 177) and **Static Route Examples** (on page 173).

3. To configure IPv4/IPv6 settings for a *wired* network, click the ETH1/ETH2 or BRIDGE section. See **Wired Network Settings** (on page 161).

   ▪ If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings.

4. To configure IPv4/IPv6 settings for a *wireless* network, click the WIRELESS section. See **Wireless Network Settings** (on page 167).

   ▪ You must connect a USB wireless LAN adapter to the SRC for wireless networking.

   Note: If the device's cascading mode is set to 'Bridging' or its role is set to 'Slave' in the port forwarding mode, the wireless settings will be disabled.

5. To configure the ETH1/ETH2 interface settings, see **Ethernet Interface Settings** (on page 164).

6. Click Save.

▶ **After enabling either or both Internet protocols:**

After enabling IPv4 and/or IPv6, all but not limited to the following protocols will be compliant with the selected Internet protocol(s):

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

Note: SRC disables TLS 1.0 and 1.1 by default. It enables only TLS 1.2 and 1.3.

Wired Network Settings

On the Network page, click the ETH1/ETH2 section to configure IPv4/IPv6 settings.

If the device's cascading mode is set to 'Bridging', the BRIDGE section appears. Then you must click the BRIDGE section for IPv4/IPv6 settings. See **Setting the Cascading Mode** (on page 177).

▶ **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETH1/ETH2 section, but not available in the BRIDGE section.

Enable interface	✔

▶ **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".
  - Example: *192.168.84.99/24*

► **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. ■ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ■ *Static*: Manually configure the IPv6 settings.
Preferred hostname	■ Enter the hostname you prefer for IPv6 connectivity

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".
  - Example: *fd07:2fa:6cff:1111::0/128*

▶ **(Optional) To view the diagnostic log for EAP authentication:**

- Click Show EAP Authentication Log. See *Diagnostic Log for Network Connections* (on page 172).

Common Network Settings

Common Network Settings are OPTIONAL, not required. Therefore, leave them unchanged if there are no specific local networking requirements.

Field	Description
Cascading mode	Leave it to the default "None" unless you are establishing a cascading chain. For more information, refer to: ▪ *Cascading Multiple SRC Devices for Sharing Ethernet Connectivity* (on page 24) ▪ *Setting the Cascading Mode* (on page 177)
DNS resolver preference	Determine which IP address is used when the DNS resolver returns both IPv4 and IPv6 addresses. ▪ IPv4 address: Use the IPv4 addresses. ▪ IPv6 address: Use the IPv6 addresses.
DNS suffixes (optional)	Specify a DNS suffix name if needed.

Field	Description
First/Second/Third DNS server	Manually specify static DNS server(s). ▪ If any static DNS server is specified in these fields, it will override the DHCP-assigned DNS server. ▪ If DHCP (or Automatic) is selected for IPv4/IPv6 settings, and there are NO static DNS servers specified, the SRC will use DHCP-assigned DNS servers.
IPv4/IPv6 routes	You need to configure these settings only when your local network contains two subnets, and you want SRC to communicate with the other subnet. If so, make sure IP forwarding has been enabled in your network, and then you can click 'Add Route' to add static routes. See *Static Route Examples* (on page 173).

Ethernet Interface Settings

By default both ETH1 and ETH2 interfaces on SRC are enabled.

▶ **Enable Interface:**

Make sure the Ethernet interface is enabled, or all networking through this interface fails. This setting is available in the ETH1/ETH2 section, but not available in the BRIDGE section.

▶ **Other Ethernet settings:**

Field	Description
Speed	Select a LAN speed. • *Auto:* System determines the optimum LAN speed through auto-negotiation. • *10 MBit/s:* Speed is always 10 Mbps. • *100 MBit/s:* Speed is always 100 Mbps. • *1 GBit/s:* Speed is always 1 Gbps (1000 Mbps).
Duplex	Select a duplex mode. • *Auto:* The SRC selects the optimum transmission mode through auto-negotiation. • *Full:* Data is transmitted in both directions

Field	Description
	simultaneously.
	• *Half:* Data is transmitted in one direction (to or from the SRC) at a time.
Current state	Show the LAN's current status, including the current speed and duplex mode.
Authentication	Select an authentication method. ▪ *No Authentication:* No authentication data is required. ▪ *EAP:* Use Protected Extensible Authentication Protocol. Enter required authentication data in the fields that appear.
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. ▪ *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. ▪ *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Identity	This field appears when 'EAP' is selected. Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected. Type your password.

Field	Description
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected.
	PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. ▪ SRC supports private keys of PKCS#1 and PKCS#8 formats. ▪ Client Private Key Password should be entered only when your private key is encrypted with a password. ▪ To view the uploaded certificate, click Show Client Certificate. ▪ To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected.
	A third-party CA certificate may or may not be needed. If needed, follow the steps below.
RADIUS authentication server name	This field appears when 'EAP' is selected.
	Type the name of the RADIUS server if it is present in the TLS certificate. ▪ The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

Note: Auto-negotiation is disabled after setting both the speed and duplex settings of the SRC to NON-Auto values, which may result in a duplex mismatch.

- **Available settings for the CA Certificate:**

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see ***TLS Certificate Chain*** (on page 638).

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the SRC to verify the validity of the TLS certificate that will be installed. ▪ For example, the SRC will check the certificate's validity period against the system time.

Raritan.
A brand of ⬛legrand®

Field/setting	Description
Browse...	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the SRC system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the SRC has once been powered off for a long time.

Wireless Network Settings

If the device's cascading mode is set to 'Bridging' or its role is set to 'Slave' in the port forwarding mode, the wireless settings will be disabled. See *Setting the Cascading Mode* (on page 177).

By default the wireless interface is disabled. You should enable it if wireless networking is wanted.

On the Network page, click the WIRELESS section to configure wireless and IPv4/IPv6 settings.

▶ **Interface Settings:**

Field/setting	Description
Enable interface	Enable or disable the wireless interface. When disabled, the wireless networking fails.
Hardware state	Check this field to ensure that the SRC has detected a wireless USB LAN adapter. If not, verify whether the

Field/setting	Description
	USB LAN adapter is firmly connected or whether it is supported.
SSID	Type the name of the wireless access point (AP).
Force AP BSSID	If the BSSID is available, select this checkbox.
BSSID	Type the MAC address of an access point.
Enable High Throughput (802.11n)	Enable or disable 802.11n protocol.
Authentication	Select an authentication method. ▪ *No Authentication:* No authentication data is required. ▪ *PSK*: A Pre-Shared Key is required. ▪ *EAP:* Use Protected Extensible Authentication Protocol. Enter required authentication data in the fields that appear.
Pre-Shared Key	This field appears only when PSK is selected. Type the PSK string.
Outer authentication	This field appears when 'EAP' is selected. There are two authentication methods for EAP. ▪ *PEAP:* A TLS tunnel is established, and an inner authentication method can be specified for this tunnel. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.
Inner authentication	This field appears when both 'EAP' and 'PEAP' are selected. ▪ *MS-CHAPv2:* Authentication based on the given password using MS-CHAPv2 protocol. ▪ *TLS:* Authentication between the client and authentication server is performed using TLS certificates.

Raritan.

A brand of ◻legrand®

Field/setting	Description
Identity	This field appears when 'EAP' is selected.
	Type your user name.
Password	This field appears only when 'EAP', 'PEAP' and 'MS-CHAPv2' are all selected.
	Type your password.
Client certificate, Client private key, Client private key password	This field appears when 'EAP', 'PEAP' and 'TLS' are all selected.
	PEM encoded X.509 certificate and PEM encoded private key are required for certification-based authentication methods. Private key password is optional. ▪ SRC supports private keys of PKCS#1 and PKCS#8 formats. ▪ Client Private Key Password should be entered only when your private key is encrypted with a password. ▪ To view the uploaded certificate, click Show Client Certificate. ▪ To remove the uploaded certificate and private key, click 'Clear Key/Certificate selection'.
CA certificate	This field appears when 'EAP' is selected.
	A third-party CA certificate may or may not be needed. If needed, follow the steps below.
RADIUS authentication server name	This field appears when 'EAP' is selected.
	Type the name of the RADIUS server if it is present in the TLS certificate. ▪ The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

Raritan.
A brand of **legrand**

- **Available settings for the CA Certificate:**

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see **TLS Certificate Chain** (on page 638).

Field/setting	Description
Enable verification of TLS certificate chain	Select this checkbox for the SRC to verify the validity of the TLS certificate that will be installed. ▪ For example, the SRC will check the certificate's validity period against the system time.
Browse…	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Allow connection if system clock is incorrect	When this checkbox is deselected, and if the system time is incorrect, the installed TLS certificate is considered not valid yet and will cause the wireless network connection to fail. When this checkbox is selected, it will make the wireless network connection successful when the SRC system time is earlier than the firmware build before synchronizing with any NTP server. ▪ The incorrect system time issue may occur when the SRC has once been powered off for a long time.

▶ **IPv4 settings:**

Field/setting	Description
Enable IPv4	Enable or disable the IPv4 protocol.
IP auto configuration	Select the method to configure IPv4 settings. ▪ *DHCP*: Auto-configure IPv4 settings via DHCP servers. ▪ *Static*: Manually configure the IPv4 settings.
Preferred hostname	Enter the hostname you prefer for IPv4 connectivity

Raritan.
A brand of ◻legrand

- **DHCP settings:** Optionally specify the preferred hostname, which must meet the following requirements:
    - Consists of alphanumeric characters and/or hyphens
    - Cannot begin or end with a hyphen
    - Cannot contain more than 63 characters
    - Cannot contain punctuation marks, spaces, and other symbols
- **Static settings:** Assign a static IPv4 address, which follows this syntax "IP address/prefix length".

    Example: *192.168.84.99/24*

▶ **IPv6 settings:**

Field/setting	Description
Enable IPv6	Enable or disable the IPv6 protocol.
IP auto configuration	Select the method to configure IPv6 settings. ▪ *Automatic*: Auto-configure IPv6 settings via DHCPv6. ▪ *Static*: Manually configure the IPv6 settings.
Preferred hostname	▪ Enter the hostname you prefer for IPv6 connectivity

- **Automatic settings:** Optionally specify the preferred hostname, which must meet the above requirements.
- **Static settings:** Assign a static IPv6 address, which follows this syntax "IP address/prefix length".

    Example: *fd07:2fa:6cff:1111::0/128*

▶ **(Optional) To view the wireless LAN diagnostic log:**
- Click Show WLAN Diagnostic Log. See **Diagnostic Log for Network Connections** (on page 172).
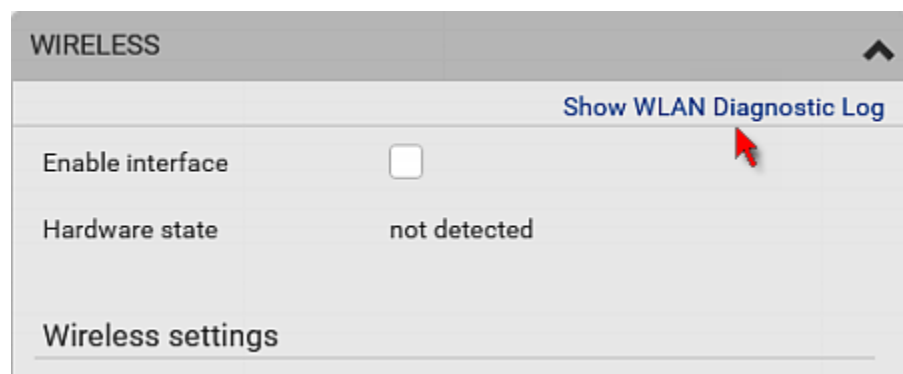
Diagnostic Log for Network Connections
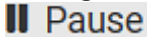
SRC provides a diagnostic log for inspecting connection errors that occurred during the EAP authentication or the wireless network connection. The information is useful for technical support.

Note that the diagnostic log shows data only after connection errors are detected.

Each entry in the log consists of:

- ID number
- Date and time
- Description

► **To view the log:**

1. Access the diagnostic log with either method below.
   - Choose Device Settings > Network > ETH1/ETH2 > Show EAP Authentication Log. See *Configuring Network Settings* (on page 160).
   - Choose Device Settings > Network > WIRELESS > Show WLAN Diagnostic Log.
2. The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking **❚❚ Pause**.
   - To restore automatic update, click **▶▶ Resume**. Those new events that have not been listed yet due to suspension will be displayed in the log now.
3. To go to other pages of the log, click the pagination bar at the bottom of the page.
   - When there are more than 5 pages and the page numbers listed does not show the desired one, click **⋯** to have the bar show the next or previous five page numbers, if available.

First	Previous	1	2	3	4	5	...	Next	Last

4. If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 101).

► **To clear the diagnostic log:**

1. On the top-right corner of the log, click **⋮** > **🗑 Clear Log**.
2. Click Clear Log on the confirmation message.

Raritan.
A brand of ◻legrand®

Static Route Examples

This section describes two static route examples: IPv4 and IPv6. Both examples assume that two network interface controllers (NIC) have been installed in one network server, leading to two available subnets, and IP forwarding has been enabled. All of the NICs and SRC devices in the examples use static IP addresses.

Most of local multiple networks are not directly reachable and require the use of a gateway. Therefore, we will select Gateway in the following examples. If your local multiple networks are directly reachable, you should select Interface rather than Gateway.

Note: If Interface is selected, you should select an interface name instead of entering an IP address. See **Interface Names** *(on page 176).*

▶ **IPv4 example:**

- Your SRC: *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*
- Prefix length: *24*
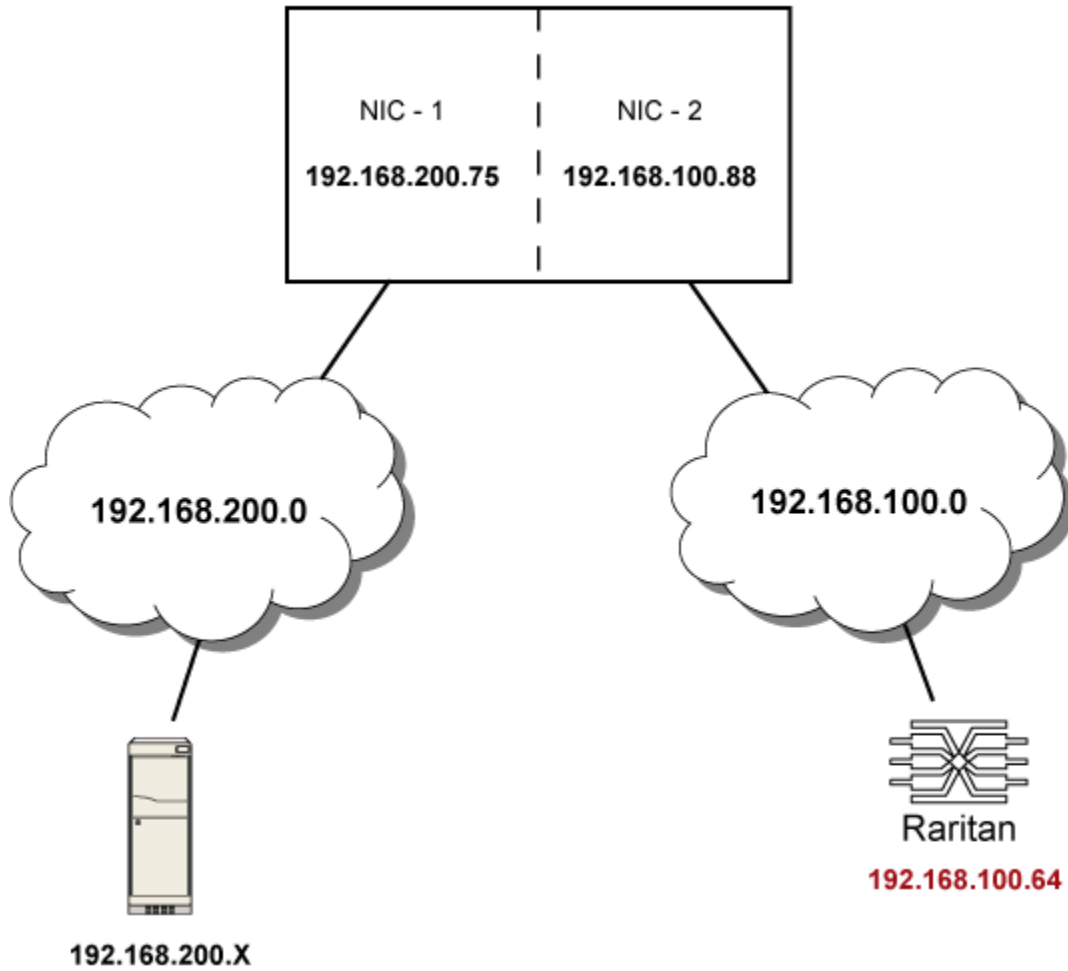
In this example, NIC-2 (192.168.100.88) is the next hop router for your SRC to communicate with any device in the other subnet 192.168.200.0.

In the IPv4 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.

1	192.168.200.0/24	Gateway ▼	192.168.100.88	↑ ↓ 🗑

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ⬆ *or* ⬇ *to re-sort the priority, or click* 🗑 *to delete it.*

▶ **IPv6 example:**

- Your SRC: *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*
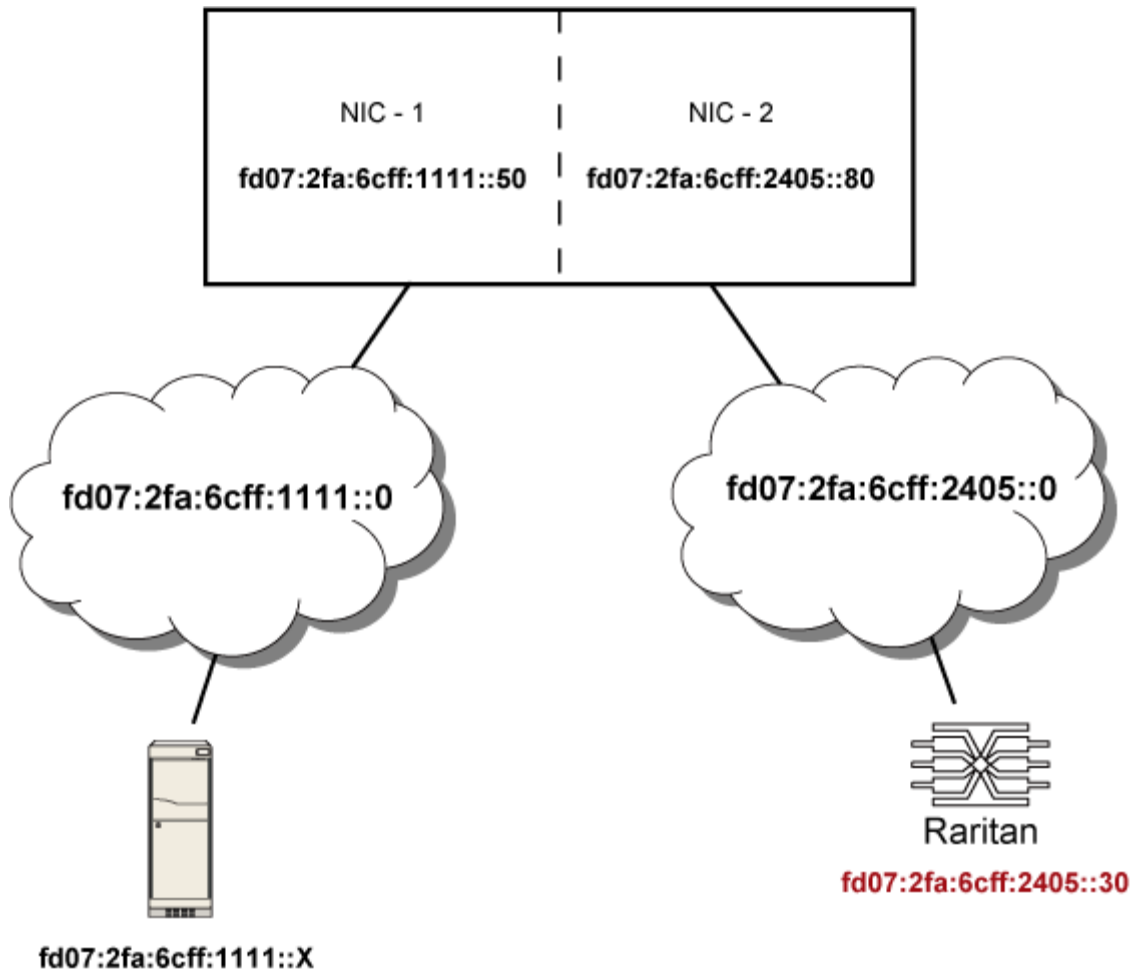
In this example, NIC-2 (fd07:2fa:6cff:2405::80) is the next hop router for your SRC to communicate with any device in the other subnet fd07:2fa:6cff:1111::0.

In the IPv6 "Static Routes" section, you should enter the data as shown below. Note that the address in the first field must be of the Classless Inter-Domain Routing (CIDR) notation.

| 1 | fd07:2fa:6cff:2405::0/64 | Gateway ▼ | fd07:2fa:6cff:2405::80 ✕ | ⬆ ⬇ 🗑 |

Tip: If you have configured multiple static routes, you can click on any route and then make changes, use ⬆ or ⬇ to re-sort the priority, or click 🗑 to delete it.

Interface Names

When your local multiple networks are "directly reachable", you should select Interface for static routes. Then choose the interface where another network is connected.

192.168.200.0/24	Interface ▼	▼	⬆ ⬇ 🗑
		BRIDGE	
		ETH1	
		ETH2	
		WIRELESS	

▶   **Interface list:**

Interface name	Description
BRIDGE	When another wired network is connected to the Ethernet port of your SRC, and your SRC has been set to the bridging mode, select this interface name instead of the Ethernet interface.
ETH1	When another wired network is connected to the ETH1 port of your SRC, select this interface name.
ETH2	When another wired network is connected to the ETH2 port of your SRC, select this interface name.
WIRELESS	When another wireless network is connected to your SRC, select this interface name.

Setting the Cascading Mode

A maximum of 16 SRC devices can be cascaded to share one Ethernet connection. See **Cascading Multiple SRC Devices for Sharing Ethernet Connectivity** (on page 24).

The cascading mode configured on the master device determines the Ethernet sharing method, which is either network bridging or port forwarding. See **Overview of the Cascading Modes** (on page 179).

The cascading mode of all devices in the chain must be the same.

Only a user with the Change Network Settings permission can configure the cascading mode.

Note: SRC in the Port Forwarding mode does not support APIPA. See **APIPA and Link-Local Addressing** (on page 6).

▶ **To configure the cascading mode:**

1. Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.

   ▪ For computer connection instructions, see **Connecting the SRC to a Computer** (on page 21).

   ▪ To find the IP address, see **Device Info** (on page 80).

2. Log in to its web interface. See **Login** (on page 89).

3. Choose Device Settings > Network.

4. Select the preferred mode in the Cascading Mode field.

Mode	Description
None	No cascading mode is enabled. This is the default.
Bridging	Each device in the cascading chain is accessed with a different IP address.
Port Forwarding	Each device in the cascading chain is accessed with the same IP address(es) but with a different port number assigned. For details on port numbers, see **Port Number Syntax** (on page 180).

Tip: If selecting Port Forwarding, the Device Information page will show a list of port numbers for all cascaded devices. Simply choose Maintenance > Device Information > Port Forwarding.

5. For the Port Forwarding mode, one to two more fields have to be configured.

   Note that if either setting below is incorrectly configured, a networking issue occurs.

Field	Description
Port forwarding role (available on all cascaded devices)	*Master or Slave.* This is to determine which device is the master and which ones are slave devices.
Downstream interface (available on the maser device only)	*USB or ETH1/ETH2.* This is to determine which port on the master device is connected to Slave 1. If ETH1 or ETH2 is selected as the downstream interface, make sure the selected Ethernet interface is enabled.

6. (Optional) Configure the network settings by clicking the BRIDGE, ETH1/ETH2, or WIRELESS section on the same page.

   ▪ In the Bridging mode, each cascaded device can have different network settings. You may need to configure each device's network settings in the BRIDGE section.

   ▪ In the Port Forwarding mode, all cascaded devices share the master device's network settings. You only need to configure the master device's network settings in the ETH1/ETH2 and/or WIRELESS section.

   See **Wired Network Settings** (on page 161) or **Wireless Network Settings** (on page 167)

   Tip: You can enable/configure multiple network interfaces in the Port Forwarding mode so that the cascading chain has multiple IP addresses.

7. Click Save.

For information on accessing each cascaded device in the Port Forwarding mode, see **Port Forwarding Examples** (on page 182).

▶ **Recommendations for cascade loops:**

   You can connect both the first and the last PDU to your network (cascade loop) under the following conditions:

a. The remaining network MUST use R/STP to avoid network loops.

   AND

Both the first and the last PDUs MUST either attach to the same switch or, if they are attached to two separate switches, you must configure both ports of these switches so that the STP costs are high. This prevents the STP protocol from sending unrelated traffic through the PDU cascade, which can cause bottlenecks that lead to connectivity issues in the whole network.

Raritan.
A brand of legrand

▶ **Online cascading information:**

For more information on cascading configurations and restrictions, refer to the *Cascading Guide* on the Raritan **Support page** (**http://www.raritan.com/support/**).

Overview of the Cascading Modes

You must apply a cascading mode to the cascading chain. See **Setting the Cascading Mode** (on page 177).

There are two cascading modes: Bridging and Port Forwarding.

In the following illustration, it is assumed that users enable the DHCP networking for the cascading chain comprising four devices. In the diagrams, "M" is the master device and "S" is a slave device.

▶ **Illustration:**

- **"Bridging" mode:**
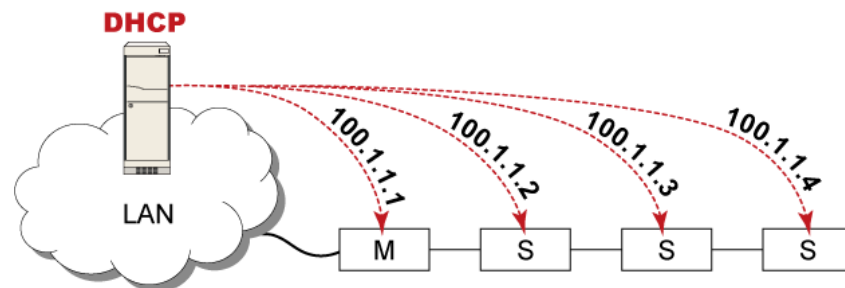
In this mode, the DHCP server communicates with every cascaded device respectively and assigns four *different* IP addresses. Each device has its own IP address.

The way to remotely access each cascaded device is completely the same as accessing a standalone device in the network.

- **"Port Forwarding" mode:**
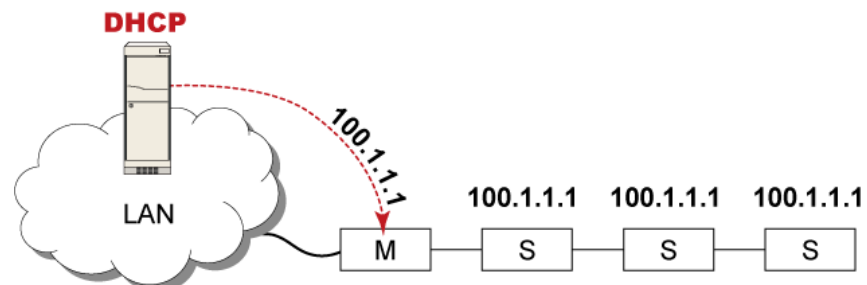
In this mode, the DHCP server communicates with the master device alone and assigns one IP address to the master device. All slave devices share the same IP address as the master device.

You must specify a 5XXXX port number (where X is a number) when remotely accessing any slave device with the shared IP address. See *Port Number Syntax* (on page 180).

▶ **Comparison between cascading modes:**

- The Bridging mode supports the wired network only, while the Port Forwarding mode supports both wired and wireless networks.
- Both cascading modes support a maximum of 16 devices in a chain.
- Both 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(es) as the master device.

- In the Bridging mode, each cascaded device has only one IP address.

  In the Port Forwarding mode, each cascaded device can have multiple IP addresses as long as the master device has multiple network interfaces enabled/configured properly.

  For example:

  - When the master device has two Ethernet ports (ETH1/ETH2), you can enable ETH1, ETH2 and WIRELESS interfaces so that the Port-Forwarding chain has two wired IP addresses and one wireless IP address.

Port Number Syntax

In the Port Forwarding mode, all devices in the cascading chain share the same IP address(es). 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

Raritan.
A brand of legrand

- XX is a two-digit number representing the device position as shown below.

Position	XX	Position	XX
Master device	00	Slave 8	08
Slave 1	01	Slave 9	09
Slave 2	02	Slave 10	10
Slave 3	03	Slave 11	11
Slave 4	04	Slave 12	12
Slave 5	05	Slave 13	13
Slave 6	06	Slave 14	14
Slave 7	07	Slave 15	15

For example, to access the Slave 4 device via Modbus/TCP, the port number is 50604. See **Port Forwarding Examples** (on page 182) for further illustrations.

Tip: The full list of each cascaded device's port numbers can be retrieved from the web interface. Choose Maintenance > Device Information > Port Forwarding.

▶ **Standard TCP/UDP ports:**

The master device can be also accessed through standard TCP/UDP ports as listed in the following table.

Protocols	Port Numbers
HTTPS	443
HTTP	80
SSH	22
TELNET	23
SNMP	161
MODBUS	502

In the Port Forwarding mode, the cascaded device does NOT allow you to modify the standard TCP/UDP port configuration, including HTTP, HTTPS, SSH, Telnet and Modbus/TCP.

Port Forwarding Examples

To access a cascaded device in the Port Forwarding mode, assign a port number to the IP address.

- Master device: Assign proper 5NNXX port numbers or standard TCP/UDP ports. See **Port Number Syntax** (on page 180) for details.
- Slave device: Assign proper 5NNXX port numbers.

Assumption: *The Port Forwarding mode is applied to a cascading chain comprising three devices. The IP address is 192.168.84.77.*

▶ **Master device:**

Position code for the master device is '00' so each port number is 5NN00 as listed below.

Protocols	Port numbers
HTTPS	50000
HTTP	50100
SSH	50200
TELNET	50300
SNMP	50500
MODBUS	50600

Examples using "5NN00" ports:

- To access the master device via HTTPS, the IP address is:
    https://192.168.84.77:50000/
- To access the master device via HTTP, the IP address is:
    http://192.168.84.77:50100/
- To access the master device via SSH, the command is:
    ssh -p 50200 192.168.84.77

Examples using standard TCP/UDP ports:

- To access the master device via HTTPS, the IP address is:
    https://192.168.84.77:443/
- To access the master device via HTTP, the IP address is:
    http://192.168.84.77:80/
- To access the master device via SSH, the command is:
    ssh -p 22 192.168.84.77

▶ **Slave 1 device:**

Position code for Slave 1 is '01' so each port number is 5NN01 as shown below.

Protocols	Port numbers
HTTPS	50001
HTTP	50101
SSH	50201
TELNET	50301
SNMP	50501
MODBUS	50601

Examples:

- To access Slave 1 via HTTPS, the IP address is:
    https://192.168.84.77:50001/
- To access Slave 1 via HTTP, the IP address is:
    http://192.168.84.77:50101/
- To access Slave 1 via SSH, the command is:
    ssh -p 50201 192.168.84.77

▶ **Slave 2 device:**

Position code for Slave 2 is '02' so each port number is 5NN02 as shown below.

Protocols	Port numbers
HTTPS	50002
HTTP	50102
SSH	50202
TELNET	50302
SNMP	50502
MODBUS	50602

Examples:

- To access Slave 2 via HTTPS, the IP address is:
    https://192.168.84.77:50002/
- To access Slave 2 via HTTP, the IP address is:
    http://192.168.84.77:50102/
- To access Slave 2 via SSH, the command is:
    ssh -p 50202 192.168.84.77

Adding, Removing or Swapping Cascaded Devices

Change a device's cascading mode first before adding that device to a cascading chain, or before disconnecting that device from the chain.

If you only want to change the cascading mode of an existing chain, or swap the master and slave device, always start from the slave device.

Note: If the following procedures are not followed, a networking issue occurs. When a networking issue occurs, check the cascading connection and/or software settings of all devices in the chain. See **Cascading Troubleshooting** *(on page 624).*

▶ **To add a device to an existing chain:**

1. Connect the device you will cascade to the LAN and find its IP address, or connect it to a computer.

2. Log in to this device and set its cascading mode to be the same as the existing chain's cascading mode. See **Setting the Cascading Mode** (on page 177).

3. (Optional) If this device will function as a slave device, disconnect it from the LAN after configuring the cascading mode.

4. Connect this device to the chain, using either a USB or Ethernet cable.

▶ **To remove a device from the chain:**

1. Log in to the desired cascaded device, and change its cascading mode to None.

Exception: If you are going to connect the removed device to another cascading chain, set its cascading mode to be the same as the mode of another chain.

2. Now disconnect it from the cascading chain.

▶ **To swap the master and slave device:**

- In the Bridging mode, you can swap the master and slave devices by simply disconnecting ALL cascading cables from them, and then reconnecting cascading cables. No changes to software settings are required.

- In the Port Forwarding mode, you must follow the procedure below:

    a. Access the slave device that will replace the master device, and set its role to 'Master', and correctly set the downstream interface.

    b. Access the master device, set its role to 'Slave'.

    c. Swap the master and slave device now.

- You must disconnect the LAN cable and ALL cascading cables connected to the two devices first before swapping them, and then reconnecting all cables.

▶ **To change the cascading mode applied to a chain:**

1. Access the last slave device, and change its cascading mode.

   - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Slave'.

2. Access the second to last, third to last and so on until the first slave device to change their cascading modes one by one.

3. Access the master device, and change its cascading mode.

   - If the new cascading mode is 'Port Forwarding', you must also set its role to 'Master', and correctly select the downstream interface.

The following diagram indicates the correct sequence. 'N' is the final one.

- M = Master device
- S = Slave device
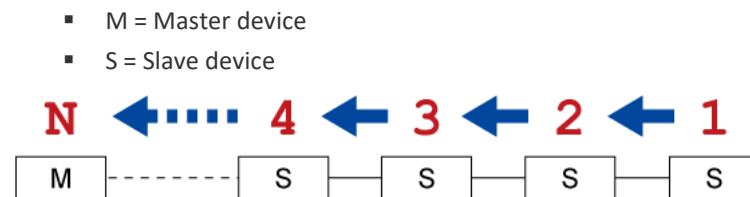
Configuring Network Services

SRC supports the following network communication services.

HTTPS and HTTP enable the access to the web interface. Telnet and SSH enable the access to the command line interface. See **Using the Command Line Interface** (on page 355).

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

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

Submenu command	Refer to
HTTP	**Changing HTTP(S) Settings** (on page 186)
SNMP	**Configuring SNMP Settings** (on page 188)
SMTP Server	**Configuring SMTP Settings** (on page 190)
SSH	**Changing SSH Settings** (on page 191)
Telnet	**Changing Telnet Settings** (on page 192)
Modbus	**Changing Modbus Settings** (on page 192)
Server Advertising	**Enabling Service Advertising** (on page 195)

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

Changing HTTP(S) Settings

HTTPS uses Transport Layer Security (TLS) technology to encrypt all traffic to and from the SRC so it is a more secure protocol than HTTP. SRC disables TLS *1.0* and *1.1* by default. It enables only TLS *1.2* and *1.3.*

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

▶ **To change HTTP or HTTPS port settings:**

1. Choose Device Settings > Network Services > HTTP.
2. Enable either or both protocols by selecting the corresponding 'Enable' checkbox.
3. To use a different port for HTTP or HTTPS, type a new port number.

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

4. To redirect the HTTP access to the SRC to HTTPS, select the "Redirect HTTP connections to HTTPS."
   - The redirection checkbox is configurable only when both HTTP and HTTPS have been enabled.

▶ **Special note for AES ciphers:**

The SRC device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between SRC and the client (such as a web browser), which is impacted by the cipher priority of SRC and the client's cipher availability/settings.

Tip: To force SRC to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings. For example, you can enable a cipher and disable the other in the Firefox via the "about:config" command.

Configuring SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the SRC. Enabling SNMP communication allows the manager to retrieve data and configures SRC.

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 224).

▶ **To configure SNMP communication:**

1. Choose Device Settings > Network Services > SNMP.

SNMP

SNMP Agent

Enable SNMP v1 / v2c	☑
Read community string	public
Write community string	
Enable SNMP v3	☐

MIB-II System Group

sysContact	
sysName	
sysLocation	

SNMP Notifications

Enable SNMP notifications	☐
Notification type	SNMPv2c trap ▼
Timeout	3 s
Number of retries	5

#	Host	Port	Community
1		162	
2		162	
3		162	

Download MIBs ⌄

✔Save

Raritan.
A brand of ☐legrand

2. Enable or disable "SNMP v1 / v2c" and/or "SNMP v3" by clicking the corresponding checkbox.

 ▪ The SNMP v1/v2c read-only access is enabled by default. The default 'Read community string' is "public."

 ▪ To enable read-write access, type the 'Write community string.' Usually the string is "private."

3. Enter the MIB-II system group information, if applicable.

 ▪ sysContact - the contact person in charge of the system

 ▪ sysName - the name assigned to the system

 ▪ sysLocation - the location of the system

4. To configure SNMP notifications:

 a. Select the 'Enable SNMP notifications' checkbox.

 b. Select a notification type -- SNMPv2c trap, SNMPv2c inform, SNMPv3 trap, and SNMPv3 inform.

 c. Specify the SNMP notification destinations and enter necessary information. For details, refer to:

 ▪ *SNMPv2c Notifications* (on page 347)

 ▪ *SNMPv3 Notifications* (on page 348)

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** *(on page 238). To add more than three SNMP destinations, you can create new SNMP notification actions. See* **Send an SNMP Notification** *(on page 253).*

5. You must download the SNMP MIB for your SRC to use with your SNMP manager.

 a. Click the Download MIBs title bar to show the download links.

 b. Click the PDU2-MIB download link. See *Downloading SNMP MIB* (on page 351).

6. Click Save.

Configuring SMTP Settings

The SRC can be configured to send alerts or event messages to a specific administrator by email. See *Event Rules and Actions* (on page 224).

To send emails, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

If any email messages fail to be sent successfully, the failure event and reason are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 308).

▶ **To set SMTP server settings:**

1. Choose Device Settings > Network Services > SMTP Server.
2. Enter the information needed.

Field	Description
IP address/host name	Type the name or IP address of the mail server.
Port	Type the port number. ▪ Default is 25
Sender email address	Type an email address for the sender.
Number of sending retries	Type the number of email retries. ▪ Default is 2 retries
Time between sending retries	Type the interval between email retries in minutes. ▪ Default is 2 minutes.
Server requires authentication	Select this checkbox if your SMTP server requires password authentication.
User name, Password	Type a user name and password for authentication after selecting the above checkbox. ▪ The length of user name and password ranges between 4 and 64. Case sensitive. ▪ Spaces are not allowed for the user name, but allowed for the password.
Enable SMTP over TLS (StartTLS)	If your SMTP server supports the Transport Layer Security (TLS), select this checkbox.

▪ **Settings for the CA Certificate:**

If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see *TLS Certificate Chain* (on page 638).

Field/setting	Description
Browse...	Click this button to import a certificate file. Then you can: ▪ Click Show to view the certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate.
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.

3. Now that you have set the SMTP settings, you can test it to ensure it works properly.

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

   b. Click Send Test Email.

   c. Check if the recipient(s) receives the email successfully.

4. Click Save.

► **Special note for AES ciphers:**

The SRC device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between SRC and the client (such as a web browser), which is impacted by the cipher priority of SRC and the client's cipher availability/settings.

Tip: To force SRC to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Changing SSH Settings

You can enable or disable the SSH access to the command line interface, change the TCP port, or set a password or public key for login over the SSH connection.

► **To change SSH settings:**

1. Choose Device Settings > Network Services > SSH.

2. To enable or disable the SSH access, select or deselect the checkbox.

3. To use a different port, type a port number.

4. Select one of the authentication methods.

   ▪ *Password authentication only:* Enables the password-based login only.

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

5. Click Save.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See **Creating Users** (on page 148).

Changing Telnet Settings

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

▶ **To change Telnet settings:**

1. Choose Device Settings > Network Services > Telnet.
2. To enable the Telnet access, select the checkbox.
3. To use a different port, type a new port number.
4. Click Save.

Changing Modbus Settings

The SRC supports both the Modbus/TCP and Modbus Gateway features. Enable either or both Modbus features according to your needs.

▶ **Modbus/TCP Access:**

You can enable or disable the Modbus/TCP access to SRC, set it to the read-only mode, or change the TCP port.

1. Choose Device Settings > Network Services > Modbus.
2. To enable the Modbus/TCP access, select the "Enable Modbus/TCP access" checkbox.
3. To use a different port, type a new port number.
4. To enable the Modbus read-only mode, select the checkbox of the "Enable read-only mode" field. To enable the read-write mode, deselect it.

▶ **Modbus Gateway:**

If connecting the Modbus RTU devices to SRC and enabling the Modbus Gateway feature, the Modbus TCP clients on your network will be able to communicate with those Modbus RTU devices attached to SRC. See ***Connecting a Modbus RTU Device or Bus*** (on page 65).

1. To allow the Modbus TCP clients on the network to communicate with the Modbus RTU devices connected to the SRC, select the 'Enable Modbus gateway' checkbox.

Modbus Gateway	
Enable Modbus gateway	✔
TCP port	503
Parity	Even ▼
Line speed	19200 ▼
Default address	1

2. Now configure the fields shown.

Field	Description
TCP port	Use the default port 503, or assign a different port. Valid range is 1 to 65535.
	Note: Port 502 is the default Modbus/TCP port for SRC, so you cannot use that port for the Modbus Gateway.
Parity, **Line speed**	Use the default values, or update if the Modbus RTU devices are using different communication parameters.
Default address	If the Modbus TCP client does not support Modbus RTU unit identifier addressing, enter a Default Address. If you must provide a unit identifier address: ▪ Only one Modbus RTU device is supported. ▪ The unit identifier address you provide is applied to the Modbus RTU device connected to SRC. Note that each Modbus RTU device's unit identifier address must be unique.
	Warning: If the connected Modbus RTU device's address does not match the address entered in this field, communications between the Modbus TCP clients and Modbus RTU device fail.

Enabling Service Advertising

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

The advertised services include the following:

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

By default, this feature is enabled.

Enabling this feature also enables Link-Local Multicast Name Resolution (LLMNR) and/or MDNS, which are required for resolving APIPA host names. See *APIPA and Link-Local Addressing* (on page 6).

The service advertisement feature supports both IPv4 and IPv6 protocols.

If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where <preferred_host_name> is the preferred host name you have specified for SRC. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

Note: For information on configuring IPv4 and/or IPv6 network settings, see **Wired Network Settings** *(on page 161).*

▶ **To enable or disable service advertising:**

1. Choose Device Settings > Network Services > Service Advertising.
2. To enable the service advertising, select either or both checkboxes.
   - To advertise via MDNS, select the Multicast DNS checkbox.
   - To advertise via LLMNR, select the Link-Local Multicast Name Resolution checkbox.
3. Click Save.

Configuring Security Settings

The SRC provides tools to control access. You can enable the internal firewall, create firewall rules, and set login limitations. In addition, you can create and install the certificate or set up external authentication servers for access control. This product supports SHA-2 TLS certificates.

Tip: To force all HTTP accesses to the SRC to be redirected to HTTPS, see **Changing HTTP(S) Settings** *(on page 186).*
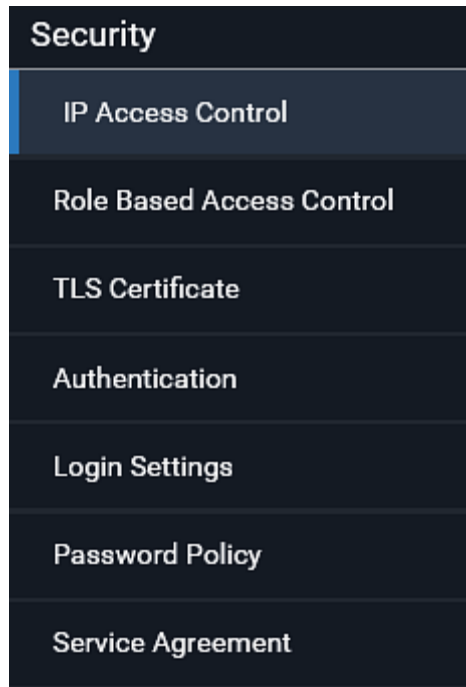
Submenu command	Refer to
IP Access Control	**Creating IP Access Control Rules** (on page 197)
Role Based Access Control	**Creating Role Based Access Control Rules** (on page 201)
TLS Certificate	**Setting Up a TLS Certificate** (on page 203)
Authentication	**Setting Up External Authentication** (on page 208)
Login Settings	**Configuring Login Settings** (on page 215)
Password Policy	**Configuring Password Policy** (on page 217)
Service Agreement	**Enabling the Restricted Service Agreement** (on page 218)

Creating IP Access Control Rules

IP access control rules (firewall rules) determine whether to accept or discard traffic to/from the SRC, based on the IP address of the host sending or receiving the traffic. When creating rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches or is sent from the SRC, 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.

- **Prefix length is required.**

  When typing the IP address, you must specify it in the CIDR notation. That is, BOTH the address and the prefix length are included. For example, to specify a single address with the 24-bit prefix length, use this format:

  x.x.x.x/24

  /24 = the prefix length.

  Note: Valid IPv4 addresses range from 0.0.0.0 through 255.255.255.255.

▶ **To configure IPv4 access control rules:**

1. Choose Device Settings > Security > IP Access Control.

2. Select the 'Enable IPv4 access control' checkbox to enable IPv4 access control rules.

3. Determine the IPv4 default policy.

   - *Accept:* Accepts traffic from all IPv4 addresses.

   - *Drop:* Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.

   - *Reject:* Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.

4. Go to the Inbound Rules section or the Outbound Rules section according to your needs.

   - Inbound rules control the data sent to the SRC.

   - Outbound rules control the data sent from the SRC.

5. Create rules. Refer to the tables below for different operations.

ADD a rule to the end of the list

- Click Append.

- Type an IP address and subnet mask in the IP/Mask field.

- Select an option in the Policy field.

  - *Accept:* Accepts traffic from/to the specified IP address(es).

  - *Drop:* Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.

  - *Reject:* Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

INSERT a rule between two rules

- Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.

- Click *Insert Above*.

- Type an IP address and subnet mask in the IP/Mask field.

- Select *Accept*, *Drop* or *Reject* in the Policy field. Refer to the above table for details.

The system automatically numbers the rule.

6. When finished, the rules are listed.

- You can select any existing rule and then click [↑] or [↓] to change its priority.

IPv4

Enable IPv4 access control ✔

Inbound Rules

Default policy   Accept ▼

#	IP/Mask	Policy	
1	192.168.8.8/32	Drop	
2	192.168.255.33/24	Accept	
3	192.210.15.30/32	Reject	

Append   Insert Above

Outbound Rules

Default policy   Accept ▼

#	IP/Mask	Policy	
1	192.23.89.100/24	Drop	

Append   Insert Above

✔ Save

7. Click Save. The rules are applied.

▶ **To configure IPv6 access control rules:**

1. On the same page, select the 'Enable IPv6 access control' checkbox to enable IPv6 access control rules.

2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting IP Access Control Rules

When an existing IP access control rule requires updates of IP address range and/or policy, modify them accordingly. Or you can delete any unnecessary rules.

▶ **To modify or delete a rule:**

1. Choose Device Settings > Security > IP Access Control.

2. Go to the IPv4 or IPv6 section.

3. Select the desired rule in the list.

   ▪ Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.

4. Perform the desired action.

   ▪ Make changes to the selected rule, and then click Save. For information on each field, see *Creating IP Access Control Rules* (on page 197).

   ▪ Click [🗑] to remove it.

   ▪ To resort its order, click [↑] or [↓].

5. Click Save.

   ▪ IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.

   ▪ IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Creating Role Based Access Control Rules

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

Same as IP access control rules, the order of role-based access control rules is important, since the rules are executed in numerical order.

▶ **To create IPv4 role-based access control rules:**

1. Choose Device Settings > Security > Role Based Access Control.

2. Select the 'Enable role based access control for IPv4' checkbox to enable IPv4 access control rules.

3. Determine the IPv4 default policy.

   ▪ *Accept:* Accepts traffic when no matching rules are present.

   ▪ *Deny:* Rejects any user's login attempt when no matching rules are present.

4. Create rules. Refer to the tables below for different operations.

ADD a rule to the end of the list
▪ Click Append.
▪ Type a starting IP address in the Start IP field.
▪ Type an ending IP address in the End IP field.
▪ Select a role in the Role field. This rule applies to members of this role only.
▪ Select an option in the Policy field.
▪ *Accept:* Accepts traffic from the specified IP address range when the user is a member of the specified role.
▪ *Deny:* Rejects the login attempt of a user from the specified IP address range when that user is a member of the specified role.

INSERT a rule between two rules
▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
▪ Click Insert Above.
▪ Type a starting IP address in the Start IP field.
▪ Type an ending IP address in the End IP field.
▪ Select a role in the Role field. This rule applies to members of this role only.
▪ Select *Accept* or *Deny* in the Policy field. Refer to the above table for details.

The system automatically numbers the rule.

5. When finished, the rules are listed on this page.

- You can select any existing rule and then click ⬆ or ⬇ to change its priority.

IPv4

Enable role based access control for IPv4 ☑

Default policy   Accept ▼

#	Start IP	End IP	Role	Policy	
1	192.168.255.0	192.168.255.255	Operator	Deny	
2	192.168.90.16	192.168.90.55	Admin	Accept	

Append   Insert Above

✔ Save

6. Click Save. The rules are applied.

▶ **To configure IPv6 access control rules:**

1. On the same page, select the 'Enable role based access control for IPv6' checkbox to enable IPv6 access control rules.

2. Follow the same procedure as the above IPv4 rule setup to create IPv6 rules.

3. **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Editing or Deleting Role Based Access Control Rules

You can modify existing rules to update their roles/IP addresses, or delete them when they are no longer needed.

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

1. Choose Device Settings > Security > Role Based Access Control.

2. Go to the IPv4 or IPv6 section.

3. Select the desired rule in the list.

- Ensure the IPv4 or IPv6 checkbox has been selected, or you may not edit or delete any rule.

4. Perform the desired action.

- Make changes to the selected rule, and then click Save. For information on each field, see *Creating Role Based Access Control Rules* (on page 201).

- Click to remove it.

- To resort its order, click or .

5. Click Save.
   - IPv4 rules: **Make sure you click the Save button in the IPv4 section**, or the changes made to IPv4 rules are not saved.
   - IPv6 rules: **Make sure you click the Save button in the IPv6 section**, or the changes made to IPv6 rules are not saved.

Setting Up a TLS Certificate

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

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

Besides, you can create or apply for a multi-domain certificate with subject alternative names.

▶ **To obtain a CA-signed certificate:**

1. Create a Certificate Signing Request (CSR) on the SRC. See *Creating a CSR* (on page 204).
2. Submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with a certificate.
3. Import the CA-signed certificate onto the SRC. See *Installing a CA-Signed Certificate* (on page 205).

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

▶ **A CSR is not required in either scenario below:**

- Make the SRC create a *self-signed* certificate. See *Creating a Self-Signed Certificate* (on page 206).
- Appropriate, valid certificate and key files are already available, and you only need to import them. See *Installing or Downloading Existing Certificate and Key* (on page 207).

Creating a CSR

Follow this procedure to create the CSR for your SRC.

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

required

▶ **To create a CSR:**

1. Choose Device Settings > Security > TLS Certificate.

2. Provide the information requested.

   ▪ **Subject:**

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
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 SRC.
Email address	An email address where you or another administrative user can be reached.

Warning: If you generate a CSR without values entered in the required fields, you cannot obtain third-party certificates.

▪ **Subject Alternative Names:**

If you want a certificate to secure multiple hosts across different domains or subdomains, you can add additional DNS host names or IP addresses of the wanted hosts to this CSR so that a single certificate will be valid for all of them.
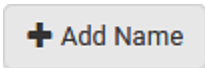
Click ➕ Add Name when there are more than one additional hosts to add.

   ▪ Examples of subject alternative names: *support.raritan.com*, *help.raritan.com*, *help.raritan.net*, and *192.168.77.50*.

▪ **Key Creation Parameters:**

Field	Do this
Key length	Select an available key length (bits). A larger key length enhances the security, but slows down the response of SRC. ▪ Only 2048 is available now.
Self-sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**
Challenge, Confirm challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional. The value should be 4 to 64 characters long. Case sensitive.

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

4. Click Download Certificate Signing Request to download the CSR to your computer.

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

 b. Submit it to a CA to obtain the digital certificate.

 c. If the CSR contains incorrect data, click Delete Certificate Signing Request to remove it, and then repeat the above steps to re-create it.

5. To store the newly-created private key on your computer, click Download Key in the **New TLS Certificate** section.

Note: The Download Key button in the Active TLS Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.

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

6. After getting the CA-signed certificate, install it. See ***Installing a CA-Signed Certificate*** (on page 205).

Installing a CA-Signed Certificate

To get a certificate from a certificate authority (CA), first create a CSR and send it to the CA. See ***Creating a CSR*** (on page 204).

After receiving the CA-signed certificate, install it onto the SRC.

▶ **To install the CA-signed certificate:**

1. Choose Device Settings > Security > TLS Certificate.

2. Click [Browse...] to navigate to the CA-signed certificate file.

3. Click Upload to install it.

4. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

Creating a Self-Signed Certificate

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

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

required

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

1. Choose Device Settings > Security > TLS Certificate.
2. Enter information.

Field	Description
Country	The country where your company is located. Use the standard ISO country code, which comprises two uppercase letters. For a list of ISO codes, google ISO 3166 country codes.
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 SRC.
Email address	An email address where you or another administrative user can be reached.
Key length	Select an available key length (bits). A larger key length enhances the security, but slows down the response of SRC. ▪ Only 2048 is available now.
Self-sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self-sign checkbox is selected. Type the number of days for which the self-signed certificate will be valid.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear.

3. Click Create New TLS Key to create both the self-signed certificate and private key. This may take several minutes to complete.
4. Once complete, do the following:

a. Double check the data shown in the New TLS Certificate section.

b. If correct, click "Install Key and Certificate" to install the self-signed certificate and private key.

Tip: To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

If incorrect, click "Delete Key and Certificate" to remove the self-signed certificate and private key, and then repeat the above steps to re-create them.

5. (Optional) To download the self-signed certificate and/or private key, click Download Certificate or Download Key in the New TLS Certificate section.

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

Note: The Download Key button in the Active TLS Certificate section is for downloading the private key of the currently-installed certificate rather than the newly-created one.

Installing or Downloading Existing Certificate and Key

You can download the already-installed certificate and private key from any SRC for backup or file transfer. For example, you can install the files onto a replacement SRC, add the certificate to your browser and so on.

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

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

▶ **To download active key and certificate files from SRC:**

1. Choose Device Settings > Security > TLS Certificate.

2. In the *Active TLS Certificate* section, click Download Key and Download Certificate respectively.

   Note: The Download Key button in the New TLS Certificate section, if present, is for downloading the newly-created private key rather than the one of the currently-installed certificate.

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

▶ **To install available key and certificate files onto SRC:**

1. Choose Device Settings > Security > TLS Certificate.

2. Select the "Upload key and certificate" checkbox at the bottom of the page.

3. The 'Key File' and 'Certificate file' buttons appear. Click each button to select the key and/or certificate file.

4. Click Upload. The selected files are installed.

5. To verify whether the certificate has been installed successfully, check the data shown in the Active TLS Certificate section.

Setting Up External Authentication

Important: Raritan uses TLS instead of SSL 3.0 due to published security vulnerabilities in SSL 3.0. Make sure your network infrastructure, such as LDAP and mail services, uses TLS rather than SSL 3.0.

For security purposes, users attempting to log in to SRC must be authenticated. SRC supports the following authentication mechanisms:

- Local user database on the SRC
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (Radius) protocol

By default, SRC is configured for local authentication. If you use this method, you only need to create user accounts. See *Creating Users* (on page 148).

If you prefer external authentication, you must provide SRC with information about the external Authentication and Authorization (AA) server.

If both local and external authentication is needed, create user accounts on the SRC in addition to providing the external AA server data.

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

If the external authentication fails, an "Authentication failed" message is displayed. Details regarding the authentication failure are available in the event log. See *Viewing or Clearing the Local Event Log* (on page 308).

Note that only users who have both the "Change Authentication Settings" and "Change Security Settings" permissions can configure or modify the authentication settings.

▶ **To enable external authentication:**

1. Collect external AA server information. See *Gathering LDAP/Radius Information* (on page 209).

2. Enter required data for external AA server(s) on the SRC. See *Adding LDAP/LDAPS Servers* (on page 210) or *Adding Radius Servers* (on page 213).

   ▪ For illustrations, see *LDAP Configuration Illustration* (on page 558) or *RADIUS Configuration Illustration* (on page 574).

3. If both the external and local authentication is needed, or you have to return to the local authentication only, see *Managing External Authentication Settings* (on page 214).

Raritan.
A brand of legrand

▶ **Special note about the AES cipher:**

The SRC device's TLS-based protocols support AES 128- and 256-bit ciphers. The exact cipher to use is negotiated between SRC and the client (such as a web browser), which is impacted by the cipher priority of SRC and the client's cipher availability/settings.

Tip: To force SRC to use a specific AES cipher, refer to your client's user documentation for information on configuring AES settings.

Gathering LDAP/Radius Information

It requires knowledge of your AA server settings to configure the SRC for external authentication. If you are not familiar with these settings, consult your AA server administrator for help.

▶ **Information needed for LDAP authentication:**

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over TLS) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*
    - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

▶ **Information needed for Radius authentication:**

- The IP address or host name of the Radius server
- Authentication protocol used by the Radius server
- Shared secret for a secure communication
- UDP authentication port and accounting port used by the Radius server

Adding LDAP/LDAPS Servers

To use LDAP authentication, enable it and enter the information you have gathered.
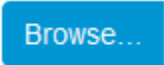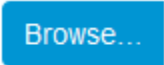
Note that you must enter information in the fields showing the message 'required.'

required

▶ **To add LDAP/LDAPS servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the LDAP Servers section.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your LDAP/LDAPS server. ▪ Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	This checkbox appears only when there are existing AA server settings on the SRC. To duplicate any existing AA server's settings, refer to the duplicating procedure below.
Type of LDAP server	Choose one of the following options: ▪ OpenLDAP ▪ Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.
Security	Determine whether you would like to use Transport Layer Security (TLS) encryption, which allows the SRC to communicate securely with the LDAPS server. Three options are available: ▪ StartTLS ▪ TLS ▪ None
Port (None/StartTLS)	▪ The default Port is 389. Either use the standard LDAP TCP port or specify another port.
Port (TLS)	**Configurable only when "TLS" is selected in the Security field.** The default is 636. Either use the default port or specify another one.

Raritan.
A brand of legrand

Field/setting	Description
Enable verification of LDAP server certificate	Select this checkbox if it is required to validate the LDAP server's certificate by the SRC prior to the connection. If the certificate validation fails, the connection is refused.
CA certificate	Consult your AA server administrator to get the CA certificate file for the LDAPS server. Click **Browse...** to select and install the certificate file. ▪ Click Show to view the installed certificate's content. ▪ Click Remove to delete the installed certificate if it is inappropriate. *Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see **TLS Certificate Chain** (on page 638).*
Allow expired and not yet valid certificates	▪ Select this checkbox to make the authentication succeed regardless of the certificate's validity period. ▪ After deselecting this checkbox, the authentication fails whenever any certificate in the selected certificate chain is outdated or not valid yet.
Anonymous bind	Use this checkbox to enable or disable anonymous bind. ▪ To use anonymous bind, select this checkbox. ▪ When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
Bind DN	**Required after deselecting the Anonymous Bind checkbox.** Distinguished Name (DN) of the user who is permitted to search the LDAP directory in the defined search base.
Bind password, Confirm bind password	**Required after deselecting the Anonymous Bind checkbox.** Enter the Bind password.
Base DN for search	Distinguished Name (DN) of the search base, which is the starting point of the LDAP search. ▪ Example: `ou=dev,dc=example,dc=com`
Login Name Attribute	The attribute of the LDAP user class which denotes the login name. ▪ Usually it is the `uid`.

Field/setting	Description
User entry object class	The object class for user entries. ▪ Usually it is `inetOrgPerson.`
User search subfilter	Search criteria for finding LDAP user objects within the directory tree.
Active Directory domain	The name of the Active Directory Domain. ▪ Example: `testradius.com`

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the SRC can connect to the new server successfully.

Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 214).*

5. Click Add Server. The new LDAP server is listed on the Authentication page.

6. To add more servers, repeat the same steps.

7. **In the Authentication Type field, select LDAP.** Otherwise, the LDAP authentication does not work.

8. Click Save. The LDAP authentication is now in place.

▶ **To duplicate LDAP/LDAPS server settings:**

If you have added any LDAP/LDAPS server to the SRC, and the server you will add shares identical settings with an existing one, the most convenient way is to duplicate that LDAP/LDAPS server's data and then revise the IP address/host name.

1. Repeat Steps 1 to 2 in the above procedure.

2. Select the "Copy settings from existing LDAP server" checkbox.

3. Click the "Select LDAP Server" field to select the LDAP/LDAPS server whose settings you want to copy.

4. Modify the IP Address/Hostname field.

5. Click Add Server.

Note: If the SRC 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 SRC and the LDAP server to use the same NTP server(s).

Adding Radius Servers

To use Radius authentication, enable it and enter the information you have gathered.

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

required

▶ **To add Radius servers:**

1. Choose Device Settings > Security > Authentication.
2. Click New in the Radius Servers section.
3. Enter information.

Field/setting	Description
IP address / hostname	The IP address or hostname of your Radius server.
Type of RADIUS authentication	Select an authentication protocol. ▪ PAP (Password Authentication Protocol) ▪ CHAP (Challenge Handshake Authentication Protocol) ▪ MS-CHAPv2 (Microsoft 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. MS-CHAPv2 provides stronger security than the above two. Selecting this option will support both MS-CHAPv1 and MS-CHAPv2.
Authentication port, Accounting port	The defaults are standard ports -- 1812 and 1813. To use non-standard ports, type a new port number.
Timeout	This sets the maximum amount of time to establish contact with the Radius server before timing out. Type the timeout period in seconds.
Retries	Type the number of retries.
Shared secret, Confirm shared secret	The shared secret is necessary to protect communication with the Radius server.

4. To verify if the authentication configuration is set correctly, click Test Connection to check whether the SRC can connect to the new server successfully.

Tip: You can also test the connection on the Authentication page after finishing adding servers. See **Managing External Authentication Settings** *(on page 214).*

5. Click Add Server. The new Radius server is listed on the Authentication page.

6. To add more servers, repeat the same steps.

7. **In the Authentication Type field, select Radius.** Otherwise, the Radius authentication does not work.

8. Click Save. Radius authentication is now in place.

Managing External Authentication Settings

Choose Device Settings > Security > Authentication to open the Authentication page, where you can:

- Enable both the external and local authentication
- Edit or delete a server
- Resort the access order of servers
- Test the connection to a server
- Disable external authentication without removing servers

▶ **To test, edit or delete a server, or resort the server list:**

1. Select a server in the list.

Access Order	IP Address / Hostname	Security	Port	LDAP Server Type
1	192.168.91.100	None	389	OpenLDAP
2	192.168.1.33	StartTLS	389	OpenLDAP
3	192.168.8.95	None	389	Microsoft Active Directory

2. Perform the desired action.

- Click Edit to edit its settings, and click Modify Server to save changes. For information on each field, see **Adding LDAP/LDAPS Servers** (on page 210) or **Adding Radius Servers** (on page 213).

- Click Delete to delete the server, and then confirm the operation.

- Click Test Connection to verify the connection to the selected server. User credentials may be required.

- Click [⌃] or [⌄] to change the server order, which determines the access priority, and click Save Order to save the new sequence.

Note: Whenever SRC is successfully connected to one external authentication server, it STOPS trying access to remaining servers in the authentication list regardless of the user authentication result.

► **To enable both external and local authentication:**

1. In the 'Authentication type' field, select the external authentication you want -- LDAP or RADIUS.

2. Select the following checkbox. Then the SRC always tries external authentication first. Whenever the external authentication fails, the SRC switches to local authentication.

☑ Use local authentication if remote authentication is not available

3. Click Save.

► **To disable external authentication:**

1. In the 'Authentication type' field, select Local.

2. Click Save.

Configuring Login Settings

Choose Device Settings > Security > Login Settings to open the Login Settings page, where you can:

- Configure the user blocking feature.

  Note: The user blocking function applies only to local authentication instead of external authentication through AA servers.

- Determine the timeout period for any inactive user.

- Prevent simultaneous logins using the same login name.

► **To configure user blocking:**

1. To enable the user blocking feature, select the 'Block user on login failure' checkbox.

2. In the 'Block timeout' field, type a value or click ▼ to select a time option. This setting determines how long the user is blocked.

   ▪ If you type a value, the value must be followed by a time unit, such as '4 min.' See **Time Units** (on page 216).

3. In the 'Maximum number of failed logins' field, type a number. This is the maximum number of login failure the user is permitted before the user is blocked from accessing the SRC.

4. Click Save.

Tip: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command over a local connection. See **Unblocking a User** *(on page 493).*

▶ **To set limitations for login timeout and use of identical login names:**

1. In the "Idle timeout period" field, type a value or click ▼ to select a time option. This setting determines how long users are permitted to stay idle before being forced to log out.

   - If you type a value, the value must be followed by a time unit, such as '4 min.' See **Time Units** (on page 216).

   - 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 SRC.

2. Select the 'Prevent concurrent login with same username' checkbox if intending to prevent multiple persons from using the same login name simultaneously.

3. Click Save.

Time Units

If you choose to type a new value in the time-related fields, such as the "Idle timeout period" field, you must add a time unit after the numeric value. For example, you can type '15 min' for 15 minutes.

Note that different fields have different range of valid values.

▶ **Time units:**

Unit	Time
min	minute(s)
h	hour(s)
d	day(s)

Configuring Password Policy

Choose Device Settings > Security > Password Policy to open the Password Policy page, where you can:

- Force users to use strong passwords.
- Force users to change passwords at a regular interval -- that is, password aging.

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the SRC.

▶ **To configure password aging:**

1. Select the 'Enabled' checkbox of Password Aging.

2. In the 'Password aging interval' field, type a value or click [▼] to select a time option. This setting determines how often users are requested to change their passwords.

    - If you type a value, the value must be followed by a time unit, such as '10 d.' See *Time Units* (on page 216).

3. Click Save.

▶ **To force users to create strong passwords:**

1. Select the 'Enabled' checkbox of Strong Passwords to activate the strong password feature. The following are the default settings:

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

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

2. Make changes to the default settings as needed.

3. Click Save.

Enabling the Restricted Service Agreement

The restricted service agreement feature, if enabled, forces users to read a security agreement when they log in to the SRC.

Users must accept the agreement, or they cannot log in.

An event notifying you if a user has accepted or declined the agreement can be generated. See *Default Log Messages* (on page 230)

▶ **To enable the service agreement:**

1. Click Device Settings > Security > Service Agreement.

2. Select the 'Enforce restricted service agreement' checkbox.

3. Edit or paste the content as needed.

    ▪ A maximum of 10,000 characters can be entered.

4. Click Save.

▶ **Login manner after enabling the service agreement:**

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen.

Do either of the following, or the login fails:

● In the web interface, select the checkbox labeled "I understand and accept the restricted service agreement."

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

● In the CLI, type y when the confirmation message "I understand and accept the restricted service agreement" is displayed.

Setting the Date and Time

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

Note: If you are using Sunbird's Power IQ to manage the SRC, you must configure Power IQ and the SRC to have the same date/time or NTP settings.

▶ **To set the date and time:**

1. Choose Device Settings > Date/Time.

2. Click the 'Time zone' field to select your time zone from the list.

3. If the daylight saving time applies to your time zone, verify the 'Automatic daylight saving time adjustment' checkbox is selected.

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

4. Select the method for setting the date and time.

Customize the date and time

▪ Select 'User specified time'.

▪ Type values in the Date field using the yyyy-mm-dd format, or click [calendar icon] to select a date. For details, see **Calendar** (on page 222).

▪ Determine the time format you want by clicking 12H or 24H button.

   ▪ **12H** represents the 12-hour format.

   ▪ **24H** represents the 24-hour format.

▪ If selecting 12-hour format, then determine the current period by clicking the AM or PM button.

▪ Type values in the Time field using the hh:mm:ss format, or click [up arrow] [down arrow] to adjust values.

   ▪ When 12H is being applied, the hour cannot exceed the maximum number 12. If exceeding 12, the time change cannot be saved.

Use the NTP server

▪ Select "Synchronize with NTP server."
 	
 ▪ There are two ways to assign the NTP servers:
 	
    ▪ To use the DHCP-assigned NTP servers, DO NOT enter any NTP servers for the First and Second time server.
 	
      DHCP-assigned NTP servers are available only when either IPv4 or IPv6 DHCP is enabled.
 	
    ▪ To use the manually-specified NTP servers, specify the primary NTP server in the "First time server" field. A secondary NTP server is optional.
 	
      Click Check NTP Servers to verify the validity and accessibility of the manually-specified NTP servers.

5.   Click Save.

SRC follows the NTP server sanity check per the IETF RFC. If your SRC has problems synchronizing with a Windows NTP server, see **Windows NTP Server Synchronization Solution** (on page 223).

Calendar

The calendar icon [calendar icon] in the Date field is a convenient tool to select a custom date. Click it and a calendar similar to the following appears.
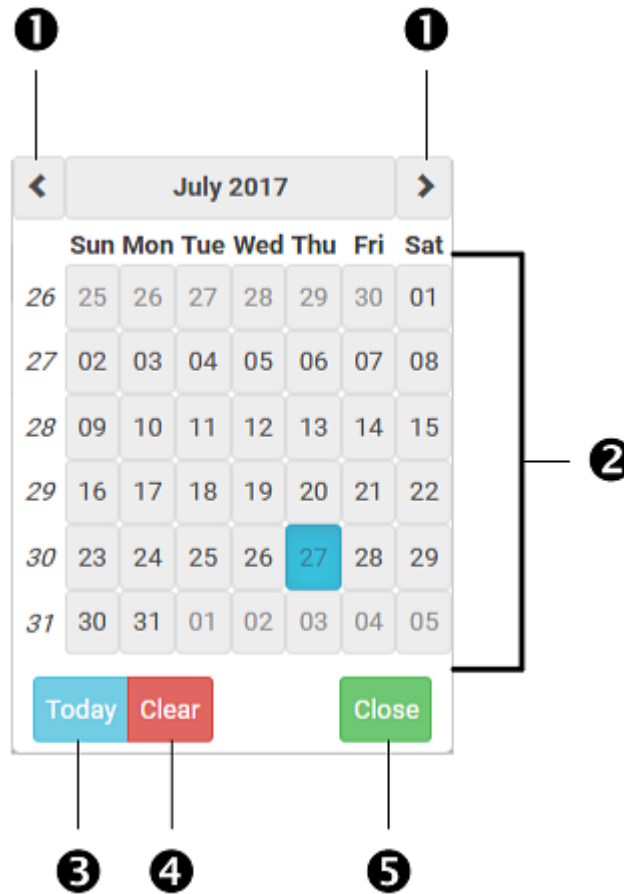
Number	Item	Description
1	arrows	Switch between months.
2	dates (01-31)	All dates of the selected month. To select a date, simply click it.
3	Today	Select today's date.
4	Clear	Clear the entry, if any, in the Date field.
5	Close	Close the calendar.

Windows NTP Server Synchronization Solution

The NTP client on the SRC follows the NTP RFC so the SRC 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 SRC.

Note: For information on NTP RFC, visit **http://tools.ietf.org/html/rfc4330 - http://tools.ietf.org/html/rfc4330** *to refer to section 5.*

Windows NTP servers may have a root dispersion of more than one second, and therefore cannot synchronize with the SRC. When the NTP synchronization issue occurs, change the dispersion settings to resolve it.

▶ **To change the Windows NTP's root dispersion settings:**

1. Access the registry settings associated with the root dispersion on the Windows NTP server.

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

2. *AnnounceFlags* must be set to 0x05 or 0x06.
   - 0x05 = 0x01 (Always time server) and 0x04 (Always reliable time server)
   - 0x06 = 0x02 (Automatic time server) and 0x04 (Always reliable time server)

   Note: Do NOT use 0x08 (Automatic reliable time server) because its dispersion starts at a high value and then gradually decreases to one second or lower.

3. *LocalClockDispersion* must be set to 0.

Event Rules and Actions

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

An event rule consists of two parts:

● Event: This is the situation where the SRC or a device connected to it meets a certain condition. For example, the inlet's voltage reaches the warning level.

● Action: This is the response to the event. For example, the SRC notifies the system administrator of the event via email.

If you want the SRC to perform one action at a regular interval instead of waiting until an event occurs, you can schedule that action. For example, you can make the SRC email the temperature report every hour.

Note that you need the Administrator Privileges to configure event rules.

▶ **To create an event rule:**

1. Choose Device Settings > Event Rules.

2. If the needed action is not available yet, create it by clicking **✚ New Action**.

    a. Assign a name to this action.

    b. Select the desired action and configure it as needed.

    c. Click Create.

    For details, see **Available Actions** (on page 238).

3. Click **✚ New Rule** to create a new rule.

    a. Assign a name to this rule.

    b. Make sure the Enabled checkbox is selected, or the new event rule does not work.

    c. In the Event field, select the event to which you want the SRC to react.

    d. In the 'Available actions' field, select the desired action(s) to respond to the selected event.

    e. Click Create.

    For details, see **Built-in Rules and Rule Configuration** (on page 225).

▶ **To create a scheduled action:**

1. If the needed action is not available yet, create it by clicking **✚ New Action**. See above.

    Note: When creating scheduled actions, available actions are less than usual because it is meaningless to schedule certain actions like "Alarm," "Log event message," "Send email," "Syslog message" and the like.

2. Click **✚ New Scheduled Action** to schedule the desired action.

a.   Assign a name to this scheduled action.

b.   Make sure the Enabled checkbox is selected, or the SRC does not perform this scheduled action.

c.   Set the interval time, which ranges from every minute to yearly.

d.   In the 'Available actions' field, select the desired action(s).

e.   Click Create.

For details, see **Scheduling an Action** (on page 257).

Built-in Rules and Rule Configuration

SRC is shipped with four built-in event rules, which cannot be deleted. If the built-in event rules do not satisfy your needs, create new rules.

▶   **Built-in rules:**

- *System Event Log Rule:*

  This causes ANY event occurred to the SRC to be recorded in the internal log. It is enabled by default.

  Note: For the default log messages generated for each event, see **Default Log Messages** *(on page 230).*

- *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 SRC. It is disabled by default.

- *System Tamper Detection Alarmed:*

  This causes the SRC to send alarm notifications if a DX tamper sensor has been connected and the SRC detects that the tamper sensor enters the alarmed state. It is enabled by default.
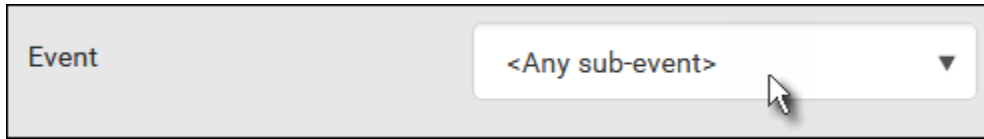
- *System Tamper Detection Unavailable:*

  This causes the SRC to send alarm notifications if a DX tamper sensor was once connected or remains connected but then the SRC does not detect the presence of the tamper sensor. It is enabled by default.

▶   **Event rule configuration illustration:**
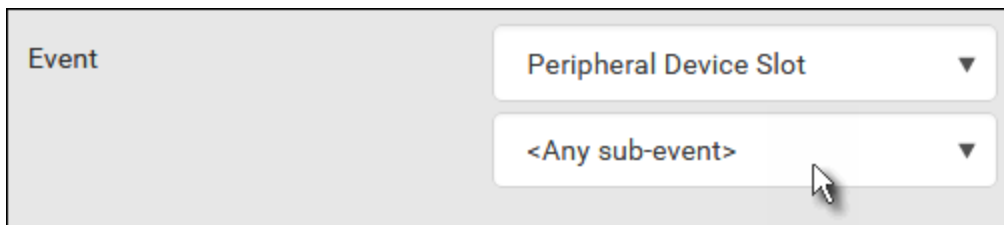
1.   Choose Device Settings > Event Rules > .

2.   Click the Event field to select an event type.

- <Any sub-event> means all events shown on the list.

- <Any Numeric Sensor> means all numeric sensors of the SRC, including internal and environmental sensors. <Any Numeric Sensor> is especially useful if you want to receive the notifications when any numeric sensor's readings pass through a specific threshold.
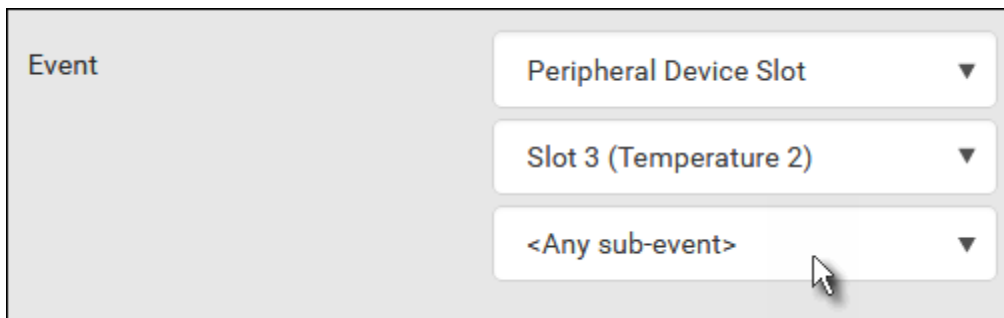
Event	<Any sub-event> ▼

3. In this example, the Peripheral Device Slot is selected, which is related to the environmental sensor packages. Then a sensor ID field for this event type appears. Click this additional field to specify which sensor should be the subject of this event.

Event	Peripheral Device Slot ▼
	<Any sub-event> ▼

4. In this example, sensor ID 3 (Slot 3) is selected, which is a temperature sensor. Then a new field for this sensor appears. Click this field to specify the type of event(s) you want.

Event	Peripheral Device Slot ▼
	Slot 3 (Temperature 2) ▼
	<Any sub-event> ▼

5. In this example, Numeric Sensor is selected because we want to select numeric-sensor-related event(s). Then a field for numeric-sensor-related events appears. Click this field to select one of the numeric-sensor-related events from the list.

Event	Peripheral Device Slot ▼
	Slot 3 (Temperature 2) ▼
	Numeric Sensor ▼
	<Any sub-event> ▼

6. In this example, 'Above upper critical threshold' is selected because we want the SRC to react only when the selected temperature sensor's reading enters the upper critical range. A "Trigger condition" field appears, requiring you to define the "exact" condition related to the "upper critical" event.

Event	Peripheral Device Slot ▼
	Slot 3 (Temperature 2) ▼
	Numeric Sensor ▼
	Above upper critical threshold ▼
Trigger condition	○ Asserted
	○ Deasserted
	● Both

7. Select the desired radio button to finish the event configuration. Refer to the following table for different types of radio buttons.

- If needed, you may refer to event rule examples in the section titled *Sample Event Rules* (on page 270).

8. To select any action(s), select them one by one from the 'Available actions' list.

- To select all available actions, click Select All.

9. To remove any action(s) from the 'Selected actions' field, click that action's
    ![x icon].

    ▪ To remove all actions, click Deselect All.

▶ **Radio buttons for different events:**

According to the event you select, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: SRC takes the action only when the selected event occurs. That is, the status of the event transits from FALSE to TRUE. ▪ Deasserted: SRC takes the action only when the selected event disappears or stops. That is, the status of the selected event transits from TRUE to FALSE. ▪ Both: SRC takes the action both when the event occurs (asserts) and when the event stops/disappears (deasserts).
State sensor state change	Available radio buttons include "Alarmed/Open/On," "No longer alarmed/Closed/Off" and "Both." ▪ Alarmed/Open/On: SRC takes the action only when the chosen sensor enters the alarmed, open or on state. ▪ No longer alarmed/Closed/Off: SRC takes the action only when the chosen sensor returns to the normal, closed, or off state. ▪ Both: SRC takes the action whenever the chosen sensor switches its state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: SRC takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: SRC takes the action only when the chosen sensor is detected and becomes available. ▪ Both: SRC takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	▪ Link state is up: SRC takes the action only when the network link state changes from down to up. ▪ Link state is down: SRC takes the action only when the network link state changes from up to down. ▪ Both: SRC takes the action whenever the network link state changes.
Function enabled or disabled	▪ Enabled: SRC takes the action only when the chosen function is enabled. ▪ Disabled: SRC takes the action only when the chosen function is disabled. ▪ Both: SRC takes the action when the chosen function is either enabled or disabled.
Restricted service agreement	▪ Accepted: SRC takes the action only when the specified user accepts the restricted service agreement. ▪ Declined: SRC takes the action only when the specified user rejects the restricted service agreement. ▪ Both: SRC takes the action both when the specified user accepts or rejects the restricted service agreement.
Server monitoring event	▪ Monitoring started: SRC takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: SRC takes the action only when the monitoring of any specified server stops. ▪ Both: SRC takes the action when the monitoring of any specified server starts or stops.
Server reachability	▪ Unreachable: SRC takes the action only when any specified server becomes inaccessible. ▪ Reachable: SRC takes the action only when any specified server becomes accessible. ▪ Both: SRC takes the action when any specified server becomes either inaccessible or accessible.

Event types	Radio buttons
Device connection or disconnection, such as a USB-cascaded slave device	▪ Connected: SRC takes the action only when the selected device is physically connected to it. ▪ Disconnected: SRC takes the action only when the selected device is physically disconnected from it. ▪ Both: SRC takes the action both when the selected device is physically connected to it and when it is disconnected.
+12V Supply Status	Available radio buttons include "Fault," "OK" and "Both." ▪ Fault: SRC takes the action only when the selected 12V power supply to the controller enters the fault state. ▪ OK: SRC takes the action only when when the selected 12V power supply to the controller enters the OK state. ▪ Both: SRC takes the action whenever the selected 12 power supply's status changes.

Default Log Messages

These default log messages are recorded internally and emailed to specified recipients when SRC events occur (are TRUE) or, in some cases, stop or become unavailable (are FALSE). See **Send Email** (on page 246) to configure email messages.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Asset Management > State	State of asset strip [AMSNUMBER] ('[AMSNAME]') changed to '[AMSSTATE]'.	
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[AMSTAGID]' connected at rack unit [AMSRACKUNITPOSITION], slot [AMSBLADESLOTPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	Asset tag with ID '[AMSTAGID]' disconnected at rack unit [AMSRACKUNITPOSITION], slot [AMSBLADESLOTPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[AMSTAGID]' connected at rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').	Blade extension with ID '[AMSTAGID]' disconnected at rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]').

Raritan.
A brand of ▢legrand®

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Asset Management > Firmware Update	Firmware update for asset strip [AMSNUMBER] ('[AMSNAME]'): status changed to '[AMSSTATE]'.	
Asset Management > Device Config Changed	Config parameter '[CONFIGPARAM]' of asset strip [AMSNUMBER] ('[AMSNAME]') changed to '[CONFIGVALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [AMSRACKUNITPOSITION] of asset strip [AMSNUMBER] ('[AMSNAME]') changed by user '[USERNAME]' to: Name '[AMSRACKUNITNAME]', LED Operation Mode '[AMSLEDOPMODE]', LED Color '[AMSLEDCOLOR]', LED Mode '[AMSLEDMODE]	
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [AMSNUMBER] ('[AMSNAME]').	Blade extension overflow cleared for strip [AMSNUMBER] ('[AMSNAME]').
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [AMSNUMBER] ('[AMSNAME]').	
Card Reader Management > Card Reader > * > Card inserted	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' inserted at Card Reader '[CARDREADERID]'.	
Card Reader Management > Card Reader > * > Card removed	Card of type '[SMARTCARDTYPE]' with ID '[SMARTCARDID]' removed at Card Reader '[CARDREADERID]'.	
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.	
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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 > Hardware failure present	Failure '[FAILURETYPESTR]' asserted for component '[COMPONENTID]'.	Failure '[FAILURETYPESTR]' deasserted for component '[COMPONENTID]'.
Device > Device identification changed	Config parameter '[CONFIGPARAM]' changed to '[CONFIGVALUE]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device settings saved	Device settings saved by user '[USERNAME]' 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 by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied by user '[USERNAME]' 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 '[SMTPRECIPIENTS]' using server '[SMTPSERVER]' failed. [ERRORDESC].	
Device > Sending SNMP inform failed or no response	Sending SNMP inform to manager [SNMPMANAGER]:[SNMPMANAGERPORT] failed or no response. [ERRORDESC].	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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: [ERRORDESC].	
Device > A Radius error occurred	A Radius error occurred: [ERRORDESC].	
Device > Raw configuration downloaded	Raw configuration downloaded by user '[USERNAME]' from host '[USERIP]'.	
Device > Raw configuration updated	Raw configuration updated by user '[USERNAME]' from host '[USERIP]'.	
Device > Unknown peripheral device attached	An unknown peripheral device with rom code '[ROMCODE]' was attached at position '[PERIPHDEVPOSITION]'.	
Device > Slave connected	Slave connected.	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 threshold	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] asserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].
Peripheral Device Slot > * > Numeric Sensor > Above upper warning threshold	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
Peripheral Device Slot > * > Numeric Sensor > Below lower warning threshold	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
Peripheral Device Slot > * > Numeric Sensor > Below lower critical threshold	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
Peripheral Device Slot > * > State Sensor/Actuator > Unavailable	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	Peripheral device '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
Peripheral Device Slot > * > State Sensor/Actuator > Alarmed/Open/On	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] is [SENSORSTATENAME].
Peripheral Device Slot > * > State Sensor/Actuator > Switched by user	Peripheral device '[EXTSENSORNAME]' in slot [EXTSENSORSLOT] has been switched to [SENSORSTATENAME] by user '[USERNAME]' from host.	
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.	
Pdu > Sensor > +12V Supply Status > Fault	Global sensor '[PDUSENSOR]' entered fault state.	Pdu > Sensor > +12V Supply Status > Fault
Pdu > Sensor > +12V Supply Status > Unavailable	Global sensor 'powerSupplyStatus' unavailable.	Global sensor 'powerSupplyStatus' available.
Server Monitoring > * > Error	Error monitoring server '[MONITOREDHOST]': [ERRORDESC]	
Server Monitoring > * > Monitored	Server '[MONITOREDHOST]' is now being monitored.	Server '[MONITOREDHOST]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[MONITOREDHOST]' is unreachable.	Server '[MONITOREDHOST]' is reachable.

Raritan.
A brand of legrand

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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 '[UMTARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[UMTARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[UMTARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[UMTARGETUSER]' 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 '[UMTARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[UMTARGETROLE]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role deleted	Role '[UMTARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
Webcam Management > Image upload started	A snapshot upload of webcam '[WEBCAMNAME]' to folder '[PATH]' was started.	
Webcam Management > Webcam attached	Webcam '[WEBCAMNAME]' ('[WEBCAMUVCID]') added to port '[WEBCAMUSBPORT]'.	

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical' at [SENSORREADING] [SENSORREADINGUNIT].
LHX/SHX > Sensor > Above upper warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning' at [SENSORREADING] [SENSORREADINGUNIT].
LHX/SHX > Sensor > Below lower warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning' at [SENSORREADING] [SENSORREADINGUNIT].
LHX/SHX > Sensor > Below lower critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical' at [SENSORREADING] [SENSORREADINGUNIT].
LHX/SHX > Base Electronics Failure	The base electronics on LHX at [PORTTYPE] port '[PORTID]' failed.	The base electronics on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
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.

Raritan.
A brand of legrand

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
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.

Event/context	Default message when the event = TRUE	Default message when the event = FALSE
LHX/SHX > Voltage Low	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is low.	The supply voltage on LHX at [PORTTYPE] port '[PORTID]' is back to normal.
LHX/SHX > Threshold Humidity	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX/SHX > External Water Cooling Failure	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX/SHX > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'.	

The asterisk symbol (*) represents anything you select for the 'trigger' events.

Available Actions

The SRC comes with three built-in actions, which cannot be deleted. You can create additional actions for responding to different events.

▶ **To test an action:**

- Click the Test button next to the Action. The action is triggered and you can verify it.

▶ **Built-in actions:**

- *System Event Log Action:*

  This action records the selected event in the internal log when the event occurs.

- *System SNMP Notification Action:*

  This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

  *Note: No IP addresses are specified for this notification action by default so you must enter IP addresses before applying this action to any event rule. See **Editing or Deleting a Rule/Action** (on page 269). Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Configuring SNMP Settings** (on page 188).*

• *System Tamper Alarm:*

This action causes the SRC to show the alarm for the Raritan tamper sensor, if any, on the Dashboard page until a person acknowledges it. By default, this action has been assigned to the built-in tamper detection event rules. For information on acknowledging an alarm, see **Dashboard - Alarms** (on page 104).

▶ **Actions you can create:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Click the Action field to select an action type from the list.

Action	-- Select an action type ▼

3. Below is the list of available actions.

Action	Function
Alarm	Requires the user to acknowledge the alert after it is generated. If needed, you can have the alert notifications regularly generated until a person takes the acknowledgment action. See **Alarm** (on page 241).
Execute an action group	Creates a group of actions comprising existing actions. See **Action Group** (on page 242).
External beeper	Enables or disables the connected external beeper, or causes it to enter an alarm cycle. See **External Beeper** (on page 242).
Internal beeper	Turns on or off the internal beeper. See **Internal Beeper** (on page 243).
Log event message	Records the selected events in the internal log. See **Log an Event Message** (on page 243).
Push out sensor readings	Sends internal sensor log, environmental sensor log or asset management strip data to a remote server using HTTP POST requests. See **Push Out Sensor Readings** (on page 243).
Record snapshots to webcam storage	Makes a connected webcam start or stop taking snapshots. See **Record Snapshots to Webcam Storage** (on page 244).

Action	Function
Request LHX/SHX maximum cooling	Applies the maximum cooling to the LHX/SHX device. See **Request LHX/SHX Maximum Cooling** (on page 246). This option is available only when the Schroff LHX/SHX support has been enabled.
Send email	Emails a textual message. See **Send Email** (on page 246).
Send sensor report	Reports the readings or status of the selected sensors, including internal or external sensors. See **Send Sensor Report** (on page 248).
Send SMS message	Sends a message to a mobile phone. See **Send SMS Message** (on page 250).
Send snapshots via email	Emails the snapshots captured by a connected Logitech® webcam (if available). See **Send Snapshots via Email** (on page 251).
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See **Send an SNMP Notification** (on page 253).
Start/stop Lua script	If you are a developer who can create a Lua script, you can upload it to the SRC, and have the SRC automatically perform or stop the script in response to an event. See **Start or Stop a Lua Script** (on page 254).
Switch LHX/SHX	Switches on or off the LHX/SHX device. See **Switch LHX/SHX** (on page 255). This option is available only when the Schroff LHX/SHX support has been enabled.
Switch peripheral actuator	Switches on or off the mechanism or system connected to the specified actuator. See **Switch Peripheral Actuator** (on page 255).
Syslog message	Makes the SRC automatically forward event messages to the specified syslog server. See **Syslog Message** (on page 256).

4. Enter the information as needed and click Create.

5. Then you can assign the newly-created action to an event rule or schedule it. See **Event Rules and Actions** (on page 224).

Raritan.
A brand of ☐legrand®

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 SRC resends or regenerates an alert notification regularly until the alert is acknowledged or the maximum number of alert notifications is sent.

For information on acknowledging an alert, see **Dashboard** (on page 102).

▶ **Operation:**

1. Choose Device Settings > Event Rules > New Action.
2. Select Alarm from the Action list.
3. In the Alarm Notifications list box, specify one or multiple ways to issue the alert notifications. Available methods vary, depending on how many notification-based actions have been created. Notification-based action types include:

   ▪ External beeper

   ▪ Syslog message

   ▪ Send email

   ▪ Send SMS message

   ▪ Internal beeper

   If no appropriate actions are available, create them first.

   a. To select any methods, select them one by one in the Available field.

   To add all available methods, simply click Select All.

   b. To delete any methods, click a method's ✖ in the Selected field.

   To remove all methods, simply click Deselect All.

4. To enable the notification-resending feature, select the 'Enable re-scheduling of alarm notifications' checkbox.
5. In the 'Re-scheduling period' field, specify the time interval (in minutes) at which the alert notification is resent or regenerated regularly.
6. In the 'Re-scheduling limit' field, specify the maximum number of times the alert notification is resent. Values range from 1 to infinite.
7. **(Optional)** You can instruct the SRC to send the acknowledgment notification after the alarm is acknowledged in the 'Acknowledgment notifications' field. Available methods are identical to those for generating alarm notifications.

   a. In the Available field, select desired methods one by one, or click Select All. See step 3 for details.

   b. In the Selected field, click any method's ✖ to remove unnecessary ones, or click Deselect All.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to any event rule rather than selecting all needed actions one by one per rule.

If the needed action is not available yet, create it first. See **Available Actions** (on page 238).

▶ **Operation:**

1. Choose Device Settings > Event Rules > **➕ New Action**.
2. Select 'Execute an action group' from the Action list.
3. To select any action(s), select them one by one from the 'Available actions' list.
   - To select all available actions, click Select All.
4. To remove any action(s) from the 'Selected actions' field, click that action's **✖**.
   - To remove all actions, click Deselect All.

External Beeper

If an external beeper is connected to the SRC, the SRC can change the beeper's behavior or status to respond to a certain event.

▶ **To control the connected external beeper:**

1. Choose Device Settings > Event Rules > **➕ New Action**.
2. Select 'External beeper' from the Action list.
3. In the 'Beeper port' field, select the port where the external beeper is connected. This port is the FEATURE port.
4. In the 'Beeper action' field, select an action for the external beeper to carry out.
   - Alarm: Causes the external beeper to sound an alarm cycle every 20 seconds - stays on for 0.7 seconds and then off for 19.3 seconds.
   - On: Turns on the external beeper so that it buzzes continuously.
   - Off: Turns off the external beeper so that it stops buzzing.

Warning: If you create an event rule for the external beeper but disconnect it when an event causes it to beep, the beeper no longer beeps after it is re-connected even though the event triggering the beeping action remains asserted.

Internal Beeper

You can have the built-in beeper of the SRC turned on or off when a certain event occurs.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action].
2. Select 'Internal beeper' from the Action list.
3. Select an option from the Operation field.
   - Turn beeper on: Turns on the internal beeper to make it buzz.
   - Turn beeper off: Turns off the internal beeper to make it stop buzzing.

Log an Event Message

The option 'Log event message' records the selected events in the internal log.

The default log message generated for each type of event is available in the section titled **Default Log Messages** (on page 230).

Push Out Sensor Readings

You can configure the SRC to push sensor log to a remote server after a certain event occurs, including logs of internal sensors, environmental sensors and actuators.

If you have connected Raritan's asset strips to the SRC, you can also configure the SRC to push the data to a server.

Before creating this action, make sure that you have properly defined the destination servers and the data to be sent on the Data Push page. See **Configuring Data Push Settings** (on page 278).

*Tip: To send the data at a regular interval, schedule this action. See **Scheduling an Action** (on page 257). Note that the "Asset management log" is generated only when there are changes made to any asset strips or asset tags, such as connection or disconnection events.*

▶ **Operation:**

1. Choose Device Settings > Event Rules > ![New Action].
2. Select 'Push out sensor readings' from the Action list.
3. Select a server or host which receives the data in the Destination field.
   - If the desired destination is not available yet, go to the Data Push page to specify it.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

Per default the snapshots are stored on the SRC. See *Viewing and Managing Locally-Saved Snapshots* (on page 331).

It is recommended to specify a remote server to store as many snapshots as possible. See *Changing Storage Settings* (on page 333).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action .

2. Select 'Record snapshots to webcam storage' from the Action list.

3. Select a webcam in the Webcam field.

4. Select the action to perform - 'Start recording' or 'Stop recording.'

   If 'Start recording' is selected, adjust the values of the following:

   ▪ Number of snapshots - the number of snapshots to be taken when the event occurs.

     The maximum amount of snapshots that can be stored on the SRC is 10. If you set it for a number greater than 10 and the storage location is on the SRC, after the 10th snapshot is taken and stored, the oldest snapshots are overwritten. Storing snapshots on a remote server does not have such a limitation.

   ▪ Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.

   ▪ Time between snapshots - the amount of time in seconds between when each snapshot is taken.

   ▪ Folder - names of the folders that will be automatically created to store webcam snapshots after the recording action is triggered by the rule you will configure.

     Note that the Folder field is available only when the selected webcam has been configured to store its snapshots on an "FTP" server. See *Changing Storage Settings* (on page 333).

Folder name options	Definition
Serial number / Webcam name	Two folders will be created. ▪ The parent folder's name is the serial number of SRC. ▪ The subfolder's name is the selected webcam's name.
Serial number / Webcam name / Rule name	Three folders will be created. ▪ Definitions of the parent folder and first subfolder are the same as the first row. ▪ The final subfolder's name is the name of event rule that triggers this recording action.

Folder name options	Definition
Serial number / Webcam name / Timestamp	Three folders will be created. ■ Definitions of the parent folder and first subfolder are the same as the first row. ■ The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.
Serial number / Webcam name / Rule name / Timestamp	Four folders will be created. ■ Definitions of the parent folder and first subfolder are the same as the first row. ■ The second subfolder's name is the name of event rule that triggers this recording action. ■ The final subfolder's name is the time when the recording event occurs, which is the accumulated time in seconds since 1970/1/1.
Serial number / Webcam name / Formatted timestamp	Three folders will be created. ■ Definitions of the parent folder and first subfolder are the same as the first row. ■ The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.
Serial number / Webcam name / Rule name / Formatted timestamp	Four folders will be created. ■ Definitions of the parent folder and first subfolder are the same as the first row. ■ The second subfolder's name is the name of event rule that triggers this recording action. ■ The final subfolder's name is the time when the recording event occurs, which is a format comprising year, month, date, hour, minute, second and timezone.

No matter which timestamp you choose, the timestamp is based on the time you have configured on the SRC. See *Setting the Date and Time* (on page 220).

To find the serial number of your SRC, see *Device Information* (on page 301). To change the webcam's name, see *Configuring Webcams and Viewing Live Images* (on page 326).

Tip: If you choose "Timestamp" as the final subfolder's name and do not understand the occurrence time indicated by the timestamp, you can always easily convert it to a readable formatted time by googling Unix timestamp converter.
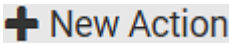
Request LHX/SHX Maximum Cooling

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See **Miscellaneous** (on page 297).

The 'Request LHX/SHX maximum cooling' action applies the maximum cooling to the SHX-30 device only. The LHX-20 and LHX-40 devices do not support this feature.

In the maximum cooling mode, an SHX-30 device runs at 100% fan speed and the cold water valve is open 100%.

▶ **Operation:**

1. Choose Device Settings > Event Rules > New Action.

2. Select 'Request LHX/SHX maximum cooling' from the Action list.

3. In the Available LHX/SHX field, select the desired SHX-30 device one by one, or click Select All.

4. To remove any SHX-30 device from the Selected LHX/SHX field, click that device's ✖ or click Deselect All.

Send Email

You can configure emails to be sent when an event occurs and can customize the message.

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

For example:

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

translates to

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

For a list and definition of available variables, see **Placeholders for Custom Messages** (on page 266).

▶ **Operation:**

1. Choose Device Settings > Event Rules > New Action.

2. Select 'Send email' from the Action list.

3. In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.

4. By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action.

To use a different SMTP server, select the 'Use custom settings' radio button. The fields for customized SMTP settings appear. For information on each field, see **Configuring SMTP Settings** (on page 190).

Default messages are sent based on the event. For a list of default log messages and events that trigger them, see **Default Log Messages** (on page 230).

5. If needed, you can customize the subject and messages sent via this email.

- Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.

- Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.

 When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just scroll down to select the desired placeholder. For details, see **Placeholders for Custom Messages** (on page 266).

- To start a new line in the text box, press Enter.

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Send Sensor Report

You may set the SRC 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 listed below.

- Peripheral device sensors, which can be any Raritan environmental sensor packages connected to the SRC, such as temperature or humidity sensors.
- SRC's +12V Supply sensor

An example of this action is available in the section titled **Send Sensor Report Example** (on page 260).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.
2. Select 'Send sensor report' from the Action list.
3. In the 'Destination actions' section, select the method(s) to report sensor readings or states. The number of available methods varies, depending on how many messaging actions have been created.

   The messaging action types include:
   - Log event message
   - Syslog message
   - Send email
   - Send SMS message
4. If no messaging actions are available, create them now. See **Available Actions** (on page 238).
   a. To select any methods, select them one by one in the Available field.
      To add all available methods, simply click Select All.
   b. To delete any methods, click a method's ✖ in the Selected field.
      To remove all methods, simply click Deselect All.
5. In the 'Available sensors' field, select the desired target's sensor.

   a. Click the first ▲▼ to select a target component from the list.

   ▲▼ Peripheral Devices ▲▼ Temperature 1 ⊕ ⊖

Raritan.
A brand of Legrand

b. Click the second ⬍ to select the specific sensor for the target from the list.

Peripheral Devices ⬍ Temperature 1 ⊕ ⊖

c. Click ⊕ to add the selected sensor to the Report Sensors list box.

For example, to monitor the current reading of the Inlet 1, select Inlet 1 from the left field, and then select RMS Current from the right field.

6. 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.

Report sensors

Peripheral Devices - Temperature 1
Peripheral Devices - Temperature 2
Peripheral Devices - Relative Humidity 1

Available sensors ⬍ Peripheral Devices ⬍ On/Off 1 ⊕
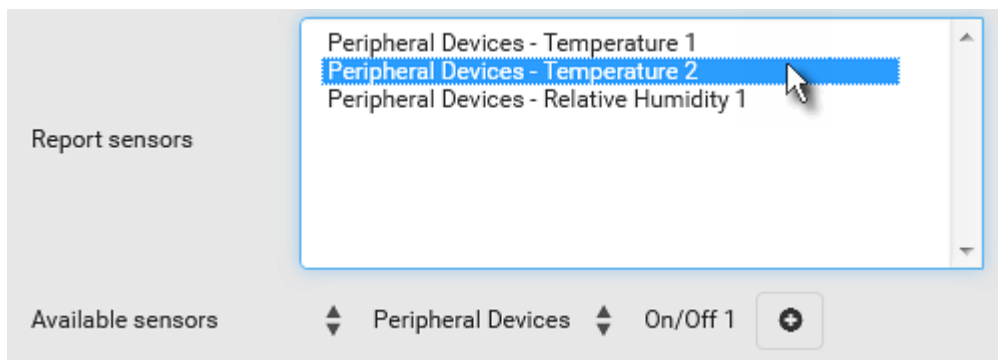
7. To immediately send out the sensor report, click Send Report Now.

*Tip: When intending to send a sensor report using custom messages, use the placeholder [SENSORREPORT] to report sensor readings. See **Placeholders for Custom Messages** (on page 266).*

Send SMS Message

You can configure SMS messages to be sent when an event occurs and can customize the message.

Only the 7-bit ASCII charset is supported for SMS messages. Messages consist of a combination of free text and SRC placeholders. The placeholders represent information which is pulled from the SRC and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged into the SRC in order to send SMS messages. See **Connecting a GSM Modem** (on page 64).

Note: The SRC cannot receive SMS messages.

For example:

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

translates to

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

For a list and definition of available variables, see **Placeholders for Custom Messages** (on page 266).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.

2. Select 'Send SMS message' from the Action list.

3. In the 'Recipient phone number' field, specify the phone number of the recipient.

4. Select the 'Use custom log message' checkbox, and then create a custom message in the provided text box.

Raritan.
A brand of ❑legrand®

- When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Just scroll down to select the desired placeholder. For details, see **Placeholders for Custom Messages** (on page 266).
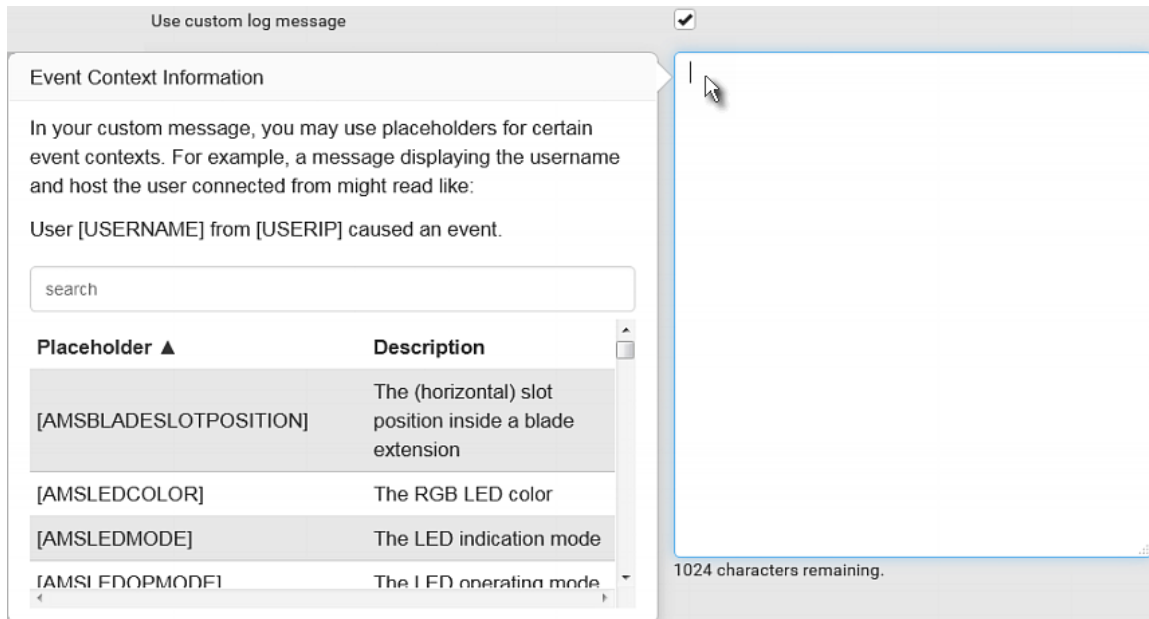
- To start a new line in the text box, press Enter.

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Send Snapshots via Email

This option notifies one or multiple persons for the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

▶ **Operation:**

1. Choose Device Settings > Event Rules > .
2. Select 'Send snapshots via email' from the Action list.
3. In the 'Recipient email addresses' field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
4. By default, the SMTP server specified on the SMTP Server page will be the SMTP server for performing this action.

   To use a different SMTP server, select the 'Use custom SMTP server' checkbox. The fields for customized SMTP settings appear. For information on each field, see **Configuring SMTP Settings** (on page 190).

5. Select the webcam that is capturing the images you want sent in the email.

6. Adjust the values of the following:

   ▪ Number of snapshots - the number of snapshots to be taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.

   ▪ Snapshots per mail - the number of snapshots to be sent at one time in the email.

   ▪ Time before first snapshot - the amount of time in seconds between when the event is triggered and the webcam begins taking snapshots.

   ▪ Time between snapshots - the amount of time in seconds between when each snapshot is taken.

7. If needed, you can customize the subject and messages sent via this email.

   ▪ Select the 'Custom subject' checkbox, and enter the text you prefer as this email's subject.

   ▪ Select the 'Use custom log message' checkbox, and then create a custom message up to 1024 characters in the provided field.
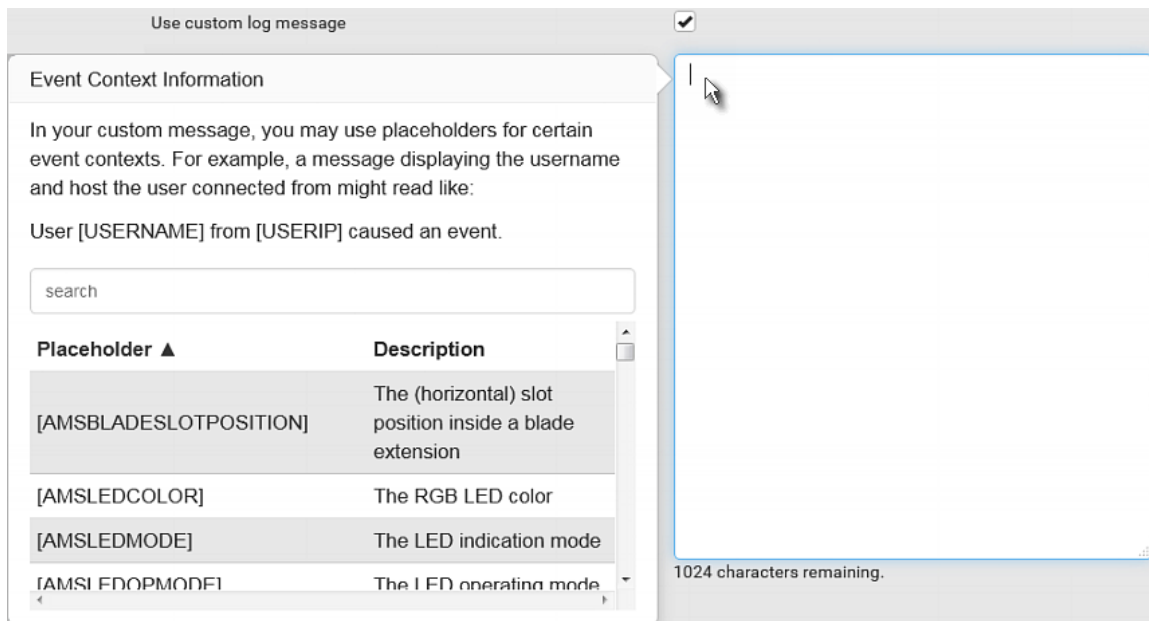
   ▪ To start a new line in the text box, press Enter.

   Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

▶ **Operation:**

1. Choose Device Settings > Event Rules > ✚ New Action.

2. Select 'Send SNMP notification' from the Action list.

3. Select the type of SNMP notification. See either procedure below according to your selection.

▶ **To send SNMP v2c notifications:**

1. In the 'Notification type' field, select 'SNMPv2c trap' or 'SNMPv2c inform.'

2. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

   b. In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent 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 SRC and all SNMP management stations.

Tip: An SNMP v2c notification action permits only a maximum of three SNMP destinations. To assign more than three SNMP destinations to a specific rule, first create several SNMP v2c notification actions, each of which contains completely different SNMP destinations, and then add all of these SNMP v2c notification actions to the same rule.

▶ **To send SNMP v3 notifications:**

1. In the 'Notification type' field, select 'SNMPv3 trap' or 'SNMPv3 inform.'

2. For SNMP TRAPs, the engine ID is prepopulated.

3. For SNMP INFORM communications, leave the resend settings at their default or do the following:

   a. In the Timeout field, specify the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

b. In the 'Number of retries' field, specify the number of times you want to re-send the inform communication if it fails. For example, inform communications are re-sent up to 5 times when the initial communication fails.

4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

a. Host name

b. Port number

c. User ID for accessing the host -- make sure the User ID has the SNMPv3 permission.

d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed.
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase

Start or Stop a Lua Script

If you have created or loaded a Lua script file into the SRC, you can have that script automatically run or stop in response to a specific event.
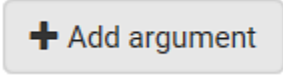
For instructions on creating or loading a Lua script into this product, see **Lua Scripts** (on page 291).

▶ **To automatically start or stop a Lua script:**

1. Choose Device Settings > Event Rules > ✚ New Action.

2. Select 'Start/stop Lua script' from the Action list.

3. In the Operation field, select 'Start script' or 'Stop script.'

Raritan.
A brand of ☐ legrand®

4. In the Script field, select the script that you want it to be started or stopped when an event occurs.

   ▪ No script is available if you have not created or loaded it into the SRC.

5. To apply different arguments than the default, do the following. Note that the newly-added arguments will override this script's default arguments.

   a. Click **+ Add argument**.

   b. Type the key and value.

   c. Repeat the same steps to enter more arguments as needed.

      ▪ To remove any existing argument, click **–** adjacent to it.

Switch LHX/SHX

If Schroff LHX/SHX Support is enabled, the LHX/SHX-related actions will be available. See **Miscellaneous** (on page 297).

Use this action to switch the LHX/SHX on or off when, for example, temperature thresholds are reached.

▶ **Operation:**

1. Choose Device Settings > Event Rules > **+ New Action**.

2. Select 'Switch LHX/SHX' from the Action list.

3. In the Operation field, select 'Turn LHX/SHX on' or 'Turn LHX/SHX off.'

4. In the Available LHX/SHX field, select the LHX/SHX device to be turned on or off. To select all available LHX/SHX devices, click Select All.

   To remove any LHX/SHX device from the Selected LHX/SHX field, click that device's **✖**. To remove all devices, click Deselect All.

Switch Peripheral Actuator

If you have any actuator connected to the SRC, you can set up the SRC so it automatically turns on or off the system controlled by the actuator when a specific event occurs.

*Note: For information on connecting actuators, see **DX2 Sensor Packages** (on page 37).*

▶ **Operation:**

1. Choose Device Settings > Event Rules > **+ New Action**.

2. Select 'Switch peripheral actuator' from the Action list.

3. In the Operation field, select an operation for the selected actuator(s).
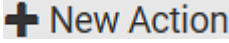
- Turn on: Turns on the selected actuator(s).
- Turn off: Turns off the selected actuator(s).

4. To select the actuator(s) where this action will be applied, select them one by one from the 'Available actuators' list.
   - To add all actuators, click Select All.

5. To remove any selected actuator from the 'Selected actuators' field, click that actuator's ✖.
   - To remove all actuators, click Deselect All.

Syslog Message

Use this action to automatically forward event messages to the specified syslog server. Determine the syslog transmission mechanism you prefer when setting it up - UDP, TCP or TLS over TCP.

SRC may or may not detect the syslog message transmission failure. If yes, it will log this syslog failure as well as the failure reason in the event log. See *Viewing or Clearing the Local Event Log* (on page 308).

▶ **Operation:**

1. Choose Device Settings > Event Rules > ➕ New Action.
2. Select 'Syslog message' from the Action list.
3. In the 'Syslog server' field, specify the IP address to which the syslog is forwarded.
4. In the 'Transport protocol' field, select one of the syslog protocols: TCP, UDP or TCP+TLS. The default is UDP.

Transport protocols	Next steps
UDP	- In the 'UDP port' field, type an appropriate port number. Default is 514. - Select the 'Legacy BSD syslog protocol' checkbox if applicable.
TCP	NO TLS certificate is required. Type an appropriate port number in the 'TCP port' field.

Transport protocols	Next steps

TCP+TLS	A TLS certificate is required. Do the following:
	
	a. Type an appropriate port number in the 'TCP port' field. Default is 6514.
	
	b. In the 'CA certificate' field, click **Browse...** to select a TLS certificate. After importing the certificate, you may:
	  ▪ Click Show to view its contents.
	  ▪ Click Remove to delete it if it is inappropriate.
	
	c. Determine whether to select the 'Allow expired and not yet valid certificates' checkbox.
	  ▪ To always send the event message to the specified syslog server as long as a TLS certificate is available, select this checkbox.
	  ▪ To prevent the event message from being sent to the specified syslog server when any TLS certificate in the selected certificate chain is outdated or not valid yet, deselect this checkbox.

Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see **TLS Certificate Chain** *(on page 638).*

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 SRC report the reading or state of a specific sensor regularly by scheduling the "Send sensor report" action.
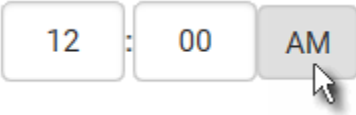
When scheduling an action, make sure you have a minimum of 1-minute buffer between this action's creation and first execution time. Otherwise, the scheduled action will NOT be performed at the specified time when the buffer time is too short. For example, if you want an action to be performed at 11:00 am, you should finish scheduling it at 10:59 am or earlier.

If the needed action is not available yet, create it first. See **Available Actions** (on page 238).

▶ **Operation:**

1. Choose Device Settings > Event Rules >
    ✚ New Scheduled Action.

2. To select any action(s), select them one by one from the 'Available actions' list.
    ▪ To select all available actions, click Select All.

3. To remove any action(s) from the 'Selected actions' field, click that action's .

   ▪ To remove all actions, click Deselect All.

4. Select the desired frequency in the 'Execution time' field, and then specify the time interval or a specific date and time in the field(s) that appear.

Execution time	Frequency settings
Minutes	Click the Frequency field to select an option. The frequency ranges from every minute, every 5 minutes, every 10 minutes and so on until every 30 minutes.
Hourly	Type a value in the Minute field, which is set to either of the following: ▪ The Minute field is set to 0 (zero). Then the action is performed at 1:00 am, 2:00 am, 3:00 am and so on. ▪ The Minute field is set to a non-zero value. For example, if it is set to 30, then the action is performed at 1:30 am, 2:30 am, 3:30 am and so on.
Daily	Type values or click ⌃ ⌄. The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. For example, if you specify 01:30PM, the action is performed at 13:30 pm every day.
Weekly	Both the day and time must be specified for the weekly option. ▪ Days range from Sunday to Saturday. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.
Monthly	Both the date and time must be specified for the monthly option. ▪ The dates range from 1 to 31. ▪ The time is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button. Note that NOT every month has the date 31, and February in particular does not have the date 30 and probably even 29. Check the calendar when selecting 29, 30 or 31.
Yearly	This option requires three settings: ▪ Month - January through December. ▪ Day of month - 1 to 31. ▪ Time - the value is measured in 12-hour format so you must correctly specify AM or PM by clicking the AM/PM button.

An example of the scheduled action is available in the section titled *Send Sensor Report Example* (on page 260).

Send Sensor Report Example

To create a scheduled action for emailing a temperature sensor report hourly, it requires:

- A 'Send email' action
- A 'Send sensor report' action
- A timer - that is, the scheduled action

▶ **Steps:**

1. Click to create a 'Send email' action that sends an email to the desired recipient(s). For details, see **Send Email** (on page 246).

  ▪ In this example, this action is named *Email a Sensor Report*.

- If wanted, you can customize the subject and content of this email in this action.

New Action

Action name	Email a Sensor Report
Action	Send email ▼

Recipient email addresses	IT-manager@raritan.com
SMTP server	⦿ Use default settings Server name: 192.168.5.50 Sender email address: manager@raritan.com Settings can be changed in SMTP Server settings. ◯ Use custom settings
Custom subject	✔ Sensor Report: [EXTSENSOR] - [EXTSENSORNAME]
Use custom log message	✔
Custom log message	The following is the complete sensor report – [SENSORREPORT] 962 characters remaining.

✖ Cancel   ✔ Create

Raritan.
A brand of ∆legrand

2. Click ![New Action] to create a 'Send sensor report' action that includes the 'Email a Sensor Report' action as its destination action. For details, see **Send Sensor Report** (on page 248).

   ▪ In this example, this action is named *Send Temperature Sensor Readings*.

- You can specify more than one temperature sensor as needed in this action.

New Action

Action name	Send Temperature Sensor Readings
Action	Send sensor report ▾

Destination actions

Selected   Email a Sensor Report ✖

Available   – Select an item – ▾

Select All   Deselect All

Report sensors

Peripheral Devices - Temperature 1
Peripheral Devices - Temperature 2

Available sensors   ▲▼ Peripheral Devices   ▲▼ Relative Humidity 1   ⊕ ⊖

Send Report Now

Note: Reported sensor units can be changed in the Default Preferences.

✖Cancel   ✔Create

3. Click ➕ New Scheduled Action to create a timer for performing the 'Send Temperature Sensor Readings' action hourly. For details, see *Scheduling an Action* (on page 257).

Raritan.
A brand of ☐legrand®

- In this example, the timer is named *Hourly Temperature Sensor Reports*.
- To perform the specified action at 12:30 pm, 01:30 pm, 02:30 pm, and so on, select Hourly, and set the Minute to 30.

Then the SRC will send out an email containing the specified temperature sensor readings hourly every day.

Whenever you want the SRC to stop sending the temperature report, deselect the Enabled checkbox in the timer.

Placeholders for Custom Messages

Actions of "Send email" and "Send SMS message" allow you to customize event messages. See **Send Email** (on page 246) or **Send SMS Message** (on page 250). In addition, you can add custom text message to the "Send snapshots via email" action. See **Send Snapshots via Email** (on page 251).

When clicking anywhere inside the text box, the Event Context Information displays, showing a list of placeholders and their definitions. Simply drag the scroll bar and then click the desired placeholder to insert it into the custom message. Or you can type a keyword in the "search" box to quickly find the desired placeholder.

Note that available placeholders are model dependent.
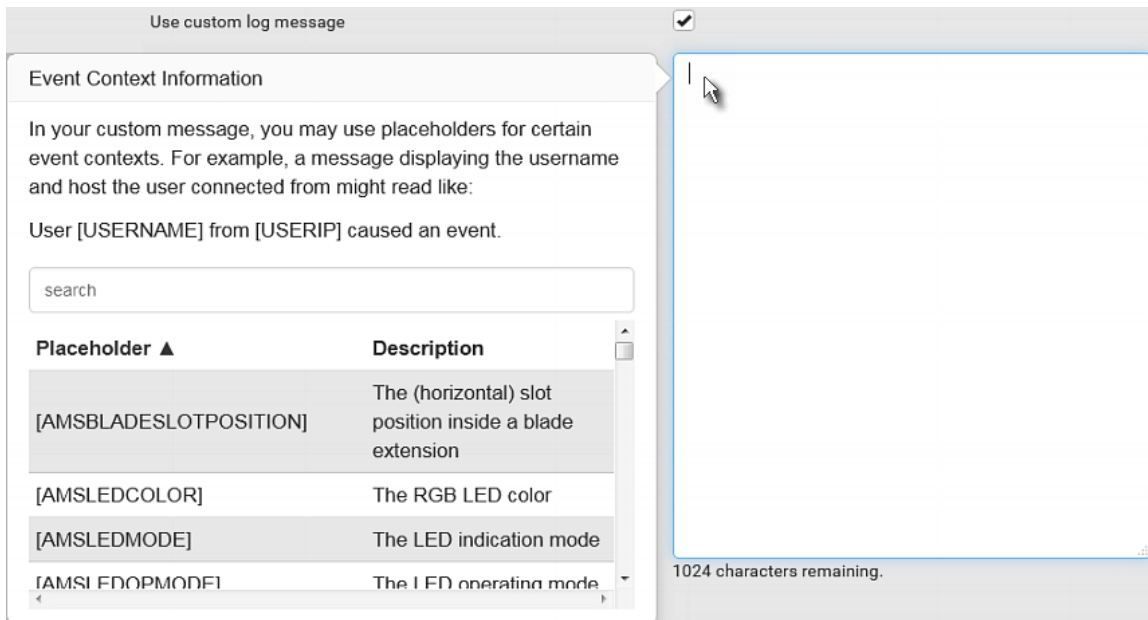
If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 101).

To make the Event Context Information disappear, click anywhere inside the browser's window.

The following are placeholders that can be used in custom messages.

Placeholder	Definition
[AMSBLADESLOTPOSITION]	The (horizontal) slot position inside a blade extension
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode

Placeholder	Definition
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position
[AMSSTATE]	The human-readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CARDREADERCHANNEL]	The channel number of a card reader
[CARDREADERID]	The id of a card reader
[CARDREADERMANUFACTURER]	The manufacturer of a card reader
[CARDREADERPRODUCT]	The product name of a card reader
[CARDREADERSERIALNUMBER]	The serial number of a card reader
[COMPONENTID]	The ID of a hardware component
[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
[DEVICESERIAL]	The unit serial number of the device the event occurred on
[ERRORDESC]	The error message
[EVENTRULENAME]	The name of the matching event rule
[EXTSENSOR]	The peripheral device identifier
[EXTSENSORNAME]	The name of a peripheral device
[EXTSENSORSLOT]	The ID of a peripheral device slot
[FAILURETYPE]	The numeric hardware failure type
[FAILURETYPESTR]	The textual hardware failure type
[IFNAME]	The human readable name of a network interface
[ISASSERTED]	Boolean flag whether an event condition became true (1) or false (0)
[LDAPERRORDESC]	The LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX/SHX
[LHXPOWERSUPPLYID]	The ID of an LHX/SHX power supply

Raritan
A brand of **legrand**

Placeholder	Definition
[LHXSENSORID]	The ID of an LHX/SHX sensor probe
[LOGMESSAGE]	The original log message
[MONITOREDHOST]	The name or IP address of a monitored host
[NETAUTHRESULTSTR]	The network authentication result string ('succeeded' or 'failed')
[OLDVERSION]	The firmware version the device is being upgraded from
[PERIPHDEVPOSITION]	The position of an attached peripheral device
[PHONENUMBER]	The destination phone number of an outgoing SMS message
[PORTID]	The label of the external port the event-triggering device is connected to
[PORTTYPE]	The type of the external port (e.g. 'feature' or 'auxiliary') the event-triggering device is connected to
[RADIUSERRORDESC]	The Radius error message
[ROMCODE]	The romcode of an attached peripheral device
[SENSORREADING]	The value of a sensor reading
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREPORT]	The formatted sensor report contents
[SENSORSTATENAME]	The human readable state of a sensor
[SENSORTHRESHOLDNAME]	The name of the threshold being crossed
[SENSORTHRESHOLDVALUE]	The value of the threshold being crossed
[SERVERPOWEROPERATION]	The power control operation that was initiated on a server (on/off)
[SERVERPOWERRESULT]	The result of a power control operation
[SMARTCARDID]	The id of a smart card
[SMARTCARDTYPE]	The type of a smart card
[SMTPRECIPIENTS]	The list of recipients of an outgoing mail
[SMTPSERVER]	The name or IP address of an SMTP server
[SYSCONTACT]	SNMP MIB-II sysContact field
[SYSLOCATION]	SNMP MIB-II sysLocation field
[SYSNAME]	SNMP MIB-II sysName field

Placeholder	Definition
[TIMEREVENTID]	The id of a timer event
[TIMESTAMP]	The timestamp of the event occurrence
[UMTARGETROLE]	The target role of a user management operation
[UMTARGETUSER]	The target user of a user management operation
[USERIP]	The IP address a user connected from
[USERNAME]	The user who performed an operation
[VERSION]	The firmware version the device is upgrading to

Note: In case you need to type any square brackets "[" and "]" in the custom message for non-placeholder words, always add a backslash in front of the square bracket. That is, \[or \]. Otherwise, the message sent will not display the square brackets.

Editing or Deleting a Rule/Action

You can change the settings of an event rule, action or scheduled action, or delete them.

Exception: Some settings of the built-in event rules or actions are not user-configurable. You cannot delete built-in rules and actions. See **Built-in Rules and Rule Configuration** *(on page 225) or* **Available Actions** *(on page 238).*

▶ **To edit or delete an event rule, action or scheduled action:**

1. Choose Device Settings > Event Rules.

2. Click the desired one in the list of rules, actions or scheduled actions. Its setup page opens.

3. Perform the desired action.

   - To modify settings, make necessary changes and then click Save.

   - To delete it, click 🗑 Delete on the top-right corner. Then click Delete on the confirmation message.

Sample Event Rules

Sample Device-Level Event Rule

In this example, we want the SRC to record in the internal log when the network link is up to down. The sample event rule looks like this:

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

▶ **To create the above event rule:**

1. In the Event field, select Device as we are specifying an event regarding the SRC device.
2. Then select "Network interface link state is up" because we want the SRC to respond to the event related to physical connections and/or disconnections from the network.
3. Select the Both radio button since we want both connection and disconnection actions to be recorded when either action is taken.
4. Select "System Event Log Action" as we intend to record this event in the internal log when the specified events occur.

Raritan.
A brand of legrand

Sample Sensor-Level Event Rule

In this example, we want the SRC to send a notification email when a contact closure sensor enters the alarmed state. This event rule requires creating a new action before creating the rule.

▶   **Step 1: create a new action for sending an email**

1.   Choose Device Settings > Event Rules > ✚ New Action.

2.   In this illustration, assign the name "Send a Notification" to the new action.

3.   In the Action field, select "Send email."

4.   In the Recipient Email Addresses field, type one or multiple recipients' email addresses.

5.   (Optional) Specify the SMTP settings and custom log message if needed.

6. Click Create to finish the creation.

| Action name | Send a Notification | **2** |
| Action | Send email | **3** ▼ |

| Recipient email addresses | IT-manager@raritan.com | **4** |

SMTP server

● Use default settings

Server name: not configured
Sender email address: not configured

Settings can be changed in SMTP Server settings.

○ Use custom settings

Use custom log message ✔

5

Custom log message

This email reports the "alarmed" state of this contact closure sensor:
#[EXTSENSORSLOT],
[EXTSENSORNAME]

918 characters remaining.

Raritan.
A brand of ⬛legrand®

After the new action is created, follow the procedure below to create an event rule that sends a notification email when the contact closure sensor enters the alarmed state. This event rule involves the following:

- Event: Peripheral Device Slot > Slot 1 > State Sensor/Actuator > Alarmed/Open/On
- Trigger condition: Alarmed
- Action: Send a Notification

▶ **Step 2: create the contact closure-triggered email event rule**

1. Click ![+ New Rule] on the Event Rules page.

2. In this illustration, assign the name "Contact Closure Triggered Email" to the new rule.

3. In the Event field, select "Peripheral Device Slot" to indicate we are specifying an event related to the environmental sensor package.

4. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1.

   Note: ID numbers of all sensors/actuators are available on the Peripherals page. See **Peripherals** *(on page 108).*

5. Select "State Sensor/Actuator" because the contact closure sensor is a state sensor.

6. Select "Alarmed" since we want the SRC to respond when the selected contact closure sensor changes its state related to the "alarmed" state.

7. In the 'Trigger condition' field, select the Alarmed/Open/On radio button so that the action is taken only when the contact closure sensor enters the alarmed state.

8. Select "Send a Notification" from the Available Actions list.

Sample Asset-Management-Level Event Rule

In this example, we want the SRC to record the connection and disconnection events of a specific asset tag in the internal log. The event rule is set like this:

- Event: Asset Management > Feature Port 1 > Rack Unit > Index 3 > Tag Connected
- Trigger condition: Both
- Actions: System Event Log Action

▶ **To create the above event rule:**

1. Select "Asset Management" in the Event field to indicate we are specifying an event regarding the asset strips and/or tags.

2. Select "Rack Unit" for events related to rack units (tag ports) of an asset strip.

3. Select "Index 3" becasue the desired asset tag is connected to the tag port #3 of the asset strip.

4. Select "Tag Connected" as the events we want to record are related to physical tag connections or disconnections.

5. Select the Both radio button since we want both connection and disconnection actions to be recorded when either event occurs.

6. 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 SRC keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one more event.

Example 1

This example illustrates an event rule which continuously causes the SRC 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 SRC to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send email

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the SRC to generate an alert. The measurement then returns to a value within the threshold, but the SRC does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the SRC uses. See *"To De-assert" and Deassertion Hysteresis* (on page 620).

Setting Data Logging

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

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

Note: The SRC device's SNMP agent must be enabled for this feature to work. See **Enabling and Configuring SNMP** *(on page 346). In addition, using an NTP time server ensures accurately time-stamped measurements.*

By default, data logging is enabled. You must have the "Administrator Privileges" or "Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration" permissions to change the setting.

▶ **To configure the data logging feature:**

1. Choose Device Settings > Data Logging.

2. To enable the data logging feature, select the "Enable" checkbox in the General Settings section.

3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.

4. Verify that all sensor logging is enabled. If not, click Enable All at the bottom of the page to have all sensors selected.

   ▪ You can also click the topmost checkbox labeled "Logging Enabled" in the header row of each section to select all sensors of the same type.

   ▪ If any section's number of sensors exceeds 35, the remaining sensors are listed on next page(s). If so, a pagination bar similar to the following diagram displays in this section, which you can click any button to switch between pages.

| First | Previous | 1 | 2 | 3 | 4 | 5 | ... | Next | Last |

5. Click Save. This button is located at the bottom of the page.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the SRC, it is NOT recommended to do so.

Configuring Data Push Settings

You can push the sensor or asset strip data to a remote server for data synchronization. The destination and authentication for data push have to be configured properly on the SRC.

The data will be sent in JSON format using HTTP POST requests. For more information on its format, see **Data Push Format** (on page 279).

For instructions on connecting asset strips, see **Connecting Asset Management Strips** (on page 53).

After configuring the destination and authentication settings, do either or both of the following:

- To perform the data push after the occurrence of a certain event, create the data push action and assign it to an event rule.
- To push the data at a regular interval, schedule the data push action.

  See **Event Rules and Actions** (on page 224).

▶ **To configure data push settings:**

1. Choose Device Settings > Data Push.
2. To specify a destination, click ✚ New Destination.
3. Do the following to set up the URL field.

   a. Click ▼ to select *http* or *https*.
   b. Type the URL or host name in the accompanying text box.

4. If selecting https, a CA certificate is required for making the connection.

   Click Browse… to install it. Then you can:

   - Click Show to view the certificate's content.
   - Click Remove to delete the installed certificate if it is inappropriate.

   Note: If the required certificate file is a chain of certificates, and you are not sure about the requirements of a certificate chain, see **TLS Certificate Chain** *(on page 638).*

5. If the destination server requires authentication, select the 'Use authentication' checkbox, and enter the following data.

   - User name comprising up to 64 characters
   - Password comprising up to 128 characters

6. In the 'Entry type' field, determine the data that will be transmitted.

   - *Asset management tag list:* Transmit the information of the specified asset strip(s), including the general status of the specified strip(s) and a list of asset tags. The asset tags list also includes the tags on blade extension strips, if any.

Raritan.
A brand of ◻legrand®

▪ *Asset management tag log:* Transmit the log of all asset strips, which is generated when there are changes made to asset tags and asset strips, including asset tag connection or disconnection events.

▪ *Sensor log:* Transmit the record of all logged sensors, including their sensor readings and/or status. Logged sensors refer to all internal and/or environmental sensors/actuators that you have selected on the Data Logging page. See *Setting Data Logging* (on page 277).

7. If 'Asset management tag list' is selected in the above step, specify the asset strip(s) whose information to send. For SRC with only one FEATURE port, only one asset strip is available.

▪ To specify the asset strip(s), select them one by one from the Available AMS Ports list. Or click Select All to add all.

▪ To remove the asset strip(s), click that asset strip's ✖ in the Selected AMS Ports field. Or click Deselect All to remove all.

8. Click Create.

9. Repeat the same steps for additional destinations. Up to 64 destinations are supported.

▶ **To immediately push out the data:**

1. On the Data Push page, choose the one whose data you want to push out.

2. Click its [⛅ Push Now].

▶ **To modify or delete data push settings:**

1. On the Data Push page, click the one you want in the list.

2. Perform either action below.

▪ To modify settings, make necessary changes and then click Save.

▪ To delete it, click [🗑 Delete], and then confirm it on the confirmation message.

Data Push Format

Each push message contains exactly one JSON object. The data format is formally defined in IDL files, sharing several definitions from the JSON-RPC data model.

IDL files are available by launching *JSON-RPC online help* (*https://help.raritan.com/json-rpc/pdu/v3.6.0/namespacedatapush.html*).

To have an overview of the data format, see the following topic.

- *Sensor Log* (on page 280)
- *Asset Management Tag List* (on page 281)
- *Asset Management Tag Log* (on page 284)

Sensor Log

The root object of the message is a `SensorLogPushMessage` structure. It comprises a list of sensor descriptors and a list of log rows.

▶ **Sensor descriptors:**

The sensor descriptor vector contains static information of all logged sensors, including:

- The electrical component a sensor is associated with.
- The sensor's type.
- Unit and range of the sensor's readings.

▶ **Log rows:**

Each log row consists of a time stamp (accumulated seconds since 1/1/1970) and a list of log records -- one for each logged sensor.

The length and order of the record list is the same as the sensor descriptor vector.

Asset Management Tag List

The root object of the asset management tag list message is an `AssetStripsMessage` structure. It contains current data about all connected asset management strips and tags, which is similar to the illustration below.

```
{
    "assetStrips": [
        {
            "stripInfo": {
                "bladeOverflow": false,
                "bladeTagCount": 0,
                "cascadeState": 0,
                "componentCount": 1,
                "mainTagCount": 2,
                "maxBladeTagCount": 128,
                "maxMainTagCount": 64,
                "rackUnitCount": 48
            },
            "deviceInfo": {
                "appVersion": 24,
                "bootVersion": 6,
                "deviceId": 48,
                "hardwareId": 2,
                "isCascadable": false,
                "orientationSensAvailable": true,
                "protocolVersion": 257,
                "rackUnitCountConfigurable": true
            },
            "settings: {
                "rackUnitCount": 48,
                "name": "Asset Strip 1",
                "scanMode": 0,
                "defaultColorConnected": { "r": 0, "g": 255, "b": 0 },
                "defaultColorDisconnected": { "r": 255, "g": 0, "b": 0 },
                "numberingMode": 1,
                "numberingOffset": 1,
                "orientation": 0
            },
```

(Continued)

```
        "tags": [
            {
                "rackUnitNumber": 4,
                "slotNumber": 0,
                "familyDesc": "Unknown",
                "rawId": "DEADBEEF0000",
                "programmable": 0
            },
            {

                "rackUnitNumber": 5,
                "slotNumber": 0,
                "familyDesc": "Unknown",
                "rawId": "DEADBEEF0500",
                "programmable": 0
            }
        ]
    }
    ]
}
```

Asset Management Tag Log

The root object of the asset management log message is an `AssetLogPushMessage` structure. It contains a list of tag or strip events since the last successful push.

Note that a Raritan-provided explanation, which is the comment beginning with // in each line, is added to the following illustration for you to understand it better.

```
{
    "records": [
        {
            "timestamp": 1334052852,      // Time stamp (seconds since 1/1/1970)
            "type": 1,                    // 0: empty, 1: tag connected, 2: tag disconnected,
                                          // 3: asset strip state changed

            "assetStripNumber": 0,        // Asset strip number
            "rackUnitNumber" : 10,        // Rack unit number
            "rackUnitPosition" : 12,      // Rack unit position
            "slotNumber",                 // Blade extension slot number
            "tagId",                      // The ID of the asset management tag
            "state": 5,                   // Sensor was in normal range
            "parentBladeId",              // ID of the parent blade extension tag
            "state": 0                    // 0: disconnected, 1: firmware update,
                                          // 2: unsupported, 3: available
        },
        {
            // [...] next record
        }
    ]
}
```

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the SRC 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.

SRC can monitor any IT device, such as database servers, remote authentication servers, power distribution units (PDUs), and so on. It supports monitoring a maximum of 64 IT devices.

To perform this feature, you need the Administrator Privileges.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings for optimal results.

Tip: To make the SRC automatically log, send notifications or perform other actions for any server monitoring events, you can create event rules. See **Event Rules and Actions** *(on page 224). An example is available in* **Example: Ping Monitoring and SNMP Notifications** *(on page 287).*

▶ **To add IT equipment for ping monitoring:**

1. Choose Device Settings > Server Reachability.

2. Click ✚ Monitor New Server.

3. By default, the "Enable ping monitoring for this server" checkbox is selected. If not, select it to enable this feature.

4. Configure the following.

Field	Description
IP address/hostname	IP address or host name of the IT equipment which you want to monitor.
Number of successful pings to enable feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait time after successful ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait time after unsuccessful ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).

Field	Description
Number of consecutive unsuccessful pings for failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait time before resuming pinging after failure	The wait time before the SRC 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 SRC disables the ping monitoring feature for it and shows "Waiting for reliable connection." Valid range is 0 to 100.

5. Click Create.
6. To add more IT devices, repeat the same steps.

Server Status Checking

After adding IT equipment for monitoring, all IT devices are listed on the Server Reachability page.

Server Reachability		✚ Monitor New Server
IP Address/Hostname ▲	**Ping Enabled**	**Status**
100.192.3.55	yes	Waiting for reliable connection
150.33.84.99	yes	Waiting for reliable connection
www.legrand.com	yes	Reachable
www.raritan.com	yes	Reachable

In the beginning, the status of the added IT equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before SRC can declare that the monitored device is reachable or unreachable.

▶ **To check the server monitoring states and results:**

1. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding IT device is activated or not.
2. The column labeled "Status" indicates the accessibility of monitored equipment.

Status	Description
Reachable	The monitored equipment is accessible.
Unreachable	The monitored equipment is inaccessible.
Waiting for reliable connection	The connection between the SRC device and the monitored equipment is not reliably established yet.

Editing or Deleting Ping Monitoring Settings

You can edit the ping monitoring settings of any IT device or simply delete it if no longer needed.

▶ **To modify or delete any monitored IT device:**

1. Choose Device Settings > Server Reachability.
2. Click the desired one in the list.
3. Perform the desired action.
   - To modify settings, make necessary changes and then click Save. For information on each field, see **Monitoring Server Accessibility** (on page 285).
   - To delete it, click 🗑 Delete on the top-right corner.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your SRC to make sure that PDU is properly operating all the time, and the SRC must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power sources are different between your SRC and the monitored PDU.

This requires the following two steps.

▶ **Step 1: Set up the ping monitoring for the target PDU**

1. Choose Device Settings > Server Reachability.
2. Click ➕ Monitor New Server.
3. Ensure the "Enable ping monitoring for this server" checkbox is selected.
4. Enter the data shown below.
   - Enter the server's data.

Field	Data entered
IP address/hostname	192.168.84.95

- To make the SRC declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, enter the following data.

Field	Data entered
Number of successful pings to enable feature	3
Wait time after successful ping	5

- To make the SRC declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 seconds * 3 pings), enter the following data.

Field	Data entered
Wait time after unsuccessful ping	4
Number of consecutive unsuccessful pings for failure	3

- To make the SRC stop pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared, enter the following data. After 60 seconds, the SRC will re-ping the target PDU,

Field	Data entered
Wait time before resuming pinging after failure	60

- The "Number of consecutive failures before disabling feature (0 = unlimited)" can be set to any value you want.

5. Click Create.

▶ **Step 2: Create an event rule to send SNMP notifications for the target PDU**

1. Choose Device Settings > Event Rules.

2. Click ➕ New Rule.

3. Select the Enabled checkbox to enable this new rule.

4. Configure the following.

Field/setting	Data specified
Rule name	Send SNMP notifications for PDU (192.168.84.95) inaccessibility
Event	Choose Server Monitoring > 192.168.84.95 > Unreachable
Trigger condition	Select the Unreachable radio button

This will make the SRC react only when the target PDU becomes inaccessible.

5. Select the System SNMP Notification Action.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Editing or Deleting a Rule/Action** *(on page 269).*

Front Panel Settings

You can set up the default mode of the front panel display, and front panel functions for outlet switching, actuator control, beeper mute or RCM self-test.

Below are available front panel settings:

*   Actuator control
*   Internal beeper's mute function
*   Default front panel mode setup

▶ **To configure the front panel settings:**

1. Choose Device Settings > Front Panel.
2. Configure the following:
    *   To configure the default view of the LCD display, select one mode below.

Note: The default view is shown in the automatic mode. See **Automatic and Manual Modes** *(on page 70).*

Mode	Data entered
Automatic mode	This is the default and the only mode. The LCD display indicates whether the current device status is normal or there are any alarms now.

*   To enable the front panel actuator-control function, select the 'Peripheral actuator control' checkbox.
*   The built-in beeper's mute control function is enabled per default. To disable it, **deselect** the 'Mute beeper' checkbox.

3. Click Save.

    If the 'Mute beeper' feature is enabled, you can operate the front panel to mute it whenever it beeps. See **Muting the Internal Beeper** (on page 75).

    Or you can turn on or off actuators by operating the front panel. See **Peripherals** (on page 76).

Configuring the Serial Port

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

The SRC supports using the following devices via the serial interface:

- A computer for console management.
- A Raritan KVM product.
- 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 SRC through the serial port, or there are communication problems.

Note: The serial port bit-rate change is required when the SRC works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

You can set diverse bit-rate settings for console and modem operations. Usually the SRC can detect the device type, and automatically apply the preset bit rate.

The SRC will indicate the detected device in the Port State section of the Serial Port page.

To configure serial port and modem settings, choose Device Settings > Serial Port.

▶ **To change the serial port's baud rate settings:**

1. Click the 'Connected device' field to make the serial port enter an appropriate state.

Options	Description
Automatic detection	The SRC automatically detects the type of the device connected to the serial port. Select this option unless your SRC cannot correctly detect the device type.
Force console	The SRC attempts to recognize that the connected device is set for the console mode.
Force analog modem	The SRC attempts to recognize that the connected device is an analog modem.
Force GSM modem	The SRC attempts to recognize that the connected device is a GSM modem.

2. Click the 'Console baud rate' field to select the baud rate intended for console management.

Note: For a serial RS-232 or USB connection between a computer and the SRC, leave it at the default (115200 bps).

3. Click the 'Modem baud rate' field to select the baud rate for the modem connected to the SRC.

The following modem settings/fields appear in the web interface after the SRC detects the connection of an analog or GSM modem.

▶ **To configure the analog modem:**

1. Select the 'Answer incoming calls' checkbox to enable the remote access via a modem. Otherwise, deselect it.

2. Type a value in the 'Number of rings before answering' field to determine the number of rings the SRC must wait before answering the call.

▶ **To configure the GSM modem:**

1. Enter the SIM PIN code.

2. Select the 'Use custom SMS center number' checkbox if a custom SMS center will be used.

   ▪ Enter the SMS center number in the 'SMS center' field.

3. If needed, click Advanced Information to view detailed information about the modem, SIM and mobile network.

4. To test whether the SRC can successfully send out SMS messages with the modem settings:

   a. Enter the number of the recipient's phone in the Recipient Phone field.

   b. Click Send SMS Test to send a test SMS message.

Lua Scripts

If you can write or obtain any Lua scripts, you can create or load them into the SRC to control its behaviors.

Raritan also provides some Lua scripts examples, which you can load as needed.

Note: Not all Raritan Lua script examples can apply to your SRC model. You should read each example's introduction before applying them.

You must have the Administrator Privileges to manage Lua scripts.

Writing or Loading a Lua Script

You can enter or load up to 4 scripts to the SRC.

Tip: If you can no longer enter or load a new script after reaching the upper limit, you can either delete any existing script or simply modify/replace an existing script's codes. See **Modifying or Deleting a Script** *(on page 296).*

▶ **To write or load a Lua script:**

1. Choose Device Settings > Lua Scripts > ➕ Create New Script .

2. Type a name for this script. Its length ranges between 1 to 63 characters.

    The name must contain the following characters only.

    -   Alphanumeric characters
    -   Underscore (_)
    -   Minus (-)
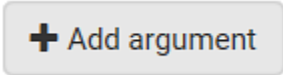
    Note: Spaces are NOT permitted.

3. Determine whether and when to automatically execute the loaded script.

Checkbox	Behavior when selected
Start automatically at system boot	Whenever the SRC reboots, the script is automatically executed.
Restart after termination	The script is automatically executed each time after 10 seconds since the script execution finishes.

4. (Optional) Determine the arguments that will be executed by default.
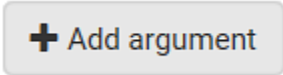
    a. Click ➕ Add argument .
    b. Type the key and value.
    c. Repeat the same steps to enter more arguments as needed.

        -   To remove any existing argument, click ➖ adjacent to it.

    Note: The above default arguments will be overridden by new arguments specified with the "Start with Arguments" command or with any Lua-script-related event rule. See **Manually Starting or Stopping a Script** *(on page 294) or* **Start or Stop a Lua Script** *(on page 254).*

5. In the Source Code section, do one of the following. It is recommended to leave the Enable Syntax Highlighting checkbox selected unless you do not need different text colors to identify diverse code syntaxes.

Raritan.
A brand of legrand

- To write a Lua script, type the codes in the Source Code section.

- To load an existing Lua script file, click Load Local File.
- To use one of Raritan's Lua script examples, click Load Example.

Warning: The newly-loaded script will overwrite all existing codes in the Source Code section. Therefore, do not load a new script if the current script meets your needs.

6. If you chose to load a script or Raritan's example in the previous step, its codes are then displayed in the Source Code section. Double check the codes. If needed, modify the codes to meet your needs.

7. Click Create.

▶ **Next steps:**

- To execute the newly-added script immediately, click ▶ Start, or click ⋮ > Start With Arguments. See *Manually Starting or Stopping a Script* (on page 294).

- To add more scripts, first return to the scripts list by clicking "Lua Scripts" on the top (see below) or in the *Menu* (on page 98), and then repeat the above steps.

Manually Starting or Stopping a Script

You can manually start or stop an existing Lua script at any time.

When starting a script, you can choose to start it either with its default arguments or with new arguments.

Tip: To have the SRC automatically start or stop a script in response to an event, create an event rule. See **Event Rules and Actions** *(on page 224) and* **Start or Stop a Lua Script** *(on page 254).*

▶ **To manually start a script:**

1. Choose Device Settings > Lua Scripts. The Lua scripts list displays.
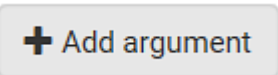
Lua Scripts			✚ Create New Script
Name	**State**	**Autostart**	**Restart**
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

2. Click the desired script whose state is either 'Terminated' or 'New.' For details, see **Checking Lua Scripts States** (on page 296).

3. To start with default arguments, click ▶ Start.

   To start with new arguments, click ⋮ > Start With Arguments. Newly-assigned arguments will override default ones.

4. If you chose "Start With Arguments" in the above step, enter the key and value in the Start Lua Script dialog.

   - Click ✚ Add argument if needing additional arguments.

Start Lua Script

Key	**Value**	
		−

✚ Add Argument

Cancel   Start

Raritan.
A brand of ☐legrand‘

5. Click Start.

6. The script output will be shown in the Script Output section.

    ▪ If needed, click **◇ Clear** to delete the existing output data.

> ### Script Output
> ◇ Clear
>
> ```
> PDU Manufacturer: Raritan
> PDU Model: PX3-5024CV-F5M5
>
> PDU metadata:
> macAddress: 00:0d:5d:64:21:33
> fwRevision: 3.4.0.5-43927
> nameplate:     -->   table: 0x113ca90
>   rating:     -->   table: 0x113fd18
>     voltage: 100-240V
>     power: 1.6-3.8kVA
>     current: 16A
> ```
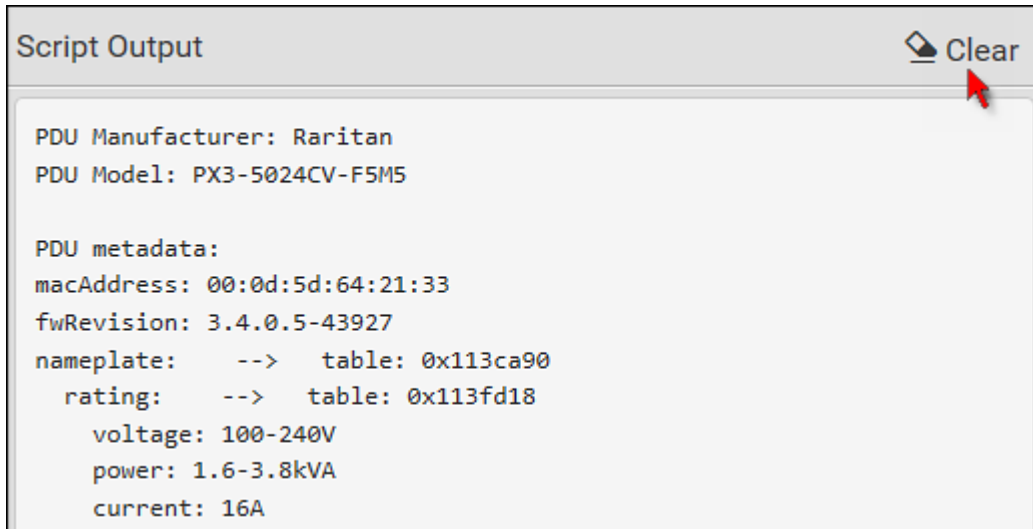
▶ **To manually stop a script:**

1. Choose Device Settings > Lua Scripts.

2. Click the desired script whose state is either 'Running' or 'Restarting.' For details, see *Checking Lua Scripts States* (on page 296).

3. Click **■ Stop** on the top-right corner.

4. Click Stop on the confirmation message.

▶ **To return to the scripts list:**

- Click "Lua Scripts" on the top of the page.

> **❮ Lua Scripts | Script Status: xxx**
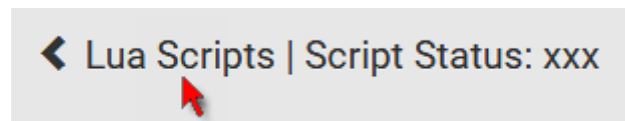
- Or click "Lua Scripts" in the *Menu* (on page 98).

Checking Lua Scripts States

Choose Device Settings > Lua Scripts to show the scripts list, which indicates the current state and settings of each script.

Lua Scripts			➕ Create New Script
Name	**State**	**Autostart**	**Restart**
script-1	Terminated	yes	no
script-2	New	no	yes
script-3	Running	no	no

▶ **State:**

Four script states are available.

State	Description
New	The script is never executed since the device boot.
Running	The script is currently being executed.
Terminated	The script was once executed, but stops now.
Restarting	The script will be executed. Only the scripts with the "Restart" column set to "yes" will show this state.

▶ **Autostart:**

This column indicates whether the checkbox labeled "Start automatically at system boot" is enabled. See *Writing or Loading a Lua Script* (on page 292).

▶ **Restart:**

This column indicates whether the checkbox labeled "Restart after termination" is enabled. See *Writing or Loading a Lua Script* (on page 292).

Modifying or Deleting a Script

You can edit an existing script's codes or even replace it with a new script. Or you can simply remove a unnecessary script from the SRC.

▶ **To modify or replace a script:**

1. Choose Device Settings > Lua Scripts.

2. Click the desired one in the scripts list.

3. Click ⋮ > Edit Script.

4. Make changes to the information shown, except for the script's name, which cannot be revised.

    ▪ To replace the current script, click Load Local File or Load Example to select a new script.

► **To delete a script:**

1. Choose Device Settings > Lua Scripts.
2. Click the desired one in the scripts list.
3. Click 　⋮　 > Delete.
4. Click Delete on the confirmation message.

► **To return to the scripts list:**

● Click "Lua Scripts" on the top of the page.

> ❮ Lua Scripts | Script Status: xxx
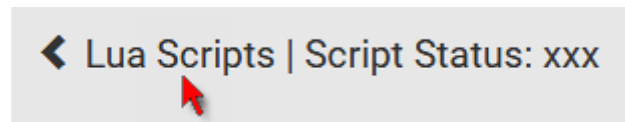
● Or click "Lua Scripts" in the *Menu* (on page 98).

Miscellaneous

By default, the support for Schroff LHX/SHX heat exchangers is disabled.

Support needs to be enabled for the LHX/SHX information to appear in the SRC web interface. Besides, Schroff LHX/SHX support must be enabled in order for the LHX-MIB to be accessible through SNMP.

To enable this feature, choose Device Settings > Miscellaneous.

In addition, if you have to prevent others from accessing your SRC via USB-A for security reasons, you can disable all of USB-A ports on the SRC. By default, USB-A ports are enabled.

Important: Disabling USB-A ports will disable all of 'USB-A' based features, such as wireless networking, USB cascading or pdView access using iOS mobile devices. Therefore, re-think about it before disabling USB-A.

► **To enable the support for Schroff LHX/SHX:**

1. Select the LHX/SHX checkbox.
2. Click Save in the *Features* section.
3. Click Apply on the confirmation message.
4. SRC reboots.

► **To disable the access to USB-A port(s):**

1. Deselect the Enable USB Host Ports checkbox.
2. Click Save in the USB Host Ports section.

Tip: After the Enable USB Host Ports checkbox is deselected, only the access to USB-A port(s) is prevented while the USB-B port works as normal. That is, users still can access the USB-B port, such as accessing CLI via USB-B. To disable the access to the USB-B port, you have to apply a mechanical method.

Maintenance

Click 'Maintenance' in the *Menu* (on page 98), and the following submenu
displays.
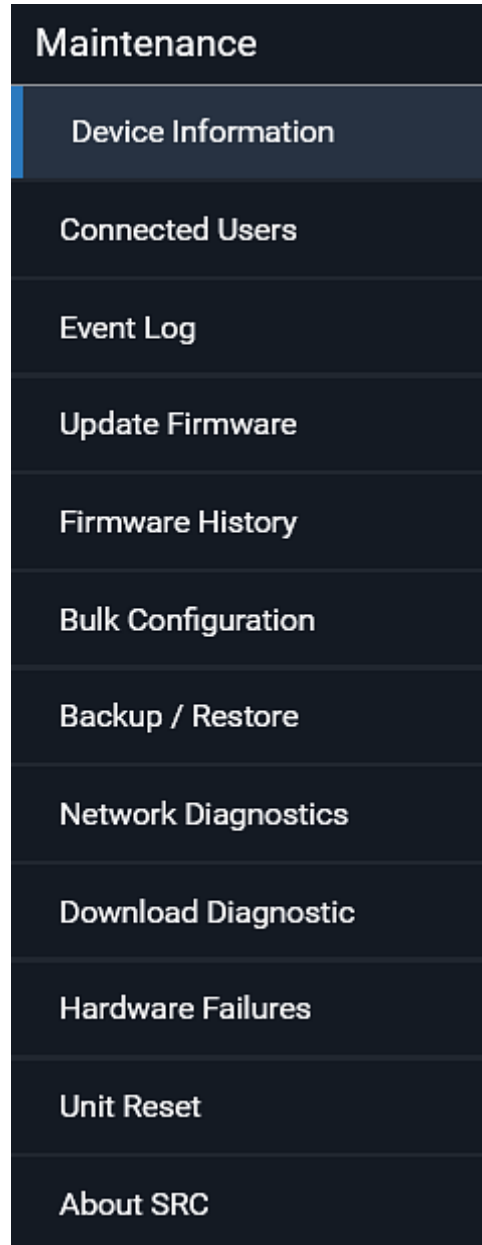
Submenu command	Refer to...
Device Information	*Device Information* (on page 301)

Submenu command	Refer to...
Connected Users	*Viewing Connected Users* (on page 306)
Event Log	*Viewing or Clearing the Local Event Log* (on page 308)
Update Firmware	*Updating the SRC Firmware* (on page 309)
Firmware History	*Viewing Firmware Update History* (on page 312)
Bulk Configuration	*Bulk Configuration* (on page 313)
Backup/Restore	*Backup and Restore of Device Settings* (on page 318)
Network Diagnostic	*Network Diagnostics* (on page 320)
Download Diagnostic	*Downloading Diagnostic Information* (on page 321)
Hardware Failures	*Hardware Issue Detection* (on page 321)
Unit Reset	▪ *Rebooting the SRC* (on page 322) ▪ *Resetting All Settings to Factory Defaults* (on page 323)
About SRC	*Retrieving Software Packages Information* (on page 324)

Device Information

Using the web interface, you can retrieve hardware and software information of components or peripheral devices connected to your SRC.

Tip: If the information shown on this page does not match the latest status, press F5 to reload it.

▶ **To display device information:**

1. Choose Maintenance > Device Information.

Device Information

Information ▲

Model	SRC-0100
Serial number	1TU1231231
Firmware version	3.5.10.5-45603
Board ID	1371234567
Board revision	0x10
PDU2-MIB	download
ASSETMANAGEMENT-MIB	download
LHX-MIB	download

Network ▼

Port Forwarding ▼

Peripheral Devices ▼

Asset Management ▼

2. Click the desired section's title bar to show that section's information. For example, click the Network section.

Network ⌄

The number of available sections is model dependent.

Section title	Information shown
Information	General device information, such as model name, serial number, firmware version, hardware revision, MIB download link(s) and so on. Note that the download link of LHX-MIB is available only after enabling the Schroff LHX/SHX support. See *Miscellaneous* (on page 297).
Network	The network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. This tab also indicates whether the SRC is part of a cascading configuration. See *Identifying Cascaded Devices* (on page 303).
Port Forwarding	If the port forwarding mode is activated, this section will show a list of port numbers for all cascaded devices.
Peripheral Devices	Serial numbers, model names, position and firmware-related information of connected Raritan's environmental sensor packages.
Asset Management	Each asset strip's ID, boot version, application version and protocol version.

Raritan.
A brand of legrand

Identifying Cascaded Devices

For information on how to cascade SRC devices, see *Cascading Multiple SRC Devices for Sharing Ethernet Connectivity* (on page 24).

This section explains how to identify a cascaded device on the Device Information page.

Note: For more information on cascading configurations and restrictions, refer to the Cascading Guide *on the Raritan* **Support page** *(***http://www.raritan.com/support/***)*.

▶ **To identify the cascading status:**

1. Choose Maintenance > Device Information.
2. Click the Network title bar.

Network   ⌄

- ▪ If the information shown on this page does not match the latest status, press F5 to reload it.

▶ **Cascading information in the Bridging mode:**

- The Common section contains two read-only fields for indicating the cascading status. Note that the cascading position is NOT available in the Bridging mode.

Fields	Description
Port forwarding	Indicates the Port Forwarding is disabled. See *Setting the Cascading Mode* (on page 177).
BRIDGE section	Indicates the device is in the Bridging mode and its IP address.
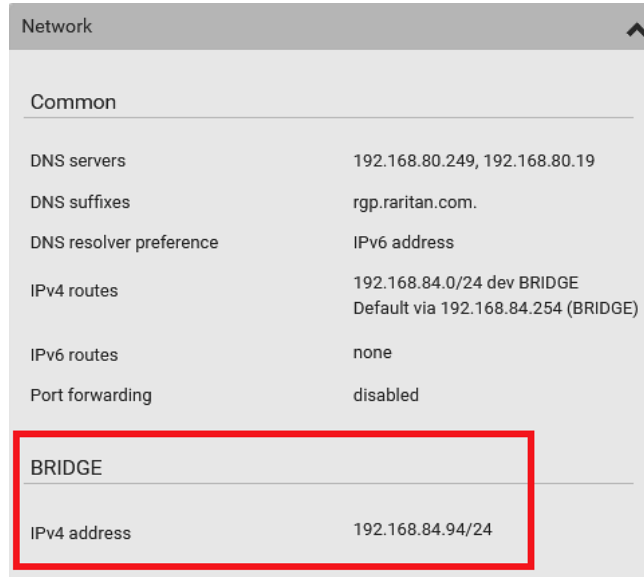
> ▶ **Cascading information in the Port Forwarding mode:**

- The Common section contains three read-only fields for indicating the cascading status.

Fields	Description
Port forwarding	Indicates the Port Forwarding is enabled. See **Setting the Cascading Mode** (on page 177).
Cascade position	Indicates the position of the SRC in the cascading chain. ▪ 0 (zero) represents the master device. ▪ A non-zero number represents a slave device. 1 is Slave 1, 2 is Slave 2, 3 is Slave 3 and so on.
Cascaded device connected	Indicates whether a slave device is detected on the USB-A or Ethernet port. ▪ yes: Connection to a slave device is detected. ▪ no: NO connection to a slave device is detected.

- A master device shows *0* (zero) in the 'Cascade position' field and *yes* in the 'Cascaded device connected' field.

Network ⌃

Common

DNS servers	192.168.80.249, 192.168.80.19
DNS suffixes	rgp.raritan.com.
DNS resolver preference	IPv6 address
IPv4 routes	192.168.84.0/24 dev ETH1 Default via 192.168.84.254 (ETH1)
IPv6 routes	none
Port forwarding	enabled
Cascade position	0 (Master)
Cascaded device connected	yes

- A slave device in the middle position shows a non-zero number which indicates its exact position in the 'Cascade position' field and *yes* in the 'Cascaded device connected' field.

  The following diagram shows 1, indicating it is the first slave device - Slave 1.

Network ⌃

Common

DNS servers	192.168.80.249, 192.168.80.19
DNS suffixes	rgp.raritan.com.
DNS resolver preference	IPv6 address
Port forwarding	enabled
Cascade position	1 (Slave)
Cascaded device connected	yes
IPv4 address	192.168.84.94

- 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 device - Slave 2. The 'Cascaded device connected' field shows *no*, indicating that it is the final one in the chain.

- For a list of port numbers required for accessing each cascaded device in the Port Forwarding mode, click the Port Forwarding title bar on the same page.

Viewing Connected Users

You can check which users have logged in to the SRC and their status. If you have administrator privileges, you can terminate any user's connection to the SRC.

▶ **To view and manage connected users:**

1. Choose Maintenance > Connected Users. A list of logged-in users displays.

If wanted, you can resort the list by clicking the desired column header. See **Sorting a List** (on page 101).

Column	Description
User Name	The login name of each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial RS-232 or USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the SRC. ▪ Web GUI: Refers to the web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user is connected to the CLI. - Serial: The local connection, such as the serial RS-232 or USB connection. - SSH: The SSH connection. - Telnet: The Telnet connection. ▪ Webcam Live Preview: Refers to the live webcam image sessions. See below.
Idle Time	The length of time for which a user remains idle.

2. To disconnect any user, click the corresponding [Disconnect].

    a. Click Disconnect on the confirmation message.

    b. The disconnected user is forced to log out.

▶ **If there are live webcam sessions:**

All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL.

User Name ▲	IP Adress	Client Type	Idle Time	
<webcam>	192.168.84.22	Webcam Live Preview	0 min	Disconnect

The IP address refers to the IP address of the host where the Primary Standalone Live Preview window exists, NOT the IP address of the other two associated sessions.

For more webcam information, see **Webcam Management** (on page 324).

Viewing or Clearing the Local Event Log

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

You can view over 2000 historical events that occurred on the SRC in the local event log. When the log size exceeds 256KB, each new entry overwrites the oldest one.

▶ **To display the local log:**

1. Choose Maintenance > Event Log.

    Each event entry consists of:
    ▪ ID number of the event
    ▪ Date and time of the event
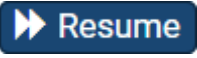
    Tip: The date and time shown on the SRC web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of SRC to your computer or mobile device.

    ▪ Event type
    ▪ A description of the event

2. To view a specific type of events only, select the desired event type in the 'Filter event class' field.

3. The log is refreshed automatically at a regular interval of five seconds. To avoid any new events' interruption during data browsing, you can suspend the automatic update by clicking **Ⅱ Pause**.

    ▪ To restore automatic update, click **▶▶ Resume**. Those new events that have not been listed yet due to suspension will be displayed in the log now.

▶ **To clear the local log:**

1. Click **🗑 Clear Log** on the top-right corner.
2. Click Clear Log on the confirmation message.

Updating the SRC Firmware

Firmware files are available on Raritan website's **Support page** (*http://www.raritan.com/support/*).

You must be the administrator or a user with the Firmware Update permission to update the SRC firmware.

Before starting the upgrade, read the release notes downloaded from Raritan website's **Support page** (*http://www.raritan.com/support/*). If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Note that firmware upgrade via iOS mobile devices, such as iPad, requires the use of iCloud Drive or a file manager app.

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

▶ **Firmware upgrade restriction:**

- **If connecting to an existing Raritan cascading CHAIN:**

  If you are connecting SRC to an existing cascading chain comprising non-SRC Raritan products, you may have to upgrade the existing chain first. See **Upgrade Guidelines for Existing Cascading Chains** (on page 310).

▶ **To update the firmware:**

1. Choose Maintenance > Update Firmware.

2. Click [Browse...] to select an appropriate firmware file.

3. Click Upload. A progress bar appears to indicate the upload process.

4. Once complete, information of both installed and uploaded firmware versions as well as compatibility and signature-checking results are displayed.

   - If anything is incorrect, click Discard Upload.

5. To proceed with the update, click Update Firmware.

   Warning: Do NOT power off the SRC during the update.

6. During the firmware update:

   - A progress bar appears on the web interface, indicating the update status.

   - The front panel display shows the firmware upgrade message. See **Showing the Firmware Upgrade Progress** (on page 87).

   - No users can successfully log in to the SRC.

   - Other users' operation, if any, is forced to suspend.

7. When the update is complete, the SRC resets, and the Login page re-appears.

▪ Other logged-in users are logged out when the firmware update is complete.

Important: If you are using the SRC 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 346).**

▶ **Alternatives:**

To use a different method to update the firmware, refer to:

- *Firmware Update via SCP* (on page 500)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 527)
- *Firmware Upgrade via USB* (on page 525)

Upgrade Guidelines for Existing Cascading Chains

You must obey the following guidelines when upgrading a chain. Otherwise, a networking issue occurs.

- Firmware version 3.3.10 or later is NOT compatible with pre-3.3.10 firmware versions in terms of the cascading feature so all Raritan devices in the cascading chain must run version 3.3.10 or later.

  Alternative: You can also choose to have the USB-cascading chain comprising Raritan devices run any pre-3.3.10 firmware. The disadvantage is that you will not benefit from the latest software enhancements and features.

- To upgrade an existing Raritan USB-cascading chain from a firmware version older than 3.3.10, you must start from the last slave device and so on until the master device. See *Upgrade Sequence in an Existing Cascading Chain* (on page 310).

Upgrade Sequence in an Existing Cascading Chain

Depending on the firmware version(s) of your cascading chain, there may or may not be limitations for the firmware upgrade sequence in the chain.

▶ **Upgrade from "pre-3.3.10" to 3.3.10 or post-3.3.10:**

You must follow the firmware upgrade sequence below to upgrade a cascading chain from a firmware version older than 3.3.10 to version 3.3.10 or later. If you do not follow this upgrade sequence, you will not be able to access some cascaded devices over the Internet.

- The upgrade must start from the last slave device (S), then the second to last, the third to last, and so on until the master device (M).

  Red numbers below represent the appropriate upgrade sequence. 'N' is the final one to upgrade.

- You must upgrade ALL devices in the chain to 3.3.10 or later. If you upgrade only some devices in the chain, networking issues occur on some cascaded devices.

Exception: A few products, such as SRC, are developed much later so they may not support older firmware versions, such as 3.5.0, 3.4.0, and so on. Therefore, it is suggested to AVOID downgrading your cascading chain unless instructed by Raritan or Legrand Technical Support. For minimum firmware versions, see Cascading Restrictions in the Cascading Guide on the **Support page** *(***http://www.raritan.com/support/***).*

▶ **Upgrade from 3.3.10 or post-3.3.10 to post-3.3.10:**

There is no upgrade sequence limitation.

Firmware version 3.3.10 is compatible with later firmware versions so you can upgrade all devices of the chain in a random order.

Important: Raritan does not guarantee that no upgrade sequence limitation will be required for all future firmware versions. It is highly suggested to check the latest revision of the Cascading Guide or your product's User Guide/Online Help before performing the firmware upgrade. The other alternative is to always stick to the same sequence as the above diagram.

▶ **Downgrade from 3.3.10 to pre-3.3.10:**

There is no downgrade sequence limitation. However, firmware downgrade in a cascading chain is NOT recommended. Consult Raritan (or Legrand) Technical Support first if downgrade is needed.

Firmware versions earlier than 3.3.10 are compatible with any pre-3.3.10 version so you can downgrade or upgrade all devices of the chain in a random order when all firmware versions in the chain are prior to version 3.3.10.

Note: It is suggested to always stick to the same sequence as the above diagram though there is no firmware downgrade limitation.

Full Disaster Recovery

For SRC, disaster recovery can be performed via the USB connection only.

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

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7/10 and Linux. In addition, an appropriate SRC firmware file is required in the recovery procedure.

Viewing Firmware Update History

The firmware upgrade history is permanently stored on the SRC. It remains available even though you perform a device reboot or any firmware update.

▶ **To view the firmware update history:**

1. Choose Maintenance > Firmware History.

   Each firmware update event consists of:

   ▪ Update date and time

   ▪ Previous firmware version

   ▪ Update firmware version

   ▪ Update result

2. If wanted, you can resort the list by clicking the desired column header. See *Sorting a List* (on page 101).

Bulk Configuration

The Bulk Configuration feature lets you save generic settings of a configured SRC device to your computer. You can use this configuration file to copy common settings to other SRC devices of the same model and firmware version.

A source device is the SRC device where the configuration file is downloaded/saved. A target device is the SRC device that loads the configuration file.

By default the configuration file downloaded from the source device contains settings based on the built-in bulk profile. The built-in bulk profile defines that all settings should be saved except for device-specific settings.

You can decide which settings are downloaded and which are not by creating your own bulk configuration profile.

Note that "device-specific" settings, such as the device's IP address or environmental sensor settings, will never be included into any profile you will create so they will never be downloaded from any source device. See *Device-Specific Settings* (on page 637).

When the date and time settings are included in the bulk configuration file, exercise caution when distributing that file to target devices located in a different time zone than the source device.

Tip: To back up or restore "all" settings, including device-specific ones, use the Backup/Restore feature instead. See **Backup and Restore of Device Settings** *(on page 318).*

▶ **Main bulk configuration procedure:**

1. If you prefer customizing the bulk configuration file, create your own bulk configuration profile(s) first. See *Customizing Bulk Configuration Profiles* (on page 314).

2. Perform the bulk configuration operation, which includes the following steps. For details, see *Performing Bulk Configuration* (on page 316).

   a. Make sure the desired bulk configuration profile has been selected on the source device.

   b. Save a bulk configuration file from the source device.

   c. Perform bulk configuration on one or multiple target devices.

Note: On startup, SRC performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

▶ **The last configuration-copying record:**

If you once copied any bulk configuration or device backup file to the SRC, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last restore: 3/16/2019, 10:11:03 AM UTC+0800, status: OK

Tip: The date and time shown on the SRC web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of SRC to your computer or mobile device.

▶ **Alternatives:**

To use a different bulk configuration method, refer to:

- *Bulk Configuration via SCP* (on page 501)
- *Bulk Configuration or Firmware Upgrade via DHCP/TFTP* (on page 527)
- *Configuration or Firmware Upgrade with a USB Drive* (on page 513)
- *Raw Configuration Upload and Download* (on page 550)

Tip: Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure device-specific settings with the upload of raw configuration but not with the 'bulk configuration' file.

Customizing Bulk Configuration Profiles

A bulk profile defines which settings are downloaded/saved from the source device and which are not. The default is to apply the built-in bulk profile, which downloads all settings from the source device except for device-specific data.

If the built-in profile does not meet your needs, you can create your own profile(s), and then apply the wanted profile before downloading/saving any settings from the source device.

▶ **To create new bulk profile(s):**

1. Log in to the source SRC, whose settings you want to download.
2. Choose Maintenance > Bulk Configuration.
3. Click ➕ in the Bulk Profiles section.
4. In the 'Profile name' and 'Description' fields, enter information for identifying the new profile.

5. To make this new profile the default one for future bulk configuration operations, select the 'Select as default profile' checkbox.

    ▪ After setting any profile as the default, the original default profile will no longer function as the default one.

6. Now decide which settings are wanted and which are not.

    a. Click ▼ of the setting which you want to configure.

    b. When the pop-up menu appears, select one of the options.

    Note that the two options 'Inherited' and 'Built-in' are mutually exclusive.

Option	Description
Excluded	The setting will *not* be downloaded.
Included	The setting will be downloaded.
Inherited	The setting will follow its parent setting (that is, the upper-level setting). ▪ If you select 'Excluded' for its upper-level setting, this setting will be also excluded. ▪ If you select 'Included' for its upper-level setting, this setting will be also included. The option inherited from its parent setting will be enclosed in parentheses.
Built-in	The setting will follow the same setting of Raritan's built-in profile. ▪ If 'Excluded' is selected in the built-in profile, this setting will be also excluded. ▪ If 'Included' is selected in the built-in profile, this setting will be also included. The option inherited from the built-in profile will be enclosed in parentheses. *Note: The option 'Built-in' is available in those settings whose corresponding settings in the built in profile have been set to a non-inherited option -- Excluded or Included.*

7. Click Save.
8. Repeat the same steps if you want to create more bulk profiles.

Performing Bulk Configuration

On the source device, make sure the wanted profile has been set as the default one. If not, start from step 1 below. If yes, go to step 2 directly.

▶ **Step 1: Select the desired bulk configuration profile (optional)**

1. Log in to the source SRC, whose settings you want to copy.
2. Choose Maintenance > Bulk Configuration.
3. Click on the row of the wanted profile to open the Edit Bulk Profile page.
4. Select the 'Select as default profile' checkbox.
5. Click Save.

▶ **Step 2: Save a bulk configuration file**

You must have the Administrator Privileges or "Unrestricted View Privileges" to download the configuration.

1. Log in to the source SRC if you have not yet.
2. Choose Maintenance > Bulk Configuration.
3. Check the 'Bulk format' field. If the chosen value does not match your need, change it.

Option	Description
Encrypted	▪ Partial content is base64 encoded. ▪ Its content is encrypted using the AES-128 encryption algorithm. ▪ The file is saved to the TXT format
Cleartext	▪ Content is displayed in clear text. ▪ The file is saved to the TXT format.

4. Click Download Bulk Configuration.
5. When prompted to open or save the configuration file, click Save.

> ▶ **Step 3: Perform bulk configuration**

You must have the Administrator Privileges to upload the configuration.

1. Log in to the target SRC, which is of the same model and runs the same firmware as the source SRC.
2. Choose Maintenance > Bulk Configuration.
3. Click [Browse...] to select the configuration file.
4. Click 'Upload & Restore Bulk Configuration' to copy it.
5. A message appears, prompting you to confirm the operation and enter the admin password.

   Enter the admin password, and click Restore.
6. Wait until the SRC resets and the login page re-appears.

> ▶ **Alternatives:**

To use a different bulk configuration method, refer to:

- ***Bulk Configuration via SCP*** (on page 501)
- ***Bulk Configuration or Firmware Upgrade via DHCP/TFTP*** (on page 527)
- ***Configuration or Firmware Upgrade with a USB Drive*** (on page 513)
- ***Raw Configuration Upload and Download*** (on page 550)

Tip: Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure device-specific settings with the upload of raw configuration but not with the 'bulk configuration' file.

Modifying or Removing Bulk Profiles

You can modify or remove any bulk profile except for the built-in one.

Note that a profile that has been set as the default cannot be removed, either. To remove it, you have to remove its default setting first.

Choose Maintenance > Bulk Configuration. A list of profiles displays and then do one of the following.

> ▶ **To modify an existing profile:**

1. Click on the row of the wanted profile in the list.
2. Change the settings you want.
3. Click Save.
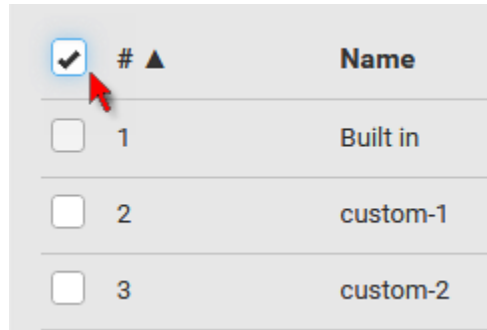
> ▶ **To remove a single profile:**

1. Click on the row of the wanted profile.

2. Click on the top-right corner.

3. Click Delete on the confirmation message.

▶ **To remove one or multiple profiles:**

1. Click to make checkboxes appear in front of profiles.

2. Select one or multiple profiles.

   ▪ To select ALL profiles, select the topmost checkbox in the header row.

3. Click on the top-right corner.

4. Click Delete on the confirmation message.

Backup and Restore of Device Settings

Unlike the bulk configuration file, the backup file contains ALL device settings, including device-specific data like device names and all network settings. To back up or restore the settings of SRC, you should perform the Backup/Restore feature.

All SRC information is captured in the plain-TEXT-formatted backup file except for the device logs and TLS certificate.

Note: To perform bulk configuration among multiple SRC devices, use the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 313).*

▶ **To download a backup SRC file:**

You must have the Administrator Privileges or "Unrestricted View Privileges" to download a backup file.

1. Choose Maintenance > Backup/Restore.

2. Check the 'Backup format' field. If the chosen value does not match your need, change it.

Option	Description
Encrypted	▪ Partial content is base64 encoded. ▪ Its content is encrypted using the AES-128 encryption algorithm. ▪ The file is saved to the TXT format
Cleartext	▪ Content is displayed in clear text. ▪ The file is saved to the TXT format.

3. Click Download Device Settings. Save the file onto your computer.

▶ **To restore the SRC using a backup file:**

You must have the Administrator Privileges to restore the device settings.

1. Choose Maintenance > Backup/Restore.

2. Click [Browse...] to select the backup file.

3. Click 'Upload & Restore Device Settings' to upload the file.

   ▪ A message appears, prompting you to confirm the operation and enter the admin password.

4. Enter the admin password, then click Restore.

5. Wait until the SRC resets and the Login page re-appears, indicating that the restore is complete.

Note: On startup, SRC performs all of its functions, including event rules and logs, based on the new configuration you have copied instead of the previous configuration prior to the device reset. For example, the "Bulk configuration copied" event is logged only when the new configuration file contains the "Bulk configuration copied" event rule.

▶ **The last configuration-copying record:**

If you once copied any bulk configuration or device backup file to the SRC, the last record similar to the following is displayed at the bottom of both the Bulk Configuration and Backup/Restore pages.

Last restore: 3/16/2019, 10:11:03 AM UTC+0800, status: OK

▶ **Alternative:**

To use a different method to perform backup/restore, refer to:

- *Backup and Restore via SCP* (on page 502)

Network Diagnostics

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

- Ping: The tool is useful for checking whether a host is accessible through the network or Internet.
- Trace Route: The tool lets you find out the route over the network between two hosts or systems.
- List TCP Connections: You can use this function to display a list of TCP connections.

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 495).*

Choose Maintenance > Network Diagnostics, and then perform any function below.

▶ **Ping:**

1. Type values in the following fields.

Field	Description
Network host	The name or IP address of the host that you want to check.
Number of requests	A number up to 20. This determines how many packets are sent for pinging the host.

2. Click Run Ping to ping the host. The Ping results are then displayed.

▶ **Trace Route:**

1. Type values in the following fields.

Field/setting	Description
Hostname	The IP address or name of the host whose route you want to check.
Timeout(s)	A timeout value in seconds to end the trace route operation.
Use ICMP packets	To use the Internet Control Message Protocol (ICMP) packets to perform the trace route command, select this checkbox.

2. Click Run. The Trace Route results are then displayed.

▶ **List TCP Connections:**

1. Click the List TCP Connections title bar to show the list.

Downloading Diagnostic Information

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

You can download the diagnostic file from the SRC 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 >

    .

2. The system prompts you to save or open the file. Save the file then.

3. E-mail this file as instructed by Raritan Technical Support.

Hardware Issue Detection

This page lists any internal hardware issues SRC has detected, including current events and historical records.

Choose Maintenance > Hardware Failures, and the page similar to either of the following diagrams opens.

▶ **NO hardware failures detected:**

▶ **Hardware failure(s) detected:**

Current Hardware Failures			
Failure Message	Last Asserted ▲	Last Deasserted	Number of Occurrences
I2C bus 0 is stuck.	1/1/2018, 1:18:24 AM UTC+0100	1/1/2018, 1:00:00 AM UTC+0100	17

Past Hardware Failures			
Failure Message	Last Asserted ▲	Last Deasserted	Number of Occurrences
Network device ETH was not detected.	8/3/2018, 3:06:46 PM UTC+0200	8/3/2018, 3:13:10 PM UTC+0200	7

▶ **Hardware Failure alerts on the Dashboard page:**

Note that *current* hardware failure events, if any, will also display on the **Dashboard** (on page 102).

▶ **Hardware failure types:**

Hardware issues	Description
Network device not detected	A specific networking interface of SRC is NOT detected.
I2C Bus stuck	A specific I2C bus is stuck, which affects the communication with sensors.

Rebooting the SRC

You can remotely reboot the SRC via the web interface.

Warning: Rebooting the SRC deletes all webcam snapshots that are saved onto the SRC locally. If needed, download important snapshots before rebooting the device. See **Viewing and Managing Locally-Saved Snapshots** (on page 331).

▶ **To reboot the device:**

1. Choose Maintenance > Unit Reset > [Reboot Unit].
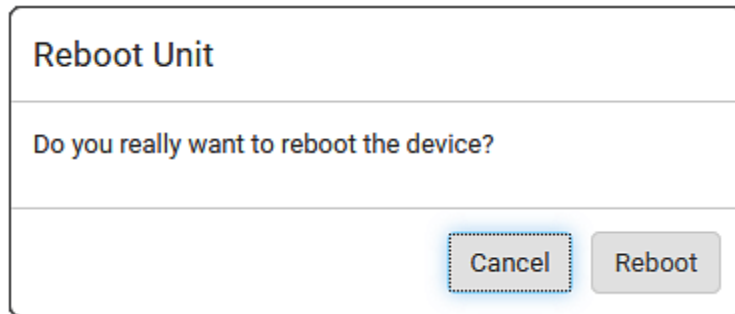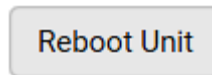
2. Click Reboot to restart the SRC.
3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the restart is complete, the login page opens.

Tip: If you are not redirected to the login page after the restart is complete, click the text "this link" in the countdown message.

Resetting All Settings to Factory Defaults

You must have the Administrator Privileges to reset all settings of the SRC to factory defaults.

Important: Exercise caution before resetting the SRC to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only firmware upgrade history is retained.

▶ **To reset the device to factory defaults:**

1. Choose Maintenance > Unit Reset > ![Reset to Factory Defaults].

2. Type your password and then click Factory Reset to reset the SRC to factory defaults.

3. A message appears, with a countdown timer showing the remaining time of the operation. It takes about two minutes to complete.

4. When the reset is complete, the login page opens.

Tip: If you are not redirected to the login page after the reset is complete, click the text "this link" in the countdown message.

▶ **Alternative:**

There are two more methods to reset the device to factory defaults.

*   Use the "mechanical" reset button
*   Perform the CLI command

For details, see **Resetting to Factory Defaults** (on page 556).

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the SRC through the web interface.

▶ **To retrieve the embedded software packages information:**

1. Choose Maintenance > About SRC. A list of open source packages is displayed.

2. You can click any link to access related information or download any software package.

Webcam Management

The 'Webcams' menu item appears when there is any webcam(s) connected to the SRC, or when there are snapshots saved onto the SRC already. See *Connecting a Logitech Webcam* (on page 63).
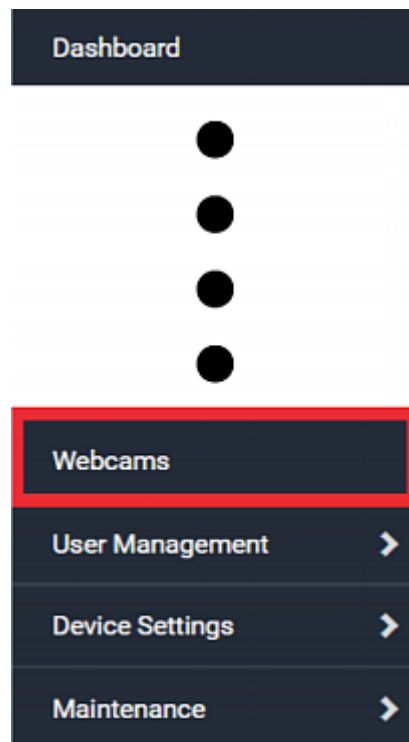
With a Logitech® webcam connected to the SRC, you can visually monitor the environment around the SRC via snapshots or videos captured by the webcam.

▶ **Permissions required:**

To do...	Permission(s) required
View snapshots and videos	Either permission below: ▪ Change Webcam Configuration ▪ View Webcam Snapshots and Configuration
Configure webcam settings	Change Webcam Configuration

▶ **Additional webcam-related actions you can take:**

Action	Refer to
Manually store snapshots taken from the webcam onto the SRC or a remote server	▪ *Configuring Webcams and Viewing Live Images* (on page 326) ▪ *Changing Storage Settings* (on page 333)
Send a snapshot or video session's link to other people via email or instant message	*Sending Links to Snapshots or Videos* (on page 329)
Create event rules to trigger emails containing snapshots from a webcam	*Available Actions* (on page 238)

For more information on your Logitech webcam, refer to the user documentation accompanying it.

Configuring Webcams and Viewing Live Images

To configure a webcam or view live snapshot/video sessions, choose Webcams in the **Menu** (on page 98). Then click the desired webcam to open that webcam's page.

Note that default webcam names are determined by the detection order. The one that is detected first is named *Webcam*, and the other that is detected later is named *Webcam 2*.

The Webcam page consists of three sections -- *Live Preview*, *Image Controls* and *Settings*.
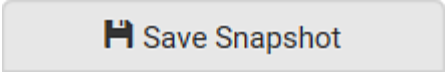
▶ **Live Preview:**

1. By default the Live Preview section is opened, displaying the live snapshot/video session captured by the webcam.

    ▪ The default is to show live snapshots. Interval time and capture date/time of the image are displayed on the top of the image.

Tip: The date and time shown on the SRC web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of SRC to your computer or mobile device.

2. To save the current image onto SRC or a remote server, click

H Save Snapshot .

- The default storage location for snapshots is the SRC device. To save them onto a remote server, see **Changing Storage Settings** (on page 333).
- To download an image onto your computer, move your mouse to that image, right click on it, and choose Save Image As.

3. To have the same live session displayed in a separate window, click

New Live Preview Window .

- A separate window appears, which is called the Primary Standalone Live Preview window in this User Guide.
- You can send out this window's URL to share the live image with others. See **Sending Links to Snapshots or Videos** (on page 329).

Note: Make sure your browser does not block the pop-up window, or the separate window does not show up.

4. To switch between snapshot and video modes, refer to the *Settings* section below.

- In the video mode, the number of frames to take per second (fps) and the video capture date/time are displayed on the top of the image.
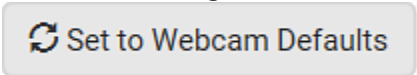
▶ **Image Controls:**

1. Click the Image Controls title bar to expand it.

Image Controls

2. Adjust the brightness, contrast, saturation and gain by modifying their values or adjusting the corresponding slide bar.

- To customize the gain value, you must deselect the Auto Gain checkbox first.
- To restore all settings to this webcam's factory defaults, click

C Set to Webcam Defaults .

▶ **Settings:**

1. By default the Settings section is open. If not, click the Settings title bar.

2. Click Edit Settings.

3. Enter a name for the webcam. Up to 64 ASCII printable characters are supported.

   ▪ If configured to store snapshots on a *remote* server, the webcam's name determines the name of the folder where snapshots are stored. See **Changing Storage Settings** (on page 333) and **Identifying Snapshots Folders on Remote Servers** (on page 335).

   ▪ It is suggested to customize a webcam's name "prior to" saving snapshots on the remote server. In case you change the webcam's name after saving any snapshots, SRC will create a new folder with the new webcam name while keeping the old folder with the old name.

4. Type the location information in each location field as needed. Up to 63 ASCII printable characters are supported.

   ▪ Note that the location data you enter is not available in those snapshots stored on remote servers.

   Tip: If the webcam's location is important, you can customize the webcam's name based on its location when configuring SRC to save snapshots onto a remote server.

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.

Mode	Description
Video	The webcam enters the video mode. ▪ Set the 'Framerate' (frames per second) as needed.
Snapshot	The webcam shows static images captured by the webcam at a regular interval. ▪ To determine the interval, set the 'Time Between Snapshots' (seconds) as needed.

7. Click Save. The changes made to the settings are applied to the live session in the above *Live Preview* section immediately.

► **To return to the Webcam Management page:**

● Click Webcam Management on the top of the page.
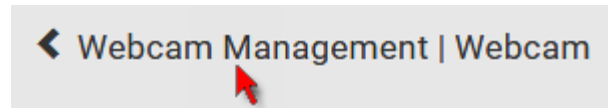
● Or click Webcams again in the **Menu** (on page 98).

Sending Links to Snapshots or Videos

When opening a Primary Standalone Live Preview window, a unique URL is generated for this window session. You can email or instant message this URL to as many people as possible as long as your system resources permit. Recipients can then click on the provided link and view live snapshots or videos simultaneously in the Secondary Standalone Live Preview window(s).

Tip: All Live Preview window sessions sharing the same URL, including one Primary Standalone Live Preview window and multiple Secondary Standalone Live Preview windows, are identified as one single "<webcam>" user in the Connected Users list. You can disconnect a "<webcam>" user to terminate all sessions sharing the same URL. See **Viewing Connected Users** *(on page 306).*

▶ **Best practice:**

1. The sender opens the Primary Standalone Live Preview window, and sends the link to one or multiple recipients.

2. The sender must wait until at least one recipient opens the Secondary Standalone Live Preview window.

3. The recipient(s) should inform the sender that the link has been opened.

4. Now the sender can close the Primary Standalone Live Preview window.
   - For additional information, see *How Long a Link Remains Accessible* (on page 331).

▶ **To send a snapshot or video link via email or instant message:**

1. Choose Webcams in the *Menu* (on page 98).

2. Click the desired webcam to open the Webcam page.
   - Note that default webcam names are determined by the detection order. The one that is detected first is named *Webcam*, and the other that is detected later is named *Webcam 2*.

Webcams			
Name ▲	Location	Resolution	Mode
Webcam		352x288	Snapshot

3. Click **⎘ New Live Preview Window** in the Live Preview section. The live snapshot or video in a standalone window opens. See *Configuring Webcams and Viewing Live Images* (on page 326).

4. Copy the URL from that live preview window.

a. Select the URL shown on the top of the image.
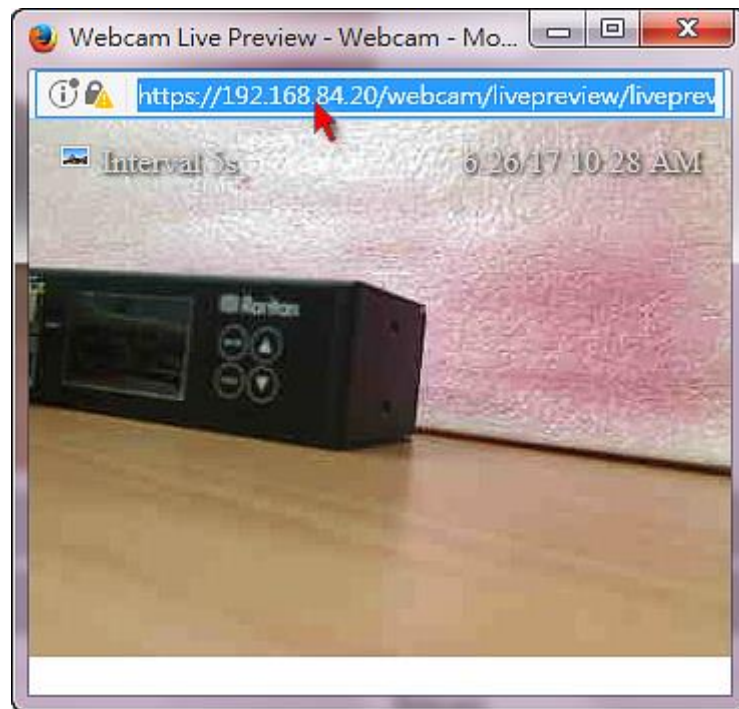
b. Right click to copy the URL, or press CTRL+ C.

5. Send the URL link through an email or instant message application to one or multiple persons.

6. Leave the live preview window open until the recipient(s) opens the snapshot or video via the link.

How Long a Link Remains Accessible

For documentation purposes, the one who opens and sends the URL of the Primary Standalone Live Preview window is called *User A* and the two recipients of the same URL link are called *User B* and *C*.

User C is able to access the snapshot or video image via the link when the URL link remains valid, which can be one of these scenarios:

- The Primary Standalone Live Preview window remains open on User A's computer. If so, even though User A logs out of the SRC or the login session times out, the link remains accessible.
- User B's Secondary Standalone Live Preview window remains open. If so, even though User A already closes the Primary Standalone Live Preview window, the link remains accessible.
- Neither User A's Primary Standalone Live Preview window nor User B's Secondary Standalone Live Preview window remains open, but it has not exceeded two minutes yet after the final live preview window session was closed.

Note: The link is no longer valid after two minutes since the final live preview window is closed.

Viewing and Managing Locally-Saved Snapshots

This section describes the operation for snapshots saved onto the SRC device only. To access snapshots saved onto remote servers, you must use appropriate third-party applications, such as an FTP client, to access them.

When saving a snapshot, it is stored locally on the SRC device by default. For snapshot-saving operations, see *Configuring Webcams and Viewing Live Images* (on page 326).

Up to 10 snapshots can be stored onto the SRC. The oldest snapshot is automatically overridden by the newest one when the total of snapshots exceeds 10, if no snapshots are deleted manually.
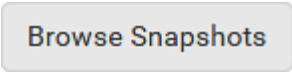
When there are more than one webcam connected, then the oldest snapshot of the webcam "with the most snapshots" is overridden.

Tip: To save more than 10 snapshots, you must change the storage location from the SRC to an FTP or Common Internet File System (CIFS)/Samba server. See **Changing Storage Settings** *(on page 333).*

Snapshots are saved as JPG files, and named based on the sequential numbers, such as *1.jpg*, *2.jpg*, *3.jpg* and the like.

Warning: Rebooting the SRC deletes all webcam snapshots that are saved onto the SRC locally. If needed, download important snapshots before rebooting the device.

▶ **To view saved snapshots:**

1. Choose Webcams > [Browse Snapshots] . The Snapshots page opens.

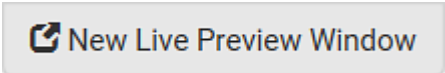2. Click the snapshot you want to view from the list.

Tip: The date and time shown on the SRC web interface are automatically converted to your computer's time zone. To avoid time confusion, it is suggested to apply the same time zone settings as those of SRC to your computer or mobile device.

3. The selected snapshot as well as its information, such as captured time and resolution, is displayed on the same page.

4. If the latest saved snapshot is not listed yet, click [icon].

▶ **To manually delete any snapshots:**

1. Click [icon] to make checkboxes appear.

2. Select the checkboxes of the images you want to remove.

   ▪ To select all images, select the topmost checkbox in the header row.

Raritan.
A brand of ⬛legrand®

3. On the top of the list, click ♻.

4. Click Delete on the confirmation message.

▶ **To download any image onto the computer:**

- To download an image onto your computer, move your mouse to that image, right click on it, and choose Save Image As.

Changing Storage Settings

Important: The SRC web interface only lists the snapshots stored locally on the SRC device, but does NOT list those saved onto remote servers. You must launch appropriate third-party applications, such as an FTP client, to access and manage the snapshots stored on remote servers.

The default is to store snapshots onto the SRC device, which has a limitation of 10 snapshots. Note that any operation involving device reboot will remove the snapshots saved on the SRC, such as firmware upgrade.

If you have either or both needs below, you must save snapshots onto a remote server like FTP or CIFS/Samba, instead of the SRC.

- Total number of saved snapshots will exceed 10.

- Saved snapshots must be stored *permanently*, or at least should *not* be removed by the SRC device's reboot.

▶ **To configure the storage settings:**

1. Choose Webcams > Edit Settings.

Snapshot Storage		
		Edit Settings
Storage Type	Local	
	Browse Snapshots	

2. Click the Storage Type field to select the desired storage location and configure as needed.

   Note: When entering user credentials for remote servers, make sure the user credentials you enter have the write permission, or NO snapshots can be successfully saved onto remote servers.

Storage location	Description
Local	'Local' means the SRC. This is the default. ▪ It can store a maximum of 10 snapshots only. ▪ The web interface can list and display all snapshots stored on the SRC. See **Viewing and Managing Locally-Saved Snapshots** (on page 331). ▪ All snapshots are CLEARED when the SRC is rebooted.

CIFS/Samba	Snapshots are saved onto a Common Internet File System/Samba.
	▪ Total number of saved snapshots depends on the server's capacity.
	▪ All saved snapshots remain available after rebooting the SRC.
	▪ Configure the following fields:
	  * *Server* - the desired CIFS/Samba server
	  * *Share/folder* - this is the share drive/folder
	  * *Username* - for server access
	  * *Password* - for server access

FTP	Snapshots are saved onto a FTP server.
	▪ Total number of saved snapshots depends on the server's capacity.
	▪ All saved snapshots remain available after rebooting the SRC.
	▪ Configure the following fields:
	  * *Server URL* - the FTP server's path
	  * *Username* - for server access
	  * *Password* - for server access

To find where the snapshots are saved on CIFS/Samba or FTP, see **Identifying Snapshots Folders on Remote Servers** (on page 335).

3. Click Save.

Warning: Before disconnecting or powering off any remote server where the webcam snapshots are being stored, you must first change the storage settings, or the connectivity issue of the remote server may degrade the performance of the SRC web interface. If this issue occurs, first restore the connectivity of the remote server and then change the storage settings of the webcam snapshots.

▶ **Tip for notifications showing the snapshots path on FTP:**

If you are using SNMP to retrieve SRC data, you can make SRC automatically send a notification containing the full path or URL to the snapshots saved onto FTP with this SNMP code: `webcamStorageUploadStarted`.

Identifying Snapshots Folders on Remote Servers

If saving snapshots onto a remote server, you can access those snapshots via an appropriate third-party application, such as an FTP client.

All snapshots are saved as JPEG and named according to the date and time when saving the snapshots. Note that the date and time of the filename are based on the time zone of the SRC rather than that of the computer or mobile device you are operating.

Tip: To check the time zone of your SRC, choose Device Settings > Date/Time. See **Setting the Date and Time** *(on page 220).*

The structure of a snapshots folder looks similar to the diagram below.
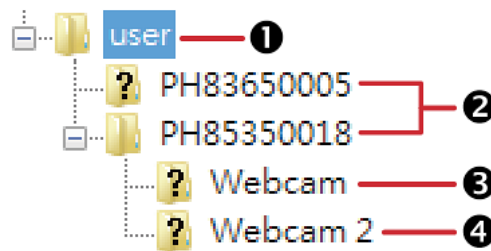
Number	Folder name description
❶	User-defined parent directory, whose name depends your server settings, such as your FTP configuration.
❷	Serial number of your SRC device where the webcam is connected. For example, *PH85350018*. ▪ To find your SRC serial number, see **Device Information** (on page 301).

Number	Folder name description
❸	The name of the webcam that your SRC detects first.
	This is the folder where the snapshots captured by the first webcam are stored.
	▪ The first webcam's default name is "Webcam".
	▪ You can customize the webcam's name, which will change the snapshots folder's name.
	See **Configuring Webcams and Viewing Live Images** (on page 326).
	▪ If the webcam's location is important, you can customize the webcam's name based on its location when configuring SRC to save snapshots onto a remote server.
❹	The name of the webcam that your SRC detects later, if an additional webcam is connected.
	This is the folder where the snapshots captured by the second webcam are stored.
	▪ The second webcam's default name is "Webcam 2".
	▪ Changing this webcam's name also changes the second snapshots folder's name.
	▪ If the webcam's location is important, you can customize the webcam's name based on its location when configuring SRC to save snapshots onto a remote server.

Note: It is suggested to customize a webcam's name "prior to" saving snapshots on the remote server. In case you change the webcam's name after saving any snapshots, SRC will create a new folder with the new webcam name while keeping the old folder with the old name.

Raritan.
A brand of legrand

SmartLock and Card Reader

SmartLock and Card Reader pages show up in the *Menu* (on page 98) in either scenario below:

- Your SRC is a model with onboard door handle ports. Such a model contains a built-in DX2-DH2C2 module. For example, SRC-0102.
- Your SRC does not have onboard door handle ports, such as SRC-0100, but you have purchased Raritan's SmartLock kit with "DX2-DH2C2" and connected it to your SRC.

Note: For more information on DX2-DH2C2, such as its hardware installation, refer to the SmartLock Quick Setup Guide accompanying the SmartLock kit, **Connecting Door Handles or a SmartLock Kit** *(on page 41), or 'Environmental Sensors and Actuators Guide' (or its Online Help version) on the Raritan* **Support page** *(***http://www.raritan.com/support/***).*
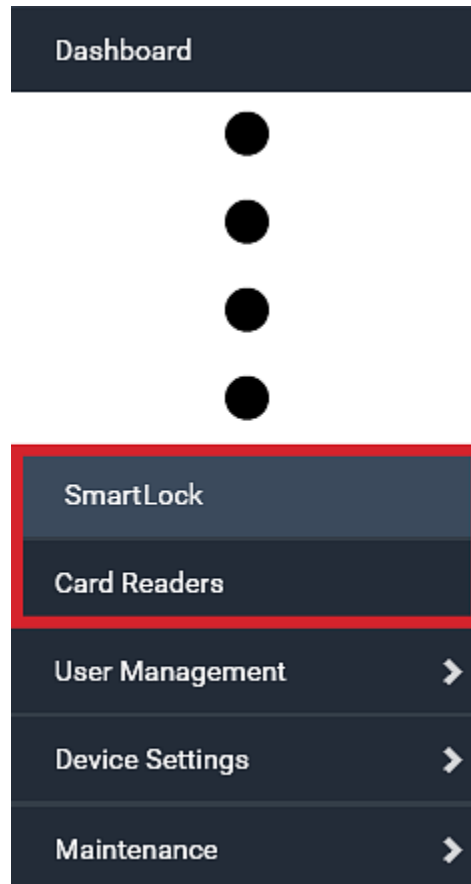
Note that "SmartLock" appears only when your door handles are connected to SRC via **DX2-DH2C2**, but "Card Readers" appears as long as SRC detects the presence of any card reader -- either a standalone USB card reader or a card reader integrated with the door handles.

▶ **"SmartLock" page:**

- Shows the information of all door handle controllers (that is, DX2-DH2C2 modules) attached to SRC.
- Shows the status of the door handle-integrated card readers connected to DX2-DH2C2.

    Note: Data of "external" USB card readers is NOT shown on the SmartLock page. It is shown on the Card Readers page instead.

- You can control the door handles on this page. See *SmartLock* (on page 339).

▶ **"Card Readers" page:**

- Shows the information of all card readers connected to SRC, including:
    - Door handle-integrated card readers connected to the DX2-DH2C2 module.
    - External USB card readers connected to the USB-A port of SRC.
- See *Card Readers* (on page 344).

SmartLock

To open the SmartLock page, choose SmartLock in the **Menu** (on page 98).

The page shows information of all DX2-DH2C2 modules attached to SRC, including its serial number, position and its door handle configuration.

On this page you can:

- View the status of the cabinet door and card reader.

    Note: Data of "external" USB card readers is NOT shown on the SmartLock page. It is shown on the Card Readers page instead.

- Configure the door handles connected to DX2-DH2C2. You must set this because SRC cannot detect the types of connected door handles.
- Control the door handles connected to DX2-DH2C2.

▶ **To configure the door handles:**

There are two door handle sections per DX2-DH2C2 because a DX2-DH2C2 has two door handle ports. Before you configure the connected door handle(s), a lock icon is displayed on each door handle section's top-right corner, and both the Door State and Card Reader sections are unavailable.
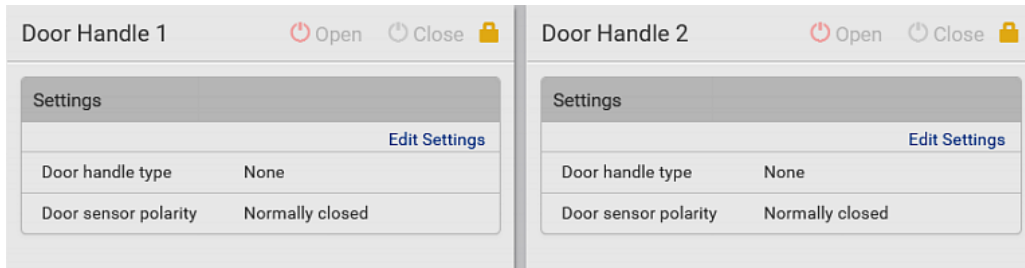
1. Click Edit Settings in the Settings section.
2. In the 'Door handle type' field, select the door handle type you are using.
   - If your specific Southco H3-EM model is listed, select it. For all other supported Southco H3-EM models, select "Southco H3-EM".
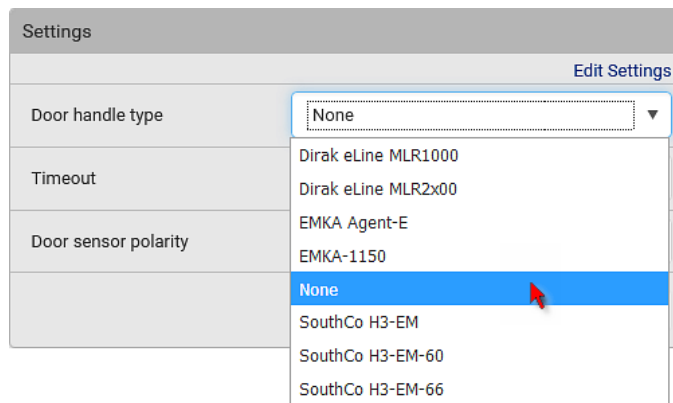
3. Make changes to the remaining fields as needed.

Section	Description
Timeout	▪ Specify how long the **door handle lock** can remain open after someone opens the door handle via a smart card or via remote control using the software. When the timeout expires, the door handle lock will be automatically closed. Default is 600 seconds (that is, 10 minutes).
Door sensor polarity	Choose the correct setting based on the type of contact closure sensors used to monitor the door: ▪ *Normally closed:* The contact is closed (conducting) when the door is closed and open (not conducting) when the door is open. This is the default. ▪ *Normally open:* The contact not conducting when the door is closed and conducting when the door is open. ▪ **Note:** For both normally closed and normally open sensors, the reported state is "alarmed" when the door is open and "normal" when the door is closed.

4. Click Save.

Door Handle Status and Control

After configuring the door handle type properly, two more sections are shown for the configured door handle -- **Door State** and **Card Reader**.

▶ **To view the status of the door and card reader:**

Section	Description
Door State	Shows all sensor states detected by DX2-DH2C2, including: ▪ *Door*: States of contact closure sensors connected to DX2-DH2C2. Contact closure sensors detect whether the door is physically opened or closed. ▪ *Door Lock*: States of door locks integrated with the door handles. ▪ *Door Handle Lock*: States of the door handle locks. Door locks and door handle locks are interrelated so their states are changed one after another. The door handle lock is opened first and then the door lock. *Exception: If you manually open the door lock with the key shipped with your door handle, the Door Lock state will enter the open state while the Door Handle Lock state remains closed.*
Card Reader	Shows the data of the smart card scanned by the internal or external card reader accompanying each door handle connected to DX2-DH2C2. *Note: It is not necessary to use the internal card reader unless you are using a third-party application, such as Power IQ, for access control. Refer to the user documentation of your third-party application for more information.*

Tip: All sensors of the connected door handles are also listed on the page of **Peripherals** *(on page 108).*

Note that the same Card Reader information is also available on the page of *Card Readers* (on page 344).

▶ **To control the door handles:**

Per default, only one door handle can be opened at the same time so you must close one door handle before opening another door handle connected to the same SRC. To increase the upper limit of concurrently opened door handles, see **Peripherals** (on page 108).

1. Make sure you have configured the door handle type properly in the above procedure.

2. Go to the proper door handle section, and click Open or Close to open or close the door handle lock.

3. Confirm the operation when prompted.
4. Now you can physically open the cabinet door with the opened door handle.

Tip: You can click Close to re-close the door handle lock when you change your mind before the door is physically opened, or when the door handle lock is mistakenly opened, or when someone opens it without pulling out the door handle. If not, then SRC will automatically close the door handle lock after its timeout expires.

▶ **DX2-DH2C2 LED information:**

- For information on DX2-DH2C2 LED, refer to 'Environmental Sensors and Actuators Guide' (or its Online Help version) on the Raritan *Support page* (*http://www.raritan.com/support/*).

Card Readers

To open the Card Readers page, choose Card Readers in the *Menu* (on page 98).

This page lists all card readers connected to SRC, including:

- Standalone USB card readers
- Card readers integrated with door handles

Note: To have card readers integrated with door handles display on this page, you must first configure the door handle properly on the page of **SmartLock** *(on page 339).*

Raritan.
A brand of ☐legrand®

When a user scans his/her smart card with the card reader, SRC will retrieve the card's type and ID and show them in the corresponding Card Type and Card ID column. If no data is shown in the two columns, it means the scanned card may not be supported by the card reader.

Tip: You can use a third-party application, such as Power IQ, to retrieve the card's data from SRC to perform security features like cabinet access control. Refer to that application's user documentation for more information.

Listed card readers can be one or both of the following types.

▶ **Door handle-integrated card readers:**

- This type of card reader is integrated in the door handle, which is any series below:
  - Emka Agent E
  - SouthCo H3-EM
  - Dirak eLine MLR 2x00

Note: Not every SouthCo H3-EM door handle has a card reader integrated. For example, H3-EM-60-100 requires an external card reader.

- It is connected to SRC via the DX2-DH2C2 module.
- The Channel column indicates which door handle port (channel) it is connected to.
- Note that the serial number displayed for this card reader is the same as DX2-DH2C2's serial number.

  Each DX2-PD2C2 module can show two card readers because they have two ports for connecting two door handles with card readers integrated.

▶ **Standalone USB card readers:**

- It is directly connected to the USB-A port of SRC.
- The Channel column does not show any data.

Chapter 7   Using SNMP

This SNMP section helps you set up the SRC for use with an SNMP manager. The SRC can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

Enabling and Configuring SNMP

To communicate with an SNMP manager, you must enable SNMP protocols on the SRC. By default the "read-only" mode of SNMP v1/v2c is enabled.

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, you must configure the users with the SNMP v3 access permission and set Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between SNMP and the SRC.

Important: You must download the SNMP MIB for your SRC to use with your SNMP manager. See *Downloading SNMP MIB* **(on page 351).**

▶ **To enable SNMP v1/v2c and/or v3 protocols:**

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Agent section, enable SNMP v1/v2c or SNMP v3, and configure related fields, such as the community strings.

   ▪ If SNMP v3 is enabled, you must determine which users shall have the SNMP v3 access permission. See below.

   For details, see **Configuring SNMP Settings** (on page 188).

▶ **To configure users for SNMP v3 access:**

1. Choose User Management > Users.

2. Create or modify users to enable their SNMP v3 access permission.

   ▪ If authentication and privacy is enabled, configure the SNMP password(s) in the user settings.

   For details, see **Creating Users** (on page 148).

▶ **To enable SNMP notifications:**

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Notifications section, enable the SNMP notification feature, and configure related fields. For details, refer to:

    ▪ **SNMPv2c Notifications** (on page 347)

    ▪ **SNMPv3 Notifications** (on page 348)

Note: Any changes made to the 'SNMP Notifications' section on the SNMP page will update the settings of the System SNMP Notification Action, and vice versa. See **Available Actions** *(on page 238).*

SNMPv2c Notifications

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.

4. Select 'SNMPv2c trap' or 'SNMPv2c inform' as the notification type.

5. Type values in the following fields.

Field	Description
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication

Field	Description
	once every 3 seconds.
Number of retries	The number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Host	The IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP agent. You can specify up to 3 SNMP destinations.
Port	The port number used to access the device(s).
Community	The SNMP community string to access the device(s). The community is the group representing the SRC and all SNMP management stations.

6. Click Save.

SNMPv3 Notifications

1. Choose Device Settings > Network Services > SNMP.

2. In the SNMP Agent, make sure the Enable SNMP v1/v2c checkbox is selected.

3. In the SNMP Notifications section, make sure the 'Enable SNMP notifications' checkbox is selected.

SNMP Notifications	
Enable SNMP notifications	✔
Notification type	SNMPv3 inform ▼
Host	required
Port	162
User ID	required
Timeout	3 s
Number of retries	5
Security level	authPriv ▼
Authentication protocol	SHA ▼
Authentication passphrase	required
Confirm authentication passphrase	
Privacy protocol	AES ▼
Privacy passphrase	required
Confirm privacy passphrase	

4. Select 'SNMPv3 trap' or 'SNMPv3 inform' as the notification type.
5. For SNMP TRAPs, the engine ID is prepopulated.
6. Type values in the following fields.

Field	Description
Host	The IP address of the device(s) you want to access.

Field	Description
	This is the address to which notifications are sent by the SNMP agent.
Port	The port number used to access the device(s).
User ID	User name for accessing the device. ▪ Make sure the user has the SNMP v3 access permission.
Timeout	The interval of time, in seconds, after which a new inform communication is resent if the first is not received. ▪ For example, resend a new inform communication once every 3 seconds.
Number of retries	Specify the number of times you want to resend the inform communication if it fails. ▪ For example, inform communications are resent up to 5 times when the initial communication fails.
Security level	Three types are available. ▪ noAuthNoPriv - neither authentication nor privacy protocols are needed. ▪ authNoPriv - only authentication is required. ▪ authPriv - both authentication and privacy protocols are required.
Authentication protocol, Authentication passphrase, Confirm authentication passphrase	The three fields are available when the security level is set to AuthNoPriv or authPriv. ▪ Select the authentication protocol - MD5 or SHA ▪ Enter the authentication passphrase
Privacy protocol, Privacy passphrase, Confirm privacy passphrase	The three fields are available when the security level is set to authPriv. ▪ Select the Privacy Protocol - DES or AES ▪ Enter the privacy passphrase and then confirm the privacy passphrase

7. Click Save.

Raritan.
A brand of Legrand

Downloading SNMP MIB

You must download an appropriate SNMP MIB file for successful SNMP communications. Always use the latest SNMP MIB downloaded from the current firmware of your SRC.

You can download the MIBs from two different pages of the web interface.

▶ **MIB download via the SNMP page:**

1. Choose Device Settings > Network Services > SNMP.
2. Click the Download MIBs title bar.

3. Select the desired MIB file to download.
   - PDU2-MIB: The SNMP MIB file for SRC management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
   - LHX-MIB: The SNMP MIB file for managing the LHX/SHX heat exchanger(s).
4. Click Save to save the file onto your computer.

▶ **MIB download via the Device Information page:**

1. Choose Maintenance > Device Information.
2. In the Information section, click the desired download link:
   - PDU2-MIB
   - ASSETMANAGEMENT-MIB
   - LHX MIB
3. Click Save to save the file onto your computer.

Note: LHX-MIB is available only after the LHX/SHX support has been enabled. See **Miscellaneous** *(on page 297).*

SNMP Gets and Sets

In addition to sending notifications, the SRC is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the SRC, 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 SRC device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

  The SRC 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 SRC MIB.

The SRC MIB

The SNMP MIB file is required for using your SRC with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Raritan.
A brand of ☐ legrand®

Layout

Opening the MIB reveals the custom objects that describe the SRC system.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.

For example, the measurementsGroup group contains objects for environmental sensors connected to the SRC 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 cause the SRC to generate a warning and send an SNMP notification when certain parameters are exceeded. See *Sensor Threshold Settings* (on page 614) for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

Configuring NTP Server Settings

Using SNMP, you can change the following NTP server-related settings in the unitConfigurationTable:

- Enable or disable synchronization of the device's date and time with NTP servers (synchronizeWithNTPServer)
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled (useDHCPProvidedNTPServer)
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled (firstNTPServerAddressType and firstNTPServerAddress)
- Manually assign the secondary NTP server (optional) (secondNTPServerAddressType and secondNTPServerAddress)

Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, see **Setting the Time Zone** *(on page 420). For the web interface, see* **Setting the Date and Time** *(on page 220).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset –v2c –c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

A Note about Enabling Thresholds

When enabling previously-disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 8   Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer the SRC.

Note that available CLI commands are model dependent.

CLI commands are case sensitive.

In This Chapter

About the Interface

The SRC 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 SRC
- Display the SRC and network information, such as the device name, firmware version, IP address, and so on
- Configure the SRC and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Changing Telnet Settings** *(on page 192).*

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 product via a local (USB or RS-232) 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 PX2Serial Console" under the Ports group.

3. In the communications program, press Enter to send a carriage return to the SRC. 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.

Raritan.
A brand of ☐legrand®

After properly entering the password, the PDU name appears at the prompt. See **Different CLI Modes and Prompts** (on page 358) in the User Guide for more information.

Tip: The 'Last login' information, including the date and time, is also displayed if the same user account 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 this product.

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. Refer to PuTTY's documentation for details on configuration.

▶ **To log in using SSH or Telnet:**

1. Ensure SSH or Telnet has been enabled. See **Configuring Network Services** (on page 185) 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 PDU name appears at the prompt. See **Different CLI Modes and Prompts** (on page 358) in the User Guide for more information.

Tip: The 'Last login' information, including the date and time, is also displayed if the same user account 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 this product.

With an Analog Modem

The SRC 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 SRC via the modem:**

1. Make sure the SRC has an analog modem connected. See *Connecting an Analog Modem* (on page 64).
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 SRC. See *Configuring the Serial Port* (on page 290).
4. Type the following AT command to make a connection with the SRC.

   `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 SRC:**

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 SRC.

   `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. The PDU name appears with the prompt.

- User Mode: When you log in as a normal user, who may not have full permissions to configure the SRC, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the SRC, 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 SRC device and network configurations. See *Entering Configuration Mode* (on page 383).
- 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 495).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing the SRC over the local connection.

> When accessing or upgrading multiple SRC devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

The ? Command for Showing Available Commands

When you are not familiar with CLI commands, you can press the ? key at anytime for one of the following purposes.

- Show a list of main CLI commands available in the current mode.
- Show a list of available commands or parameters for the command you type. See **Querying Available Parameters for a Command** (on page 360).

► **In the administrator mode:**

```
#           ?
```

► **In the configuration mode:**

```
config:#    ?
```

► **In the diagnostic mode:**

```
diag:#      ?
```

Press Enter after pressing the ? command, and a list of main commands for the current mode is displayed.

*Tip: To automatically complete a command after typing part of the full command, see **Automatically Completing a Command** (on page 498). To re-execute one of the previous commands, see **Retrieving Previous Commands** (on page 498).*

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 (?) or list command (ls) 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 role configuration parameters:**

```
config:#    role ?
```

▶ **To query available parameters for the "role create" command:**

```
config:#    role create ?
```

*Tip: To automatically complete a command after typing part of the full command, see **Automatically Completing a Command** (on page 498). To re-execute one of the previous commands, see **Retrieving Previous Commands** (on page 498).*

Showing Information

You can use the show commands to view current settings or the status of the SRC 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 358).*

Network Configuration

This command shows all network configuration and all network interfaces' information, such as the IP address, MAC address, the Ethernet interfaces' duplex mode, and the wireless interface's status/settings.

```
#       show network
```

IP Configuration

This command shows the IP settings shared by all network interfaces, such as DNS and routes. Information shown will include both IPv4 and IPv6 configuration.

*Tip: To show IPv4-only and IPv6-only configuration data, see **IPv4-Only or IPv6-Only Configuration** (on page 363).*

```
#       show network ip common
```

To show the IP settings of a specific network interface, use the following command.

```
#       show network ip interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Show the IP-related configuration of the ETH1 interface.
eth2	Show the IP-related configuration of the ETH2 interface.
wireless	Show the IP-related configuration of the WIRELESS interface.
bridge	Show the IP-related configuration of the BRIDGE interface.
all	Show the IP-related configuration of all interfaces. *Tip: You can also type the command without adding this option "all" to get the same data. That is,* show network ip interface*.*

IPv4-Only or IPv6-Only Configuration

To show IPv4-only or IPv6-only configuration, use any of the following commands.

Tip: To show both IPv4 and IPv6 configuration data, see **IP Configuration** *(on page 362).*

▶ **To show IPv4 settings shared by all network interfaces, such as DNS and routes:**

```
#       show network ipv4 common
```

▶ **To show IPv6 settings shared by all network interfaces, such as DNS and routes:**

```
#       show network ipv6 common
```

▶ **To show the IPv4 configuration of a specific network interface:**

```
#       show network ipv4 interface <ETH>
```

▶ **To show the IPv6 configuration of a specific network interface:**

```
#       show network ipv6 interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Show the IPv4 or IPv6 configuration of the ETH1 interface.
eth2	Show the IPv4 or IPv6 configuration of the ETH2 interface.
wireless	Show the IPv4 or IPv6 configuration of the WIRELESS interface.

Interface	Description
bridge	Show the IPv4 or IPv6 configuration of the BRIDGE interface.
all	Show the IPv4 or IPv6 configuration of all interfaces.
	Tip: You can also type the command without adding this option "all" to get the same data. That is, show network ipv4 interface*.*

Network Interface Settings

This command shows the specified network interface's information which is NOT related to IP configuration. For example, the Ethernet port's LAN interface speed and duplex mode, or the wireless interface's SSID parameter and authentication protocol.

```
#       show network interface <ETH>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Show the ETH1 interface's non-IP settings.
eth2	Show the ETH2 interface's non-IP settings.
wireless	Show the WIRELESS interface's non-IP settings.
bridge	Show the BRIDGE interface's non-IP settings.
all	Show the non-IP settings of all interfaces.
	Tip: You can also type the command without adding this option "all" to get the same data. That is, show network interface*.*

Raritan.
A brand of ⬜legrand®

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS, SSH and Modbus/TCP services, and SNMP settings.

```
#      show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp*, *modbus* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP.
	Tip: You can also type the command without adding this option "all" to get the same data.
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
modbus	Only displays the settings of the Modbus/TCP service.
zeroconfig	Only displays the settings of the zero configuration advertising.

SRC Configuration

This command shows the SRC configuration, such as the device name, firmware version, model type and upper limit of active powered dry contact actuators.

```
#      show src
```

To show detailed information, add the parameter "details" to the end of the command.

```
#      show src details
```

Date and Time Settings

This command shows the current date and time settings on the SRC.

```
#        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 SRC 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. See **Existing User Profiles** *(on page 374) for the preferred measurement units for a specific user.*

Raritan.
A brand of legrand

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
```

```
# show externalsensors 2 details
External sensor 2 ('Temperature 2')
Sensor type: Temperature
Reading:     24.0 deg C (normal)

Serial number:              QMSemu0004
Description:                Not configured
Location:               X Not configured
                        Y Not configured
                        Z Not configured
Position:                   Port 1, Chain Position 4
Using default thresholds: yes
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information of all environmental sensors.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the SRC web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A state sensor displays the sensor state instead of the reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number, sensor position, and X, Y, and Z coordinates.

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. Peripheral Device Package refers to an environmental sensor package.

```
Peripheral Device Package 1
Serial Number:    1GE7A00022
Package Type:            DX2-T1H1
Position:         Port 1, Chain Position 1
Package State:    operational
Firmware Version: 33.0

Peripheral Device Package 2
Serial Number:    1GE7A00021
Package Type:            DX2-T3H1
Position:         Port 1, Chain Position 2
Package State:    operational
Firmware Version: 33.0
```

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 SRC 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 1 (Temperature):
Reading: 22.6 deg C
State:    normal

Active Thresholds: Default 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: 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
```

Raritan.
A brand of ❑legrand®

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the Peripherals page of the SRC web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including resolution and range.

Note: For a state sensor, the threshold-related and accuracy-related data is NOT available.

Environmental Sensor Default Thresholds

This command syntax shows a certain sensor type's default thresholds, which are the initial thresholds applying to the specified type of sensor.

```
#       show defaultThresholds <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show defaultThresholds <sensor type> details
```

Variables:

- <sensor type> is one of the following numeric sensor types:

Sensor types	Description
absoluteHumidity	Absolute humidity sensors
relativeHumidity	Relative humidity sensors
temperature	Temperature sensors
airPressure	Air pressure sensors
airFlow	Air flow sensors
vibration	Vibration sensors

Sensor types	Description
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 SRC.

```
#       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).

Raritan.
A brand of 🔲legrand

Authentication Settings

▶ **General authentication settings:**

This command displays the authentication settings of the SRC, including both LDAP and Radius settings.

```
#        show authentication
```

▶ **One LDAP server's settings:**

To show the configuration of a specific LDAP server, assign the desired LDAP server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
#        show authentication ldapServer <server_num>
```

-- OR --

```
#        show authentication ldapServer <server_num>
```

▶ **One Radius server's settings:**

To show the configuration of a specific Radius server, assign the desired Radius server with its sequential number in the command. To get detailed information, add "details" to the end of the command.

```
#        show authentication radiusServer <server_num>
```

-- OR--

```
#        show authentication radiusServer <server_num> details
```

Variables:

* <server_num> is the sequential number of the specified authentication server on the LDAP or Radius server list.

Displayed information:

* Without specifying any server, SRC shows the authentication type and a list of both LDAP and Radius servers that have been configured.
* When specifying a server, only that server's basic configuration is displayed, such as IP address and port number.
* With the parameter "details" added, detailed information of the specified server is displayed, such as an LDAP server's bind DN and the login name attribute, or a Radius server's timeout and retries values.

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 SRC.

```
#       show serial
```

Asset Strip Settings

This command shows the asset strip settings, such as the total number of rack units (tag ports), asset strip state, numbering mode, orientation, available tags and LED color settings.

```
#       show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset strip information.
	Tip: You can also type the command without adding this option "all" to get the same data.
A specific asset strip number	Displays the settings of the asset strip connected to the specified FEATURE port number.
	For the SRC device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Strip

A rack unit refers to a tag port on the asset strips. This command shows the settings of a specific rack unit or all rack units on an asset strip, such as a rack unit's LED color and LED mode.

```
#       show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset strip.
	Tip: You can also type the command without adding this option "all" to get the same data.

Option	Description
A specific number	Displays the settings of the specified rack unit on the specified asset strip.
	Use the index number to specify the rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.

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.

Event type	Description
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.
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.

Network Connections Diagnostic Log

This command shows the diagnostic log for both the EAP authentication and wireless LAN connection.

```
#       show network diagLog
```

Server Reachability Information

This command shows all server reachability information with a list of monitored servers and status.

```
#       show serverReachability
```

Raritan.
A brand of ☐legrand®

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 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.

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.*
A specific integer number	Displays the specified number of last entries in the reliability error log.

Reliability Hardware Failures

This command shows a list of detected hardware failures.

```
#       show reliability hwfailures
```

For details, see **Hardware Issue Detection** (on page 321).

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

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: 10 minutes

Strong passwords: Disabled

Restricted Service Agreement: disabled
Restricted Service Agreement Banner Content:
Unauthorized access prohibited; all access and activities not explicitl
y authorized by management are unauthorized. All activities are monitor
ed and logged. There is no privacy on this system. Unauthorized access
and activities or any criminal activity will be reported to appropriate
 authorities.

Front-Panel Permissions:
  Switch Outlet:                 no
  Switch Peripheral Actuator: no
```

Clearing Information

You can use the clear commands to remove unnecessary data from the SRC.

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 358).*

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 Diagnostic Log for Network Connections

This command removes all data from the diagnostic log for both the EAP authentication and WLAN connection.

```
#        clear networkDiagLog
```

   -- OR --

```
#        clear networkDiagLog /y
```

If you entered the command without "/y," a message appears, prompting you to confirm the operation. Type y to clear the log or n to abort the operation.

Configuring the SRC Device and Network

To configure the SRC 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 358).*

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 384).**

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 358).

SRC Configuration Commands

One SRC configuration command begins with *src*. You can use the SRC configuration commands to change the settings that apply to the whole SRC device.

Configuration commands are case sensitive so ensure you capitalize them correctly.

Raritan.
A brand of ▢legrand®

Changing the SRC Name

This command changes the device name of SRC.

```
config:#   src name "<name>"
```

Variables:

- <name> is a string comprising up to 64 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:#   src 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 277).

Setting Data Logging Measurements Per Entry

This command defines the number of measurements accumulated per log entry.

```
config:#   src 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 277).

Specifying the Device Altitude

This command specifies the altitude of your SRC above sea level (in meters). You must specify the altitude of SRC above sea level if a Raritan's 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 623).

```
config:#    src deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between -425 and 3000 meters.
- Note that the lower limit "-425" is a negative value because some locations are below the seal level.

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:#    src 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.
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 471).*

Network Configuration Commands

A network configuration command begins with *network*. A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Configuring IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

Setting the IPv4 Configuration Mode

This command determines the IP configuration mode.

```
config:#   network ipv4 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv4 configuration mode of the ETH1 interface (wired networking).
eth2	Determine the IPv4 configuration mode of the ETH2 interface (wired networking).
wireless	Determine the IPv4 configuration mode of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv4 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv4 preferred host name of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 preferred host name of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command to assign a permanent IP address to the SRC.

```
config:#   network ipv4 interface <ETH> address <ip address>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv4 address of the ETH1 interface (that is, wired networking).
eth2	Determine the IPv4 address of the ETH2 interface (that is, wired networking).
wireless	Determine the IPv4 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv4 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your SRC. Its format is "IP address/prefix". For example, *192.168.84.99/24*.

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:#   network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Setting IPv4 Static Routes

If the IPv4 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the SRC and devices in the other subnet.

These commands are prefixed with *network ipv4 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see **Static Route Examples** (on page 173).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> nextHop <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv4 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv4 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv4 staticRoutes modify <route_ID> dest <dest-2> nextHop <hop>
```

-- OR --

```
config:#    network ipv4 staticRoutes modify <route_ID> dest <dest-2> interface
            <ETH>
```

Variables:

- <dest-1> is a combination of the IP address and subnet mask of the other subnet. The format is *IP address/subnet mask*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ETH1/ETH2*, *WIRELESS* and *BRIDGE*. Type "bridge" only when your SRC is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/subnet mask*. You can modify either the IP address or the subnet mask or both.

Configuring IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

Setting the IPv6 Configuration Mode

This command determines the IP configuration mode.

```
config:#    network ipv6 interface <ETH> configMethod <mode>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv6 configuration mode of the ETH1 interface (wired networking).
eth2	Determine the IPv6 configuration mode of the ETH2 interface (wired networking).
wireless	Determine the IPv6 configuration mode of the WIRELESS interface (that is, wireless networking).

Interface	Description
bridge	Determine the IPv6 configuration mode of the BRIDGE interface (that is, bridging mode).

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.
static	The IPv6 configuration mode is set to static IP address.

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command:

```
config:#   network ipv6 interface <ETH> preferredHostName <name>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv6 preferred host name of the ETH1 interface (wired networking).
eth2	Determine the IPv6 preferred host name of the ETH2 interface (wired networking).
wireless	Determine the IPv6 preferred host name of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 preferred host name of the BRIDGE interface (that is, bridging mode).

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters

Raritan.
A brand of ⬜legrand®

- 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 SRC.

```
config:#   network ipv6 interface <ETH> address <ip
           address>
```

Variables:

- <ETH> is one of the network interfaces: *ETH1/ETH2*, *WIRELESS*, or *BRIDGE*. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

  Note: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Interface	Description
eth1	Determine the IPv6 address of the ETH1 interface (wired networking).
eth2	Determine the IPv6 address of the ETH2 interface (wired networking).
wireless	Determine the IPv6 address of the WIRELESS interface (that is, wireless networking).
bridge	Determine the IPv6 address of the BRIDGE interface (that is, the bridging mode).

- <ip address> is the IP address being assigned to your SRC. This value uses the IPv6 address format. Note that you must add */xx*, which indicates a prefix length of bits such as /64, to the end of this IPv6 address.

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command to specify the gateway.

```
config:#   network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Setting IPv6 Static Routes

If the IPv6 network mode is set to static IP and your local network contains two subnets, you can configure static routes to enable or disable communications between the SRC and devices in the other subnet.

These commands are prefixed with *network ipv6 staticRoutes*.

Depending on whether the other network is directly reachable or not, there are two methods for adding a static route. For further information, see **Static Route Examples** (on page 173).

▶ **Method 1: add a static route when the other network is NOT directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> nextHop <hop>
```

▶ **Method 2: add a static route when the other network is directly reachable:**

```
config:#   network ipv6 staticRoutes add <dest-1> interface <ETH>
```

▶ **Delete an existing static route:**

```
config:#   network ipv6 staticRoutes delete <route_ID>
```

▶ **Modify an existing static route:**

```
config:#   network ipv6 staticRoutes modify <route_ID> dest <dest-2>
           nextHop <hop>
```

-- OR --

Raritan.
A brand of ☐legrand®

```
config:#    network ipv6 staticRoutes modify <route_ID> dest <dest-2> interface
            <ETH>
```

Variables:

- <dest-1> is the IP address and prefix length of the subnet where the SRC belongs. The format is *IP address/prefix length*.
- <hop> is the IP address of the next hop router.
- <ETH> is one of the interfaces: *ETH1/ETH2*, *WIRELESS* and *BRIDGE*. Type "bridge" only when your SRC is in the bridging mode.
- <route_ID> is the ID number of the route setting which you want to delete or modify.
- <dest-2> is a modified route setting that will replace the original route setting. Its format is *IP address/prefix length*. You can modify either the IP address or the prefix length or both.

Configuring DNS Parameters

Use the following commands to configure static DNS-related settings.

▶ **Specify the primary DNS server:**

```
config:#    network dns firstServer <ip address>
```

▶ **Specify the secondary DNS server:**

```
config:#    network dns secondServer <ip address>
```

▶ **Specify the third DNS server:**

```
config:#    network dns thirdServer <ip address>
```

▶ **Specify one or multiple optional DNS search suffixes:**

```
config:#    network dns searchSuffixes <suffix1>
```

-- OR --

```
config:#    network dns searchSuffixes <suffix1>,<suffix2>,<suffix3>,...,<suffix6>
```

▶ **Determine which IP address is used when the DNS server returns both IPv4 and IPv6 addresses:**

```
config:#    network dns resolverPreference <resolver>
```

Variables:

- <ip address> is the IP address of the DNS server.
- <suffix1>, <suffix2>, and the like are the DNS suffixes that automatically apply when searching for any device via SRC. For example, <suffix1> can be *raritan.com*, and <suffix2> can be *legrand.com*. You can specify up to 6 suffixes by separating them with commas.
- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.
preferV6	Use the IPv6 addresses returned by the DNS server.

Setting LAN Interface Parameters

A LAN interface configuration command begins with *network ethernet*.

Enabling or Disabling the LAN Interface

This command enables or disables the LAN interface.

```
config:#    network ethernet <ETH> enabled <option>
```

Variables:

- <ETH> is one of the options -- *eth1 or eth2.*

Option	Description
eth1	ETH1 port
eth2	ETH2 port

Raritan.
A brand of **legrand**

- <option> is one of the options: *true or false*.

Option	Description
true	The specified network interface is enabled.
false	The specified network interface is disabled.

Changing the LAN Interface Speed

This command determines the LAN interface speed.

```
config:#   network ethernet <ETH> speed <option>
```

Variables:

- <ETH> is one of the options -- *eth1 or eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <option> is one of the options: *auto, 10Mbps, 100Mbps or 1000Mbps*.

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.
1000Mbps	The LAN speed is always 1000 Mbps.

Changing the LAN Duplex Mode

This command determines the LAN interface duplex mode.

`config:#`   network ethernet <ETH> duplexMode <mode>

Variables:

- <ETH> is one of the options -- *eth1 or eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The SRC selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the SRC) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Setting the Ethernet Authentication Method

This command sets the authentication method for the selected Ethernet interface to either none or Extensible Authentication Protocol (EAP).

`config:#`   network ethernet <ETH> authMethod <method>

Variables:

- <ETH> is one of the options -- *eth1 or eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

Raritan.
A brand of legrand

- <method> is one of the authentication methods: *NONE* or *EAP*.

Method	Description
NONE	The authentication method is set to NONE.
EAP	The authentication method is set to EAP.

Setting Ethernet EAP Parameters

When the selected Ethernet interface's authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server. For more information, see **Ethernet Interface Settings** (on page 164).

▶ **Determine the outer authentication protocol:**

```
config:#   network ethernet <ETH> eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol for authentication set to "EAP + PEAP":**

```
config:#    network ethernet <ETH> eapInnerAuthentication <inner_auth>
```

▶ **Set the EAP identity:**

```
config:#    network ethernet <ETH> eapIdentity <identity>
```

▶ **Set the EAP password:**

```
config:#    network ethernet <ETH> eapPassword
```

After performing the above command, the SRC prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a client certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:#    network ethernet <ETH> eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key. For an example with detailed procedure, see *EAP CA Certificate Example* (on page 402).

▶ **Provide a client private key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:#    network ethernet <ETH> eapClientPrivateKey
```

▶ **Provide a CA TLS certificate for EAP:**

```
config:#    network ethernet <ETH> eapCACertificate
```

▶ **Eable or disable verification of the TLS certificate chain:**

```
config:#    network ethernet <ETH> enableCertVerification <option1>
```

▶ **Allow expired and not yet valid TLS certificates:**

```
config:#    network ethernet <ETH> allowOffTimeRangeCerts <option2>
```

▶ **Allow network connection with incorrect system time:**

Raritan.
A brand of legrand

```
config:#    network ethernet <ETH> allowConnectionWithIncorrectClock
            <option3>
```

> ► **Set the RADIUS authentication server for EAP:**

```
config:#    network ethernet <ETH> eapAuthServerName <FQDN>
```

Variables:

- <ETH> is one of the options -- *eth1 or eth2*.

Option	Description
eth1	ETH1 port
eth2	ETH2 port

- <outer_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

- <inner_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

- <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 network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.
false	The 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 network connection successful when the SRC system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the SRC finds that the TLS certificate is not valid due to incorrect system time.

- <FQDN> is the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

EAP CA Certificate Example

This section provides a CA certificate example for the Ethernet interface "ETH1". Your CA certificate contents should be different from the contents displayed in this example.

In addition, the procedure of uploading the client certificate and client private key in CLI is similar to the following example, except for the CLI command.

▶ **To provide a CA certificate:**

1. Make sure you have entered the configuration mode. See **Entering Configuration Mode** (on page 383).

2. Type the following command for ETH1 and press Enter.

```
config:#   network ethernet eth1 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, including the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE."

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:#
   ```

Removing the Uploaded Certificate or Private Key

The procedures of removing an existing client certificate, client private key or CA certificate in CLI are similar.

This section illustrates such a procedure for the Ethernet interface "ETH1."

▶ **To remove a certificate or private key for ETH1:**

1. Make sure you have entered the configuration mode. See **Entering Configuration Mode** .

2. Type the appropriate command, depending on which file you want to remove, and press Enter.

   ▪ *Client certificate:*

   ```
   config:#   network ethernet eth1 eapClientCertificate
   ```

   ▪ *Client private key:*

   ```
   config:#   network ethernet eth1 eapClientPrivateKey
   ```

- *CA certificate:*

```
config:#   network ethernet eth1 eapCACertificate
```

3. The system prompts you to enter the contents of the chosen certificate or private key.
4. Press Enter without typing any data.
5. Verify whether the system shows the following command prompt, indicating the existing certificate or private key has been removed.
```
config:#
```

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 wireless networking mode is not enabled, the SSID, PSK and BSSID values are not applied until the wireless networking mode is enabled. 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

Enabling or Disabling 802.11n High Throughput

This command enables or disables the 802.11n high throughput protocol.

```
config:#   network wireless enableHT <option>
```

Variables:

- <option> is one of the options: *true or false*.

Option	Description
true	802.11n is enabled.
false	802.11n is disabled.

Setting the Wireless 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 authentication method is set to PSK.
EAP	The 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 Wireless EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, client certificate, client private key, password, CA certificate, and RADIUS authentication server. For more information, see *Wireless Network Settings* (on page 167).

▶ **Determine the outer authentication protocol:**

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

▶ **Determine the inner authentication protocol for authentication set to "EAP + PEAP":**

```
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 SRC prompts you to enter the password. Then type the password and press Enter.

▶ **Provide a Client Certificate for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:#   network wireless eapClientCertificate
```

After performing any certificate or private key commands, including commands for the client certificate, client private key, and CA certificate, the system prompts you to enter the contents of the wanted certificate or key. For an example with detailed procedure, see *EAP CA Certificate Example* (on page 402).

▶ **Provide a Client Private Key for authentication set to "EAP + TLS" or "EAP + PEAP + TLS":**

```
config:#   network wireless eapClientPrivateKey
```

▶ **Provide a CA TLS certificate for EAP:**

```
config:#   network wireless eapCACertificate
```

▶ **Eable 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>
```

> ► **Set the RADIUS authentication server for EAP:**

```
config:#   network wireless eapAuthServerName <FQDN>
```

Variables:

- <outer_auth> is one of the options: *PEAP* or *TLS*.

Option	Description
PEAP	Outer authentication is set to Protected Extensible Authentication Protocol (PEAP).
TLS	Outer authentication is set to TLS.

- <inner_auth> is one of the options: *MS-CHAPv2* or *TLS*.

Option	Description
MSCHAPv2	Inner authentication is set to Microsoft's Challenge Authentication Protocol Version 2 (MS-CHAPv2).
TLS	Inner authentication is set to TLS.

- <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 network connection successful even though the TLS certificate chain contains any certificate which is outdated or not valid yet.

Option	Description
false	The 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 network connection successful when the SRC system time is earlier than the firmware build before synchronizing with the NTP server, causing the TLS certificate to become invalid.
false	The network connection is NOT successfully established when the SRC finds that the TLS certificate is not valid due to incorrect system time.

- <FQDN> is the name of the RADIUS server if it is present in the TLS certificate. The name must match the fully qualified domain name (FQDN) of the host shown in the certificate.

Setting the BSSID

This command specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* for automatic selection.

Configuring the Cascading Mode

This command determines the cascading mode.

```
config:#   network <mode> enabled <option1>
```

Variables:

- <mode> is one of the following cascading modes.

Mode	Description
bridge	The Bridging mode, where each cascaded device is assigned a unique IP address.

Raritan.
A brand of legrand

Mode	Description
portForwarding	The Port Forwarding mode, where every cascaded device in the chain shares the same IP address, with diverse port numbers assigned.

Important: When enabling either cascading mode, you must make sure the other cascading mode is disabled, or the preferred cascading mode may not be enabled successfully.

- <option1> is one of the following options:

Option	Description
true	The selected cascading mode is enabled.
false	The selected cascading mode is disabled.

▶ **If Port Forwarding mode is enabled, you must configure two more settings to finish the configuration:**

On ALL cascaded devices, you must configure the 'role' setting one by one.

```
config:#    network portForwarding role <option2>
```

On the master device, you must configure the 'downstream interface' setting.

```
config:#    network portForwarding
            masterDownstreamInterface <option3>
```

Variables:

- <option2> is one of the following cascading roles:

Role	Description
master	The device is a master device.
slave	The device is a slave device.

- <option3> is one of the following options:

Option	Description
ETH1/ETH2	ETH1/ETH2 port is the port where the 1st slave device is connected.
Usb	USB port is the port where the 1st slave device is connected.

Setting Network Service Parameters

A network service command begins with *network services*.

Setting the HTTP Port

The commands used to configure the HTTP port settings begin with *network services http*.

▶ **Change the HTTP port:**

```
config:#   network services http port <n>
```

▶ **Enable or disable the HTTP port:**

```
config:#   network services http enabled <option>
```

▶ **Enforce redirection from HTTP to HTTPS:**

```
config:#   network services http enforceHttps <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. - OR - ▪ HTTP redirection to HTTPS is enabled.
false	▪ The HTTP port is disabled. - OR - ▪ HTTP redirection to HTTPS is disabled.

Raritan.
A brand of legrand

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 SRC via HTTP to be redirected to HTTPS.
false	No HTTP access is redirected to HTTPS.

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.

Option	Description
false	The Telnet service is disabled.

Changing the Telnet Port

This command changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Changing the SSH Port

This command changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Determining the SSH Authentication Method

This command syntax determines the SSH authentication method.

```
config:#   network services ssh authentication <auth_method>
```

Variables:

- <option> is one of the options: *passwordOnly*, *publicKeyOnly* or *passwordOrPublicKey*.

Option	Description
passwordOnly	Enables the password-based login only.
publicKeyOnly	Enables the public key-based login only.
passwordOrPublicKey	Enables both the password- and public key-based login. This is the default.

If the public key authentication is selected, you must enter a valid SSH public key for each user profile to log in over the SSH connection. See **Specifying the SSH Public Key** (on page 450).

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Enabling or Disabling SNMP v3

This command enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Setting the SNMP Read Community

This command sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the SNMP Write Community

This command sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Setting the sysContact Value

This command sets the SNMP MIB-II sysContact value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysName Value

This command sets the SNMP MIB-II sysName value.

```
config:#    network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Setting the sysLocation Value

This command sets the SNMP MIB-II sysLocation value.

```
config:#    network services snmp sysLocation <value>
```

Variables:

<value> is a string comprising 0 to 255 alphanumeric characters.

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command enables or disables the Modbus protocol.

```
config:#    network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Enabling or Disabling the Read-Only Mode

This command enables or disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Changing the Modbus Port

This command changes the Modbus port.

```
config:#   network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Enabling or Disabling Service Advertising

This command enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See **Enabling Service Advertising** (on page 195) for details.

```
config:#   network services zeroconfig <method> <option>
```

Variables:

- <method> is one of the options: *mdns* or *llmnr.*

Option	Description
mdns	Service advertisement via MDNS is enabled or disabled.
llmnr	Service advertisement via LLMNR is enabled or disabled.

Raritan.

A brand of ⬚legrand®

- <option> is one of the options: *enable* or *disable.*

Option	Description
enable	Service advertisement via the selected method (MDNS or LLMNR) is enabled.
disable	Service advertisement via the selected method (MDNS or LLMNR) is disabled.

Examples

This section illustrates several network configuration examples.

Example 1 - Wireless Networking Mode

The following command enables the wireless networking mode.

```
config:#    network wireless enabled true
```

Example 2 - Enabling IPv6 Protocol on the Ethernet Interface

The following command enables the IPv6 protocol on the ETH1 interface.

```
config:#    network ipv6 interface eth1 enabled true
```

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 IPv4 configuration mode on the ETH1 interface.

```
config:#    network ipv4 interface eth1 configMethod static
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Setting NTP Parameters

A time configuration command for NTP-related parameters begins with *time ntp*.

▶ **Specify the primary time server:**

```
config:#   time ntp firstServer <first_server>
```

▶ **Specify the secondary time server:**

```
config:#   time ntp secondServer <second_server>
```

▶ **To delete the primary time server:**

```
config:#   time ntp firstServer ""
```

▶ **To delete the secondary time server:**

```
config:#   time ntp secondServer ""
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.
- The <second_server> is the IP address or host name of the secondary NTP server.

Customizing the Date and Time

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 418).*

▶ **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 Time Zone

The CLI has a list of time zones to configure the date and time for SRC.

```
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.

Setting the Automatic Daylight Savings Time

This command determines whether the daylight saving 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 SRC and then shows the result. For instructions on specifying NTP servers via CLI, see **Setting NTP Parameters** (on page 419).

To perform this command successfully, you must:

- Own the "Change Date/Time Settings" permission.
- Customize NTP servers. See **Setting NTP Parameters** (on page 419).

This command is available either in the administrator/user mode or in the configuration mode. See **Different CLI Modes and Prompts** (on page 358).

▶ **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 SRC 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 491).*

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.

Direction	Description
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values (or prefix length), which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from/to the specified IP address(es).
drop	Discards traffic from/to the specified IP address(es), without sending any failure notification to the source or destination host.
reject	Discards traffic from/to the specified IP address(es), and an ICMP message is sent to the source or destination host for failure notification.

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

▶ IPv4 commands

```
config:#    security ipAccessControl ipv4 rule delete <direction> <rule_number>
```

▶ IPv6 commands

```
config:#    security ipAccessControl ipv6 rule delete <direction> <rule_number>
```

Variables:

- <direction> is one of the options: *in* or *out*.

Direction	Description
in	Inbound traffic.
out	Outbound traffic.

- <rule_number> is the number of the existing rule that you want to remove.

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begins with `security restrictedServiceAgreement,`

Enabling or Disabling the Restricted Service Agreement

This command activates or deactivates the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

Raritan.
A brand of legrand

After the Restricted Service Agreement feature is enabled, the agreement's content is displayed on the login screen.

Do either of the following, or the login fails:

- In the web interface, select the checkbox labeled "I understand and accept the restricted service agreement."

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

- In the CLI, type y when the confirmation message "I understand and accept the restricted service agreement" is displayed.

Specifying the Agreement Contents

This command allows you to create or modify contents of the Restricted Service Agreement.

```
config:#    security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the CLI prompts you to enter the content.

2. To end the content:

    a. Press Enter.

    b. Type `--END--` to indicate the end of the content.

    c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` *command. See* **Quitting Configuration Mode** *(on page 384).*

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 491).

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.

Raritan.

A brand of **Llegrand**

Option	Description
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 SRC 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 491).

▶ **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 491).

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.

Raritan
A brand of **legrand**

Option	Description
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.

Raritan.

A brand of legrand

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 491).*

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.

Enabling or Disabling Front Panel Actuator Control

The following CLI commands control whether you can turn on or off connected actuator(s) by operating the front panel LCD display.

▶ **To enable the front panel actuator control feature:**

```
config:#   security frontPanelPermissions add switchActuator
```

▶ **To disable the front panel actuator control feature:**

```
config:#   security frontPanelPermissions remove switchActuator
```

Tip: If your SRC supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and the internal beeper-muting functions simultaneously. `security frontPanelPermissions add switchActuator;muteBeeper`

Enabling or Disabling Front Panel Beeper-Sound Control

The following CLI commands control whether you can mute the internal beeper by operating the front panel LCD display when the beeper sounds.

▶ **To enable the front panel beeper sound control feature:**

```
config:#   security frontPanelPermissions add muteBeeper
```

▶ **To disable the front panel actuator control feature:**

```
config:#   security frontPanelPermissions remove muteBeeper
```

Tip: If your SRC supports multiple front panel permissions, you can combine them into one command by adding a semicolon (;) between different permissions. For example, the following CLI command enables both front panel actuator control and the the internal beeper-muting functions simultaneously. `security frontPanelPermissions add switchActuator;muteBeeper`

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.

Raritan.
A brand of legrand

```
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 in 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 SRC 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 491).*

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, SRC 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 383).
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 491).

▶ **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 64 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 SRC 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.

Option	Description
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 491).

▶ **Enable or disable the SNMP v3 access to SRC for the specified user:**

```
config:#   user modify <name> snmpV3Access <option1>
```

▶ **Determine the security level:**

```
config:#   user modify <name> securityLevel <option2>
```

▶ **Determine whether the authentication passphrase is identical to the password:**

```
config:#    user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

▶ **Determine the authentication passphrase:**

```
config:#    user modify <name> authenticationPassPhrase
```

After performing the above command, SRC prompts you to enter the authentication passphrase.

▶ **Determine whether the privacy passphrase is identical to the authentication passphrase:**

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

▶ **Determine the privacy passphrase:**

```
config:#    user modify <name> privacyPassPhrase
```

After performing the above command, SRC prompts you to enter the privacy passphrase.

▶ **Determine the authentication protocol:**

```
config:#    user modify <name> authenticationProtocol <option5>
```

▶ **Determine the privacy protocol:**

```
config:#    user modify <name> privacyProtocol <option6>
```

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.

Option	Description
disable	Disables the SNMP v3 access permission for the specified user.

- <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.

- <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.

- <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.

- <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.

- <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.

- An authentication or privacy passphrase is a string comprising 8 to 32 ASCII printable characters.

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 454).

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 491).

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

Raritan.
A brand of legrand

Tip: To set the default measurement units applied to the SRC user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 451).*

▶ **Set the preferred temperature unit:**

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

▶ **Set the preferred length unit:**

```
config:#   user modify <name> preferredLengthUnit <option2>
```

▶ **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.
- <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.

- <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.

- <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 383).

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>
```

Raritan.

A brand of legrand

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 SRC 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 383).

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 SRC 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 491).

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 SRC user interfaces for a specific user via CLI, see **Changing Measurement Units** *(on page 448).*

▶ Set the default temperature unit:

```
config:#    user defaultpreferences preferredTemperatureUnit <option1>
```

▶ Set the default length unit:

```
config:#    user defaultpreferences preferredLengthUnit <option2>
```

▶ Set the default pressure unit:

```
config:#    user defaultpreferences preferredPressureUnit <option3>
```

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.

- <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.

- <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 Mary enable admin
```

Results:

- A new user profile "Mary" 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 Mary roles admin,tester
```

Results:

- The user Mary 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 454).
- <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

Privilege	Description
changeExternalSensorsConfiguration	Change Peripheral Device Configuration
changeLhxConfiguration	Change LHX/SHX Configuration
changeModemConfiguration	Change Modem Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change SRC device settings
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchActuator*	Switch Actuator
viewAuthSettings	View Authentication Settings
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 SRC web interface. It is an integer.

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>"
```

▶ **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>...;
           ...
```

▶ **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.

Raritan.

A brand of ☐legrand®

```
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.

- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

- <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 454).

- <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. For arguments syntax, see ***All Privileges*** (on page 454).

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).

Authentication Commands

An authentication configuration command begins with *authentication*.

Determining the Authentication Method

You can choose to set the authentication type only, or both set the authentication type and determine whether to switch to local authentication in case the remote authentication is not available.

▶ **Determine the authentication type only:**

```
config:#   authentication type <option1>
```

▶ **Determine the authentication type and enable/disable the option of switching to local authentication:**

```
config:#   authentication type <option1> useLocalIfRemoteUnavailable <option2>
```

Note: You cannot enable or disable the option of switching to local authentication without determining the authentication type in the CLI. Therefore, always type "authentication type <option1>" when setting up "useLocalIfRemoteUnavailable".

Variables:

- <option1> is one of the options: *local* , *ldap* or *radius*.

Option	Description
local	Enable Local authentication only.
ldap	Enable LDAP authentication.
radius	Enable Radius authentication.

- <option2> is one of the options: *true* or *false*.

Option	Description
true	Remote authentication is the first priority. The device will switch to local authentication when the remote authentication is not available.
false	Always stick to remote authentication regardless of the availability of remote authentication.

LDAP Settings

All LDAP-related commands begin with *authentication ldap*.

If you enable LDAP authentication, you must add at least one LDAP server. Later you can modify or delete any existing LDAP server as needed.

Adding an LDAP Server

Adding an LDAP server requires the entry of quite a lot of parameters, such as the server's IP address, TCP port number, Base DN and so on.

You can repeat the following CLI command to add more than one LDAP server.

Tip: If any LDAP server's settings are identical to an existing LDAP server's, you can add it by just copying the existing one, instead of using the following command. See **Copying an Existing Server's Settings** *(on page 463).*

▶   **Add a new LDAP server:**

config:#   `authentication ldap add <host> <port> <ldap_type> <security>`
`<bind_type> <base_DN> <login_name_att> <user_entry_class>` **"Optional**
Parameters"

Note: **"Optional Parameters"** *refer to one or multiple parameters listed in the section* **Optional Parameters** *(on page 460). They are required only when your server settings need to specify these parameters. For example, if setting the <bind_type> to "authenticatedBind", then you must add the parameter "bindDN" to this command.*

When the above command is successfully performed, a list of all LDAP servers, including the newly-added one, will be displayed, which is similar to the following diagram.

```
#  IP address                  Server type
------------------------------------------
1  192.1.1.1                   OpenLDAP
2  192.2.2.2                   OpenLDAP
```

Tip: To verify all settings of a newly-added server, see **Authentication Settings** *(on page 373).*

Variables:

- <host> is the IP address or host name of the LDAP server.
- <port> is the port number assigned for communication with the LDAP server.
- <ldap_type> is one of the LDAP server types: *openldap* or *activeDirectory*.

Type	Description
openldap	OpenLDAP server
activeDirectory	Microsoft Active Directory

- <security> is one of the security options: *none*, *startTls* or *tls*.

Type	Description
none	No security
startTls	StartTLS
tls	TLS

- <bind_type> is one of the bind options: *anonymouseBind*, or *authenticatedBind*.

Type	Description
anonymousBind	Enable the anonymous Bind. Bind DN and password are NOT required.
authenticatedBind	Enable the Bind with authentication. Bind DN and password are required.

- <base_DN> is the base DN for search.
- <login_name_att> is the login name attribute.
- <user_entry_class> is the User Entry Object Class.

Optional Parameters

You can add one or multiple "optional parameters", such as specifying the Bind DN or certificate upload, to an LDAP-server-adding command as illustrated below. If adding multiple optional parameters, you must add them to the END of the command and separate them with a space.

- *Example 1 -- Specify an Active Directory Domain's name:*

```
config:#    authentication ldap add <host> <port> <ldap_type> <security>
            <bind_type><base_DN><login_name_att><user_entry_class> adDomain
            <AD_domain>
```

- *Example 2 -- Set up the bind DN:*

```
config:#    authentication ldap add <host> <port> <ldap_type> <security>
            <bind_type> <base_DN> <login_name_att> <user_entry_class> bindDN
            <bind_DN>
```

▶ **"Optional Parameters" table:**

Parameters	To configure
userSearchSubfilter <filter>	User search subfilter
bindDN <bind_DN>	bind DN • The system will prompt you to enter and re-confirm the bind password after adding this parameter to the command. • For details, see ***Illustrations of Adding LDAP Servers*** (on page 462).
adDomain <AD_domain>	Active Directory Domain name
verifyServerCertificate <verify_cert>	Certificate verification setting • After setting to true, the system will prompt you to upload a certificate. For details, see ***Illustrations of Adding LDAP Servers*** (on page 462).
allowExpiredCertificate <allow_exp_cert>	Whether to accept expired or not valid yet certificate

Variables:

- <filter> is the user search subfilter you specify.
- <bind_DN> is bind DN.
- <AD_domain> is the Active Directory Domain.
- <verify_cert> is one of the options: *true* or *false*.

Option	Description
true	Enable the verification of the LDAP server certificate.
false	Disable the verification of the LDAP server certificate.

- <allow_exp_cert> is one of the options: *true* or *false*.

Option	Description
true	Certificates that are either expired or not valid yet are all accepted.
false	Only valid certificates are accepted.

Illustrations of Adding LDAP Servers

This section shows several LDAP command examples. Those words highlighted in bold are required for their respective examples.

▶ **An OpenLDAP server:**

config:# authentication ldap add op-ldap.raritan.com 389 **openldap** none anonymousBind dc=raritan,dc=com **uid inetOrgPerson**

▶ **A Microsoft Active Directory server:**

config:# authentication ldap add ac-ldap.raritan.com 389 **activeDirectory** none anonymousBind dc=raritan,dc=com **sAMAccountName user adDomain raritan.com**

▶ **An LDAP server with a TLS certificate uploaded:**

a. Enter the CLI command with the following two TLS-related options set and/or added:
   - *<security> is set to tls or startTls.*
   - *The "verifyServerCertificate" parameter is added to the command and set to "true."*

config:# authentication ldap add ldap.raritan.com 389 openldap **startTls ...** inetOrgPerson **verifyServerCertificate true**

b. The system now prompts you to enter the certificate's content.

c. Type or copy the certificate's content in the CLI and press Enter.

Note: The certificate's content is located between the line containing "BEGIN CERTIFICATE" and the line containing "END CERTIFICATE".

▶ **An LDAP server with the bind DN and bind password configured:**

a. Enter the CLI command with the "bindDN" parameter and its data added.

config:# authentication ldap add op-ldap.raritan.com 389 openldap none **authenticatedBind** cn=Manager,dc=raritan,dc=com uid inetOrgPerson **bindDN user@raritan.com**

Raritan.
A brand of ⊔legrand®

      b.   The system prompts you to specify the bind DN password.

      c.   Type the password and press Enter.

      d.   Re-type the same password.

Copying an Existing Server's Settings

If the server that you will add completely shares the same settings with any server that has been configured, use the following command.

▶ **Add an LDAP server by copying an existing server's settings:**

```
config:#   authentication ldap addClone <server_num> <host>
```

Variables:

- <host> is the IP address or host name of the LDAP server.
- <server_num> is the sequential number of the specified server shown on the server list of the SRC. See **Authentication Settings** (on page 373).

Modifying an Existing LDAP Server

You can modify one or multiple parameters of an existing LDAP server, such as its IP address, TCP port number, Base DN and so on. Besides, you can also change the priority or sequence of existing LDAP servers in the server list.

▶ **Command syntax:**

A command to modify an existing LDAP server's settings looks like the following:

```
config:#   authentication ldap modify <server_num> "parameters"
```

Variables:

- <server_num> is the sequential number of the specified server in the LDAP server list.
- Replace **"parameters"** with one or multiple commands in the following table, depending on which parameter(s) you want to modify.

▶ **A list of "parameters":**

Parameters	Description
host <host>	Change the IP address or host name. ▪ <host> is the new IP address or host name.
port <port>	Change the TCP port number. ▪ <port> is the new TCP port number.
serverType <ldap_type>	Change the server type. ▪ <ldap_type> is the new type of the LDAP server. ▪ <ldap_type> values include: `openldap` and `activeDirectory`.
securityType <security>	Change the security type. ▪ <security> is the new security type. ▪ <security> values include: `none`, `startTls`, and `ssl`
bindType <bind_type>	Change the bind type. ▪ <bind_type> is the new bind type. ▪ <bind_type> values include: `anonymousBind` and `authenticatedBind`.
searchBaseDN <base_DN>	Change the base DN for search. ▪ <base_DN> is the new base DN for search.
loginNameAttribute <login_name_att>	Change the login name attribute. ▪ <login_name_att> is the new login name attribute.
userEntryObjectClass <user_entry_class>	Change the user entry object class. ▪ <user_entry_class> is the new user entry class.
userSearchSubfilter <user_search_filter>	Change the user search subfilter. ▪ <user_search_filter> is the new user search subfilter.
adDomain <AD_domain>	Change the Active Directory Domain name. ▪ <AD_domain> is the new domain name of the Active Directory.
verifyServerCertificate <verify_cert>	Enable or disable the certificate verification. ▪ <verify_cert> enables or disables the certificate verification feature. ▪ Available values include: `true`, `false`

Raritan.
A brand of **legrand**

Parameters	Description
certificate	Re-upload a different certificate. a. First add the "certificate" parameter to the command, and press Enter. b. The system prompts you for the input of the certificate. c. Type or copy the content of the certificate in the CLI and press Enter.
allowExpiredCertificate <allow_exp_cert>	Determine whether to accept a certificate which is expired or not valid yet. ▪ <allow_exp_cert> determines whether to accept an expired or not valid yet certificate ▪ <allow_exp_cert> values include: `true`, and `false`
bindDN <bind_DN>	Change the bind DN. ▪ <bind_DN> is the new bind DN.
bindPassword	Change the bind DN password. a. First add the "bindPassword" parameter to the command, and press Enter. b. The system prompts you for the input of the password. c. Type the password and press Enter.
sortPosition <position>	Change the priority of the server (that is, resorting). ▪ <position> is the new sequential number of the server in the LDAP server list.

Note: For details of the above variables' values, see **Adding an LDAP Server** *(on page 459).*

▶ **Examples:**

• **Change the IP address of the 1st LDAP server**

```
config:#   authentication ldap modify 1 host 192.168.3.3
```

• **Change both the IP address and TCP port of the 1st LDAP server**

```
config:#   authentication ldap modify 1 host 192.168.3.3 port 633
```

• **Change the IP address, TCP port and the type of the L1st DAP server**

```
config:#   authentication ldap modify 1 host 192.168.3.3 port 633
           serverType activeDirectory
```

Removing an Existing LDAP Server

This command removes an existing LDAP server from the server list.

```
config:#   authentication ldap delete <server_num>
```

Variables:

- <server_num> is the sequential number of the specified server in the LDAP server list.

Radius Settings

All Radius-related commands begin with *authentication radius*.

If you enable Radius authentication, you must add at least one Radius server. Later you can modify or delete any existing Radius server as needed.

Adding a Radius Server

You can repeat the following commands to add Radius servers one by one.

▶ **Command syntax:**

```
config:#   authentication radius add <host> <rds_type> <auth_port> <acct_port> <timeout>
           <retries>
```

Variables:

- <host> is the IP address or host name of the Radius server.
- <rds_type> is one of the Radius authentication types: *pap, chap, msChapV2*.

Type	Description
chap	CHAP
pap	PAP
msChapV2	MSCHAP v2

- <auth_port> is the authentication port number.
- <acct_port> is the accounting port number.
- <timeout> is the timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the number of retries. It ranges between 0 to 5.

▶ **To enter the shared secret:**

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

Raritan.
A brand of **legrand**

▶ **Example:**

```
config:#   authentication radius add 192.168.7.99 chap 1812 1813 10 3
```

Modifying an Existing Radius Server

You can modify one or multiple parameters of an existing Radius server, or change the priority or sequence of existing servers in the server list.

▶ **Change the IP address or host name:**

```
config:#   authentication radius modify <server_num> host <host>
```

▶ **Change the Radius authentication type:**

```
config:#   authentication radius modify <server_num> authType <rds_type>
```

▶ **Change the authentication port:**

```
config:#   authentication radius modify <server_num> authPort <auth_port>
```

▶ **Change the accounting port:**

```
config:#   authentication radius modify <server_num> accountPort <acct_port>
```

▶ **Change the timeout value:**

```
config:#   authentication radius modify <server_num> timeout <timeout>
```

▶ **Change the number of retries:**

```
config:#   authentication radius modify <server_num> retries <retries>
```

▶ **Change the shared secret:**

```
config:#   authentication radius modify <server_num> secret
```

▶ **Change the priority of the specified server:**

```
config:#    authentication radius modify <server_num> sortPositon <position>
```

> *Tip: You can add more than one parameters to the command. For example,*
> *"authentication radius modify <server_num> host <host>*
> *authType <rds_type> authPort <auth_port> accountPort*
> *<acct_port> ...".*

Variables:

- <server_num> is the sequential number of the specified server in the Radius server list.
- <host> is the new IP address or host name of the Radius server.
- <rds_type> is one of the Radius authentication types: *pap, chap, msChapV2.*
- <auth_port> is the new authentication port number.
- <acct_port> is the new accounting port number.
- <timeout> is the new timeout value in seconds. It ranges between 1 to 10 seconds.
- <retries> is the new number of retries. It ranges between 0 to 5.

▶ **To enter the shared secret:**

1. After executing the above Radius command, the system automatically prompts you to enter the shared secret.
2. Type the secret and press Enter.
3. Re-type the same secret and press Enter.

▶ **Example:**

```
config:#    authentication radius add 192.168.7.99 chap 1812 1813 10 3
```

Removing an Existing Radius Server

This command removes an existing Radius server from the server list.

```
config:#    authentication radius delete <server_num>
```

Variables:

- <server_num> is the sequential number of the specified server in the Radius server list.

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 478).*

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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <name> is a string comprising up to 64 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 478).*

Specifying the CC Sensor Type

Raritan's contact closure sensor supports the connection of diverse third-party. 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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <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.

Type	Description
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Raritan.
A brand of legrand

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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- 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 386).*

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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <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 Raritan 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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.
- <time> is an integer number in seconds, ranging between 0 and 300.

Examples

This section illustrates several environmental sensor configuration examples.

Raritan.

A brand of legrand

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 491).

▶ **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/m³)
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 $°C$ and Upper Critical threshold to 24 $°C$ for all temperature sensors.

```
config:#   defaultThresholds temperature upperWarning 20
           upperCritical 24
```

Environmental Sensor Threshold Configuration Commands

You can use the sensor threshold configuration commands to set the threshold, hysteresis and assertion timeout values for any environmental sensor.

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold has been enabled.

Threshold Configuration Commands for a Sensor

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

You can configure various environmental sensor threshold settings at a time by combining multiple commands. See ***Multi-Command Syntax*** (on page 491).

▶ **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 SRC web interface or using the command "`show externalsensors <n>`" in the CLI. It is an integer starting at 1.

- <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

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.

Raritan.
A brand of legrand

- <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 620).

- <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 618).

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 491).

▶ **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 SRC web interface or CLI. It is an integer starting at 1.
- <name> is a string comprising up to 64 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 386).*

- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes when it contains spaces.

Example - Actuator Naming

The following command assigns the name "Door lock of cabinet 3" to the actuator whose ID number is 9.

```
config:#   actuator 9 name "Door lock of cabinet 3"
```

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 SRC 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 SRC 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 491).

▶ **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 SRC 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 SRC disables the ping monitoring feature for the monitored device and returns to the "Waiting for reliable connection" state. Valid range is 1 to 100 or *unlimited*.

Example - Server Settings Changed

The following command modifies several ping monitoring settings for the second server in the server reachability list.

```
config:#    serverReachability modify 2 numberOfSuccessfulPingsToEnable 10
            numberOfUnsuccessfulPingsForFailure 8
            waitTimeAfterSuccessfulPing 30
```

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset strip (if any) or the settings of LEDs on the asset strip.

Asset Strip Management

An asset strip management configuration command begins with `assetStrip`.

Naming an Asset Strip

This command syntax names or changes the name of an asset strip connected to the SRC device.

```
config:#   assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset strip connected to the SRC device.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Note: A rack unit refers to a tag port on the asset strips.

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <number> is the total number of rack units available on the connected asset strip. This value ranges from 8 to 64.

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset strips connected to the SRC device. The numbering mode changes the rack unit numbers.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset strips connected to the SRC device.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <number> is a starting number for numbering rack units on the connected asset strip. This value is an integer number.

Raritan.
A brand of legrand

Specifying the Asset Strip Orientation

This command syntax specifies the orientation of the asset strips connected to the SRC device. Usually you do not need to perform this command unless your asset strips do NOT come with the tilt sensor, causing the SRC unable to detect the asset strips' orientation.

```
config:#    assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC 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 strip is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset strip is mounted with the RJ-45 connector located at the bottom.

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset strip #1 to indicate the presence of a connected asset tag.

```
config:#    assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset strip(s) to indicate the absence of a connected asset tag.

```
config:#    assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Rack Unit Configuration

A rack unit refers to a tag port on the asset strips. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset strip.

```
config:#    rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <name> is a string comprising up to 64 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Raritan.
A brand of ☐legrand®

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset strip follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See **Setting LED Colors for Connected Tags** (on page 485) and **Setting LED Colors for Disconnected Tags** (on page 486). 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 488) and **Setting an LED Mode for a Rack Unit** (on page 488) to set different LED settings.

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset strip. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it. See **Setting LED Colors for Connected Tags** *(on page 485) and* **Setting LED Colors for Disconnected Tags** *(on page 486).*

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset strip. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset strip is physically connected. For the SRC device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number is available on the asset strip or the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.

Mode	Description
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Examples

This section illustrates several asset management examples.

Example 1 - Asset Strip LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#    assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Example 2 - Rack Unit Naming

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#    rackUnit 1 25 name "Linux server"
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Baud Rates

The following commands set the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the SRC 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 SRC or power cycle the connected device for proper communications.

▶ **Determine the CONSOLE baud rate:**

```
config:#   serial consoleBaudRate <baud_rate>
```

Note: The serial port bit-rate change is required when the SRC works in conjunction with Raritan's Dominion LX KVM switch. Dominion LX only supports 19200 bps for communications over the serial interface.

▶ **Determine the MODEM baud rate:**

```
config:#   serial modemBaudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the baud rate options: *1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200*.

Forcing the Device Detection Mode

This command forces the serial port on the SRC 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 SRC automatically detects the type of the device connected to the serial port. Select this option unless your SRC cannot correctly detect the device type.
forceConsole	The SRC attempts to recognize that the connected device is set for the console mode.

Option	Description
forceAnalogModem	The SRC attempts to recognize that the connected device is an analog modem.
forceGsmModem	The SRC attempts to recognize that the connected device is a GSM modem.

Example

The following command sets the CONSOLE baud rate of the SRC device's serial port to 9600 bps.

```
config:#   serial consoleBaudRate 9600
```

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 ETH1's Activation, Configuration Method and IP

The following multi-command syntax configures IPv4 address, configuration method and activation status for ETH1's network connectivity simultaneously.

```
config:#   network ipv4 interface eth1 enabled true configMethod static
           address 192.168.84.225/24
```

Results:

- The ETH1 interface is enabled.
- ETH1's configuration method is set to static IP address.
- ETH1's IPv4 address is set to 192.168.84.225/24.

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 Raritan sensor package, 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 358).

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 SRC web interface or using the show command in the CLI. It is an integer starting at 1.

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

Raritan.
A brand of **legrand**

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 SRC web interface or using the show command in the CLI. It is an integer starting at 1.

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 SRC, you can unblock them at the local console.

▶ **To unblock a user:**

1. Access the CLI interface using any terminal program via a local connection. See **With HyperTerminal** (on page 356).
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 SRC

You can reset the SRC to factory defaults or simply restart it using the CLI commands.

Restarting the Device

This command restarts the SRC. It is not a factory default reset.

▶ **To restart the SRC:**

1. Ensure you have entered administrator mode and the # prompt is displayed.

2. Type either of the following commands to restart the SRC.

   `#      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 reset is complete.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Resetting to Factory Defaults

The following commands restore all settings of the SRC to factory defaults.

▶ **To reset SRC settings after login, use either command:**

   `#      reset factorydefaults`

       -- OR --

   `#      reset factorydefaults /y`

▶ **To reset SRC settings before login:**

   `Username:   factorydefaults`

See **Using the CLI Command** (on page 557) for details.

Note: Device reset will cause CLI communications over an "USB" connection to be lost. Therefore, re-connect the USB cable after the reset is complete.

Network Troubleshooting

The SRC 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 358).

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.

Raritan.
A brand of legrand

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.
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 SRC and a network host.

```
diag>      traceroute <host> <useICMP>
```

Variables:

- <host> is the name or IP address of the host you want to trace.
- <useICMP> is optional. It has only one value -- `useICMP`. Type `useICMP` in the end of this command only when you want to use ICMP packets rather than UDP packets.

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 several times 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.

3. If there are more than one possible commands, a list of these commands is displayed. Then type the full command.

Raritan.
A brand of ❏ legrand®

▶ **Examples:**

- **Example 1 (only one possible command):**

    a.   Type the first word and the first letter of the second word of the "`reset factorydefaults`" command -- that is, `reset f`.

    b.   Then press Tab or Ctrl+i to complete the second word.

- **Example 2 (only one possible command):**

    a.   Type the first word and initial letters of the second word of the "`security strongPasswords`" command -- that is, `security str`.

    b.   Then press Tab or Ctrl+i to complete the second word.

- **Example 3 (more than one possible commands):**

    a.   Type only the first two words of the "`network ipv4 gateway xxx.xxx.xxx.xxx`" command -- that is, `network ipv4.`

    b.   Then press Tab or Ctrl+i one or two times, a list of possible commands displays as shown below.

    ```
    gateway              interface          staticRoutes
    ```

    c.   Type the full command "`network ipv4 gateway xxx.xxx.xxx.xxx`", according to the onscreen command list.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

▶ **To log out of the CLI:**

1.   Ensure you have entered administrator mode and the # prompt is displayed.

2.   Type `exit` and press Enter.

Chapter 9　Using SCP Commands

You can perform a Secure Copy (SCP) command to update the SRC firmware, do bulk configuration, or back up and restore the configuration.

In This Chapter

Firmware Update via SCP

Same as any SRC firmware update, all user management operations are suspended and all login attempts fail during the SCP firmware update. For details, see **Updating the SRC Firmware** (on page 309).

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

▶ To update the firmware via SCP:

1. Type the following SCP command and press Enter.

   ```
   scp <firmware file> <user name>@<device ip>:/fwupdate
   ```

   - *<firmware file>* is the SRC 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 or hostname of the SRC where you want to upload the specified file.

2. Type the password when prompted, and press Enter.

3. The system transmits the specified firmware file to the SRC, and shows the transmission speed and percentage.

4. When the transmission is complete, it shows the following message, indicating that the SRC starts to update its firmware now. Wait until the upgrade completes.

   ```
   Starting firmware update. The connection will be closed
   now.
   ```

▶ **SCP example:**

```
scp  pdu-px2-030410-44599.bin
admin@192.168.87.50:/fwupdate
```

▶ **Windows PSCP command:**

PSCP in Windows works in a similar way to the SCP.

- `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 SRC.

b. Copy the configuration file to one or multiple destination SRC.

For detailed information on the bulk configuration requirements, see ***Bulk Configuration*** (on page 313).

▶ **To save the configuration via SCP:**

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/bulk_config.txt <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges.
- *<device ip>* is the IP address or hostname of the SRC whose configuration you want to save.
- *<filename>* is the custom filename you assign to the "bulk_config.txt" of the source SRC.

2. Type the user password when prompted.

3. The system saves the configuration from the SRC to a file named "bulk_config.txt."

▶ **To copy the configuration via SCP:**

1. Type the following SCP command and press Enter.

```
scp bulk_config.txt <user name>@<device ip>:/bulk_restore
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges
- *<device ip>* is the IP address of the SRC whose configuration you want to copy.

2. Type the user password when prompted.

3. The system copies the configuration included in the file "bulk_config.txt" to another SRC, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

▶ **SCP examples:**

- Save operation:

```
scp admin@192.168.87.50:/bulk_config.txt today_config.txt
```

- Copy operation:

```
scp today_config.txt admin@192.168.87.47:/bulk_restore
```

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- Save operation:

```
pscp <user name>@<device ip>:/bulk_config.txt today_config.txt
```

- Copy operation:

```
pscp today_config.txt <user name>@<device ip>:/bulk_restore
```

▶ **Alternative of bulk configuration via SCP:**

Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure *device-specific* settings with the upload of raw configuration but not with the 'bulk configuration' file.

- ***Uploading or Downloading Raw Configuration Data*** (on page 505)

Backup and Restore via SCP

To back up ALL settings of a SRC, including device-specific settings, you should perform the backup operation instead of the bulk configuration.

You can restore all settings to previous ones after a backup file is available.

▶ **To back up the settings via SCP:**

1. Type the following SCP command and press Enter.

```
scp <user name>@<device ip>:/backup_settings.txt
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges

Raritan.
A brand of **legrand**

- *<device ip>* is the IP address or hostname of the SRC whose settings you want to back up.

2. Type the user password when prompted.

3. The system saves the settings from the SRC to a file named "backup_settings.txt."

▶ **To restore the settings via SCP:**

1. Type the following SCP command and press Enter.

```
scp backup_settings.txt <user name>@<device
ip>:/settings_restore
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges

- *<device ip>* is the IP address or hostname of the SRC whose settings you want to restore.

2. Type the user password when prompted.

3. The system copies the configuration included in the file "backup_settings.txt" to the SRC, and displays the following message.

```
Starting restore operation. The connection will be
closed now.
```

▶ **SCP examples:**

- Backup operation:

```
scp  admin@192.168.87.50:/backup_settings.txt
```

- Restoration operation:

```
scp  backup_settings.txt
admin@192.168.87.50:/settings_restore
```

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- Backup operation:

```
pscp <user name>@<device ip>:/backup_settings.txt
```

- Restoration operation:

```
pscp backup_settings.txt <user name>@<device
ip>:/settings_restore
```

Downloading Diagnostic Data via SCP

You can download the diagnostic data via SCP.

▶ **To download the diagnostic data via SCP:**

1. Type one of the following SCP commands and press Enter.

Scenario 1: Use the default SCP port and default filename

- SSH/SCP port is the default (22), and the accessed SRC is a standalone device.
- The diagnostic file's default filename "diag-data.zip" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/diag-data.zip .
```

Scenario 2: Specify a different SCP port but use the default filename

- SSH/SCP port is NOT the default (22), or the accessed SRC is a Port-Forwarding slave device.
- The diagnostic file's default filename "diag-data.zip" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip .
```

Scenario 3: Specify a new filename but use the default SCP port

- SSH/SCP port is the default (22), and the accessed SRC is a standalone device.
- Renaming the diagnostic file is wanted.

```
scp <user name>@<device ip>:/diag-data.zip <filename>
```

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed SRC is a Port-Forwarding slave device.
- Renaming the diagnostic file is wanted.

```
scp -P <port> <user name>@<device ip>:/diag-data.zip <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges or "Unrestricted View Privileges" privileges.
- *<device ip>* is the IP address or hostname of the SRC whose data you want to download.
- <port> is the current SSH/SCP port number, or the port number of a specific slave device in the Port-Forwarding chain.
- *<filename>* is the new filename of the downloaded file.

2. Type the password when prompted.

3. The system downloads the specified data from the SRC onto your computer.

- If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "diag-data.zip."
- If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

Raritan.
A brand of **legrand**

▶ **SCP example:**

```
scp  admin@192.168.87.50:/diag-data.zip .
```

▶ **Windows PSCP command:**

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/diag-data.zip <filename>`

Uploading or Downloading Raw Configuration Data

You can download the raw configuration data of a specific SRC for review, backup or modification.

After modifying or creating any raw configuration data, you can upload it to a specific SRC for changing its configuration. The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Syntax of the raw configuration data is completely the same as the syntax in the config.txt file. See *config.txt* (on page 520).

Warning: Some configuration keys in the downloaded raw configuration are commented out, and those must NOT be part of the configuration that will be uploaded to any SRC. See *Keys that Cannot Be Uploaded* (on page 508).

▶ **To download raw configuration data:**

1. Type one of the following SCP commands and press Enter.

Scenario 1: Use the default SCP port and default filename
- SSH/SCP port is the default (22), and the accessed SRC is a standalone device.
- The raw configuration file's default filename "raw_config.txt" is wanted. Then add a dot (.) in the end of the SCP command as shown below.

```
scp <user name>@<device ip>:/raw_config.txt .
```

Scenario 2: Specify a different SCP port but use the default filename
- SSH/SCP port is NOT the default (22), or the accessed SRC is a Port-Forwarding slave device.
- The raw configuration file's default filename "raw_config.txt" is wanted. Then add a dot in the end of the SCP command as shown below.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt .
```

Scenario 3: Specify a new filename but use the default SCP port

- SSH/SCP port is the default (22), and the accessed SRC is a standalone device.
- Renaming the raw configuration file is wanted.

```
scp <user name>@<device ip>:/raw_config.txt <filename>
```

Scenario 4: Specify a different SCP port and a new filename

- SSH/SCP port is NOT the default (22), or the accessed SRC is a Port-Forwarding slave device.
- Renaming the raw configuration file is wanted.

```
scp -P <port> <user name>@<device ip>:/raw_config.txt <filename>
```

- *<user name>* is the "admin" or any user profile with Administrator Privileges.
- *<device ip>* is the IP address or hostname of the SRC whose data you want to download.
- <port> is the current SSH/SCP port number, or the port number of a specific slave device in the Port-Forwarding chain.
- *<filename>* is the new filename of the downloaded file.

2. Type the password when prompted.

3. The system downloads the specified data from the SRC onto your computer.

    - If you do NOT specify a new filename in the command, such as Scenarios 1 or 2, the downloaded file's default name is "raw_config.txt."
    - If you specify a new filename in the command, such as Scenarios 3 or 4, the downloaded file is renamed accordingly.

▶ **To upload raw configuration data:**

1. Type one of the following SCP commands and press Enter.

Scenario 1: Only one SRC to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed SRC is a standalone device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp <config file> <user name>@<device ip>:/raw_config_update
```

Raritan.
A brand of ☐legrand'

Scenario 2: Only one SRC to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed SRC is a Port-Forwarding slave device.
- There is only one device to configure so a CSV file for device-specific settings is NOT needed.

```
scp -P <port> <config file> <user name>@<device ip>:/raw_config_update
```

Scenario 3: Multiple SRC to configure, with the default SCP port

- SSH/SCP port is the default (22), and the accessed SRC is a standalone device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp <dev_list file> <config file> <user name>@<device
ip>:/raw_config_update /match=<col>
```

Scenario 4: Multiple SRC to configure, with a non-default SCP port

- SSH/SCP port is NOT the default (22), or the accessed SRC is a Port-Forwarding slave device.
- There are multiple devices to configure so a CSV file for device-specific settings is needed during the upload.

```
scp -P <port> <dev_list file> <config file> <user name>@<device
ip>:/raw_config_update /match=<dev_col>
```

- `<config file>` is the filename of the custom raw configuration that you want to upload.
- *<user name>* is the "admin" or any user profile with Administrator Privileges.
- <device ip> is the IP address or hostname of the SRC where you want to upload the specified file.
- <port> is the current SSH/SCP port number, or the port number of a specific slave device in the Port-Forwarding chain.
- `<dev_list file>` is the name of the CSV file for configuring multiple SRC with device-specific settings. For this file's format, see ***devices.csv*** (on page 522).
    - For device-specific settings in the `<config file>`, refer each device-specific configuration key to a specific column in the `<dev_list file>`. See ***config.txt*** (on page 520).
- `<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each SRC is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings.

    For example:

- If the second column contains each device's serial number, the parameter is then `serial:2`.
- If the seventh column contains each device's MAC address, the parameter is then `mac:7`.

▶ **SCP examples:**

- Raw configuration download example --

  `scp  admin@192.168.87.50:/raw_config.txt config.txt`

- Raw configuration upload example with the configuration file only --

  `scp  config.txt`
  `admin@192.168.87.50:/raw_config_update`

- Raw configuration upload example with both configuration and device list files --

  `scp  devices.csv config.txt`
  `admin@192.168.87.50:/raw_config_update`
  `/match=serial:2`

▶ **Windows PSCP commands:**

PSCP in Windows works in a similar way to the SCP.

- `pscp -P <port> <user name>@<device ip>:/raw_config.txt`
  `<filename>`

- `pscp -P <port> <CSV file> <config file> <user`
  `name>@<device ip>:/raw_config_update /match=<col>`

▶ **Alternative of bulk configuration via SCP:**

Both methods of uploading 'bulk configuration' file or 'raw configuration' file via SCP can serve the purpose of bulk configuration. The only difference is that you can configure *device-specific* settings with the upload of raw configuration but not with the 'bulk configuration' file.

- *Bulk Configuration via SCP* (on page 501)

Keys that Cannot Be Uploaded

The raw configuration downloaded from any SRC contains a few configuration keys that are commented out with either syntax below.

Comment syntax	Description
#INTERNAL#	These keys are internal ones. They are NOT user configurable settings.
#OLD/INVALID#	These keys are old or invalid ones.

Raritan.
A brand of legrand

Note that these configuration keys cannot be part of the configuration that you will upload to any SRC. That is, they should be either not available or they remain to be commented out in the configuration file you will upload.

Appendix A   Specifications

In This Chapter

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for SRC is 60 degrees Celsius.

Serial RS-232 "RJ-45" Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	RTS	Output	Request to send
2	DTR	Output	Data terminal ready
3	TxD	Output	Transmit data
4	GND	—	Signal ground
5	DCD	Input	Data
6	RxD	Input	Receive data (data in)
7	DSR	Input	Data set ready
8	CTS	Input	Clear to send

Sensor RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (fuse protected)

RJ-45 Pin/signal definition			
2	+12V	—	Power (fuse protected)
3	GND	—	Signal Ground
4	RS485_DP	bi-directional	Data Positive of the RS-485 bus
5	RS485_DN	bi-directional	Data Negative of the RS-485 bus
6	GND	—	Signal Ground
7	1-wire	—	1-wire signal for Raritan environmental sensor packages
8	GND	—	Signal Ground

Note: A maximum of 500mA power is permitted for both pin 1 and pin 2 altogether.

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	+12V	—	Warning: Pin 6 is only intended for use with Raritan devices. Do NOT

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
			connect.
7	GND	—	Signal Ground
8	DCD	Input	Reserved

The front panel display shows one of the following diagrams.

Note that both diagrams represent the same state, but one uses larger text to indicate firmware upgrade is in progress.

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 SRC.

- Configuration changes
- Firmware upgrade
- Diagnostic data download

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 527).*

In This Chapter

Device Configuration/Upgrade Procedure

Any firmware **downgrade** using "fwupdate.cfg" is NOT supported by default. Only firmware upgrade is permitted with "fwupdate.cfg". A special parameter is required to permit firmware downgrade via "fwupdate.cfg". See *fwupdate.cfg* (on page 516).

Therefore, **firmware downgrade via USB** is disallowed by default.

You can use one USB drive to configure or upgrade multiple SRC devices one by one as long as it contains valid configuration files.

▶ **To use a USB drive to configure the SRC or upgrade firmware:**

1. Verify that both the USB drive and your SRC meet the requirements. See *System and USB Requirements* (on page 514).
2. Prepare required configuration files. See *Configuration Files* (on page 515).
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 SRC.
5. The initial message shown on the front panel display depends on the first task performed by the SRC.

> ▪ If no firmware upgrade task will be performed, a happy smiley is displayed after around 30 seconds.
>
> The happy smiley looks like the following diagram and its background color will turn green.

> ▪ If the USB drive contains the firmware upgrade data, the SRC:
>
> a. First performs the firmware upgrade, showing the upgrade message on the front panel display.
>
> b. Then shows the happy smiley when the firmware upgrade completes successfully. See **Firmware Upgrade via USB** (on page 525).

6. After the happy smiley appears, press one of the control buttons next to the display for one second until the smiley disappears.

Tip: You can remove the USB drive and plug it into another SRC device for performing the same task(s) once the happy smiley or the firmware upgrade message displays.

7. Wait for several seconds until the SRC resumes normal operation, indicated by the normal message of the display.

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.

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.

▶ **SRC system requirements:**

- There is at least one USB-A port available on your Raritan device.
- Your SRC must run firmware version   or later.

Note that the SRC interpreted the USB drive's contents using the firmware which was running when plugging the USB drive, not the new firmware after firmware upgrade.

▶ **USB drive requirements:**

- The drive contains either a single partition formatted as a Windows FAT32 filesystem, or NO partition tables (that is, a superfloppy-formatted drive).
- The drive contains a configuration file called *fwupdate.cfg* in its root directory. See **fwupdate.cfg** (on page 516).

Raritan.
A brand of ▢ legrand

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 516).

- **config.txt:**

  This file is used for configuring device settings. See *config.txt* (on page 520).

- **devices.csv:**

  This file is required only when there are device-specific settings to configure for multiple SRC devices. See *devices.csv* (on page 522).

Raritan provides a Mass Deployment Utility, which helps you quickly generate all configuration files for your SRC. See *Creating Configuration Files via Mass Deployment Utility* (on page 523).

---

fwupdate.cfg

The configuration file, *fwupdate.cfg*, is an ASCII text file containing key-value pairs, one per line.

Each value in the file must be separated by an equal sign (=), without any surrounding spaces. Keys are not case sensitive.

Illustration:

```
user=admin
password=raritan
logfile=log.txt
config=config.txt
device_list=devices.csv
```

This section only explains common options in the file.

Note: To make sure all of the following options work fine, you must update your SRC to the latest firmware version.

▶ **user**

- A required option.
- Specify the name of a user account with Administrator Privileges.
- For SRC with factory default configuration, set this option to `admin`.

▶ **password**

- A required option.
- Specify the password of the specified admin user.
- For SRC with factory default configuration, set this option to `raritan`.

Tip: You can add multiple user credentials to fwupdate.cfg. Each 'user' line must be immediately followed by its 'password' line. SRC will authenticate listed user credentials one by one until one of them succeeds, or until all user credentials fail.

Raritan.
A brand of ☐ legrand®

▶ **logfile**

• Specify the name of a text file where the SRC 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 messages are recorded. The disadvantage is that no feedback is available if the SRC detects a problem with the USB drive contents.

▶ **firmware**

• Specify the name of a firmware binary file used to upgrade your SRC.

• The specified firmware file must be compatible with your SRC and have an official Raritan signature.

• If the specified firmware file is the same as the current firmware version of your SRC, no firmware upgrade is performed.

• The default is to NOT permit any firmware **downgrade** via USB drive on Raritan power products with "USB-A" port(s). To do this, the parameter "allow_downgrade" must be present and properly set in the *fwupdate.cfg* file.

▶ **config**

• Specify the name of the configuration file containing device settings.

• The suggested filename is *config.txt*. See ***config.txt*** (on page 520).

▶ **device_list**

• Specify the name of the configuration file listing all SRC 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 522).

▶ **match**

• Specify a match condition for identifying a line or one SRC 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 SRC to search for the MAC address in the 7th column of the "devices.csv" file.

- The default value is `serial:1`, making the SRC search for its serial number in the first column.
- This option is used only if the "device_list" option has been set.

▶ **factory_reset**

- If this option is set to `true`, the SRC 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**

- Specify the name of the bulk configuration file used to configure or restore the SRC.

  Note: See **Bulk Configuration** *(on page 313) 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**

- Specify the name of the full configuration backup file used to restore the SRC.

  Note: See **Backup and Restore of Device Settings** *(on page 318) 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.

▶ **collect_diag**

- If this option is set to `true`, the diagnostic data of the SRC is transmitted to the USB drive.
- The filename of the diagnostic data written into the USB drive is:

  diag_<unit-serial>.zip

- The SRC device beeps after it finishes writing the diagnostic data to the USB drive.

▶ **tls_cert_file**

- Specify the filename of the wanted TLS server certificate. The filename can contain a single placeholder ${SERIAL} that is replaced with the serial number of the SRC.
- This option should be used with **tls_key_file** listed below.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

▶ **tls_key_file**

- Specify the filename of the wanted TLS server key. The filename can contain a single placeholder ${SERIAL} that is replaced with the serial number of the SRC.
- This option should be used with **tls_cert_file** listed above.
- *This option is NOT supported by bulk configuration or backup/restore via DHCP/TFTP.*

▶ **execute_lua_script**

- Specify a Lua script file. For example:
  ```
  execute_lua_script=my_script.lua
  ```
- Script output will be recorded to a log file -- <BASENAME_OF_SCRIPT>.<SERIAL_NUMBER>.log. Note this log file's size is limited on DHCP/TFTP.
- A DHCP/TFTP-located script has a timeout of 60 seconds. After that duration the script will be removed.
- This feature can be used to manage LuaService, such as upload, start, get output, and so on.
- If you unplug the USB drive while the Lua script is still running, the script will be removed.
- An exit handler can be used but the execution time is limited to three seconds. Note that this is not implemented on DHCP/TFTP yet.

▶ **allow_downgrade**

- This parameter is required for any firmware **downgrade** via *USB drive*, or the firmware upgrade via USB drive will fail.
- Add this parameter to this configuration file and set its value to *yes*.

Tip: Only firmware downgrade via USB is disabled by default. To downgrade firmware using other methods is still feasible by default, such as firmware downgrade via web interface.

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 516).

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 SRC 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 SRC model and firmware version.

Tip: You can choose to encrypt important data in the "config.txt" file so that people cannot easily recognize it, such as the SNMP write community string. See **Data Encryption in 'config.txt'** *(on page 524).*

▶ **Regular configuration key syntax:**

- Each configuration key and value pair is in a single line as shown below:

```
key=value
```

Note: Each value in the file must be separated by an equal sign (=), without any surrounding spaces.

- 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.

Raritan.

A brand of ⬛legrand®

▶ **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.

  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.

  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 522)

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:

   ```
   net.interfaces[eth0].ipv4.static.addr_cidr.addr=${4
   }
   pdu.name=${16}
   ```

▶ **To rename the admin user:**

You can rename the admin user by adding the following configuration key:

```
users[0].name=new admin name
```

Example:

```
users[0].name=May
```

▶ **To encrypt any settings:**

You can encrypt the value of any setting in the config.txt. See ***Data Encryption in 'config.txt'*** (on page 524).

▶ **To restore a specific setting to factory default:**

Add "delete:" to the beginning of the key whose setting you want to remove. The custom setting will be removed and then reset to factory default.

Example:

```
delete:net.port_forwarding
```

Raritan.
A brand of **legrand**

521

▶ **Tip:**

You can also download "config.txt" from a specific SRC or upload it to a specific SRC from anywhere in the world via Internet. See *Raw Configuration Upload and Download* (on page 550).

---

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 SRC device.

This file must be:

- A CSV (comma-separated values) format file exported from a spreadsheet application like Excel.
- Copied to the root directory of USB drive.
- Referenced in the *device_list* option of the "fwupdate.cfg" file. See *fwupdate.cfg* (on page 516).

Every SRC identifies its entry in the "devices.csv" file by comparing its serial number or MAC address to one of the columns in the file.

▶ **Determine the column to identify SRC devices:**

- By default, the SRC searches for its serial number in the 1st column of "devices.csv".
- To override the default, set the *match* option in the "fwupdate.cfg" file to a different column.

▶ **Syntax:**

- 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
  ```

Raritan.
A brand of **legrand**

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 firmware version number).

   ▪ It is available on the SRC product section of Raritan website's ***Support page*** (***http://www.raritan.com/support/***).

2. Launch Excel to open this utility.

   Note: Other office suites, such as OpenOffice and LibreOffice, are not supported.

3. Read the instructions in the 1st worksheet of the utility, and make sure Microsoft Excel's security level has been set to Medium or the equivalent for executing unsigned macros of this utility.

4. Enter information in the 2nd and 3rd worksheets.

   ▪ The 2nd worksheet contains information required for *fwupdate.cfg* and *config.txt*.

   ▪ The 3rd worksheet contains device-specific information for *devices.csv*.

5. Return to the 2nd worksheet 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 root directory of a connected USB drive.

   b. Click Export Lists to generate configuration files.
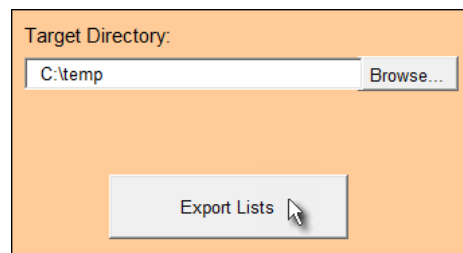
Verify that at least 3 configuration files are created - *fwupdate.cfg*, *config.txt* and *devices.csv*. You are ready to configure or upgrade any SRC with these files.

See ***Configuration or Firmware Upgrade with a USB Drive*** (on page 513).

Data Encryption in 'config.txt'

When intending to prevent people from identifying the values of any settings, you can encrypt them. Encrypted data still can be properly interpreted and performed by any SRC running firmware version 3.6.0 or later.

▶ **Data encryption procedure:**

1. Open the "config.txt" file to determine which setting(s) to encrypt.

   ▪ If an appropriate "config.txt" is not created yet, see *Creating Configuration Files via Mass Deployment Utility* (on page 523).

2. Launch a terminal to log in to the CLI of any SRC running version 3.6.0 or later. See *Logging in to CLI* (on page 356).

3. Type the encryption command and the value of the setting you want to encrypt.

   ▪ The value *cannot* contain any double quotes (") or backslashes (-).

   ▪ If the value contains spaces, it must be enclosed in double quotes.

   ```
   # config encrypt <value>

   -- OR --

   # config encrypt "<value with spaces>"
   ```

4. Press Enter. The CLI generates and displays the encrypted form of the typed value.

5. Go to the "config.txt" file and replace the chosen value with the encrypted one by typing or copying the encrypted value from the CLI.

6. Add the text "encrypted:" to the beginning of the encrypted setting.

7. Repeat steps 3 to 6 for additional settings you intend to encrypt.

8. Save the changes made to the "config.txt" file. Now you can use this file to configure any SRC running version 3.6.0 or later. See *Configuration or Firmware Upgrade with a USB Drive* (on page 513).

▶ **Illustration:**

In this example, we will encrypt the word "private", which is the value of the SNMP write community in the "config.txt" file.

snmp.write_community=private

1. In the CLI, type the following command to encrypt "private."

config encrypt private

2. The CLI generates and shows the encrypted form of "private."

```
ZTtnYcvQUw==
```

3. In the "config.txt" file, make the following changes to the SNMP write community setting.

   a. Replace the word "private" with the encrypted value that CLI shows.

```
snmp.write_community=ZTtnYcvQUw==
```

   b. Add "encrypted:" to the beginning of that setting.

```
encrypted:snmp.write_community=ZTtnYcvQUw==
```

Firmware Upgrade via USB

Firmware files are available on Raritan website's **Support page** (**http://www.raritan.com/support/**).

Note that if the firmware file used for firmware upgrade is the same as the firmware version running on the SRC, 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 516).

▶ **To use a USB drive to upgrade the SRC:**

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 *firmware* option of the "fwupdate.cfg" file.

3. Plug the USB drive into the USB-A port on the SRC.

4. The SRC performs the firmware upgrade.

   ▪ The front panel display shows the firmware upgrade progress.

   Tip: You can remove the USB drive and plug it into another SRC 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 SRC 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 SRC devices to configure or upgrade.

Warning: The feature of bulk configuration or firmware upgrade via DHCP/TFTP only works on standalone SRC devices directly connected to the network. This feature does NOT work for slave devices in the cascading configuration.

Tip: For the other alternatives, see **Configuration or Firmware Upgrade with a USB Drive** *(on page 513) or* **Raw Configuration Upload and Download** *(on page 550).*

In This Chapter

Bulk Configuration/Upgrade Procedure

> Any firmware **downgrade** using "fwupdate.cfg" is NOT supported by default. Only firmware upgrade is permitted with "fwupdate.cfg". A special parameter is required to permit firmware downgrade via "fwupdate.cfg". See *fwupdate.cfg* (on page 516).
>
> Therefore, firmware "downgrade" via DHCP/TFTP is disallowed by default.

▶ **Steps of using DHCP/TFTP for bulk configuration/upgrade:**

1. Create configuration files specific to your SRC models and firmware versions. See *Configuration Files* (on page 515) 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 529).

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 SRC.

   Click one or more of the following links for detailed DHCP configuration instructions, based on your operating system and the IP address type.

   - *DHCP IPv4 Configuration in Windows* (on page 529)
   - *DHCP IPv6 Configuration in Windows* (on page 539)
   - *DHCP IPv4 Configuration in Linux* (on page 546)
   - *DHCP IPv6 Configuration in Linux* (on page 548)

5. Make sure all of the desired SRC devices use DHCP as the IP configuration method and have been *directly* connected to the network.

6. Re-boot these SRC devices. The DHCP server will execute the commands in the "fwupdate.cfg" file on the TFTP server to configure or upgrade those SRC 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 528).

If you are going to upload any SRC 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 longer.

DHCP IPv4 Configuration in Windows

For those SRC 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's SRC under IPv4.

   a. Right-click the IPv4 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.
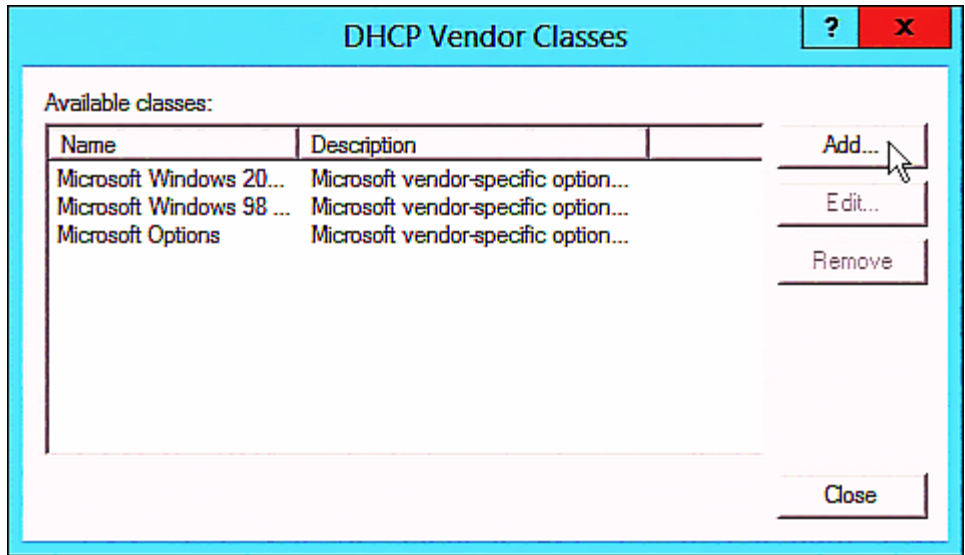
c. Specify a unique name for this vendor class and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU" in this illustration.
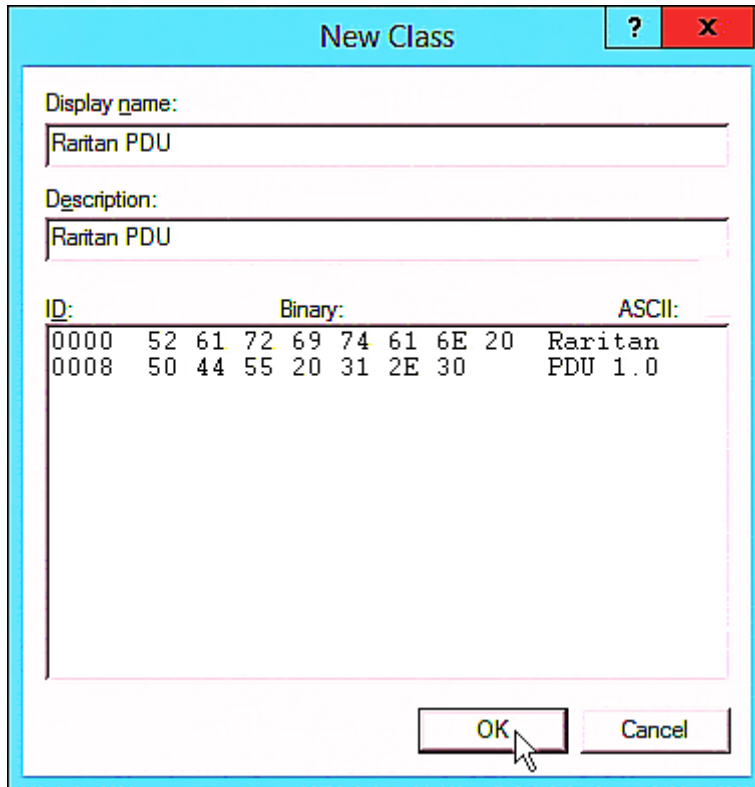
2. Define one DHCP standard option - Vendor Class Identifier.

a. Right-click the IPv4 node in DHCP to select Set Predefined Options.

b. Select DHCP Standard Options in the "Option class" field, and Vendor Class Identifier in the "Option name" field. Leave the String field blank.
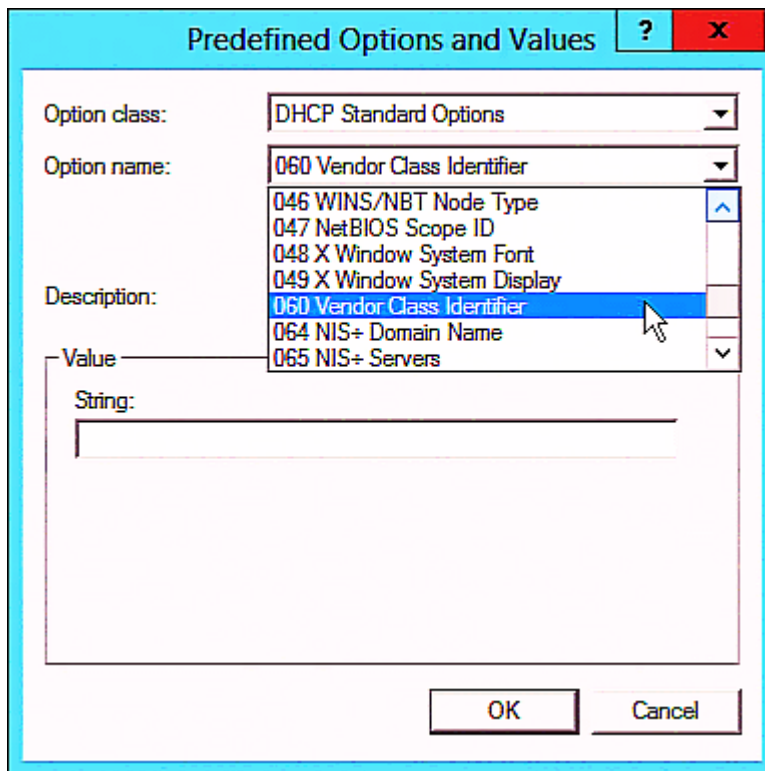
3. Add three options to the new vendor class "Raritan PDU" in the same dialog.

a. Select Raritan PDU in the "Option class" field.

b. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.

     c. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

     d. Click Add to add the third one. Type "pdu-update-magic" in the Name field, select String as the data type, and type 3 in the Code field.

4. Create a new policy associated with the "Raritan PDU" vendor class.

     a. Right-click the Policies node under IPv4 to select New Policy.

     b. Specify a policy name, and click Next.

The policy is named "PDU" in this illustration.

c.   Click Add to add a new condition.

d. Select the vendor class "Raritan PDU" in the Value field, click Add and then Ok.

e. Click Next.

f. Select DHCP Standard Options in the "Vendor class" field, select "060 Vendor Class Identifier" from the Available Options list, and type "Raritan PDU 1.0" in the "String value" field.

g. Select the "Raritan PDU" in the "Vendor class" field, select "001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv4 address in the "IP address" field.

h. Select "002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.

i. Select "003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv4 magic cookie is identical to or different from the IPv6 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Raritan.
A brand of legrand

Important: The magic cookie is transmitted to and stored in SRC 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 SRC. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

DHCP IPv6 Configuration in Windows

For those SRC 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's SRC under IPv6.

a. Right-click the IPv6 node in DHCP to select Define Vendor Classes.

b. Click Add to add a new vendor class.
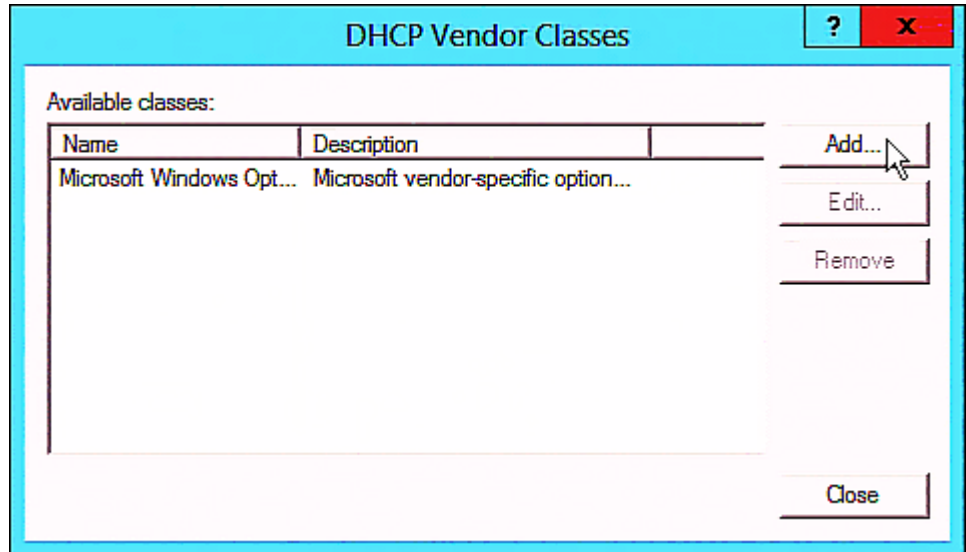
c. Specify a unique name for the vendor class, type "13742" in the "Vendor ID (IANA)" field, and type the binary codes of "Raritan PDU 1.0" in the New Class dialog.

The vendor class is named "Raritan PDU 1.0" in this illustration.

2. Add three options to the "Raritan PDU 1.0" vendor class.

    a. Right-click the IPv6 node in DHCP to select Set Predefined Options.

b. Select Raritan PDU 1.0 in the "Option class" field.

c. Click Add to add the first option. Type "pdu-tftp-server" in the Name field, select IP Address as the data type, and type 1 in the Code field.

d. Click Add to add the second option. Type "pdu-update-control-file" in the Name field, select String as the data type, and type 2 in the Code field.

Option Type

Class:	Raritan PDU 1.0
Name:	pdu-update-control-file
Data type:	String ▼ ☐ Array
Code:	2
Description:	

OK   Cancel

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.

Option Type

Class:	Raritan PDU 1.0
Name:	pdu-update-magic
Data type:	String ▼ ☐ Array
Code:	3
Description:	

OK   Cancel

3. Configure server options associated with the "Raritan PDU 1.0" vendor class.

a. Right-click the Server Options node under IPv6 to select Configure Options.

b. Click the Advanced tab.

c. Select "Raritan PDU 1.0" in the "Vendor class" field, select "00001 pdu-tftp-server" from the Available Options list, and type your TFTP server's IPv6 address in the "IPv6 address" field.

d. Select "00002 pdu-update-control-file" from the Available Options list, and type the filename "fwupdate.cfg" in the "String value" field.
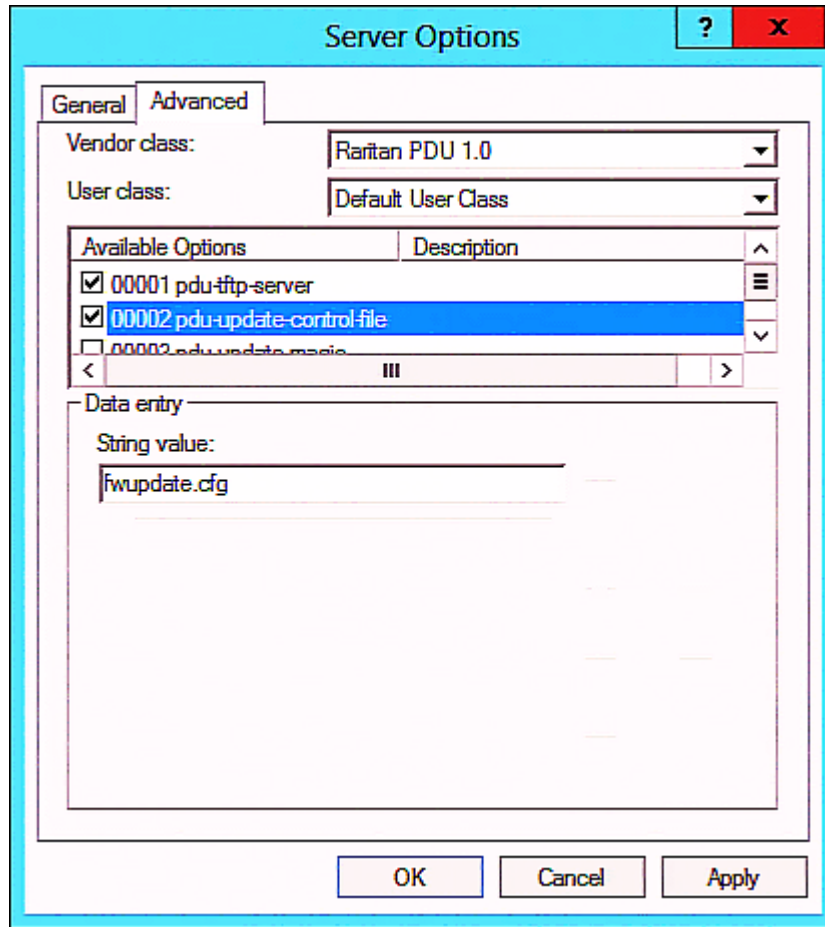
e. Select "00003 pdu-update-magic" from the Available Options list, and type any string in the "String value" field. This third option/code is the magic cookie to prevent the *fwupdate.cfg* commands from being executed repeatedly. It does NOT matter whether the IPv6 magic cookie is identical to or different from the IPv4 magic cookie.

The magic cookie is a string comprising numerical and/or alphabetical digits in any format. In the following illustration diagram, it is a combination of a date and a serial number.

Important: The magic cookie is transmitted to and stored in SRC 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 SRC. Therefore, you must modify the magic cookie's value in DHCP when intending to execute the "fwupdate.cfg" commands next time.

DHCP IPv4 Configuration in Linux

Modify the "dhcpd.conf" file for IPv4 settings when your DHCP server is running Linux.

▶ **Required Linux IPv4 settings in DHCP:**

1. Locate and open the "dhcpd.conf" file of the DHCP server.

2. The SRC 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 SRC 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 SRC 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 SRC. 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 SRC 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 SRC 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 SRC. 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　Raw Configuration Upload and Download

You can modify any existing "config.txt", and then upload it to a specific SRC for modifying part or all of its settings.

There are two ways to get one "config.txt":

- You create this file by yourself, either using or not using the Mass Deployment Utility. See **Configuration Files** (on page 515) and **config.txt** (on page 520).
- You download the raw configuration data from any SRC.

The downloaded raw configuration contains "almost" all of current settings on your SRC.

> Warning: Some configuration keys in the downloaded raw configuration are commented out, and those must NOT be part of the configuration that will be uploaded to any SRC. See **Keys that Cannot Be Uploaded** (on page 508).

Both configuration download and upload operations require the Administrator Privileges.

In This Chapter

Downloading Raw Configuration

There are three download methods:

- *Web browsers:* See **Download via Web Browsers** (on page 550).
- *SCP or PSCP command:* See **Uploading or Downloading Raw Configuration Data** (on page 505).
- *CURL command:* See **Download via Curl** (on page 551).

Download via Web Browsers

There are two scenarios by using web browsers.

▶　**URL containing login credentials:**

To log in immediately while issuing the download request, type an URL containing the login credentials in the web browser.

```
http(s)://<user>:<password>@<device IP>/cgi-bin/raw_config_download.cgi
```

Parameter	Description
`<user>`	Any user name that has the Administrator Privileges.
`<password>`	The password of the specified user name.
`<device IP>`	Hostname or IP address of the SRC whose raw configuration you want to download.

- For example:

```
https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

▶ **URL without login credentials contained:**

If you would like to log in after issuing the download request, type an URL without login credentials contained in the web browser. The system will then prompt you to enter the login credentials.

```
http(s)://<device IP>/cgi-bin/raw_config_download.cgi
```

- For example:

```
https://192.168.84.114/cgi-bin/raw_config_download.cgi
```

Download via Curl

If you have installed curl on your computer, you can download the raw configuration from your SRC by performing the curl command.

▶ **To download raw configuration from SRC via curl:**

1. Type the following curl command in the command line interface.

```
curl -k https://<user>:<password>@<device
IP>/cgi-bin/raw_config_download.cgi > config.txt
```

Parameter	Description
`<user>`	Any user name that has the Administrator Privileges.

Parameter	Description
`<password>`	The password of the specified user name.
`<device IP>`	Hostname or IP address of the SRC whose raw configuration you want to download.

2. When the download is complete, a line indicates 100 in the first % column.

3. Go to the directory where you perform the curl command to find the "config.txt" file.

Tip: In the above curl command, you can replace the filename "config.txt" with any filename you prefer.

▶ **Example:**

```
curl -k https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi >
config.txt
```

Uploading Raw Configuration

There are two upload methods:

- *SCP or PSCP command:* See **Uploading or Downloading Raw Configuration Data** (on page 505).
- *CURL command:* See **Upload via Curl** (on page 553).

The uploaded raw configuration file can contain only partial configuration keys that you want to modify. Other settings that are not contained in the uploaded file will remain unchanged.

Authentication-related data or HTTP(S) port may be no longer the same after uploading raw configuration. Therefore, it is suggested to **double check** what configuration keys will be changed in the raw configuration file that you will upload.

Upload via Curl

If curl is available on your computer, you can upload the raw configuration to SRC with the curl command.

There are two scenarios with the curl upload methods.

- When there are NO device-specific settings involved, you upload the configuration file only, regardless of the number of SRC devices to update.
- When there are device-specific settings involved for updating more than one SRC devices, you must upload two files. including one configuration file and one device list file.

▶ **To upload one configuration file only:**

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi
```

Parameter	Description
`<user>`	Any user name that has the Administrator Privileges.
`<password>`	The password of the specified user name.
`<device IP>`	Hostname or IP address of the SRC whose raw configuration you want to upload.
`<config file>`	Filename of the configuration file. ▪ For the syntax, see ***config.txt*** (on page 520).

2. When the upload is completed successfully, the curl returns the code 0 (zero).

   Note: If the upload fails and curl returns other codes, see **Curl Upload Return Codes** *(on page 554).*

3. After several seconds, SRC reboots automatically. Changed settings take effect after the reboot process finishes.

▶ **To upload both configuration and device list files:**

1. Type the following curl command in the command line interface.

```
curl -k -F "config_file=@<config file>" -F "device_list_file=@<dev_list file>" https://<user>:<password>@<device IP>/cgi-bin/raw_config_update.cgi?match=<dev_col>
```

Parameter	Description
`<user>`, `<password>`, `<device IP>`, `<config file>`	Refer to the above table for explanation. ■ For device-specific settings in the `<config file>`, refer each device-specific configuration key to a specific column in the `<dev_list file>`. See **config.txt** (on page 520).
`<dev_list file>`	Filename of the device list file in CSV format. ■ For the content format, see **devices.csv** (on page 522).
`<dev_col>`	`<dev_col>` comprises "serial:" or "mac:" and the number of the column where the serial number or MAC address of each SRC is in the uploaded CSV file. This is the data based on which each device finds its device-specific settings. For example: ■ If the second column contains each device's serial number, the parameter is then `serial:2`. ■ If the seventh column contains each device's MAC address, the parameter is then `mac:7`.

2. SRC will reboot after Curl shows the return code 0. For details, refer to above steps 2 to 3.

▶ **Examples:**

• Upload of the configuration file only:

```
curl -k -F "config_file=@config.txt"
https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

• Upload of both configuration and device list files:

```
curl -k -F "config_file=@config.txt" -F "device_list_file=@devices.csv"
https://admin:raritan@192.168.84.114/cgi-bin/raw_config_download.cgi
```

Curl Upload Return Codes

After performing raw configuration **Upload via Curl** (on page 553), curl will return a code to indicate the result of the file upload.

Code	Description
0	Operation was successful.

Raritan.
A brand of legrand

Code	Description
1	An internal error occurred.
2	A parameter error occurred.
3	A raw configuration update operation is already running.
4	The file is too large.
5	Invalid raw configuration file provided.
6	Invalid device list file or match provided.
7	Device list file required but missing.
8	No matching entry in device list found.
9	Macro substitution error.
10	Decrypting value failed.
11	Unknown magic line.
12	Processing magic line failed.

Appendix E   Resetting to Factory Defaults

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

Important: Exercise caution before resetting the SRC to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only firmware upgrade history is retained.

▶ **Alternative:**

Another method to reset it to factory defaults is to use the web interface. See *Resetting All Settings to Factory Defaults* (on page 323).

In This Chapter

Using the Reset Button

An RS-232 serial connection to a computer is required for using the reset button.
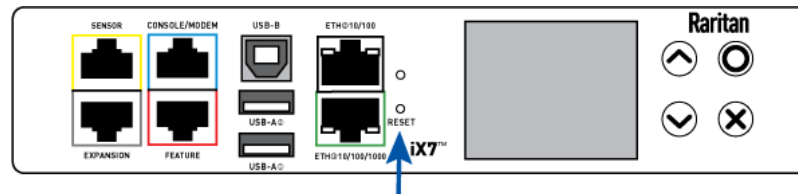
▶ **To reset to factory defaults using the reset button:**

1. Connect a computer to the SRC. See *Connecting the SRC to a Computer* (on page 21).

2. Launch a terminal emulation program such as Kermit or PuTTY, and open a window on the SRC. For information on the serial port configuration, see Step 2 of *Initial Network Configuration via CLI* (on page 630).

3. Press (and release) the Reset button of the SRC 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 SRC to its factory defaults.

5. Wait until the reset is complete.

Note: PuTTY 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 SRC to factory defaults. For information on CLI, see **Using the Command Line Interface** (on page 355).

▶ **To reset to factory defaults after logging in to the CLI:**

1. Connect to the SRC. See **Logging in to CLI** (on page 356) or **Connecting the SRC to a Computer** (on page 21).

2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the SRC. For information on the serial port configuration, see Step 2 of **Initial Network Configuration via CLI** (on page 630).

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 reset is complete.

▶ **To reset to factory defaults without logging in to the CLI:**

The SRC provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect to the SRC 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 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 SRC

b. Create user groups for the SRC on the AD server

c. Configure LDAP authentication on the SRC

d. Configure roles on the SRC

Important: Raritan disables SSL 3.0 and uses TLS 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 SRC. 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)
SRC_User	usera
	emxuser2
SRC_Admin	userb
	emxuser

Group permissions:

- The SRC_User role will only have read-only permissions.
- The SRC_Admin role will have full system permissions.

Step B. Configure User Groups on the AD Server

You must create the groups (roles) for the SRC on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups (roles) for the SRC are named *SRC_Admin* and *SRC_User*.
- User accounts *srcuser*, *srcuser2*, *usera* and *userb* already exist on the AD server.

▶ **To configure user groups on the AD server:**

1. On the AD server, create new groups -- *SRC_Admin* and *SRC_User*.

   Note: Refer to the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *srcuser2* and *usera* accounts to the SRC_User group.
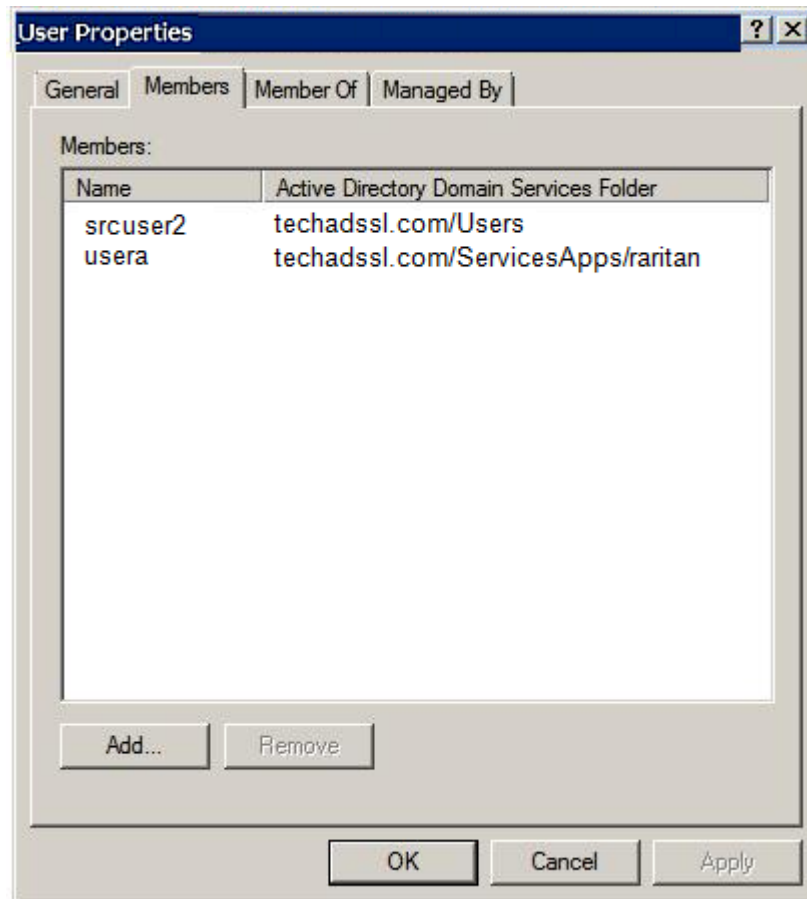
3. Add the *srcuser* and *userb* accounts to the SRC_Admin group.
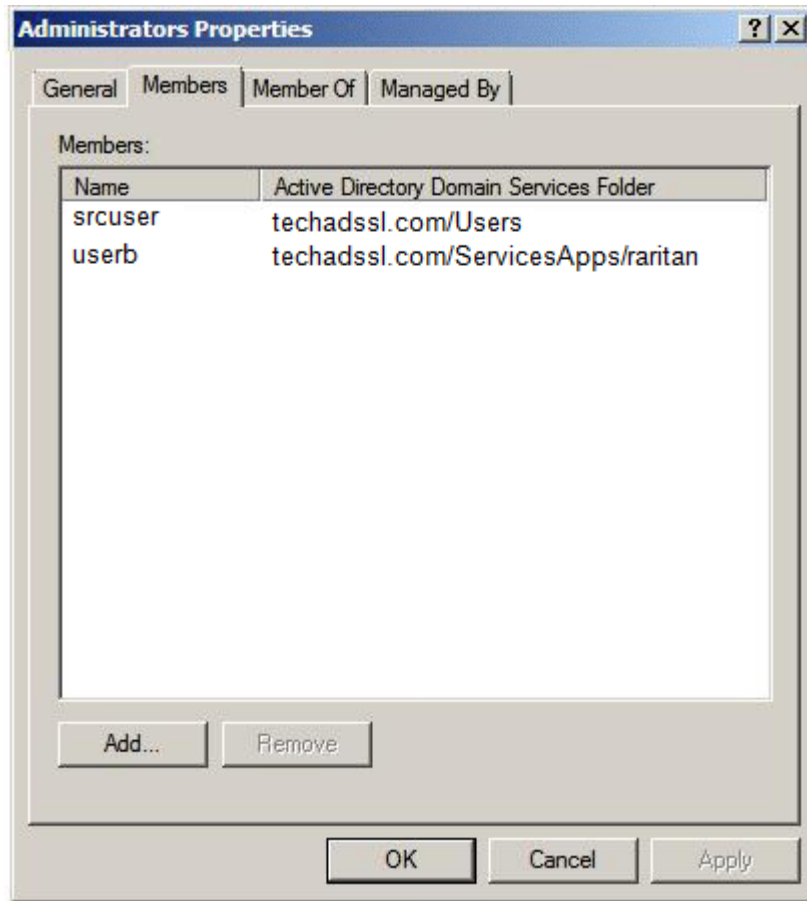
4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the SRC

You must enable and set up LDAP authentication properly on the SRC to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See **Wired Network Settings** (on page 161) and **Role of a DNS Server** (on page 624).

- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.

- The AD protocol is NOT encrypted over TLS.

- The AD server uses the default TCP port *389*.

- Anonymous bind is used.

▶ **To configure LDAP authentication:**

1. Choose Device Settings > Security > Authentication.

2. In the LDAP Servers section, click New to add an LDAP/LDAPS server.

3. Provide the SRC with the information about the AD server.

Field/setting	Do this...
IP address / hostname	Type the domain name `techadssl.com` or IP address `192.168.56.3`. ▪ Without the encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the encryption is enabled.
Copy settings from existing LDAP server	Leave the checkbox deselected unless the new LDAP server's settings are similar to any existing LDAP settings.
Type of LDAP server	Select "Microsoft Active Directory."
Security	Select "None" since the TLS encryption is not applied in this example.
Port (None/StartTLS)	Ensure the field is set to `389`.
Port (TLS), CA certificate	Skip the two fields since the TLS encryption is not enabled.
Anonymous bind	Select this checkbox because anonymous bind is used.
Bind DN, Bind password, Confirm bind password	Skip the three fields because of anonymous bind.
Base DN for search	Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.

Field/setting	Do this...
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`.

Raritan.
A brand of legrand

Add LDAP Server

IP address/hostname	192.168.52.55
	☐ Copy settings from existing 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 Show Remove
	Browse… Certificate file
	☐ Allow expired and not yet valid certificates
	☑ Anonymous bind
Bind DN	
Bind password	
Confirm bind password	
Base DN for search	techadssl.dc-com
Login Name Attribute	sAMAccountName
User entry object class	user
User search subfilter	
Active Directory domain	techadssl.com
	Test Connection

Note: LDAP authenticated users will see units from Default Preferences.

✖ Cancel   ✔ Add Server

4. Click Add Server.The LDAP server is saved.

5. In the Authentication Type field, select LDAP.

6. Click Save. The LDAP authentication is activated.

> *Note: If the SRC 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 SRC and the LDAP server to use the same NTP server(s).*

Step D. Configure Roles on the SRC

A role on the SRC determines the system permissions. You must create the roles whose names are identical to the user groups created for the SRC on the AD server or authorization will fail. Therefore, we will create the roles named *SRC_User* and *SRC_Admin* on the SRC device.

In this illustration, we assume:

- Users assigned to the *SRC_User* role can only access the SRC device and view settings.
- Users assigned to the *SRC_Admin* role can both access and configure the SRC device because they have the Administrator permissions.

▶ **To create the SRC_User role with appropriate permissions assigned:**

1. Choose User Management > Roles.

2. Click ![icon] to add a new role.

    a. Type `SRC_User` in the Role Name field.

    b. Type a description for the SRC_User role in the Description field. In this example, we type "View SRC settings" to describe the role.

Raritan.
A brand of **legrand**

c. In the Privileges list, select Unrestricted View Privileges, which includes all View permissions. The Unrestricted View Privileges permission lets users view all settings without the capability to configure or change them.

✔	Unrestricted View Privileges
☐	View Authentication Settings
☐	View Event Settings
☐	View Local Event Log
☐	View Local User Management
☐	View Security Settings
☐	View SNMP Settings
☐	View Webcam Snapshots and Configuration

d. Click Save.

3. The SRC_User role is created.

Role Name ▲	Description	
Admin	System defined administrator role including all privileges.	🔒
Operator	Predefined operator role.	
SRC_User	View SRC settings	

4. Keep the Roles page open to create the SRC_Admin role.

▶ **To create the SRC_Admin role with full permissions assigned:**

1. Click 👤➕ to add another role.

   a. Type `SRC_Admin` in the Role Name field.

   b. Type a description for the SRC_Admin role in the Description field. In this example, we type "Includes all SRC privileges" to describe the role.

c. In the Privileges list, select Administrator Privileges. The Administrator Privileges allows users to configure or change all SRC settings.

d. Click Save.

2. The SRC_Admin role is created.

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 SRC determines the permissions for a given user based on the permissions of the user's role. Your remote LDAP server can provide these user role names by returning an attribute named as follows:

rciusergroup   attribute type: string

This may require a schema extension on your LDAP/LDAPS server. Consult your authentication server administrator to enable this attribute.

In addition, for Microsoft® Active Directory®, the standard LDAP memberOf is used.

From Microsoft Active Directory

Note: This should be attempted only by an experienced Active Directory® administrator.

Returning user role information from Microsoft's® Active Directory for Windows 2000® operating system server requires updating the LDAP/LDAPS schema. See your Microsoft documentation for details.

1. Install the schema plug-in for Active Directory. See Microsoft Active Directory documentation for instructions.

2. Run Active Directory Console and select Active Directory Schema.

Setting the Registry to Permit Write Operations to the Schema

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

▶ **To permit write operations to the schema:**

1. Right-click the Active Directory® Schema root node in the left pane of the window and then click Operations Master. The Change Schema Master dialog appears.
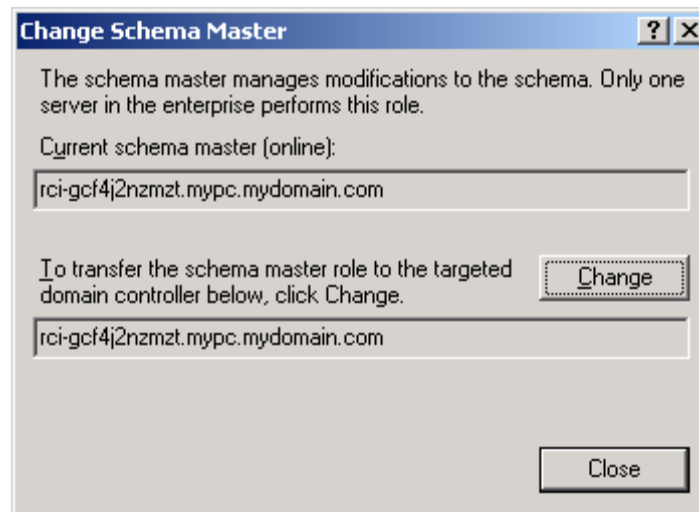
2. Select the "Schema can be modified on this Domain Controller" checkbox. **Optional**

3. Click OK.

Creating a New Attribute

▶ **To create new attributes for the rciusergroup class:**

1. Click the + symbol before Active Directory® Schema in the left pane of the window.

2. Right-click Attributes in the left pane.

3. Click New and then choose Attribute. When the warning message appears, click Continue and the Create New Attribute dialog appears.

4. Type *rciusergroup* in the Common Name field.
5. Type *rciusergroup* in the LDAP Display Name field.
6. Type *1.3.6.1.4.1.13742.50* in the Unique x5000 Object ID field.
7. Type a meaningful description in the Description field.
8. Click the Syntax drop-down arrow and choose Case Insensitive String from the list.
9. Type *1* in the Minimum field.
10. Type *24* in the Maximum field.
11. Click OK to create the new attribute.

Adding Attributes to the Class

▶ **To add attributes to the class:**

1. Click Classes in the left pane of the window.

2. Scroll to the user class in the right pane and right-click it.
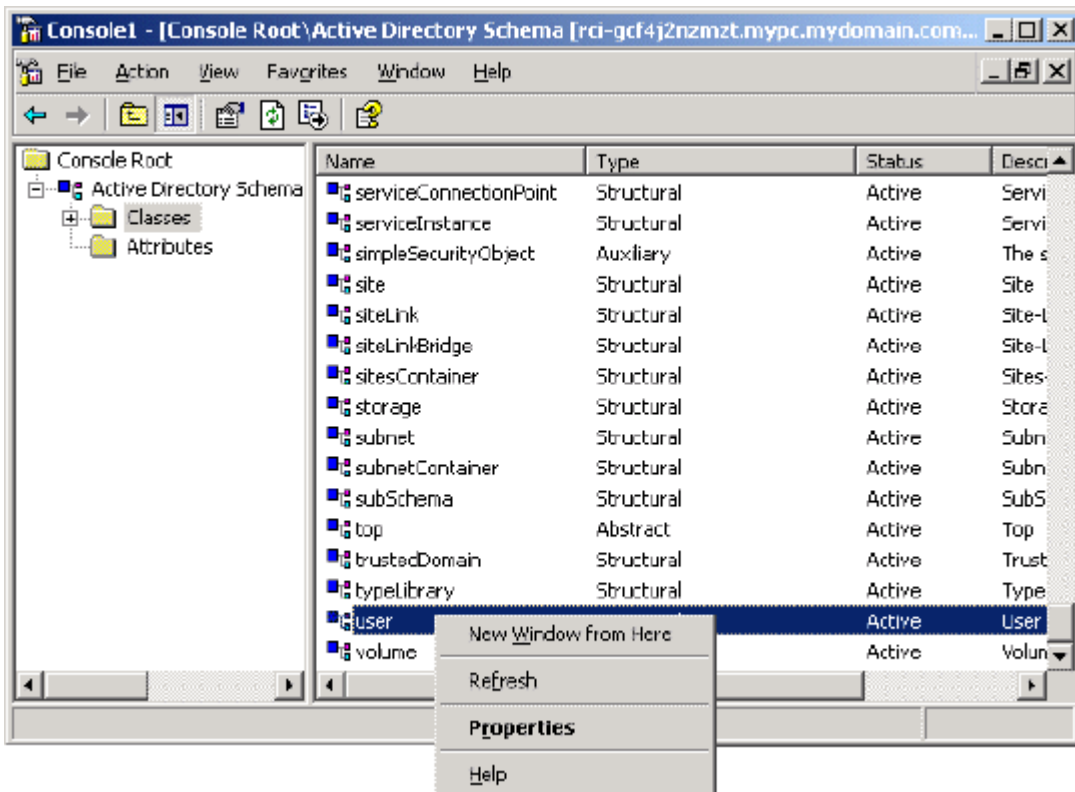
3. Choose Properties from the menu. The user Properties dialog appears.

4. Click the Attributes tab to open it.

5. Click Add.

6. Choose rciusergroup from the Select Schema Object list.
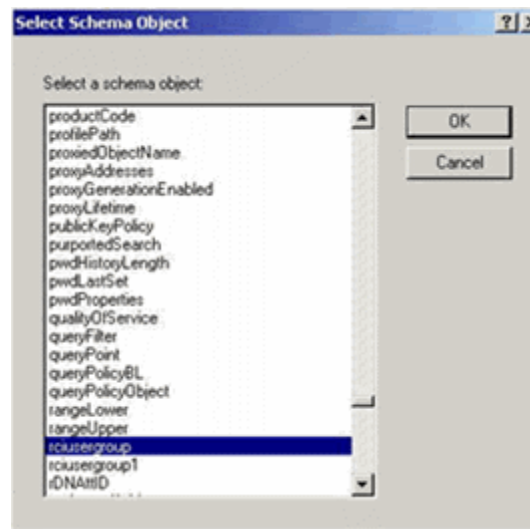
7. Click OK in the Select Schema Object dialog.

8. Click OK in the User Properties dialog.

Updating the Schema Cache

▶ **To update the schema cache:**

1. Right-click Active Directory® Schema in the left pane of the window and select Reload the Schema.

2. Minimize the Active Directory Schema MMC (Microsoft® Management Console) console.

Editing rciusergroup Attributes for User Members

To run the Active Directory® script on a Windows 2003® server, use the script provided by Microsoft® (available on the Windows 2003 server installation CD). These scripts are loaded onto your system with a Microsoft® Windows 2003 installation. ADSI (Active Directory Service Interface) acts as a low-level editor for Active Directory, allowing you to perform common administrative tasks such as adding, deleting, and moving objects with a directory service.

▶ **To edit the individual user attributes within the group rciusergroup:**

1. From the installation CD, choose Support > Tools.

2. Double-click SUPTOOLS.MSI to install the support tools.

3. Go to the directory where the support tools were installed. Run adsiedit.msc. The ADSI Edit window opens.
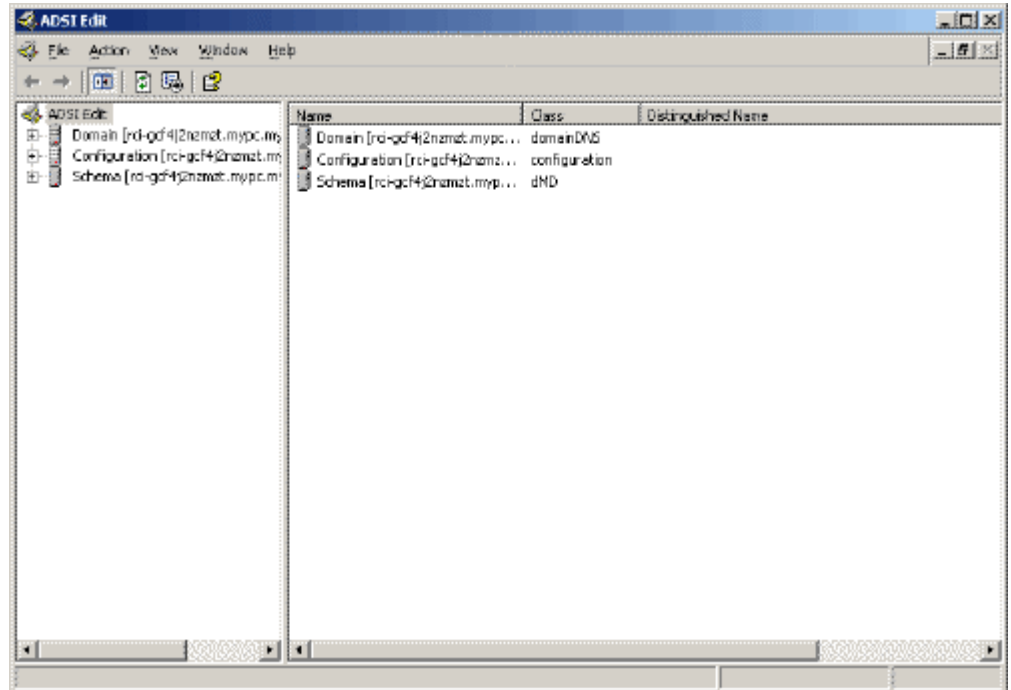
4. Open the Domain.

5. In the left pane of the window, select the CN=Users folder.
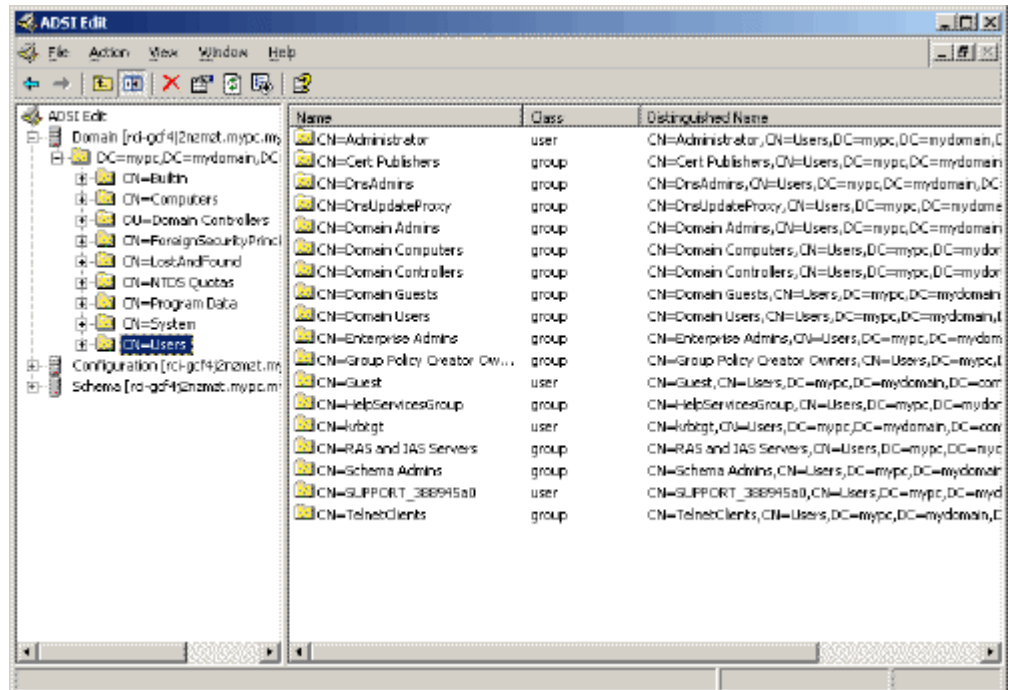
6. Locate the user name whose properties you want to adjust in the right pane. Right-click the user name and select Properties.

7. Click the Attribute Editor tab if it is not already open. Choose rciusergroup from the Attributes list.
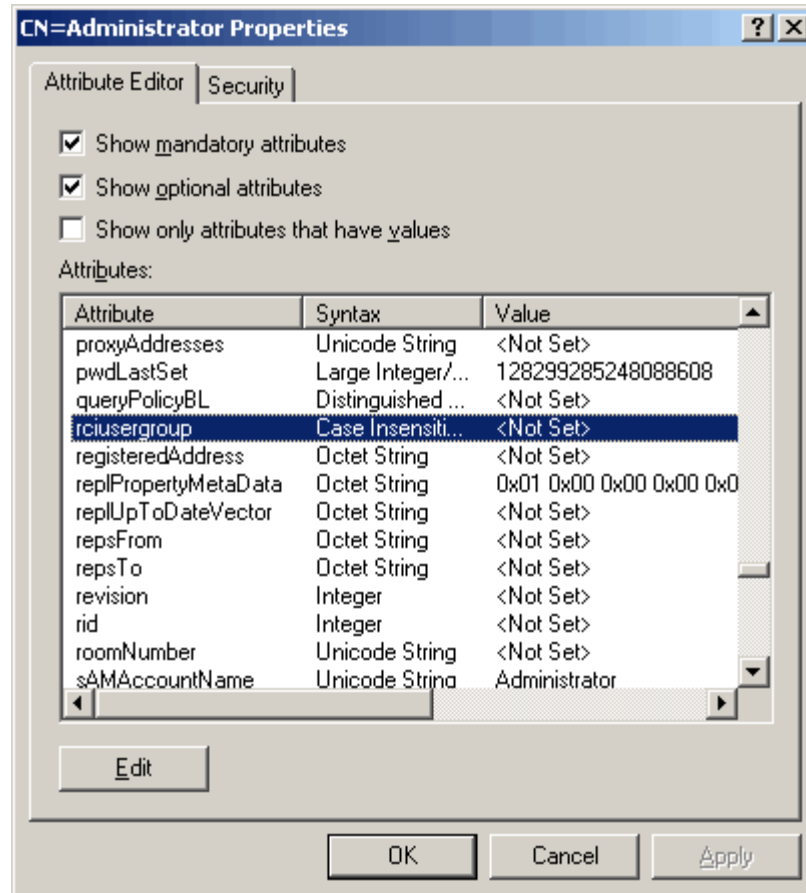
8. Click Edit. The String Attribute Editor dialog appears.

9. Type the user role (created in the SRC) in the Edit Attribute field. Click OK.
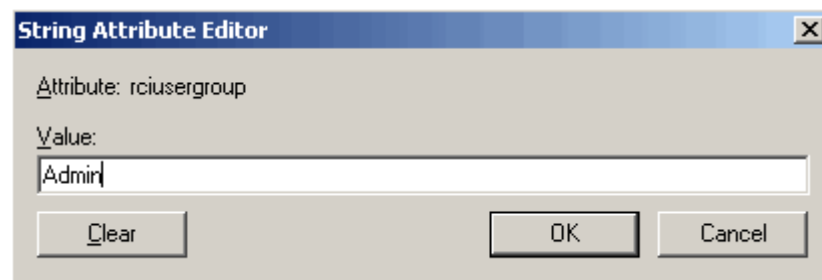
Appendix H   RADIUS Configuration Illustration

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 FreeRADIUS server.

The following steps are required for any RADIUS authentication:

1. Configure RADIUS authentication on the SRC. See *Adding Radius Servers* (on page 213).

2. Configure roles on the SRC. See *Creating Roles* (on page 153).

3. Configure SRC user credentials and roles on your RADIUS server.

   ▪ To configure using standard attributes, see *Standard Attributes* (on page 574).

   ▪ To configure using vendor-specific attributes, see *Vendor-Specific Attributes* (on page 593).

Note that we assume that the NPS is running on a Windows 2008 system in the NPS illustrations.

In This Chapter

Standard Attributes

The RADIUS standard attribute "Filter-ID" is used to convey the group membership, that is, roles.

- If a user has multiple roles, configure multiple standard attributes for this user.

- The syntax of a standard attribute is:

  `Raritan:G{role-name}`

For configuration on NPS, see *NPS Standard Attribute Illustration* (on page 574).

For configuration on FreeRADIUS, see *FreeRADIUS Standard Attribute Illustration* (on page 592).

NPS Standard Attribute Illustration

To configure Windows 2008 NPS with the *standard attribute*, you must:

a. Add your SRC to NPS. See *Step A: Add Your SRC as a RADIUS Client* (on page 575).

b. On the NPS, configure Connection Request Policies and the standard attribute. See **Step B: Configure Connection Policies and Standard Attributes** (on page 579).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See **AD-Related Configuration** (on page 606).

Step A: Add Your SRC as a RADIUS Client

The RADIUS implementation on the SRC follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

▶ **Presumptions in the illustration:**

• IP address of your SRC = `192.168.56.29`

• RADIUS authentication port specified for SRC: *1812*

• RADIUS accounting port specified for SRC: *1813*

▶ **To add your SRC to the RADIUS NPS:**

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.

2. Right-click NPS (Local), and select Properties.

Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your SRC. In this example, they are 1812 and 1813. Then close this dialog.

3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.

4. Do the following to add your SRC to NPS:

   a. Verify the "Enable this RADIUS client" checkbox is selected.

   b. Type a name for identifying your SRC 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 SRC.

5. Click OK.

Step B: Configure Connection Policies and Standard Attributes

You need to configure the following for connection request policies:

- IP address or host name of the SRC
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ **Presumptions in the illustration:**

- IP address of your SRC = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your SRC = `CHAP`
- Existing role of your SRC = `Admin`

▶ **Illustration:**

1. Open the NPS console, and expand the Policies folder.

2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.

3. Type a descriptive name for identifying this policy in the "Policy name" field.

- You can leave the "Type of network access server" field to the default
  -- Unspecified.

4.   Click Next to show the "Specify Conditions" screen. Click Add.

5.   The "Select condition" dialog appears. Click Add.

6. The NAS IPv4 Address dialog appears. Type the SRC IP address -- *192.168.56.29*, and click OK.

7. Click Next in the New Connection Request Policy dialog.

8. Select "Authenticate requests on this server" because a local NPS server is used in this example. Then click Next.

Note: Connection Request Forwarding options must match your environment.

9. When the system prompts you to select the authentication method, select the following two options:

   ▪ Override network policy authentication settings

   ▪ CHAP -- the SRC uses "CHAP" in this example

Raritan.
A brand of legrand

Note: If your SRC uses PAP, then select "PAP."

10. Select Standard to the left of the dialog and then click Add.
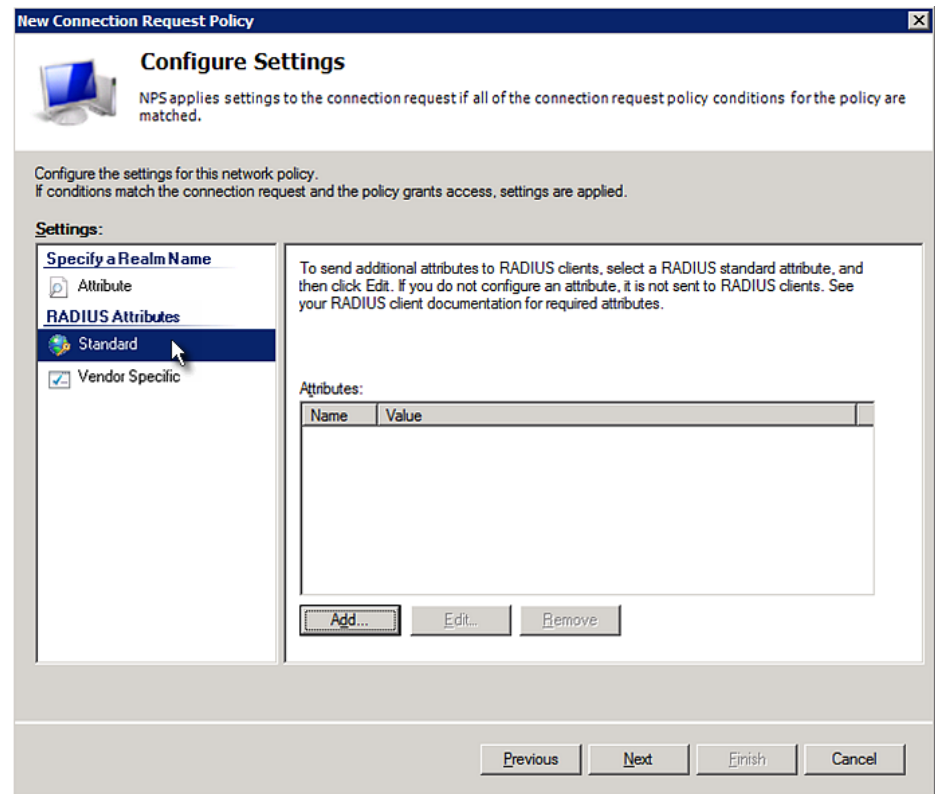
11. Select Filter-Id from the list of attributes and click Add.
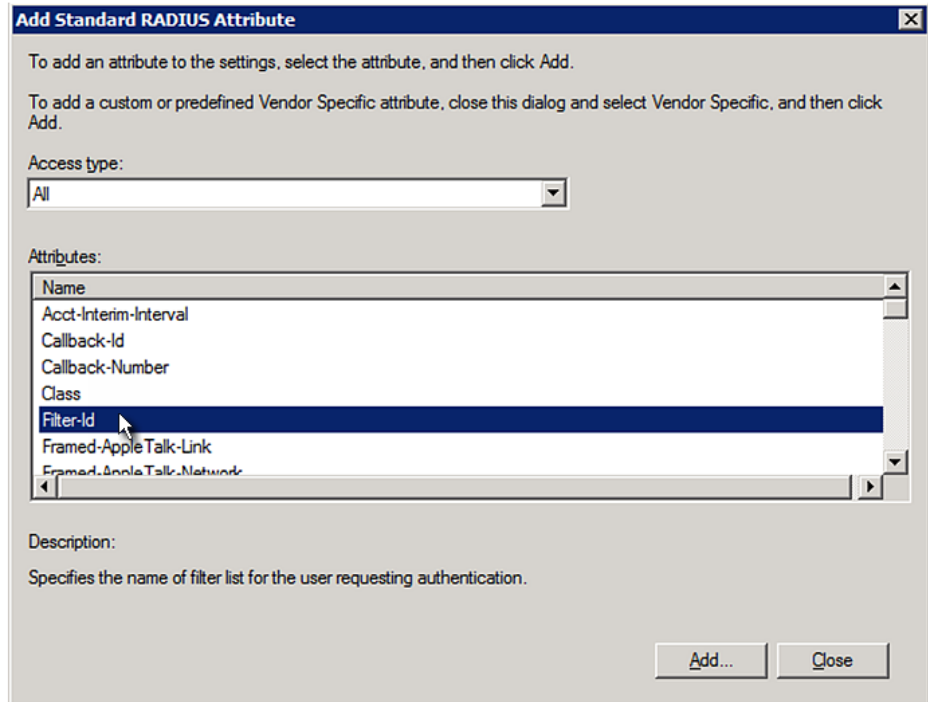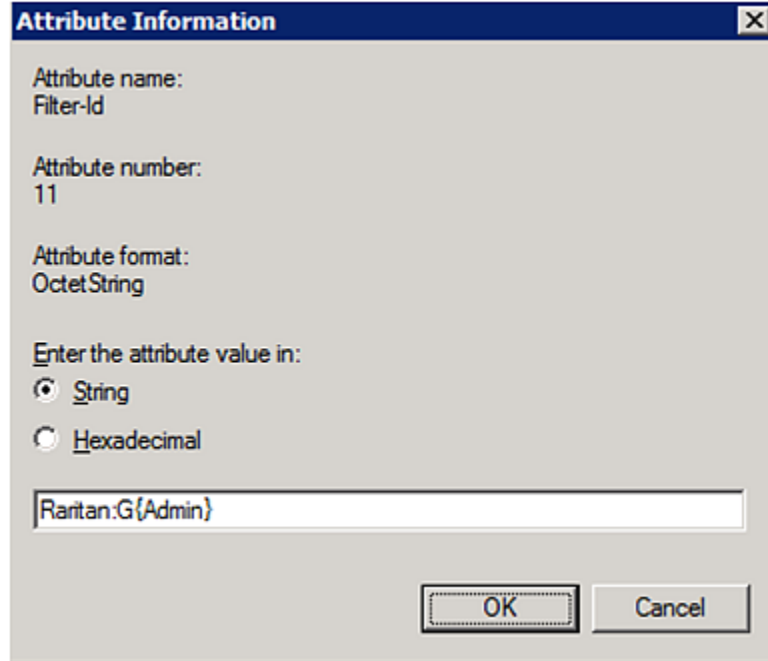
12. In the Attribute Information dialog, click Add.
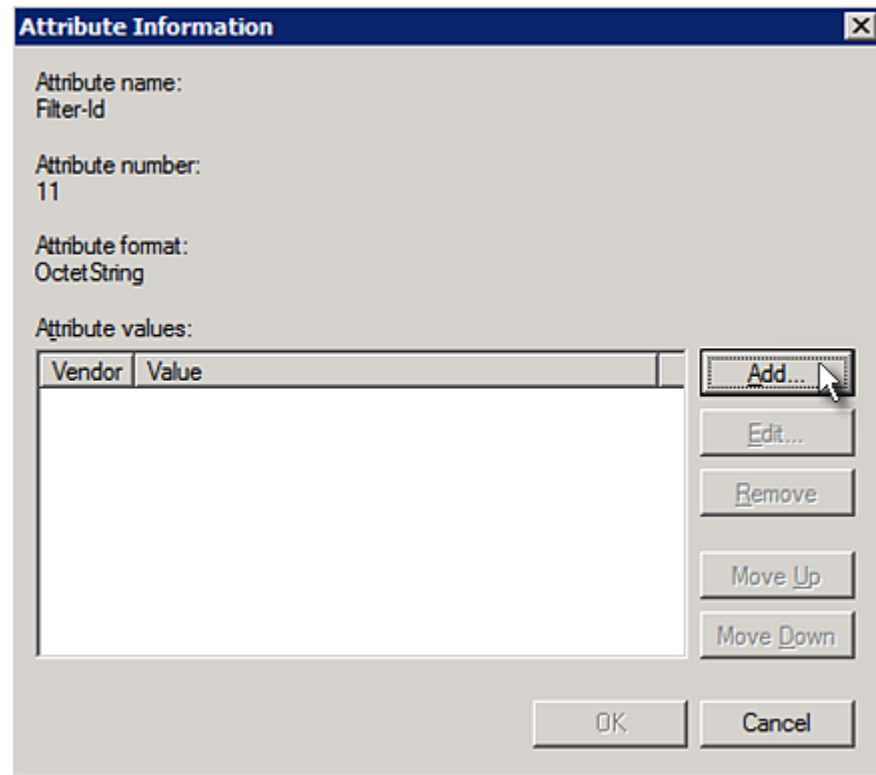
13. Select String, type *Raritan:G{Admin}* in the text box, and then click OK.

Admin inside the curved brackets {} is the existing role on the SRC. It is recommended to use the Admin role to test this configuration. The role name is case sensitive.

14. The new attribute is added. Click OK.

15. Click Next to continue.

16. A summary showing connection request policy settings is displayed. Click Finish to close the dialog.
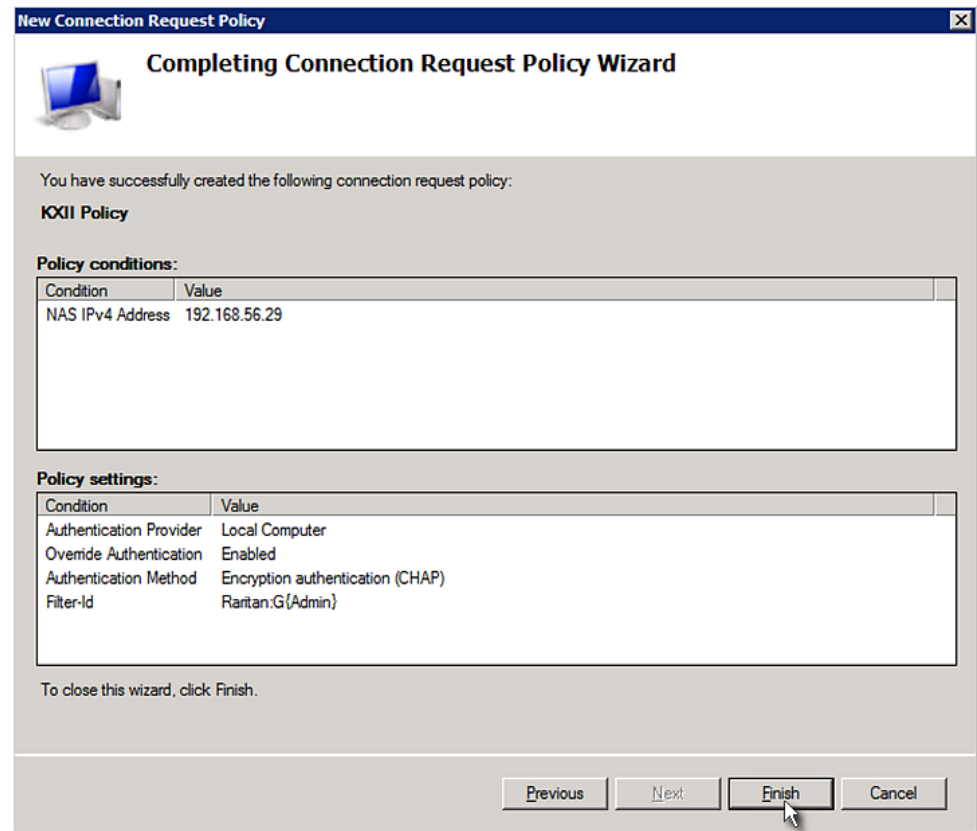
FreeRADIUS Standard Attribute Illustration

With standard attributes, NO dictionary files are required. You simply add all user data, including user names, passwords, and roles, in the following FreeRADIUS path.

```
/etc/raddb/users
```

▶ **Presumptions in the illustration:**

- User name = `steve`
- Steve's password = `test123`
- Steve's roles = `Admin` and `SystemTester`

▶ **To create a user profile for "steve" in FreeRADIUS:**

1. Go to this location: `/etc/raddb/users.`

2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Filter-ID = "Raritan:G{Admin}",
Filter-ID = "Raritan:G{SystemTester}"
```

Vendor-Specific Attributes

You must specify the following properties when using a RADIUS vendor-specific attribute (VSA).

- Vendor code = `13742`
- Vendor-assigned attribute number = `26`
- Attribute format = `String`

The syntax of the vendor-specific attribute for specifying one or multiple roles is:

```
Raritan:G{role-name1 role-name2 role-name3}
```

For configuration on NPS, see *NPS VSA Illustration* (on page 593).

For configuration on FreeRADIUS, see *FreeRADIUS VSA Illustration* (on page 605).

NPS VSA Illustration

To configure Windows 2008 NPS with the *vendor-specific attribute*, you must:

a. Add your SRC to NPS. See *Step A: Add Your SRC as a RADIUS Client* (on page 575).

b. On the NPS, configure connection request policies and the vendor-specific attribute. See *Step B: Configure Connection Policies and Vendor-Specific Attributes* (on page 598).

Some configuration associated with Microsoft Active Directory (AD) is also required for RADIUS authentication. See *AD-Related Configuration* (on page 606).

Step A: Add Your SRC as a RADIUS Client

The RADIUS implementation on the SRC follows the standard RADIUS Internet Engineering Task Force (IETF) specification so you must select "RADIUS Standard" as its vendor name when configuring the NPS server.

▶ **Presumptions in the illustration:**

- IP address of your SRC = `192.168.56.29`

- RADIUS authentication port specified for SRC: *1812*

- RADIUS accounting port specified for SRC: *1813*

▶ **To add your SRC to the RADIUS NPS:**

1. Choose Start > Administrative Tools > Network Policy Server. The Network Policy Server console window opens.

2. Right-click NPS (Local), and select Properties.

Verify the authentication and accounting port numbers shown in the properties dialog are the same as those specified on your SRC. In this example, they are 1812 and 1813. Then close this dialog.

3. Under "RADIUS Clients and Servers," right-click RADIUS Client and select New RADIUS Client. The New RADIUS Client dialog appears.

4. Do the following to add your SRC to NPS:

   a. Verify the "Enable this RADIUS client" checkbox is selected.

   b. Type a name for identifying your SRC 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 SRC.

5. Click OK.

Step B: Configure Connection Policies and Vendor-Specific Attributes

You need to configure the following for connection request policies:

- IP address or host name of the SRC
- Connection request forwarding method
- Authentication method(s)
- Standard RADIUS attributes

▶ **Presumptions in the illustration:**

- IP address of your SRC = `192.168.56.29`
- *Local* NPS server is used
- RADIUS protocol selected on your SRC = `CHAP`
- Existing roles of your SRC = `Admin, User` and `SystemTester`

▶ **Illustration:**

1. Open the NPS console, and expand the Policies folder.

2. Right-click Connection Request Policies and select New. The New Connection Request Policy dialog appears.

3. Type a descriptive name for identifying this policy in the "Policy name" field.

- You can leave the "Type of network access server" field to the default
-- Unspecified.

4. Click Next to show the "Specify Conditions" screen. Click Add.

5. The "Select condition" dialog appears. Click Add.

6. The NAS IPv4 Address dialog appears. Type the SRC IP address --
   192.168.56.29, and click OK.

7. Click Next in the New Connection Request Policy dialog.

8. Select "Authenticate requests on this server" because a local NPS server is
   used in this example. Then click Next.

Raritan.
A brand of ☐ legrand®

Note: Connection Request Forwarding options must match your environment.

9. When the system prompts you to select the authentication method, select the following two options:

   ▪ Override network policy authentication settings

   ▪ CHAP -- the SRC uses "CHAP" in this example

Note: If your SRC uses PAP, then select "PAP."

10. Select Vendor Specific to the left of the dialog, and click Add. The Add Vendor Specific Attribute dialog appears.

11. Select Custom in the Vendor field, and click Add. The Attribute Information dialog appears.

12. Click Add, and the Vendor-Specific Attribute Information dialog appears.

13. Click "Enter Vendor Code" and type *13742*.

14. Select "Yes, it conforms" to indicate that the custom attribute conforms to the RADIUS Request For Comment (RFC).

15. Click Configure Attribute, and then:

    a. Type *26* in the "Vendor-assigned attribute number" field.

    b. Select String in the "Attribute format" field.

    c. Type *Raritan:G{Admin User SystemTester}* in the "Attribute value" field. In this example, three roles 'Admin,' 'User' and 'SystemTester' are specified inside the curved brackets {}.

Note that multiple roles are separated with a space.
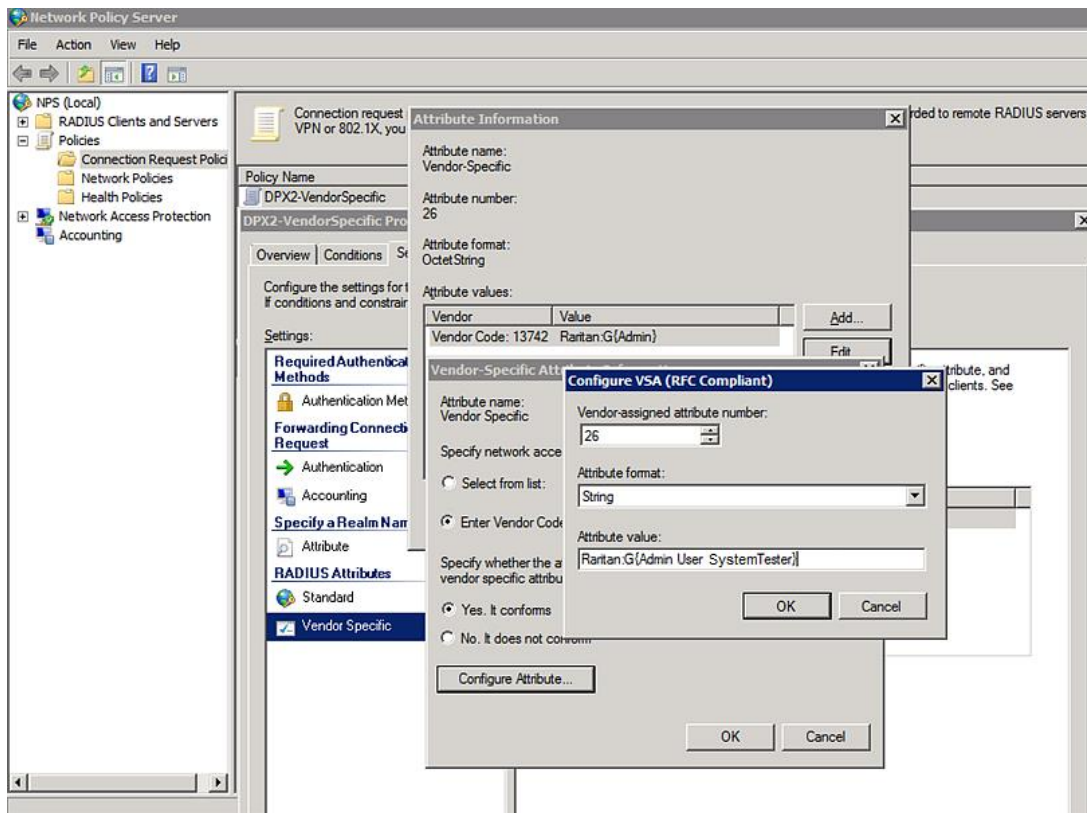
16. Click OK.

FreeRADIUS VSA Illustration

A vendor-specific dictionary file is required for the vendor-specific-attribute configuration on FreeRADIUS. Therefore, there are two major configuration steps.

a. Use a dictionary to define the Raritan vendor-specific attribute

b. Add all user data, including user names, passwords, and roles

▶ **Presumptions in the illustration:**

• Raritan attribute = `Raritan-User-Roles`

• User name = `steve`

• Steve's password = `test123`

• Steve's roles = `Admin`, `User` and `SystemTester`

▶ **Step A -- define the vendor-specific attribute in FreeRADIUS:**

1. Go to this location: `/etc/raddb/dictionary`.

2. Type the following in the Raritan dictionary file.

```
VENDOR Raritan 13742
BEGIN-VENDOR Raritan
ATTRIBUTE Raritan-User-Roles 26 string
END-VENDOR Raritan
```

▶ **Step B -- create a user profile for "steve" in FreeRADIUS:**

1. Go to this location: `/etc/raddb/users`.

2. Add the data of the user "steve" by typing the following. Note that the values after the equal sign (=) must be enclosed in double quotes (").

```
steve Cleartext-Password := "test123"
Raritan-PDU-User-Roles = "Raritan:G{Admin User SystemTester}"
```

AD-Related Configuration

When RADIUS authentication is intended, make sure you also configure the following settings related to Microsoft Active Directory (AD):

- Register the NPS server in AD
- Configure remote access permission for users in AD

The NPS server is registered in AD only when NPS is configured for the FIRST time and user accounts are created in AD.

If CHAP authentication is used, you must enable the following feature for user accounts created in AD:

- Store password using reversible encryption

Important: Reset the user password if the password is set before you enable the "Store password using reversible encryption" feature.

▶ **To register NPS:**

1. Open the NPS console.

Raritan.
A brand of ⬜legrand

2. Right-click NPS (Local) and select "Register server in Active Directory."
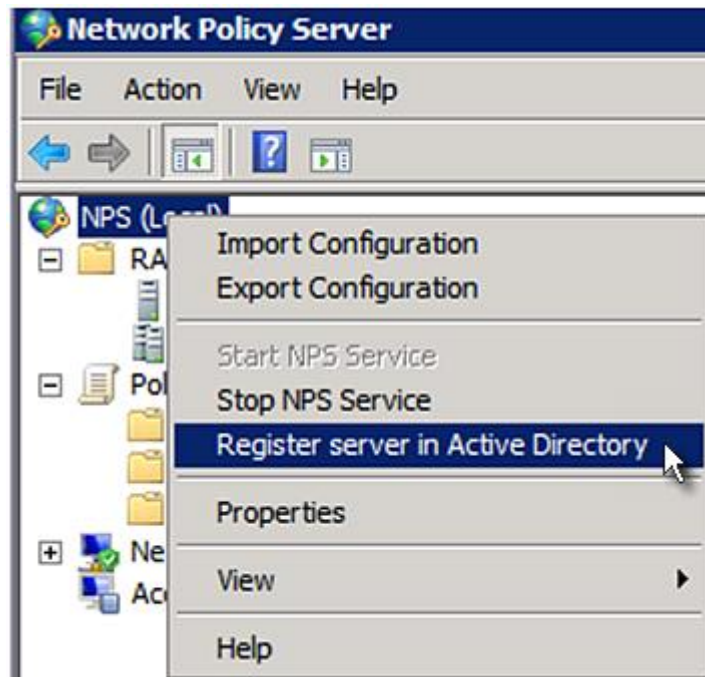
3. Click OK, and then OK again.
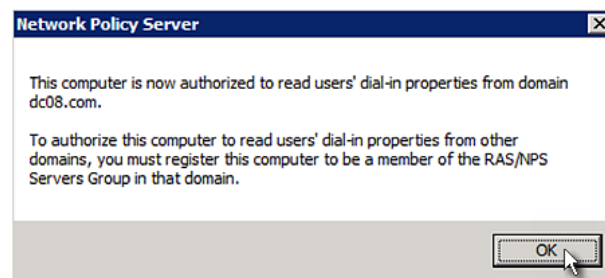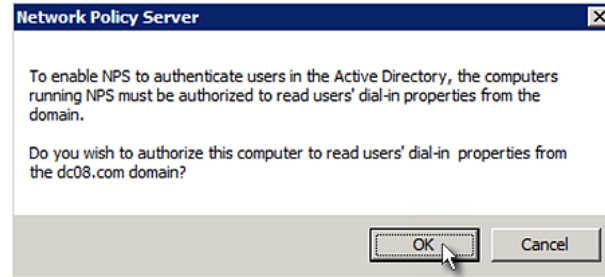
▶ **To grant SRC users remote access permission:**

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.
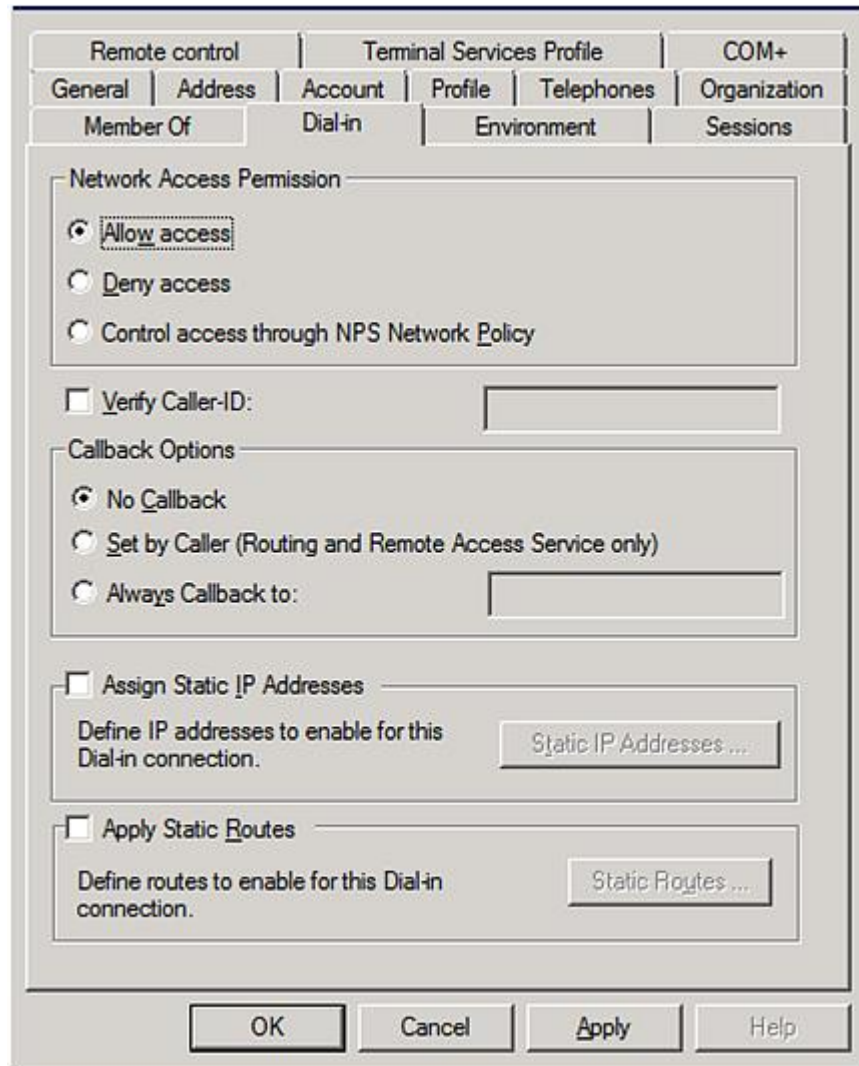
▶   **To enable reversible encryption for CHAP authentication:**

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.

Appendix I   Additional SRC Information

In This Chapter

RJ45-to-DB9 Cable Requirements for Modem Connections

An RJ45-to-DB9 adapter/cable is required for connecting a modem to the SRC device.

A third party RJ45-to-DB9 adapter/cable needs to meet the following requirements.

- RJ-45 to "DB9 male"
- RX/TX and according control pins are NOT crossed
- With the following pin assignments:

Pin signal	DB9 pin No.	RJ-45 pin No.
DCD	1	5
RxD	2	6
TxD	3	3
DTR	4	2
GND	5	4
DSR	6	7
RTS	7	1
CTS	8	8
RIR	9	N/A

Note: The RJ45-to-DB9 adapter/cable used for connecting modems CANNOT be used to connect the SRC to a computer. See **RJ45-to-DB9 Cable Requirements for Computer Connections** *(on page 22).*

Reserving IP Addresses in DHCP Servers

SRC uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the SRC in a DHCP server, use the SRC device's serial number as the unique ID instead of the MAC address.

Since all network interfaces of the SRC can be simultaneously enabled and configured with diverse static IP addresses, the client identifier of each network interface is different. The main difference is the absence/presence of a suffix, which is the interface name added to the end of the serial number. The table below lists the client identifiers of all network interfaces.

Interface	Client identifier
ETH1	serial number
ETH2	serial number plus the uppercase suffix "-ETH2"
WIRELESS	serial number plus the uppercase suffix "-WIRELESS"
BRIDGE	serial number

You can reserve the IP addresses of more than one interfaces in the DHCP server if preferred. Note that you must choose/configure the bridge interface if your SRC is set to the bridging mode.

Important: In the bridging mode, only the IP parameters of the BRIDGE interface function. The IP parameters of ETH1/ETH2 and WIRELESS interfaces do NOT function.

Reserving IP in Windows

To reserve the IP address of any network interface in the Windows DHCP server, you must convert that interface's client identifier into *hexadecimal* ASCII codes.

For each interface's client identifier, see **Reserving IP Addresses in DHCP Servers** (on page 611).

In the following illustration, it is assumed that the SRC serial number is PEG1A00003.

▶ **Windows IP address reservation illustration:**

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 54 48 32** ▪ The suffix comprising the dash symbol and the word "ETH2" is also converted.
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ▪ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. In your DHCP server, bring up the New Reservation dialog, and separate the converted ASCII codes with spaces.

    For example, to reserve the ETH1 interface's IP address, enter the following data in the dialog.

Field	Data entered
IP address	The IP address you want to reserve.
MAC address	The following ASCII codes. `50 45 47 31 41 30 30 30 30 33`
Other fields	Configure as needed.

Raritan.
A brand of legrand

Reserving IP in Linux

There are two methods to reserve the IP address of any network interface in the standard Linux DHCP server (ISC DHCP server):

- Convert an interface's client identifier into *hexadecimal* ASCII codes.
- Use an interface's original client identifier without converting it into ASCII codes.

For each interface's client identifier, see **Reserving IP Addresses in DHCP Servers** (on page 611).

In the following illustrations, it is assumed that the SRC serial number is PEG1A00003, and the IP address you want to reserve is 192.168.20.1.

▶ **Illustration with ASCII code conversion:**

1. Convert the client identifier of the desired network interface into ASCII codes (*hexadecimal*).

Interface	Client identifier conversion
ETH1	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33
ETH2	PEG1A00003-**ETH2** = 50 45 47 31 41 30 30 30 30 33 **2D 45 54 48 32** ■ The suffix comprising the dash symbol and the word "ETH2" is also converted.
WIRELESS	PEG1A00003-**WIRELESS** = 50 45 47 31 41 30 30 30 30 33 **2D 57 49 52 45 4C 45 53 53** ■ The suffix comprising the dash symbol and the word "WIRELESS" is also converted.
BRIDGE	PEG1A00003 = 50 45 47 31 41 30 30 30 30 33

2. Separate the converted ASCII codes with a colon, and a prefix "00:" must be added to the beginning of the converted codes.

   For example, the *converted* client identifier of the ETH1 interface looks like the following:
   ```
   00:50:45:47:31:41:30:30:30:30:33
   ```

3. Now enter the converted client identifier with the following syntax.

   ```
   host mypx {
   option dhcp-client-identifier = 00:50:45:47:31:41:30:30:30:30:33;
   fixed-address 192.168.20.1;
   }
   ```

▶   **Illustration without ASCII code conversion:**

1. Use the original client identifier of the desired network interface. DO NOT convert them into ASCII codes.

2. A prefix "\000" must be added to the beginning of the client identifier.

    For example, the client identifier of the ETH1 interface looks like the following:

    `\000`PEG1A00003

3. Now enter the original client identifier with the following syntax. The client identifier is enclosed in quotation marks.

    ```
    host mypx {
    option dhcp-client-identifier = "\000PEG1A00003";
    fixed-address 192.168.20.1;
    }
    ```

Sensor Threshold Settings

This section explains the thresholds settings for a numeric sensor.

Thresholds and Sensor States

A numeric sensor has four thresholds: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

The threshold settings determine how many sensor states are available for a certain sensor and the range of each sensor state. The diagram below shows how each threshold relates to each state.

| above upper critical |
| Upper Critical |
| above upper warning |
| Upper Warning |
| normal |
| Lower Warning |
| below lower warning |
| Lower Critical |
| below lower critical |
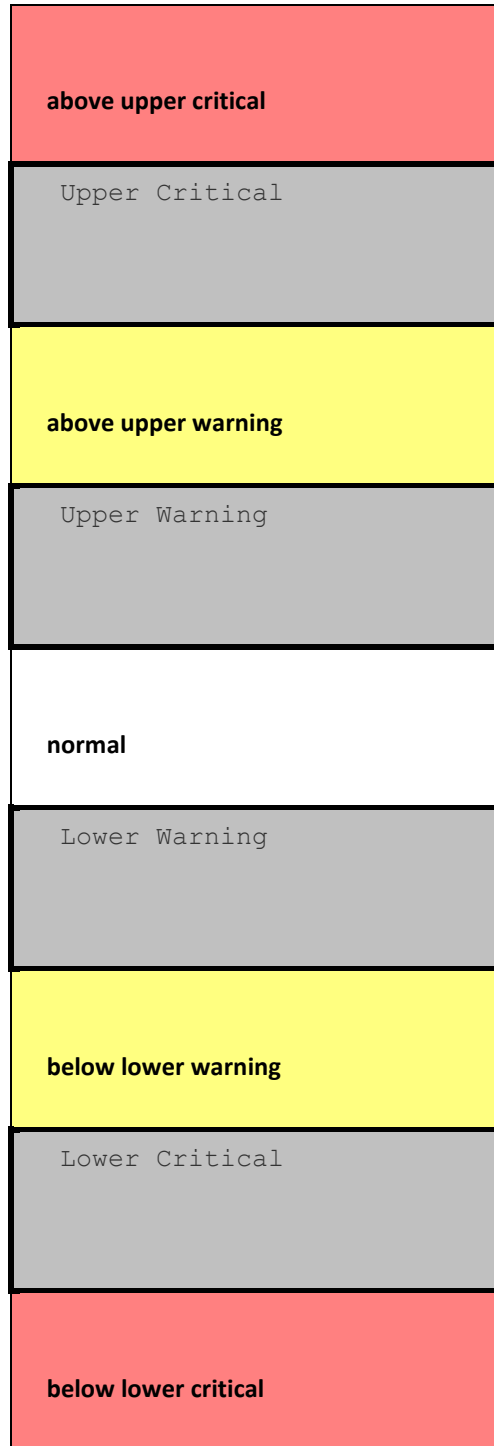
▶   **Available sensor states:**

The more thresholds are enabled for a sensor, the more sensor states are available for it. The "normal' state is always available regardless of whether any threshold is enabled.

For example:

- When a sensor only has the Upper Critical threshold enabled, it has two sensor states: normal and above upper critical.
- When a sensor has both the Upper Critical and Upper Warning thresholds enabled, it has three sensor states: normal, above upper warning, and above upper critical.

States of "above upper warning" and "below lower warning" are warning states to call for your attention.

States of "above upper critical" and "below lower critical" are critical states that require you to immediately handle.

▶ **Range of each available sensor state:**

The value of each enabled threshold determines the reading range of each available sensor state. For details, see *Yellow- or Red-Highlighted Sensors* (on page 115).

"To Assert" and Assertion Timeout

If multiple sensor states are available for a specific sensor, the SRC asserts a state for it whenever a bad state change occurs.

▶ **To assert a state:**

To assert a state is to announce a new, "worse" state.

Below are bad state changes that cause the SRC to assert.
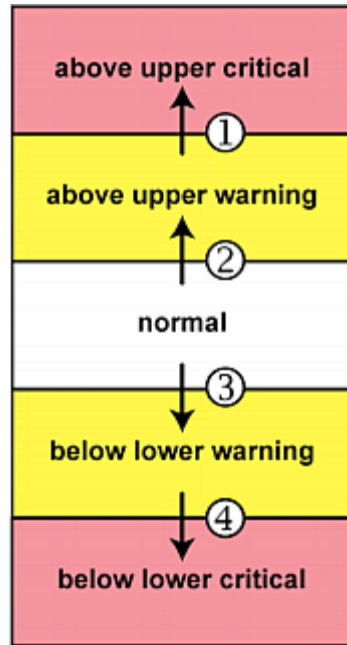
1. above upper warning --> above upper critical

2. normal --> above upper warning

3. normal --> below lower warning

4. below lower warning --> below lower critical

▶ **Assertion Timeout:**

In the threshold settings, the Assertion Timeout field postpones the "assertion" action. It determines how long a sensor must remain in the "worse" new state before the SRC triggers the "assertion" action. If that sensor changes its state again within the specified wait time, the SRC does NOT assert the worse state.

To disable the assertion timeout, set it to 0 (zero).

Note: For most sensors, the measurement unit in the "Assertion Timeout" field is sample. Sensors are measured every second, so the timing of a sample is equal to a second. Raritan's BCM2 is an exception to this, with a sample of 3 seconds.

▶ **How "Assertion Timeout" is helpful:**

If you have created an event rule that instructs the SRC to send notifications for assertion events, setting the "Assertion Timeout" is helpful for eliminating a number of notifications that you may receive in case the sensor's readings fluctuate around a certain threshold.

Assertion Timeout Example for Temperature Sensors

Assumption:
```
Upper Warning threshold is enabled.
Upper Warning = 25 (degrees Celsius)
Assertion Timeout = 5 samples (that is, 5 seconds)
```

When a temperature sensor's reading exceeds 25 degrees Celsius, moving from the "normal" range to the "above upper warning" range, the SRC 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 SRC performs the "assertion" action to announce the "above upper warning" state.

- If the temperature drops below 25 degrees Celsius within 5 seconds, the SRC does NOT perform the "assertion" action.

"To De-assert" and Deassertion Hysteresis

After the SRC asserts a worse state for a sensor, it may de-assert that state later on if the readings improve.

▶ **To de-assert a state:**

To de-assert a state is to announce the end of the previously-asserted worse state.

Below are good state changes that cause the SRC to de-assert the previous state.
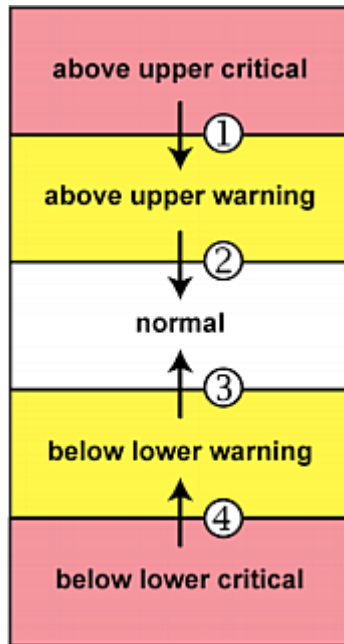
1. above upper critical --> above upper warning

2. above upper warning --> normal

3. below lower warning --> normal

4. below lower critical --> below lower warning

▶ **Deassertion Hysteresis:**

In the threshold settings, the Deassertion Hysteresis field determines a new level to trigger the "deassertion" action.

This function is similar to a thermostat, which instructs the air conditioner to turn on the cooling system when the temperature exceeds a pre-determined level. "Deassertion Hysteresis" instructs the SRC to de-assert the worse state for a sensor only when that sensor's reading reaches the pre-determined "deassertion" level.

For upper thresholds, this "deassertion" level is a decrease against each threshold. For lower thresholds, this level is an increase to each threshold. The absolute value of the decrease/increase is exactly the hysteresis value.

For example, if Deassertion Hysteresis = 2, then the deassertion level of each threshold is either "+2" or "-2" as illustrated below.

Threshold value	Deassertion value
Upper Critical = 33	Deassertion level = 31 • 33 - 2 = 31
Upper Warning = 25	Deassertion level = 23 • 25 - 2 = 23
Lower Critical = 10	Deassertion level = 12 • 10 + 2 = 12
Lower Warning = 18	Deassertion level = 20 • 18 + 2 = 20

To use each threshold as the "deassertion" level instead of determining a new level, set the Deassertion Hysteresis to 0 (zero).

Note: The difference between Upper Warning and Lower Warning must be at least "two times" of the deassertion value.

▶ **How "Deassertion Hysteresis" is helpful:**

If you have created an event rule that instructs the SRC to send notifications for deassertion events, setting the "Deassertion Hysteresis" is helpful for eliminating a number of notifications that you may receive in case a sensor's readings fluctuate around a certain threshold.

Deassertion Hysteresis Example for Temperature Sensors

Assumption:
```
Upper Warning threshold is enabled.
Upper Warning = 20 (degrees Celsius)
Deassertion Hysteresis = 3 (degrees Celsius)
"Deassertion"  level = 20-3 = 17 (degrees Celsius)
```

When the SRC 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 SRC does NOT perform the "deassertion" action.
- If the temperature drops to 17 degrees Celsius or lower, the SRC performs the "deassertion" action to announce the end of the "above upper warning" state.

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 SRC.

- With SNMP v3 activated, you get the "user unknown" error when the user name used to authenticate does not exist.

- Any user with the permission to view event rules can query all local existing users via JSON RPC.

- Any user with the permission to view the event log may get information about existing users from the log entries.

- Any authenticated users can query currently-existing connection sessions, including Webcam-Live-Preview sessions, which show a list of associated user names.

Raritan Training Website

Raritan offers free training materials for various Raritan products on the *Raritan training website http://www.raritantraining.com*. The Raritan products introduced on this website include intelligent PDU, KVM, EMX, BCM, and CommandCenter Secure Gateway (CC-SG).

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.

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 SRC may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the SRC 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 208).

Cascading Troubleshooting

Any accessibility problem occurred on one of the devices in the cascading chain may result in failure to access all downstream slave devices that are connected to it.

Raritan.
A brand of ◻legrand

Possible Root Causes

The following lists the network accessibility issues and possible root causes.

You can always troubleshoot the software settings by connecting the SRC to a computer if network access to that SRC fails. See *Connecting the SRC to a Computer* (on page 21).

Symptom	Probable cause

Failure to access the master device	• Anything below is lost or loose on the master device:
	  ▪ Network connection
	  ▪ Power supply
	• Anything below is disabled on the master device:
	  ▪ The Ethernet or wireless interface
	  ▪ IPv4 or IPv6 settings
	• In the Port Forwarding mode, related settings are incorrectly configured on the master device.
	  ▪ The master device's role is incorrectly set to 'Slave'.
	  ▪ The interface where the network is connected is incorrectly set as the downstream interface.
	• For the wireless networking, one of the following issues occurs:
	  ▪ The USB wireless LAN adapter attached to the master device is not the Raritan USB WIFI LAN adapter. See *USB Wireless LAN Adapters* (on page 12).
	  ▪ The wireless LAN configuration is not supported. See *Supported Wireless LAN Configuration* (on page 13).
	  ▪ The installed CA certificate chain contains any certificate that has expired or is not valid yet.

Symptom	Probable cause

Failure to access a slave device	• One of the following issues occurs on the master device:
	
	  ▪ Network connection is lost.
	
	  ▪ Power is lost.
	
	  ▪ The Ethernet or wireless interface is disabled.
	
	• One of the following issues occurs on the slave device in question or any upstream device (if available):
	
	  ▪ Connection of the cascading cable is loose or lost.
	
	  ▪ No power supply.
	
	  ▪ The cascading mode is set incorrectly.
	
	    For example, the master device is set to Bridging, but the slave device in question or any upstream device is set to Port Forwarding.
	
	• In the Bridging mode, IPv4 (or IPv6) settings are disabled on the slave device in question.
	
	• In the Port Forwarding mode, one of the following issues occurs:
	
	  ▪ The master device's role is incorrectly set to 'Slave'.
	
	  ▪ The master device's downstream interface is incorrectly set. For example, you use a USB cable to connect the 1st slave device, but select the Ethernet port as the downstream interface.
	
	  ▪ The role of the slave device in question or any upstream device is set to 'Master' instead of 'Slave'.
	
	  ▪ The port number you added to the IP address is incorrect. See **Port Number Syntax** (on page 180).
	
	  ▪ IPv4 (or IPv6) settings are disabled on the master device.
	
	• The slave device in question or any upstream device is a Raritan product that runs a "pre-3.3.10" firmware version while the rest of the chain runs firmware version 3.3.10 or later.

Raritan.
A brand of legrand

Tip: To determine which SRC may be the failure point of network, you may ping each SRC in the cascading chain, or check the slave-related events in the event log of each SRC. See **The Ping Tool** *(on page 628) and* **Slave Device Events in the Log** *(on page 627).*

▶ **For a cascading chain comprising only products with "dual" Ethernet ports, also check the following:**

- Whether the Ethernet interface (ETH1 or ETH2) where the network or cascading cable is connected is disabled on the cascaded device in question or any upstream device.

- Whether the connection complies with the cascading guidelines, when set to the Port Forwarding mode. See *Restrictions of Port-Forwarding Connections* (on page 32).

- Whether a newer product model, if involved in the chain, runs the appropriate minimum firmware version or later.

Slave Device Events in the Log

The log messages for connection/disconnection of a cascaded device are different for USB-cascading and Ethernet-cascading chains.

▶ **Messages for the Ethernet-cascading chain:**

Whenever the connection or disconnection of a master/slave device is detected, both SRC devices connected via that network cable record this event in their internal logs.

There are two slave-related events:

Event	Description
The ETH1/2 network interface link is now up.	This log entry is generated when the SRC detects the connection of the upstream or downstream cascaded device on one of its Ethernet ports.
The ETH1/2 network interface link is now down.	This log entry is generated when the SRC detects the disconnection of the upstream or downstream cascaded device on one of its Ethernet ports.

▶ **Messages for the USB-cascading chain:**

In the Bridging mode, events regarding connection/disconnection of a downstream slave device via USB is NOT logged.

However, in the Port Forwarding mode, whenever the connection or disconnection of a downstream slave device via USB is detected, the SRC at the USB-A end of the USB cable logs it in the internal log. Note that the SRC at the USB-B end of the cable does NOT log these events.

There are two slave-related events in the Port Forwarding mode:

Event	Description
Slave connected	This log entry is generated when the SRC detects the presence of a slave device on its USB-A port.
Slave disconnected	This log entry is generated when it detects the disconnection of a slave device from its USB-A port.

The Ping Tool

The SRC provides a ping tool in the web interface and CLI so you can ping any host or SRC in your data center.

▶ **Ping via the Web Interface:**

To log in to the web interface, see *Login* (on page 89).

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

* Choose Maintenance > Network Diagnostics

▶ **Ping via the CLI:**

You can access the CLI interface by connecting a computer to the SRC or using SSH/Telnet. See *With SSH or Telnet* (on page 357).

1. You must perform the ping command in the diagnostic mode. See *Entering Diagnostic Mode* (on page 495).

2. Then perform the ping command. See *Testing the Network Connectivity* (on page 497).

Installing the USB-to-Serial Driver (Optional)

The SRC can emulate a USB-to-serial converter over a USB connection. A USB-to-serial driver named "Dominion PX2Serial Console" is required for Microsoft® Windows® operating systems.

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

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

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

1. Make sure the SRC 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 SRC to the computer via a USB cable. The driver is automatically installed.

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

1. Make sure the SRC 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 PX2Serial 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 SRC 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 SRC to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

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

> set line /dev/ttyACM0

> Connect

Initial Network Configuration via CLI

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

This section describes the initial network configuration via a serial RS-232 or USB connection. To configure the network settings using the web interface, see **Configuring Network Settings** (on page 160).

▶ **To configure the SRC:**

1. On the computer connected to the SRC, open a communications program such as HyperTerminal or PuTTY.

    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 PX2Serial Console" under the Ports group.

2. In the communications program, press Enter to send a carriage return to the SRC.

3. The SRC prompts you to log in. Both user name and password are case sensitive.

    a. Username: `admin`

    b. Default password: `raritan` (or a new password if you have changed it).

4. 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.

5. The # prompt appears.

6. Type `config` and press Enter.

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

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

▶ **Commands for wired networking:**

The <ipvX> variable in the following commands is either ipv4 *or* ipv6, *depending on the type of IP protocol you are configuring.*

Replace the variable <ETH> with either 'ETH1' or 'ETH2', depending on which Ethernet port you are configuring.

- **General IP settings:**

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

- **Static IP configuration:**

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

▶ **Commands for "Ethernet" authentication method:**

To set or enable	Use this command
Authentication method	`network ethernet <ETH> authMethod <method>` <method> = *none* or *eap*
EAP outer authentication	`network ethernet <ETH> eapOuterAuthentication <outer_auth>` <outer_auth> = *PEAP* or *TLS*
EAP inner authentication	`network ethernet <ETH> eapInnerAuthentication <inner_auth>` <inner_auth> = *MSCHAPv2* or *TLS*

To set or enable	Use this command
EAP identity	`network ethernet <ETH> eapIdentity <identity>` <identity> = your user name for EAP authentication
EAP TLS client certificate	`network ethernet <ETH> eapClientCertificate` When prompted to enter the client certificate, open the certificate with a text editor, copy and paste the content into the communications program.
EAP TLS client private key	`network ethernet <ETH> eapClientPrivateKey` When prompted to enter the private key, open the key with a text editor, copy and paste the content into the communications program.
EAP password	`network ethernet <ETH> eapPassword` When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	`network ethernet <ETH> eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.
Radius authentication server's name	`network ethernet <ETH> eapAuthServerName <FQDN>` <FQDN> = Fully qualified domain name of the Radius server name shown in the CA certificate

Raritan.
A brand of **legrand**

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 ethernet <ETH> enableCertVerification <option1>` `<option1>` = *true* or *false*
Accept an expired or not valid certificate	`network ethernet <ETH> allowOffTimeRangeCerts <option2>` `<option2>` = *true* or *false*
Make the connection successful by ignoring the "incorrect" system time	`network ethernet <ETH> allowConnectionWithIncorrectClock <option3>` `<option3>` = *true* or *false*

▶ **Commands for wireless networking:**

● **General wireless settings**:

To set or enable	Use this command
Wireless interface	`network wireless enabled <option>` `<option>` = *true*, or *false*
SSID	`network wireless SSID <ssid>` `<ssid>` = SSID string
BSSID	`network wireless BSSID <bssid>` `<bssid>` = AP MAC address or *none*
802.11n protocol	`network wireless enableHT <option>` `<option>` = *true*, or *false*

Raritan.
A brand of Legrand®

To set or enable	Use this command
Wireless authentication method	`network wireless authMethod <method>` \<method\> = *psk* or *eap*
PSK	`network wireless PSK <psk>` \<psk\> = PSK string
Wireless EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` \<outer_auth\> = *PEAP* or *TLS*
Wireless EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` \<inner_auth\> = *MSCHAPv2* or *TLS*
Wireless EAP identity	`network wireless eapIdentity <identity>` \<identity\> = your user name for EAP authentication
Wireless EAP TLS client certificate	`network wireless eapClientCertificate` When prompted to enter the client certificate, open the certificate with a text editor, copy and paste the content into the communications program.
Wireless EAP TLS client private key	`network wireless eapClientPrivateKey` When prompted to enter the private key, open the key with a text editor, copy and paste the content into the communications program.
Wireless EAP password	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.

To set or enable	Use this command
Wireless 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.
Radius authentication server's name for wireless connection	`network wireless eapAuthServerName <FQDN>` <FQDN> = Fully qualified domain name of the Radius server name shown in the CA certificate

The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE." If a certificate is installed, configure the following:

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

- **Wireless IPv4 / IPv6 settings:**

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

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

▶ **To verify network settings:**

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

- `show network`

The IP address configured may take seconds to take effect.

Device-Specific Settings

A bulk configuration file will NOT contain any device-specific information like the following list.

For further information, simply open the built-in bulk profile for a detailed list of 'excluded' settings.

- Device name
- SNMP system name, contact and location
- Part of network settings (IP address, gateway, netmask and so on)
- Device logs
- Names, states and values of environmental sensors and actuators
- TLS certificate
- Server monitoring entries
- Asset strip names and rack unit names

TLS Certificate Chain

A TLS server sends out a certificate to any client attempting to connect to it. The receiver determines whether a TLS server can be trusted by verifying that server's certificate, using the certificate (chain) stored on the receiver.

Therefore, to successfully connect to a TLS server, you must upload a valid certificate or (partial) certificate chain to the receiver.

The uploaded certificate (chain) must contain all missing certificates "related to" that TLS server's certificate in some way. Otherwise, the connection made to that TLS server will fail.

- For information on how the uploaded certificate (chain) is related to a TLS server's certificate, see *What is a Certificate Chain* (on page 638).
- For an example of creating and uploading a TLS certificate to SRC, see *Illustration - GMAIL SMTP Certificate Chain* (on page 641).

What is a Certificate Chain

If you are familiar with a certificate chain, you can ignore this topic and refer to *Illustration - GMAIL SMTP Certificate Chain* (on page 641).

A certificate or a chain of certificates is used for trusting a TLS server that you want to connect.

The receiver, such as SRC, can trust a TLS server only after an appropriate certificate (chain) which is "related to" that TLS server's certificate is uploaded to the receiver.

▶ **How a certificate chain is generated:**

To explain how a TLS server's certificate is "related to" the certificate (chain) that is uploaded to the receiver, we assume that there are three "related" certificates.

- **Certificate C**. The certificate issued to the TLS server you want to connect.

  'Certificate C' is issued by the certificate authority (CA) entity called 'Issuer B'.

- **Certificate B**. The certificate issued to 'Issuer B'.

  'Certificate B' is issued by a CA entity called 'Issuer A', and it is an intermediate certificate.

Raritan.

A brand of ☐legrand®

- **Certificate A**. The self-signed certificate issued by Issuer A. Issuer A is a root CA.

The above three certificates form a certificate path, which is called the "certificate chain".

Each certificate in the chain is the issuer certificate of the certificate that follows it. That is, A is the issuer certificate of B, and B is the issuer certificate of C.

Note: In fact many certificate chains may comprise only the root certificate and a TLS server's certificate and do not have any intermediate certificate(s) like 'Certificate B' involved. Or some chains may contain more than one intermediate certificates.

▶ **Certificate (chain) that you must upload to the receiver, such as SRC:**

Because the TLS server provides only 'Certificate C', you need to upload a file containing the missing certificates of the chain (that is, 'Certificate A' and 'Certificate B') to the receiver.
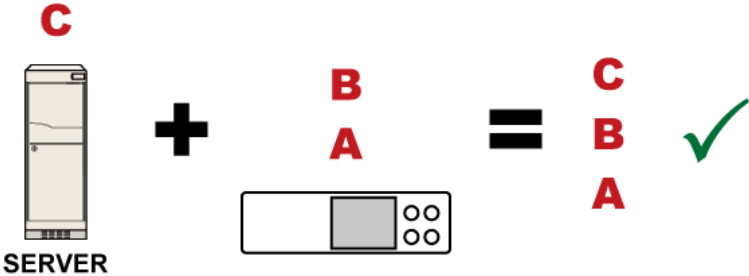
In reality some servers may provide a partial (or even a full) certificate chain instead of a single server certificate. If your server provides a partial certificate chain containing 'Certificate B' and 'Certificate C', then you only need to upload 'Certificate A" to the receiver. If the server has a full certificate chain containing Certificates 'A', 'B', and 'C', then you also need to upload the root certificate 'A".
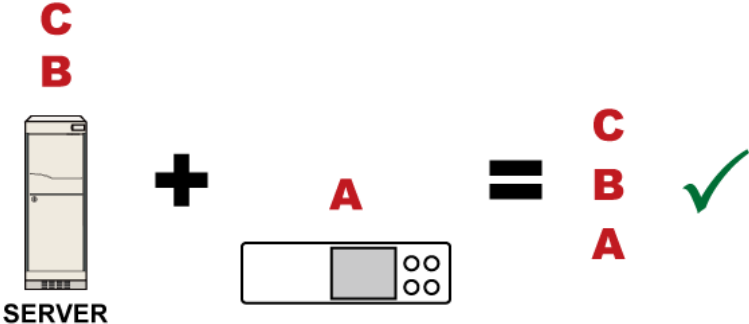
Warning: The certificate (chain) uploaded to the receiver must always contain the ROOT certificate even though the TLS server provides the root certificate. When uploading a (partial) chain onto the SRC, it means you trust each certificate in the chain to certify the authenticity of certificates a server sends to SRC. Therefore, at least the root certificate must be authentic, issued by a CA you trust, and downloaded from that CA over a secure channel. Never implicitly trust a root certificate that is sent by the server which you want to connect to. It could have been created by an attacker.

If either certificate 'A' or 'B' is missing in the certificate file uploaded to the receiver, the connection to the wanted TLS server will fail.
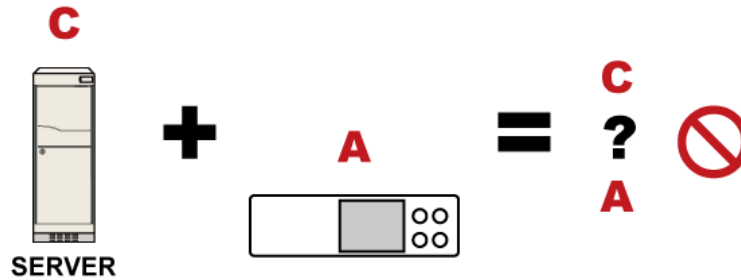
For SRC, if any required certificate is missing, a certificate error message similar to the following is shown on the SRC web interface.
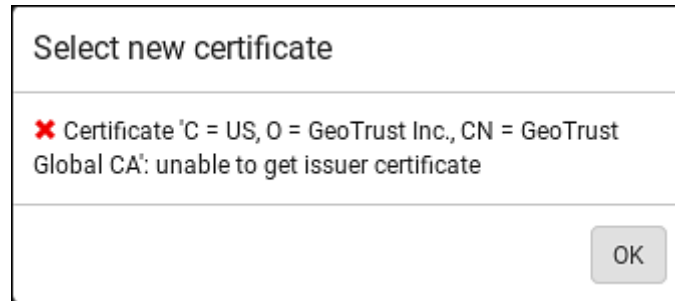
It is NOT recommended to upload the server certificate to the receiver except when it is a self-signed certificate. Using self-signed server certificates is also not recommended and may not even work in all cases.

▶ **Order of the chain in the certificate file:**

The order of a certificate chain's content in the certificate file uploaded to the receiver must look like the following.
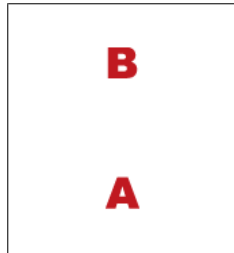
- The top is the final intermediate certificate of the chain "B" if you have to upload a partial chain.
- The bottom is always the root certificate "A".
- When copying multiple certificates to a single file, make sure you also copy the lines of BEGIN CERTIFICATE and END CERTIFICATE from each certificate.

Illustration - GMAIL SMTP Certificate Chain

If you will apply your company's SMTP service to SRC, ignore this GMAIL illustration topic. Simply contact your IT department to retrieve the appropriate certificate (chain) file and upload it to the SRC.

This section illustrates the upload of a TLS "root" certificate for using the "gmail.com" SMTP service.

Unlike normal TLS websites, where you can easily find its server certificate by using a Web browser, the method to find an SMTP server's certificate is more difficult, which requires appropriate tools and sufficient technical knowledge. For example, you may have to use the openssl command as illustrated below to retrieve the certificate of the GMAIL SMTP server.

▶ **Step 1 -- Find the certificate(s) the SMTP server has:**

1. Issue the following command in the appropriate command line application.
   - In the following example command, we assume the server "smtp.gmail.com" provides the SMTP service. You can change the server name, port number, command or even the tool as needed.

```
openssl s_client -showcerts -connect smtp.gmail.com:465
```

Alternative: To view the certificate chain instead of all certificates, you can remove the "-showcerts" option from the above command.

2. Information that shows the certificates the SMTP server has is displayed.

```
.
.
.
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
MIIEdjCCA16gAwIBAgIIbzO9vIL2OXcwDQYJKoZIhvcNAQELBQAwSTELMAkGA1UE
.
.
YHKKJH96sSNC+6dLpOOoRritL5z+jn2WFLcQkL2mRoWQi6pYTzPyXB4D
-----END CERTIFICATE-----
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
MIIEKDCCAxCgAwIBAgIQAQAhJYiw+lmnd+8Fe2Yn3zANBgkqhkiG9w0BAQsFADBC
.
.
MqO5tzHpCvX2HzLc
-----END CERTIFICATE-----
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
MIIDfTCCAuagAwIBAgIDErvmMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNVBAYTAlVT
.
.
b8ravHNjkOR/ez4iyz0H7V84dJzjA1BOoa+Y7mHyhD8S
-----END CERTIFICATE-----
---
Server certificate
subject=/C=US/ST=California/L=Mountain View/O=Google
Inc/CN=smtp.gmail.com
issuer=/C=US/O=Google Inc/CN=Google Internet Authority G2
.
.
.
```

3. Onscreen information under the title 'Certificate chain' indicates that there are three issuers and three certificates on this server.

      ▪ Each line beginning with the letter "i" indicates an issuer. They are:

Raritan.
A brand of ▢legrand

- *Google Internet Authority G2*
- *GeoTrust Global CA*
- *Equifax Secure Certificate Authority*

- Each certificate's content is located between the line of "BEGIN CERTIFICATE" and the line of "END CERTIFICATE".
- The topmost certificate is the server certificate.

4. The section titled "Server certificate" indicates that the issuer (CA) *Google Internet Authority G2* issues the server certificate.

5. As the server has the server certificate and two intermediate certificates, we conclude that this server sends a partial certificate chain to the receiver.

6. Check whether the issuer "Equifax Secure Certificate Authority" is the root CA.

- If yes, you only need to upload the root certificate self-signed by *Equifax Secure Certificate Authority* to SRC.
- If not, you need to find all missing issuer certificates, including the root certificate, and upload them to SRC.

▶ **Step 2 -- Find and download the content of missing issuer certificate(s):**

1. View the name of the issuer (CA) at the bottom. In this example, this issuer is 'Equifax Secure Certificate Authority'.

2. Use the issuer's name 'Equifax Secure Certificate Authority' to search for its certificate on the Internet, and then download or copy the content from an authentic source, which is usually its official website.

Important: To prevent the downloaded certificate from being modified or manipulated, you must secure the download with TLS via a trusted certificate.

3. As it is found the Equifax Secure Certificate Authority's certificate is self signed by 'Equifax Secure Certificate Authority', which indicates it is the root CA, there are no more missing certificates to search for.

▶ **Step 3 -- Upload the missing certificate(s) to SRC:**

1. Paste the root certificate's content into a plain text file that will be uploaded to SRC.

- Content copying must include the lines of "BEGIN CERTIFICATE" and "END CERTIFICATE".

2. Save that file as a *.pem*, *.crt* or *.cer* file. In this example, it is named as "my-root.pem."

3. Upload the file "my-root.pem" to SRC for using the GMAIL SMTP service.

Note: If your SMTP server requires the upload of a certificate file comprising multiple certificates, make sure the order of these certificates is correct in the file. See **What is a Certificate Chain** *(on page 638).*

▶ **IMPORTANT NOTE:**

If your SMTP server provides a full certificate chain, you should be suspicious whether any attacker fakes the certificate chain and doubt whether the root certificate on that server is authentic. It is STRONGLY recommended to download the root certificate from an authentic source, which is usually the root CA's website, rather than from the server you want to connect.

Browsing through the Online Help

The SRC Online Help is accessible over the Internet.

To use online help, Active Content must be enabled in your browser. Consult your browser help for information on enabling the feature.

▶ **To use the SRC online help:**

1. Click Online Documentation. See **Web Interface Overview** (on page 94).

2. The online help opens in the default web browser.

3. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.

4. To select a different topic, do any of the following:

   ▪ To view the next topic, click the Next icon in the toolbar.

   ▪ To view the previous topic, click the Previous icon .

   ▪ To view the first topic, click the Home icon .

5. To expand or collapse a topic that contains sub-topics, do the following:

   ▪ To expand any topic, click the white arrow ▷ prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow ◢, and sub-topics appear below the topic.

   ▪ To collapse any expanded topic, click the black, gradient arrow ◢ prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow ▷, and all sub-topics below that topic disappear.

6. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon to start the search.

   ▪ If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.

Raritan.
A brand of **Llegrand**

7. To have the left pane show the list of topics, click the Contents tab at the bottom.

8. To show the Index page, click the Index tab.

9. To email any URL link to the currently selected topic to any person, click the "Email this page" icon in the toolbar.

10. To email your comments or suggestions regarding the online help to Raritan, click the "Send feedback" icon .

11. To print the currently selected topic, click the "Print this page" icon .

Appendix J   Integrating Asset Management Strips with Other Products

In This Chapter

Asset Management Strips and Raritan PDUs

Asset strips also work with the following Raritan power distribution units (PDUs) or transfer switches:

- PX2 PDUs
- PX3 PDUs
- PX3TS transfer switches
- Branch Circuit Monitor (BCM) series
- PMC models of BCM2 series

Warning: Other BCM2 models than PMC models do NOT support asset management strips.

For information on setting up asset strips to work with each product, refer to each product's User Guide or Online Help on the Raritan website's *Support page* (*http://www.raritan.com/support/*).

Asset Management Strips and dcTrack

If any asset strips are connected to the SRC, the SRC can transmit their information to Sunbird's dcTrack. All you have to do is to add the SRC to dcTrack, and also add each IT item where an asset tag is attached to dcTrack.

Note: For instructions on connecting asset strips, see **Connecting Asset Management Strips** *(on page 53).*

If SNMP is enabled, event information can be transmitted to dcTrack. Specifically, Sunbird's Power IQ detects when an asset tag is connected or disconnected from an asset strip. Power IQ then generates a connection or disconnection event. When dcTrack polls Power IQ, the connection/disconnection events are pulled into dcTrack, and displayed in the dcTrack Web Client.

▶ **To poll and display asset management events in dcTrack**

- The SRC that the asset strip is connected to must exist in dcTrack.
- Each IT item connected to the asset strip via an asset tag must exist in dcTrack.

  You do not need to manually enter the asset tag IDs for IT items that already exist in dcTrack as long as these items are in the Installed status.

  Simply, plug the item's asset tag into an asset strip that is connected to the SRC that exists in dcTrack. dcTrack automatically assigns the asset tag ID to the existing IT item.

  Note: If needed, the asset tag number can be overwritten.

For more information on dcTrack as well as how asset strips work with dcTrack, contact Sunbird Professional Services and Support from the http://support.sunbirddcim.com.

Index

Raritan.
A brand of legrand

Raritan.
A brand of ⊔legrand®

Raritan.
A brand of legrand

Raritan
A brand of **legrand**

Raritan.
A brand of legrand